TO CATCH A THIEF

The role of the banking Chief Control Officer

A series of papers investigating the evolution of the CCO in the new regulatory era

By Maurice Evlyn-Bufton

TO CATCH A THIEF

The Evolution of the Chief Control Officer

A series of papers investigating the evolution of the CCO in the new regulatory era

By Maurice Evlyn-Bufton

ARMSTRONG WOLFE
Collaborative Ventures

To Catch a Thief; The Evolution of the Chief Control Officer
First published in Great Britain in 2018 by Armstrong Wolfe
Eagle Tower Suite 120, Montpellier Drive, Cheltenham,
Gloucestershire GL50 1TA United Kingdom
www.armstrongwolfe.com
Copyright © 2018 Armstrong Wolfe

Design and production: Rob Walster, Big Blu
Edited by Kate Owen-Dixon

All rights reserved. No part of this publication may be produced, stored or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of both the copyright owner and the publisher of this book. This book is intended for general guidance on matters of interest only and does not constitute professional advice. Whilst precautions have been taken to ensure that the source of the information that any judgements are based upon is reliable, you should not act upon the information contained in this book without specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this book and, to the extent permitted by the law, the author and distributors do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this book or for any decision based upon it.

The views reflected in this publication are the views of the author and do not necessarily reflect the views of any of its contributing firms or individuals.

For general information, please contact +44 203 664 8863 (UK) or email TCAT@armstrongwolfe.com

ISBN 978-1-9996177-1-4

CONTENTS

ABOUT THE AUTHOR v

ABOUT ARMSTRONG WOLFE xiii

CHARITABLE CAUSES x

ACKNOWLEDGEMENTS xi

CONTRIBUTORS xiv

FOREWORD xxxi

ABOUT FORCEPOINT xxxiv

PREFACE xxxvi

GREED AND THE BIRTH OF CONDUCT RISK 5

SETTING THE SCENE 19

DEFINING THE INDEFINABLE 27

CONDUCT AND CONTROL 43

CHARACTER'S ESSENTIAL ROLE IN ADDRESSING MISCONDUCT IN FINANCIAL INSTITUTIONS 55

By Furlong, Crossan M, Ganz and Crossan L

LEADERSHIP AND DECISION-MAKING 93

By Stuart Tootal

CROSS-INDUSTRY COLLABORATION 111

KEWKU ADOBOLI: HOW TO CLONE THE BIGGEST TRADING FRAUD IN THE HISTORY OF BANKING 139

By Hagen Rafeld and Dr Sebastian G. Fritz-Morgenthal

THE NEW RULES FOR MANAGING RISK 163
By David Pogemiller
THE PEOPLE SIDE OF CONTROL AND THE POWER OF FAILURE 181
By Bobby Chatterjee
TECHNOLOGY AND CULTURE 199
IMPROVING BANKS' ORGANISATIONAL CULTURE 217
THE FUTURE OF CONTROLS SURVEILLANCE 235
By David Pogemiller
EMERGING CONDUCT THEMES 251
By David Long and Charanpal Matharu
THE CHIEF CONTROL OFFICER: PAST, PRESENT AND FUTURE 277
THE CONDUCT ACADEMY 293
MARKET AND ORGANISATIONAL SUMMARY 2015 TO 2018 309
ABOUT GCF BOSNIA 321
ABOUT SIGHTSAVERS 325
ABOUT ST. GEORGE'S SOCIETY OF NEW YORK 329
EPILOGUE - 2021 A CHANGE IN DIRECTION FOR THE CCO 335
POV - CULTURAL SURVEILLANCE 343
POV - THREAT MANAGEMENT 349
BIBLIOGRAPHY 364

ABOUT THE AUTHOR

Maurice Evlyn-Bufton has more than twenty years' experience in investment banking and global markets executive search and advisory.

Maurice set up his company, Armstrong Wolfe, in 2011. He has subsequently established it as a market leader within business management, more commonly identified as the office of the Chief Operating Officer (COO), Chief Administrative Officer (CAO), Chief of Staff (CoS) and the Chief Control Officer (CCO) 1 & 2LOD.

He continues to manage Armstrong Wolfe's day-to-day business, working with his clients on global search mandates, having personally delivered retained searches in twenty-five countries since 2012.

Maurice's regular industry papers have helped establish his reputation as a leading voice in this ever-evolving field. The quarterly COO and CCO industry forums and debates he facilitates internationally afford him a unique insight into this community.

This is Maurice's third published book *No Place to Hide,* was published in 2017 and investigates the role of the banking Chief Operating Officer in the new regulatory era, to which this book is a sequel. *Donkey Mail and Bully Beef; The Art of Survival* was

published in 2018 and is Maurice's personal account of his time spent in Bosnia in 1994–95 as part of the United Nations' peacekeeping force during the Balkans War.

Maurice is a graduate of Cardiff University, which he completed through an Army scholarship. He attended the Royal Military Academy Sandhurst and was subsequently commissioned into the Gloucestershire Regiment. He saw service in the Balkans War, where he was second in command of the British UN forces protecting the south bank of the River Drina, which bisected the safe haven of Goražde.

He has returned to Goražde on several occasions and has raised funds for the town's primary school through his charity, GCF Bosnia (gcfbosnia.org), in honour of his comrades who died in service in 1994–95.

Maurice is married to Joanna and has three sons, Simon, Monty and Alfie. They are expecting a fourth child in November 2018. He lives in Gloucestershire, England, and spends his spare time with his family, marathon running, mountaineering, walking his four dogs, writing and carrying out his charity work.

ABOUT ARMSTRONG WOLFE

Armstrong Wolfe is a global executive search and advisory firm focused on investment banking and the financial markets. Its clients are some of the world's leading banking and financial institutions.

Armstrong Wolfe bridges traditional competitive lines to identify possible areas for cooperation and collaboration.

By partnering some of the world's principal banks, Armstrong Wolfe hosts Chief Operating Officer (COO) and Chief Control Officer (CCO) forums and workshops in New York, London, Toronto, Singapore and Hong Kong. These events are attended by senior representatives from twenty-four of the principal global banks.

The firm also holds a regular Brexit dinner and an Asset Management forum, as well as a series of events focused on leadership, conduct and ethics. Its Women in the COO Community initiative focuses on encouraging more women into senior positions in banking.

Through these events, the firm promotes and fosters cross-industry teamwork and partnerships. This brings the banking community and its business leaders together to create innovative solutions that meet the common challenges and demands of regulation and cost efficiencies in testing market conditions.

The platform for open dialogue that these forums provide affords Armstrong Wolfe an exact and evolving understanding of the challenges facing the industry today.

Armstrong Wolfe complements this work with the provision of executive search. The firm is recognised as an authority within business management; namely the roles of the COO, CAO, CCO (1&2 LOD) and CoS, as well as roles that are embedded in business management and/or the executive management office.

For more information, visit armstrongwolfe.com or contact info@armstrongwolfe.com.

ADVANCE PRAISE

"I've known and worked with Maurice for over ten years and he has always been a thought leader in the COO and CCO space. He is someone to go to for advice on the evolving banking operating models, but more significantly someone who has leveraged his extensive network to bring this community together to discuss pertinent and emerging risks such as conduct risk management and how to improve standards in the industry as a whole."

Libby Denchfield
Head of Conduct and Senior Manager Regime, Financial Markets, Standard Chartered Bank

No one understands the convoluted role of the business manager within the financial services industry better than Maurice Evlyn-Bufton, and certainly no one else has had the same forethought and wherewithal to put that knowledge down in print. Maurice is a trusted advisor to a wide spectrum of people in the square-mile and now he has brought the role of the Chief Control Officer into his purview as well. This is essential reading for anyone considering a career in this domain.

Paul Maley
Managing Director, COO Institutional Client Group and Global Head, Business Solutions Group (BSG), Deutsche Bank

"Through his deep knowledge of the markets and the CCO function, Maurice has brought much-needed focus to the challenges of active business line supervision required in our industry today. His discussion of the issues and success criteria is a must read for all managers tasked with fulfilling a controls mandate in a complex and global operating environment."

Larry List
Chief Conduct and Controls Officer Global Markets Americas, BNP Paribas

"With this book, Maurice has made an important contribution to the thinking around the ongoing evolution of the Chief Control Officer's role within banks."

Darren Jarvis
Managing Director, Global Head Markets Business Control and Supervision, Markets, Citigroup

"I have known Maurice in various capacities ranging from client to colleague for more than fifteen years. In all my dealings with Maurice, he has been professional, highly competent and - if anything- over enthusiastic and passionate about all he does! He always displays the highest levels of personal integrity and is a role model in delivering results in an ethical manner. I count myself lucky to have had the opportunity to work with him."

Neil Smith
CEO, The Conduct Academy

"I have known Maurice for some time and have attended his Chief Control Officer and 1LOD forums as an observer and active participant. His unique and engaging style has enabled him to bring together a CCO community that enjoys an active and open dialogue as they seek to meet common challenges being imposed upon them within control and conduct. Such debate is beneficial not just to this community, but the industry as a whole."

Pierre Pourquery
UK Head of Capital Markets Advisory, EY

CHARITABLE CAUSES

This book will be distributed free of cost, with a suggested charity donation, to individuals within the CCO community.

All proceeds from this book will be donated to our three chosen charities:

GCF Bosnia – gcfbosnia.org
Sightsavers – sightsavers.org
St. George's Society of New York – stgeorgessociety.org

For more information regarding the work of these charities, please see page 309.

To donate, please visit armstrongwolfe.com/charity and click the donation button to reach our JustGiving page.

For more information, email TCAT@armstrongwolfe.com

Your donation is greatly appreciated. Thank you.

ACKNOWLEDGEMENTS

There are many to thank, but also some to recognise. To recognise the support and influence they have had on developing my interest in conduct, enabling me to engage on this most emotive of subjects with hundreds of bankers. The very community chastened by broader society for its bad behaviour and poor conduct. The community shackled with the burden of the past and its catastrophes, and the few that broke its reputation. I wish to thank, however, the high percentage of the banking community that are hard-working, honest people and are committed to putting right the wrongs of the past.

At its helm today are the business heads and leaders of the banking industry, the CEOs, that carry the responsibility and accountability for the conduct of those under them. It is, however, the Chief Control Officers, who occupy no-man's-land. The land between the business and its drive to make profit, and the regulators who demand they do it in a just and proper way, both rightly so. They sit in the business responsible for delivering a deterrent, for developing methods of detection and for policy and procedure-making, the friend and the foe of all. They seek to help the CEO and the business heads steer their ship towards better and calmer seas.

It is this few I thank, and more so a small handful of them, to whom I owe my right to put pen to paper. Kevin Sawle and Toby Billington (HSBC), Darren Jarvis (Citi), Nick Lovett (Credit Suisse), Larry List and George Nunn (BNP Paribas), Libby Denchfield (Standard Chartered Bank), Eric Rabin and Rajeev Mehta (Société Générale), Joe Campione (BNY Mellon) and David Barrons (TD Securities). They have attended and hosted my forums, listened and offered their informed opinions and collectively shaped my own, and they have enabled me to bring this book together.

A further thanks to the powerhouse of EY and those within it, namely Steve Krueger, Pierre Pourquery, David Williams, Tim Rooke, Chris Richardson, Chris Bowles and Mary Lou Peters. All have added to my understanding and, dare I say it, enjoyment of this subject.

To Neil Smith, previously my client at Deutsche Bank and now the CEO of The Conduct Academy, who has brought a new enthusiasm and drive to getting something done about this common challenge. He took The Conduct Academy from a good idea to something that is alive and working.

There are thanks due to Hagen Rafeld, Dr Sebastian G. Fritz-Morgenthal, David Pogemiller, David Long, Charanpal Matharu, Pierre Pourquery, Frantz Maurer, Bobby Chatterjee, Professor Mary Crossan, Bill Furlong, Professor Jeffrey Gandz and Larry Crossan for their contributions and articles in this book. To Stuart Tootal, who has offered me his ear and counsel from university days to all through the Army, and now as a banker, with me as one working with his industry.

To Guy Filippelli, Brian White and David Pogemiller, the former CEO, COO and VP, Customer Success of RedOwl, what was a truly innovative U.S. FinTech company focused on surveillance. They

took me on as an advisor to their business, and many good days, evenings and conversations were had with this most eclectic trio of intellectuals. Fine men with fine minds. Guy and Brian agreed to sponsor this book, and halfway through its writing, RedOwl was acquired by U.S. technology company Forcepoint. Good to their word, the baton was picked up by Heath Thompson (Senior Vice President and General Manager, Commercial Security, Forcepoint), and it is Forcepoint I now thank for their support in bringing this book to completion and publication.

To my wife Joanna, for her patience and support. To my boys, Simon, Monty and Alfie, I apologise as they waited many evenings for me, Simon holding hope for a fatherly chat and Monty and Alfie waiting for Daddy to read a story. I will make good on these shortfalls now this book is done, but will not punish any of them with its reading!

CONTRIBUTORS

Dr. Mary Crossan
Ivey Business School

Dr. Mary Crossan is a distinguished University Professor and Professor of Strategic Leadership at the Ivey Business School, Western University. Amongst the most highly cited researchers in her field, her research on leadership character, organisational learning and strategic renewal, and improvisation is published in the top management journals including the Academy of Management Review, Strategic Management Journal, Leadership Quarterly and Organization Science. Her article on Developing Leadership Character in Business Programs was awarded the Outstanding Article of the Year for 2013 in the Academy of Management Learning and Education. The book Developing Leadership Character is a culmination of the team's research on leader character.

In a joint venture with The Second City, she developed a management video entitled Improvise to Innovate. Her textbook Strategic Analysis and Action is widely used in strategy courses. She has been identified as one of the top 40 case-writers in the world with her Starbucks business case selling over 100,000 copies to

business schools worldwide. Her research, teaching, and consulting have provided her with exposure to a variety of companies and industries in North America, Europe and Asia.

Bill Furlong
Ivey Business School

Bill Furlong is a senior banking executive with more than twenty years of experience in Canadian and international capital markets. He has expertise in asset-backed securitisation, structured derivatives and the governance and oversight of trading businesses. He retired from TD Securities in 2012, having held the position of Vice-Chair and Senior Vice President, Global Head of Trading Business Management and was a member of the most senior TD Securities business committees. Mr. Furlong's seventeen-year career at TD saw him build and lead front-office, middle-office and back-office business groups with operations in Toronto, New York, London, Tokyo and Singapore.

He is currently an Executive-in-Residence at the Ian O. Ihnatowycz Institute for Leadership at the Ivey Business School, where he is also a member of the Institute's Leadership Council. He has given speeches, written cases and published articles on the topic of Leadership Character, with a particular emphasis on Character and Financial Markets.

In January 2015 Mr. Furlong was appointed a Commissioner at the Ontario Securities Commission, where he chairs the Audit and Finance Committee and is a member of the Adjudicative Committee.

Mr. Furlong holds a Bachelor of Commerce (Honours) from Memorial University of Newfoundland, an MBA from the Ivey Business School at Western University and the Institute of Corporate Directors, ICD.D designation.

Larry Crossan
Ivey Business School

Larry Crossan is a Lawyer, entrepreneur, educator, software developer and strategist. Starting with a B.Comm. from McGill University, Larry first gained business experience in banking and corporate finance, general management and the hospitality industry before completing Law school at Western University and an MBA from the Richard Ivey Business School. He was called to the bars of New York and Ontario in 1987 and 1988, respectively. Larry has practised with two of Canada's national firms and is equally comfortable with Bay Street and Main Street transactions.

Larry founded Lexcor Business Lawyers after a short stint in provincial politics because he believed legal services could be delivered more efficiently in a smaller office with greater use of technology. Similarly, when his law firm was unable to find corporate software that did what they thought it should do, they sought out technical partners and co-founded SpeedMatters for Corporate Law. Larry is a registered trade-mark agent, has been an instructor in the business law section of the Bar Admissions Course for many years and has spoken on and taught business law in various other settings.

Dr. Jeffrey Gandz
Ivey Business School

Dr. Jeffrey Gandz is Professor of Emeritus (Strategic Leadership), former Associate Dean Programs, MB Program Director and Managing Director, Executive Education at the Ivey Business School. His research on leadership and organisational behaviour has been published in leading peer-reviewed journals including the Journal of Business Studies, Academy of Management Journal, Organisational Dynamics, Journal of Business Ethics, and Academy of Management Learning and Education. He has also been a Visiting Professor at HEC/ISA in France and the Darden School at the University of Virginia. Before becoming an academic, Dr. Gandz had a career in sales and marketing with companies in the pharmaceutical, petrochemical and consumer products industries in Europe and North America and has been on the board or directors of Maple Leaf Foods and CMA (Holdings).

Dr. Gandz has designed executive education programs and consulted with many governments and corporations around the world, including Hutchison Ports, TD Bank Financial Group, Royal Bank Group, J.D. Irving, Manuife. General Electric, OMERS, the governments of Hong Kong, Canada, Ontario and many municipalities. He is the co-author of seven books and over 100 case studies used in business schools and corporate education programmes around the world.

Ivey Business School

The Ivey Business School at Western University in London, Canada is at the forefront of leader character research. With

campuses in London, Toronto and Hong Kong, Ivey's mission is "to develop business leaders who think globally, act strategically and contribute to the societies in which they operate." The Ian O. Ihnatowycz Institute for Leadership at Ivey is a global leader in knowledge creation and dissemination with a focus on developing leader character and embedding it in organizations. The Institute, with its award winning research and practical tools and approaches, seeks to elevate character alongside competence in both education and practice.

Stuart Tootal DSO OBE BA (Hons) MA M Phil (cantab)

After passing out from Sandhurst, Stuart completed several tours of Northern Ireland during the 'Troubles'. He saw active service in the 1991 Gulf War and during the invasion of Iraq in 2003. He has also served on the Army staff at the MoD, for which he was awarded an OBE in 2005.

In 2006 he commanded the Third Battalion of the Parachute Regiment (3 Para), which was the first UK Battle Group to be sent to southern Afghanistan, for which he was awarded the Distinguished Service Order (DSO). The fighting 3 Para participated in has been described as the most intense level of combat experienced by the British Army since the Korean War. Promoted to full colonel, he subsequently resigned shortly after commanding 3 Para over the issue of the poor treatment of his wounded soldiers.

Since 2008 Stuart has held a number of senior MD global head positions in Barclays. He also set up a major industry leading programme called Barclays AFTER to help veterans transition into civilian employment, which has raised more than £4 million for service charities, assisted 5,500 ex-military personnel in

their transition and led to the recruitment of 500 veterans into the company. Stuart was also the founder and chairman of the Parachute Regiment's Afghanistan Trust charity. Between 2009 and 2014, the charity raised £3.4 million for wounded paratroopers.

Stuart regularly lectures on leadership in adversity and the 'transferables' from the military to corporate sector. He is author of the Sunday Times best seller Danger Close – Leading 3 Para in Afghanistan and The Manner of Men – 9 Para's Heroic D-Day Mission his third book, Tank Action – An Armoured Troop Commander's War 1944–45 was published in June 2016.

Hagen Rafeld

Hagen Rafeld is Vice President at the Divisional Control Office of the Global Markets Division at a Frankfurt-based financial institution.

He has more than twelve years of Risk and Project Management experience with specialisation in Operational/Non-Financial Risk (NFR) including fraud risk in multi-national corporations, advising senior management up to supervisory board level.

He is a frequent lecturer, with consecutive teaching assignments on corporate governance, risk, and compliance topics at, for example, Frankfurt School of Finance and Management and most recently on Rogue Trading and Organisational Misbehaviour at WHU Otto Beisheim School of Management in Vallendar, conference speaker (House of Finance/Goethe University Frankfurt, Bundesbank), and author.

Hagen holds a Master's Degree of Business and Engineering from Steinbeis University Berlin and a Bachelor of Arts in Banking and Finance.

Sebastian Fritz-Morgenthal
Bain & Company

Sebastian Fritz-Morgenthal is Expert Principal and member of the Risk, Finance and Regulation Practice at Bain & Company. He has more than twenty years of experience in top management risk and consulting functions at Deutsche Bank, West LB, HSH Nord-bank, Booz & Co and the Frankfurt School of Finance and Management.

The focus of his work is risk management (credit, market, operational, liquidity/treasury, reputational, enterprise wide), riskstrategy, risk appetite, target operating model, client profitability, restructuring and crisis management, regulation implementation, quantitative methodologies and data analysis.Sebastian holds a Diploma in Physics from University of Hamburg and a PhD in Physics from Goethe University Frankfurt.

Sebastian served at the Board of Trustees of GARP from 2005 until 2012, was member of IIF, ISDA, BdB and VoeB working groups/committees and is member of the Frankfurt Institute of Risk Management and Regulation (FIRM) since 2011. He is a frequent lecturer (Frankfurt School of Finance and Management, Cambridge University, LSE, WHU, Goethe University), conference speaker (Risk Minds, Bundesbank, House of Finance, FIRM, etc.) and author.

David Pogemiller
Forcepoint

David has spent the last four years helping implement next generation regulatory surveillance programmes at leading financial institutions and insider threat programmes

across the public and private sector. He currently runs strategic partnerships and the lighthouse customer programme at Forcepoint and, prior to Forcepoint's acquisition of RedOwl in 2017, David ran both strategy and the Customer Success group that was responsible for implementing the RedOwl platform.

He brings fifteen years of experience in delivering industry-leading research, data and analytics, consulting, and software services that enable corporations, financials, and government enterprises to make the best decisions possible.

Immediately prior to RedOwl, David spent over two years at Bridgewater Associates, first running data operations and later serving as the chief of staff to the research department head.

Prior to Bridgewater Associates, David served as Chief Operating Officer of Economy.com where he helped grow the firm from a small regional economic consulting company into a leading global economic and financial research, data, and forecasting firm. After being purchased by Moody's in 2005, David spent two years in London expanding Economy.com's international footprint and integrating with Moody's products and services and their international sales team. Also during that time, he led the development and launch of a new consumer credit set of services that were a holistic combination of unique data, powerful forecasting, and intuitive software.

Upon returning to the U.S. in 2008, David ran product strategy for Moody's newly created pricing service: its suite of quantitative credit risk measures, its credit default database and related services, and the Capital Markets Research Group. Prior to his departure in late 2010, David helped to integrate all of Moody's analytics services into a cohesive web-based research and data analytics platform.

David was born in Minneapolis, Minnesota, and holds a B.A. in Economics and Business Administration from the University of New Hampshire where he also played four years of NCAA Division I soccer.

Dr. Frantz Maurer
KEDGE Business School

Frantz Maurer, PhD, is a Professor of finance at KEDGE Business School. During the last 20 years, he has collaborated with different institutions such as the University of Bordeaux, ESCP Europe, and HEC Paris. Frantz has collaborated extensively with large financial institutions in the domain of risk management, culture and the use of data and analytics to better predict crisis and abnormal situations. He is the author of several publications on risk management in the banking industry, that includes a Harvard Business School Industry and Background note.

KEDGE Business School

KEDGE Business School is a benchmark French business school with four campuses in France, three abroad and three partner campuses. The KEDGE BS community is made up of 12,000 students (25% of whom are international students), 196 permanent professors (44% of whom are international), 300 international academic partners and 54,000 alumni around the world. Kedge Business School is AACSB, EQUIS and AMBA accredited, recognized and approved by the French government, and a member of the Conférence des Grandes Ecoles in France. The school is internationally recognised for the management research it conducts in the areas covered by its centers of excellence and specialisms, which puts the school in second place for research in the French Business Schools rankings.

Bobby Chatterjee

Managing Director, People & Transformation, FTI Consulting

Bobby is responsible for leading on the design and delivery of strategic learning and development, team effectiveness, change management and restructuring.

She has spent 20 years working in or with major banks, using this experience to design initiatives that build confidence and confidence to maximise the potential of individuals and companies. She has delivered leadership and management interventions across 30 countries, many of which are award-winning.

Prior to 12 years in consulting, she spent 10 years working for a leading bank, supporting strategic change up to board level. She worked with the business to enhance employee engagement, coach leaders, design effective organisational structures and manage significant change and restructure programmes.

Clients appreciate Bobby's infectious enthusiasm to help leaders bring the best out of their people, coupled with her credibility from an extensive working knowledge of their business. She is a warm, engaging individual who builds trusted client relationships and keeps a cool head in a crisis. She was a finalist in the Learning and Performance Institute's global Learning Professional of the Year awards.

Lucy Phillips

Managing Director, People & Transformation, FTI Consulting

Lucy has 20 years' corporate communications experience in public and private companies ranging from start-ups to the Fortune 10. Lucy is responsible for helping organisations manage moments of change and transformation and her experience encompasses M&A, integration, divestments, leadership changes and changes in strategy. She has spent over 20 years working across a range of sectors including work in the financial sector where she recently spearheaded the internal engagement 'reset' of a leading insurer as well as driving the pre and post integration planning for a multibillion dollar merger in the asset management sector. Her private equity experience includes advising on all communications within two companies being acquired by a leading PE firm to form a new globally integrated chemicals organization.

Prior to joining FTI, she spent 8 years at GE leading change initiatives for multiple GE Corporate Officers including two Chief Executive Officers within GE's Healthcare Division.

Prior to GE, she led North American Media and Investor Relations for FTSE-listed Amersham, plc., which was acquired by GE in 2004.

She is Prosci® accredited in Change Management and is also certified in the GC Index®.

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. For more information, visit www.fticonsulting.com and connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.www.fticonsulting.com

David Long

Pall Mall Risk Reduction

David Long has had an extensive and broad career spanning more than thirty years of Tier 1 Investment Banking Experience. He has held a number of senior positions including Head of Brexit, Group COO for EMEA, COO Fixed Income, Executive Board membership and legal entity directorships of both Credit Suisse and industry-wide entities including the British Bankers Association and EBS Ltd (World's largest FX broker).

Throughout his career David has been based in the Trading Divisions of global banks. Starting as a Trading Assistant in Interest Rate Derivatives, David's career has taken him through a wide-ranging product suite including FX, Fixed Income, Commodities and Equities. David is an expert in the effective operation of Trading Businesses, including First Line of Defence controls and commercial strategy optimisation.

Charanpal Matharu
Pall Mall Risk Reduction

Charanpal Matharu is a qualified accountant with more than twenty years of Tier 1 Investment Banking experience. He is a highly accomplished and experienced Chief Operating Officer with industry leading experience in the First Line of Defence. This includes pioneering the Front Office Controls COO role, implementing robust supervisory frameworks, performing operational risk evaluations, conduct risk assessments and implementing measurement techniques to identify emerging trends. Charanpal has in excess of ten years' experience analysing audit and S166 regulatory observations and designing practical and effective remediation solutions. He has developed roles and responsibilities clearly distinct from the Second Line of Defence. Charanpal is a highly effective partner, having held and collaborated in a number of inter-bank COO forums and partnerships.

About Pall Mall Risk Reduction

Pall Mall Risk Reduction is a specialist COO practice with extensive risk management experience in wholesale banking and capital markets. Founding members David Long, Nick Wilcock and Charanpal Matharu have more than 70 years of combined experience within Tier 1 organisations.

As skilled practitioners, they have an exemplary reputation both within the industry and with regulators across multiple jurisdictions. They possess a proven track record of delivery and pride themselves on their client focus.

Pall Mall Risk Reduction is committed to reducing Operational

Risk and Conduct Risk across the industry. Their team's experience profile allows clients to save time and money when implementing enhancements across the First, Second and Third Lines of Defence.

Their clients include Tier 1, 2 and 3 banks, asset managers, hedge funds, Big 4 consulting practices, FinTech and start-ups.

Pierre Pourquery
EY

After initially joining EY in 2012 as a Partner, Pierre now leads Capital Markets for the UK. He is based in London.

Prior to that, from 2005 to 2012 Pierre was a Partner at the Boston Consulting Group in London, focusing on capital markets, risk management and cultural change. From 1999 to 2005, Pierre held the position of the Global Head of Risk and Compliance at IBM. Initially, Pierre started his career as a bond option trader for Credit Lyonnais Bank.

Additionally, Pierre has written numerous articles on risk management and regulations and co-authored a book on operational resilience in financial markets.

FOREWORD

By David Pogemiller, Senior Director,
Strategic Partnerships, Forcepoint

Those charged with enabling the business to succeed whilst protecting it from potential harm from malicious and even simply negligent actors, have never been in more challenging times. Faced with rapidly evolving, yet often ambiguous, demands from regulators, increasingly dynamic markets, and complex new technologies, they are being pressure-tested like never before.

For the controls and compliance teams, much of today's pressure can be traced back to the forex market manipulation scandal first brought to the public's attention by Bloomberg News in 2013. The scandal has since resulted in somewhere over $6 billion in fines, spurred a much more aggressive regulatory posture, led to more personal liability for senior managers, and driven significant expenditure in both the first line (the trading functions) and second lines (the compliance functions) to fund the increased mandate. For many, this was the clarion call that awoke the industry to the magnitude of the challenges and a need to change fundamentally.

For those with a mandate to protect sensitive information – intellectual property such as trading algorithms, customer data, and more – the increasing frequency and magnitude of data breaches is having the same effect. In today's world every organisation is exposed to material financial and reputational harm from a breach.

There is little debate on the material cost of data breaches and it is sizable. In fact, the 2017 Cost of Data Breach Study from the Ponemon Institute puts the global average cost at $3.6 million, or $141 per data record. However, for many in the industry the long-term effects on reputation are still a matter of debate.

Will Equifax suffer material long-term harm from what now looks like to be the most significant breach on record, or will it prove to be 'too big to fail' like many financial institutions during the latest financial crisis? The unfortunate reality seems to be that the general populace has for the most part unknowingly and, unreasonably, given away much of its right and expectation to privacy. The good news is that many do remain aware of the risks and are pushing regulators to fight for our privacy rights. In Europe, for example, the new General Data Protection Regulation (GDPR) act is broadly viewed as a powerful, if imperfect, step in the right direction to protecting privacy.

This book comes at a critical time for leaders facing these seemingly intractable challenges. The rise in personal responsibility, visibility and, at times, personal liability has redefined what success means for them and their organisation. And, while that success still depends on a deep understanding of the business, it has never before been as dependent on truly understanding the art of the possible with technology, the right education and training of the team, and an active role in a vibrant community of like-minded leaders and organisations. Ultimately, it will be a shift in paradigm from an all-out focus on 'stopping the bad' to 'freeing the good' that enables the controls teams, the employees, and the business to truly win the day.

It's for this reason that I view Maurice and his team's work as so valuable. Over the past four years I have seen Maurice and the Armstrong Wolfe team become an increasingly important agent of

change for the controls community. As an agitator, Maurice has helped to eliminate barriers and drive important new thinking on why and how the community can come together to be more effective and efficient. As an educator, he has helped introduce and inform the community on the incredibly powerful, yet complex technologies available today and on new ways of thinking about and solving the problems. And, going forward, he is increasingly helping to shape the next generation of leaders through innovative training and certification.

Of all the ways that Maurice has impacted the industry, I think the most important is his continual drive to help the industry become more proactive and, in the words of Jack Welch, 'change before you have to'.

ABOUT FORCEPOINT

Forcepoint is transforming financial institutions' ability to meet their cybersecurity and regulatory compliance mandates through its Human Point System. The Human Point System focuses on what matters most: understanding people's behaviour and intent as they make decisions and interact with critical data across all aspects of the business – communications, physical movement, digital activity, and execution of transactions.

At its core, Forcepoint helps protect the organisation, its people, and its customers from the growing and evolving human-based threats within the enterprise. These threats can take the form of malicious actors that are out to harm the organisation or accidental or negligent actions by employees that expose material operational or reputational risks. Critical to the organisation's ability to effectively reduce the risk of illegal, non-compliant or simply unwanted behaviour is its ability to comprehensively identify activity and implement risk-adaptive controls that enable the good while stopping the bad.

Forcepoint's human-centric portfolio is purpose-built to provide the necessary visibility, controls and analytics to understand context and intent. It starts at the perimeter, with an industry-leading next generation firewall (NGFW) that protects against malicious

external threats. Within the enterprise, Forcepoint's integrated suite of data loss prevention (DLP), user and entity behaviour analytics (UEBA), cloud access security broker (CASB), endpoint monitoring, cloud and on-premises web and email security and cross-domain transfer products protect the people and data.

Forcepoint UEBA enables best-in-class eCommunications surveillance and holistic trader assessment that integrates an employee's activity, their intrinsic risk and risk signals from other tools in the security and compliance ecosystem for first and second lines of defence. This next generation approach focuses on the integration of previously disparate signals, analytics to reduce false positives and find true positives and a user interface designed to enable fast review and investigation.

Forcepoint is fully committed to fostering collaboration within the financial community. By reducing the barriers to collaboration and helping to operationalise outcomes, the first and second line of defence community will create incredible new efficiencies, new and more effective surveillance strategies and best practices and better guidance to help their software partners deliver powerful new solutions.

Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries. To learn more about Forcepoint or to get involved in the growing set of community initiatives, visit Forcepoint.com.

PREFACE

By Kevin Sawle,
Global Chief Control Officer Markets, HSBC

I returned to London in 2013, having worked for Global Markets in HSBC's offices in New York and Paris since 2008. The years abroad had been spent working through the issues that the financial crisis had highlighted in our business, alongside trying to develop those businesses. My career in the trading world was about to end as I was asked to move into the COO office.

I was reluctant at first to accept the new challenge, not realising the breadth of responsibility this entailed, but I quickly realised the importance of the role and the value I could add by making processes more efficient and thereby improving customer experience.

Within a short period the role became far more complex as HSBC, along with our peers in the UK market, were asked to review our sale of interest rate derivative products to retail corporate clients. This was just the beginning of a series of reviews that changed the nature of the COO's office. Up until that point the COO's role was to manage the operational risk framework within the front office, to investigate and fix all issues that arose, improve the control environment and enhance the clients' experience with HSBC, front to back. The book of work from the review of sales relating to interest rate hedging products grew to the point whereby I could

not carry out all my responsibilities effectively, so a new operating structure was needed.

At HSBC we created a Chief Control Officer's (CCO) role within the Markets COO's office. This officer's responsibility was to build the foundations that would enhance controls globally. This meant reviewing all policies and enhancing them in line with the current environment, something that is obvious now, but which the industry had not done diligently enough in the past. I was asked to participate in regulatory investigations that were taking place at the time in order to feed back issues directly into remediation programmes.

What concerned me throughout the first eighteen months in my role was how reliant we were on findings from our own investigations, and articles we read in the newspapers or heard from regulators. We were not sure whether similar or different issues had been identified at other institutions and therefore whether we were addressing all the issues within our control framework.

Nazir Badat, COO for Markets and my functional manager, had been attending industry forums arranged by Maurice, discussing with his peers the main issues within the COO's world. This forum suggested that a similar forum for CCOs may be of value. This was music to my ears. I knew that we at HSBC, or any of our peers, would not have all the best ideas in this field and that open discussions would be the best way to help all the banks move more quickly to the right place. In my mind this had to be the right outcome for all our clients.

What followed was regular gatherings of financial institutions, discussing conduct topics that were important to improve the standing of our business in the eyes of our customers and the public. Maurice has facilitated this by having either one of the banks lead a discussion, or by inviting an outside guest speaker. One of the most interesting evenings was when a former Top Gun

pilot described the process the US Air Force went through when it faced a similar conduct challenge.

Maurice was always looking for ways to embed the forum within the conduct world and expand coverage. The latter was achieved with forums in New York and Hong Kong, and more institutions have asked to be included as news of the success of the forums spread.

The first objective was harder, much to Maurice's frustration, as competition law concerns were always at the forefront of everyone's minds. Then, at a meeting a year ago, we discussed how difficult a topic conduct must be for the financial institutions that had not been part of the regulatory investigations and how we could help all these institutions globally. This is when the idea of a conduct academy was born, a training academy that would encompass the best training techniques and ideas from all the participating institutions and roll this out to all institutions globally who wished to participate. The Conduct Academy is now successfully up and running, with the support of several financial institutions.

The journey to this point has not been easy, but delivering something of real value never is. Without the drive and enthusiasm of Maurice and his team I do not believe we would have reached this point.

Maurice has been invaluable in helping develop the role of the CCO in the banking industry, through his forums and introductions to people in other industries with similar roles. This book follows his thought process on that journey, sharing his frustrations as well as his triumphs. It is a must read for every control officer.

Conduct (Noun)
1. 1. The way a person behaves, especially in a particular place or situation.

'They were arrested for disorderly conduct'.
'A code of conduct for directors of listed companies.'

2. The way an organisation or activity is managed or directed.

'The conduct of the elections'.

(Oxford Dictionary)

GREED AND THE BIRTH OF CONDUCT RISK

How avarice shaped my view on ethical behaviour

Conduct Risk (Definition)

This is often defined as risk to the delivery of fair customer outcomes, or to market integrity. In other words, conduct risk touches every part of an enterprise framework.

> *Conduct risk is the term used by financial services firms to describe risks associated with the way organisations, and their staff, relate to customers and the wider financial markets. The UK Financial Conduct Authority (FCA) has no master definition of conduct risk, however, in its Retail Conduct Risk Outlook 2011, the UK FCA referred to conduct risk as '...the risk that firm behaviour will result in poor outcomes for customers'. Good customer outcomes may be defined as customers getting financial services and products that meet their needs.*

In addition, the UK FCA has stated that 'a firm's conduct risk profile will be unique to it, and there is no one-size-fits-all framework that can be put in place to assess it'.

Speech by Linda Woodall, Director of Mortgages and Consumer Lending FCA at the Council of Mortgage Lenders (CML) – Mortgage Industry Conference and Exhibition. 6 November 2013.

Firm-specific definitions of conduct risk will need to be reviewed on a regular basis and may need to change in line with lessons learned, changing regulatory expectations as well as changes to the business activities or operating model.

(Chartered Institute of Internal Auditors, 1 April 2016)

I have spent the last twelve years trying to work out exactly what 'conduct' and 'conduct risk' means and how it can be defined in context to banking. This book itself came about in no small part due to this effort and more so because of greed, not my own, but the greed of a small group of bankers.

There are, of course, multiple reasons why the 2008 crash happened, but we all agree that greed played its part. Avarice, like a fifth and to date unknown rider of the apocalypse, had ridden steadily and progressively into the banking sector since the deregulation of banking sector (which started as early as 1980 with the Regulatory Reform Act in the US).

Unfettered and not controlled by regulation and associated controls, accountability and oversight, avarice extended temptation with little recourse for bad behaviour or loss, but offered a huge upside for those who took advantage of the loosely monitored environment. This allowed greed to become systemic and led the sector unknowingly and yet inevitably towards catastrophe.

> *Whoever loves money never has enough; whoever loves wealth is never satisfied with their income. This too is meaningless.*
>
> (Ecclesiastes 5:10)

Avarice, greed, greediness, materialism, covetousness, acquisitiveness, avariciousness, cupidity, avidity; all siblings of avarice. These siblings danced their merry way through the streets of the great City of London and pranced like peacocks along Wall Street and in and out of the mighty grid-squared and high-rise blocks of New York.

Very few had foreseen the coming of this disaster, where it was the employees of Lehman Brothers that first felt its immediate impact, followed by the other banks. Almost in parallel, businesses closely or intricately aligned and dependent upon the banking sector quickly suffered, many (like my own) crumbled as client revenues dried up

1 The Financial Crisis Inquiry Commission concluded that the financial crisis was avoidable and was caused by 'widespread failures in financial regulation and supervision'; 'dramatic failures of corporate governance and risk management at many systemically important financial institutions'; 'a combination of excessive borrowing, risky investments, and lack of transparency' by financial institutions, ill preparation and inconsistent action by government that 'added to the uncertainty and panic', a 'systemic breakdown in accountability and ethics', 'collapsing mortgage-lending standards and the mortgage securitisation pipeline', deregulation of over-the-counter derivatives, especially credit default swaps, and 'the failures of credit rating agencies' to correctly price risk'.

or disappeared overnight. Through the tortuous unravelling of the banking crash, its implications started to become apparent.

Ultimately millions of innocent people who had entrusted their life's savings, their homes or possessions found themselves with broken dreams and, in many cases, a life's endeavour, so carefully stored away in investments being managed by trusted bankers, lost.

At the time, I was running my own recruitment company, my first independent enterprise, focused wholly, and what proved to be naively, on the financial markets, with Lehman Brothers and RBS as our principal clients. It is fair to say I had ridden the gravy train of eternal optimism about these markets, been a beneficiary of them and as quickly as I had risen, I would fall.

As 2008 ended and the calamity of the crash was starting to become truly understood, I found a little time to contemplate the events of the immediate past. At that time, I was struggling to see a future, but recall reading an article that captured the reasons for the crash. More so, it pointed to the loss of honourable behaviour and professional standards in the period that led to the economic implosion. It asserted that the true casualty of the dancing siblings of avarice had been its opposing force, the force for good, their collective antonym, ethics and ethical behaviour.

Extract from The Financial Crisis and the Collapse of Ethical Behaviour: 4 December 2008 by Gregory Curtis, Chairman of Greycourt & Co., Inc.

Most assessments of the financial crisis that began in August of 2007 identify as the source of the problem such issues as poor risk controls, too much leverage, and an almost wilful blindness to the bubble-like conditions in the housing market. Well, maybe. These issues were certainly the proximate causes of the crisis we find ourselves in, and if only one or two firms had drunk the Kool-Aid – a Drexel Burnham, let's say, or a Long Term Capital Management – we could buy the usual

nostrums as the full story. But we suspect that the financial firms and their executives aren't quite so collectively stupid as this explanation would imply. We think there was something else going on, something that allowed intelligent people to persist in unintelligent behaviour. In our view, poor risk controls, massive leverage, and the blind eye were really symptoms of a much worse disease: the root cause of the crisis was the gradual but ultimately complete collapse of ethical behaviour across the financial industry. Once the financial industry came unmoored from its ethical base, financial firms were free to behave in ways that were in their – and especially their top executives' – short-term interest without any concern about the longer-term impact on the industry's customers, on the broader American economy, or even on the firms' own employees.

By a collapse of ethical behaviour, we mean exactly what we say – that the actions of many, if not most, of the large American financial firms (and of the many foreign firms that succumbed to the 'American disease') would strike an ordinary person as unethical – repulsive and scurrilous. But we also mean something more specific to the long-term viability of the financial industry, namely, the disappearance of any sense of fiduciary responsibility to the ultimate client. Integrity and a sense of responsibility to the industry's customers are at the core of what a financial industry must be all about; otherwise, it's just a big Ponzi scheme.

For many, not just bankers, 2008 was their annus horribilis, as UK statistics show company and personal liquidations rose by c.220% year-on-year 2007 through to 2009, as a direct consequence of the depression, triggered by the banking industry. In the US similar statistics show the cross-border, multi-regional and global impact of the depression. In the States much was made, quite rightly, of the impact on the average hard-working American and the erosion of economic confidence within its entrepreneurial base.

Perhaps this was not the most important subject of the media at the time, as it focused understandably on the corporate world and

dramatic events unfolding daily. However, the breadth and depth of the damage caused by the banking crash is now understood, with the small- to medium-sized enterprises known to have equally carried the burden of the banking industry's failure, as their irresponsibility drove the world into a depression.

The follow-on phase and the onset of the credit crunch impacted businesses as they struggled to secure funding to help them through the interim period, which left many feeling the brunt of the economic downturn. It is arguable that this impact was more personal, more immediate and painful for SMEs and especially those who owned and led their businesses, their lives and livelihoods being intricately linked. Most companies had no hand-of-hope offered, unlike the hand put forward in the shape of governmental funding and rescue packages for the banks.

The defining and pivotal point was Lehman Brothers filing for bankruptcy in September 2008, despite its best efforts to find a solution. Looking back after being amidst these unfolding events, Lehman's and the industry's failure throughout 2008 ran in my memory as if in slow motion, as the industry slid irreversibly into upheaval and calamity.

With Lehman Brothers under the water, and in November RBS securing a £15 billion rescue package from the UK government, followed by Lloyds, the other UK bank that was a major recipient of government funding, a period of instability and lack of opportunity was to unfold. This was mirrored and magnified in the US, as contagion and the banking industry's demise dragged great institutions into the mire, with the US government bailing out, amongst others, Bank of America, Citigroup, JP Morgan, Wells Fargo, Goldman Sachs and Morgan Stanley.

No one saw it coming until it was too late, although the signs were clear in the latter stages of 2007. If I had read the signals better, believing the head count freezes and therefore our ability to secure revenues through placing people, to be momentary and reversible, as opposed to

being long-term and not a temporary aberration, then perhaps I would have not lost in my pursuit to keep my company afloat. At the time, I had no reference point and the events that unfolded were unique and so underestimated that they overrode me, as they did many others.

Hindsight is a wonderful thing and as my father used to say, and an adage we have all heard many times, 'what doesn't kill you makes you stronger'.

It was perhaps the aligned catastrophe in 2008 of my father passing away due to medical negligence that helped me put things in perspective. Whilst having withdrawn equity from my home to recapitalise and stabilise my business, eventually having to lose it in entirety in this pursuit (which was both the right and, looking back, the wrong thing to do), my own challenges and losses appeared nothing amidst the far more meaningful and personal loss of my father.

More so, as a retired retail banker and 40-year employee of Barclays, he had taken his life's bonus' in Barclays' stock. I did not have the heart to tell him in his last few months as he lay in hospital that his belief, he would be leaving my mother with financial security was a falsehood. His thoughts were based upon a 2007 stock price trading at £7.90 per share (or there and thereabouts), which within a year of it reaching this high saw Barclays' share price dropping nearly 50%. Within the space of two years these declines had accelerated to 92% and Barclays shares traded at 64p.

His tragedy and that the reward for his life's work and endeavour had been taken away from him (by the very industry to which he had dedicated his life), ironically became united to my own situation. Right or wrongly, my view was and is that we had both been undone financially by the banking industry, and specifically greed and poor conduct within it had played an instrumental role.

I had certainly made mistakes on my journey, which if time could be rerun could have conceivably put my business in better shape (to deal with the downturn). Not least I should have been

more decisive in downsizing, soon after upsizing. As it turns out, my decision to significantly expand the business in the autumn of 2007, in the anticipation of good things to come, proved to be ill-timed, overly confident, naïve to a degree and unfortunate.

It was these events that took me on my journey to understand conduct and why I aligned my business (set up in 2011) to it. It married well with the understanding I already had of the COO and front office business management function, which gave me access to those charged with changing culture and managing conduct. At their centre was understanding the role of greed and human behaviour.

In the Motley Fool article, '25 Major Factors That Caused or Contributed to the Financial Crisis', John Maxfield (28 February 2015) states: 'While it's always tempting to boil things down to one or two root causes, the reality is that financial crisis of 2008–09 was caused by a confluence of dozens of factors.' It is his seventh cause that I read with deep-rooted interest:

Greed: The desire to get rich isn't a bad thing from an economic standpoint. I'd even go so far as to say that it's necessary to fuel economic growth. But greed becomes bad when it's taken to the extreme. And that's what happened in the lead-up to the crisis. Homeowners wanted to get rich quick by flipping real estate. Mortgage originators went to great lengths, legal and otherwise, to maximise loan volumes. Home appraisers did the same. Bankers were paid absurd amounts of money to securitise toxic subprime mortgages. Rating agencies raked in profits by classifying otherwise toxic securities as investment-grade. Regulators were focused on getting a bigger pay check in the private sector. And politicians sought to gain popularity by forcing banks to lend money to their un-creditworthy constituents.

It is with the wind behind us and lessons learnt from the dark days of 2008 that the conduct risk, cultural and behavioural change

agendas have blossomed, grown and sponsored meaningful debate and ongoing analysis. No one has the answer yet, if in fact an answer exists. As Matthew Hancock[2] explains in his book *Masters of Nothing: How the Crash Will Happen Again Unless We Understand Human Nature*, we must seek to understand human behaviour if we are to avoid future misfortunes and cataclysms.

In this enthralling volume, two noted political economists, using a model of a better understanding of human behaviour, lay down a blueprint for the solution to the status quo of financial boom and bust. It further investigates the behaviour of those who rode the boom and switched at the tipping point to ride the bust, and the behaviour of those who held on to their principles as the system collapsed around them, these being all important. It argues successfully that it was human behaviour after all that led us to construct a bubble nobody suspected was dangerous, yet nonetheless would burst with disastrous consequences. This book is what I would say is a 'must read' for anyone looking to understand the deep-rooted reasons and their human nature that led to the financial crisis. It captures the very essence of ethics and behaviour and how they must exist in a free market and capitalist economy if it is to serve all of us and not the few. It is linked therefore to that most human of behaviours, that feeds upon us and throws temptation before us; greed. My views on greed may appear a little narrow for many of my learned colleagues and those I know and don't know across the banking industry, but they appear to reconcile with voices well above my own in gravitas, station and importance, as Mark Cobley (Financial News, 16 March 2017), outlined in his article 'FCA Chief Bailey takes aim at "greed is good" culture'. In this article (below) he summarises how Andrew

[2]Matthew Hancock is the Member of Parliament for West Suffolk and was formerly Chancellor of the Exchequer George Osborne's Chief of Staff and an economist at the Bank of England.

Bailey, the former chief executive of the FCA, states the regulator will not cap bonuses or control levels of pay, but remuneration is a focus as it tries to change the ethos in the City:

The changes to bonus and conduct rules at the UK's finance firms over the past few years are aimed at driving a 'profound' change in the culture of banking, according to the City's top regulator – moving it away from the 'greed is good' attitudes of the 1980s.

Andrew Bailey, the chief executive of the Financial Conduct Authority, set out the regulator's thinking on banking culture in a speech to company directors in Hong Kong today.

He said the steps the regulator has taken to reform the way bankers are paid, together with a new certification process for senior managers, were about 'learning the lessons of history'.

He laid the blame for the global financial crisis of 2008–2009 at the door of a rapid increase in pay and bonuses for bankers and company executives from the 1980s onwards, including the greater use of stock option plans – 'to create a stronger link between pay and performance, or so it was presumed'.

This, coupled with accounting standards that allowed the presumed or expected profits from multi-year contracts and deals to be booked immediately, stored up problems. Bailey said: 'There is to my mind no doubt that it influenced the culture of firms. What happened next is, as they say, history.'

Bailey said that while the regulator will not try to cap bonuses or control the level of pay, it is interested in the structure of remuneration and the incentives it creates. He said: 'The influence that we do have will affect the culture of firms. That is intended.'

He also set out how the FCA's new Senior Managers and Certification Regime is intended to put senior bankers on the hook for the actions of their junior staff.

He said: 'One of the strong responses to the financial crisis, not

least from our Parliament, was to ask who was responsible … why responsibility did not, in the formal sense of regulatory action, sit with senior managers, and in particular CEOs.'

Regulators had wrongly confused 'responsibility' with 'culpability', he said: 'There is an important difference. Culpability is more about direct blame for an action whereas responsibility is about leadership. But direct culpability in banks during the crisis … was often with others lower down.

The FCA's new conduct rules are intended to make sure senior managers and board directors 'know what they are responsible for', while junior staff will be certified under the supervision of their bosses and the regulator. Bailey said: 'The effect on culture should be profound, and I say that in a good sense.'

Whatever the correct view, greed and its consequence within banking, past and present, have impacted my circumstance and subsequently shaped my views, driving me continuously to understand its root cause.

I view with genuine interest how the market is striving to address this common challenge. In a small part, I hope this book and my focus on the role of the COO and the Chief Control Officer and the forums my Company has run since 2014, help this effort, and in doing so help me push some challenging and dark times of my past permanently into the shadows. They are still there, twelve years on, but my focus is wholeheartedly on the future and taking advantage of all that the past may give us in helping us to understand the root cause of its errors and miscalculations. As the maxim states: 'the best predictor of future behaviour is, past behaviour', understand this and hope for mitigating failure in the future truly exists.

Regardless, I remain eternally optimistic in the human spirit and that good will always prevail, although it will have to overcome temptation and materialism if it is to do so in banking, an industry that serves us all.

HOFEN
bleibt!
19
Lebensfreude & Ges

Sei schlau
mach b au
keep YOUR
eyes open!
TROUBLE
IN
PARADISE
SPIDERMEN
=Verteidigungs Politik
18

"A fundamental component of the COO's responsibility is the management of control and operational risk."

SETTING THE SCENE: AN ADVENTURE INTO THE CONTROL WORLD

In 2013, I wrote my first paper investigating the role of the COO. Specifically, it focused on operational risk responsibilities and how I saw the COO as the de facto control officer. Back then I would never have guessed that a few years later much of my time would be taken up grappling with this same subject. Interestingly, when re-reading my poorly informed opinions, much of what I concluded remains surprisingly relevant and pertinent today. As such, I felt it important to include these initial thoughts as a sort of reference point within this book. And for it to find its place here, in the section dedicated to the role of the Chief Control Officer, which evolved from the COO's office in the interim period.

2013: The COO and the divisional control framework

A fundamental component of the COO's responsibility is the management of control and operational risk. This is especially true today, when the direct responsibilities and therefore the experiences and competencies of a COO demand a comprehensive understanding of non-financial risk and a passion to ensure its application and management. The way non-financial risk is

conducted in each bank is very different. Organisational design fluctuates; accountability is distributed in some cases equally, in others less so. However, whether explicitly stated or not, today's COOs understand that control and operational risk management are the cornerstones of their mandate.

Most people define 'operational risk' as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. It should also be noted that reputational risk goes hand in hand with operational risk, and has become increasingly important at a time when scrutiny of the banking industry by investors and the general public is more intense than ever before.

In most banks the COO has moved to be the operational risk 'contact' person for the business line. What started as a loosely configured contact, where each business and infrastructure department had a risk and control officer working within the bank-wide operational risk framework, the role of the COO today is far more central. This has come about partly by regulatory need and partly by recognition that the COO position is more visible and accountable than in the past. COOs' responsibilities in this context include:

- Providing of information and data for Group reporting
- Escalating any operational risk issues to management
- Acting as the primary point of contact for operational risk within the department
- Ensuring the control and operational risk framework is implemented in line with Group-wide policy

The COO's office, therefore, becomes the primary risk interface at Group level, with its in-business COO control officers within the Fixed Income and/or Equities divisions partnering and working with their Operations and Product Control counterparts and their

respective control functions, seeking to provide a uniform approach to developing a risk culture and risk awareness at all levels and with all staff. Importantly, the COO must take responsibility for all this – from embedding risk awareness into the culture to implementing the controls and processes to manage and mitigate events. Their role is pivotal in making this happen. Early in the evolution of the front office approach to managing real-time operational risk, Credit Suisse had a control team in the management office of the COO Fixed Income, with individual product COOs committed to delivering data and information on a weekly and monthly basis, and ad hoc information upon demand. The business heads committed to this internal service level agreement. In many ways is became a blue-print for this activity. At the same time UBS, its Global COO Fixed Income had a Global Control Officer, all be it with a smaller team than Credit Suisse, acting as a policy-overview and data-assessment contact, replying in turn to Group demands for divisional data and information. Other banks had less advanced variants of these two models, all be it all mature organisations then (as now) based their risk management practices on a series of well-defined principles, derived from experience, best practice and corporate governance, as follows:

- Systematic and structured risk management
- Evidence-based risk management
- Addressing uncertainty and its causes
- Risk management as part of decision-making
- Human factors and behaviour
- Tailoring risk management
- Transparency and inclusion of stakeholders
- Responding to change
- Enterprise-wide risk management.

Moreover, the COO is now empowered to innovate and adapt risk-management practices to reflect the size and extent of the business's operations and services. They must remain competitive in a changing environment, so that the business can respond to and exploit new opportunities. In their control function, therefore, the COO should:

- Be global, with regional teams focused on local regulatory demands
- Possess a team with direct internal organisational experience, supplemented by external hires with industry-wide experience
- Carry out a monthly 'controls committee' to ensure business-wide transparency, development of common practices and transferability of working controls
- Play an ambassadorial role in embedding risk and control awareness into the business at all levels
- Be the interface to internal departments (Operational Risk, Audit, Operations, Product Control, etc.) and external to the regulators

With successful implementation and executive support, many COOs are now able to:

- Deliver a robust control framework
- Assess individual and divisional businesses for key controls
- Ensure business lines are compliant with internal audit and external regulatory demands
- Provide aggregated control indicators and processes to effectively deal with key risk events
- Lead risk and control innovation with a commitment to continual improvement

To achieve all these points, a structured and centralised team is required and our research suggests that this has been done or is being done at most banks, mostly sitting within the Global COO's office. Whilst invariably centralised at global level, however, it may be dissipated to varying degrees to the regions and/or the products. Nonetheless, COOs are addressing these issues and accept their role and mandate is to be the Global Control Officer for the business.

In the context of the evolution of the COO's approach to managing control, over time this moved into the industry framework of the three lines of defence, with many COOs appointing a Chief Control Officer (CCO) to be directly responsible for 1LOD. In some cases, the CCO now reports directly to the CEO, sitting alongside and of equal importance to the COO. The article above, written in 2013, would appear to offer a reasonably accurate foothold and reference point as to the genesis of this evolution.

26
CHAMBERLAIN'S
PIZZAEXPRESS
22

LUC's
PIZZAEXPRESS
BROKERS
THE PE

"This complexity in responsibilities and deliverables demands diversity in competencies for any lead member of the Control Function."

DEFINING THE INDEFINABLE

The evolution and responsibilities of the Chief Control Officer

Executive summary

The role of Chief Control Officer might seem self-explanatory. However, situated within a complex and multifaceted banking environment, the simplicity of the title does not reflect the position's responsibilities and deliverables. The CCO occupies a space at the top of the executive agenda, as banks continue to struggle to meet regulatory obligations and head off the ever-present political posturing and venomous assaults of the media. To avoid in the future, the catastrophic events of the past, banks need control as well as employee and investor confidence. Most banks have appointed a corporate or divisional CCO to steer them through on-going troubled waters, and this position may prove essential in doing so. Importantly, while the market continues to grapple with control and conduct issues, themes have evolved feeding the debate on how best to meet these challenges:

Trust and control:

- These two issues are synonymous; both take time to build and establish, and both can be lost easily.

- Banks do not treat them as differentiators today in the way they did from the 1950s to the early 1980s.
- It is a fallacy today that society trusts IT companies more than banks (Edelman argues that IT companies are more insecure than banks).

Control and reputational risk:

- The control, legal and compliance functions are the custodians of the firm's reputation.
- Reputational risk is arguably the most important focus for a CCO. For example, when Standard Chartered Bank was fined in 2012 by the US regulator, the fine itself paled in comparison with the $billions then wiped off its share price in the days that followed. This punishing equation has been repeated multiple times since, with recent fines being announced amidst the extraordinary demands presented by COVID-19
- First line control functions still lack the technology, resources and experience to effectively undertake their role; most are unskilled in social media and 'search and discovery' processes. Instead they are focused on traditional regulatory face-offs and internal controls, and even then, most lack the tools to track 'big regulation'.
- The most severe external threats are from big data, social media, the dark web and cyber-attacks, and in investment banking these investigative skills are not truly valued in the way a quant or trader is.
- These threats are increasingly exacerbated by geo-political events and a need to understand how these translate into internal and external threats to the industry.
- Conversely, these skills do exist in some parts of Markets now and are increasingly integrated into its control framework.

As a principal historical case for reference, it is possible to view examples such as JPMorgan (see below) as control failures where managing risk and losses in the trading sense is key to managing 'control'. However, this is not the only perspective. In the case of JPMorgan, many maintain that the real issue was a conflict of interest within the CIO function: when does liability management become investment management and alpha creation? Was this a failure that could have been mitigated by control processes? Most think not.

My conclusions are that control officers need to be polymaths – not only conversant in investment-bank regulation and the risks inherent in the core business (market, counterparty, operational), but also equipped with the skills and technologies to manage the broader risks of big data, dark internet, cyber and denial-of-service attacks, geo-political impacts, etc. This is what I believe is more appropriately captured in the use of the term threat management, which is focused equally on horizon scanning and looking for emerging risks as to looking over your shoulder to the past, where the CCO is mandated to prevent history repeating itself. As such too many of mandates of the CCO have become administrative, lacking the mandate (and resources) to promote lateral-thinking, to allow the imagination to flourish. These behavioural and qualitative skills and attributes are required to identify real threats and work out how to respond to them. There is an argument here between quantitative and qualitative assessment, as a differentiator between market, credit and operational risk. However, unlike these risk disciplines, to maximise impact the control officer will need to bridge all effectively – and this is no easy task.

Control in evolution – Basel sets the stage

As the flourishing banking sector raced towards the twenty-first century, the Basel Committee distributed numerous papers to the supervisory authorities worldwide in the belief that the principles presented would provide a useful framework for the effective supervision of internal control systems. 'Control' was on the agenda, but it was propping up other, more important, revenue-generating items. Today, however, control and conduct have developed their own agenda and are unquestionably a leading item for discussion, dissection and digestion at employee to board level. How did this promotion to pre-eminence happen and what does it mean in practice?

In the late 1990s, the Basel Committee wanted to emphasise the importance of sound internal controls to the prudent operation of banks and to the stability of the financial system as a whole. While the Committee recognised that not all institutions would implement every aspect of its framework, banks were encouraged to work towards this end.

The guidance previously issued by the Basel Committee typically included discussions of internal controls affecting specific areas of activity, including interest rate risk, and trading and derivatives activities. The new guidance encouraged supervisors to use the framework in evaluating the internal controls over all on- and off-balance sheet activities in banks and consolidated banking organisations. However, there was no focus on specific areas or activities within a banking organisation. The exact application depended on the nature, complexity and risks of the bank's activities. This was an evolutionary step rather than a revolutionary one, and the qualitative and untested nature of its recommendations left the framework open to interpretation and, consequently, inconsistent implementation.

There is no doubt that this was a valiant attempt to build a regulated, operating framework to reduce the chances of individual banks repeating the mistakes of the past, by taking a new approach to operational risk management and capital allocation. Areas where a breakdown in control had been identified became the focus for this new regulatory and risk framework, but were found to be woefully inadequate as the financial sector galloped headlong into the credit crunch. This financial cataclysm was a series of interlinked events whose aftershocks still ripple through the sector today, each delivering a call for further regulation.

Despite the Basel Committee's regulatory initiatives and the subsequent market-wide attempts to introduce control mechanisms to mitigate organisational, enterprise-wide and systemic risk, it is clear that early attempts at regulation failed. Things could certainly have been worse without the Basel initiative, but how much worse, and in what ways, we will never really know.

Too big to fail – a call for control

As a result of the credit crunch, the banking sector found itself under intense scrutiny. From the unwinding of Lehman Brothers to the present day, every action is eyeballed, every stone turned over and every discovery played out on the media stage. There was a clear need to implement both company and market-wide control, and, significantly, to do so publicly. The media and politicians demanded it, clamouring for executive and corporate scalps, and by default the general public became the de facto judge and jury. The banking sector was found guilty on all counts and a return to the realms of respectability and responsibility depended on individuals and the sector as a whole being seen to embrace regulation and control. To understand this dynamic, we will investigate the example mentioned above – JPMorgan Chase & Co.

JPMorgan and its Chief Executive Jamie Dimon came under fire in 2012, when a massive, money-losing derivatives trade came to light. This eventually cost the bank more than $6 billion in trading losses, and led to the indictment of two former employees. The bank expected to pay (and did) at least $700 million to settle civil law investigations into the matter. As a result of this, in July 2013 Reuters reported that JPMorgan was bracing itself for more legal and regulatory scrutiny, but that it had outlined a series of steps taken to improve operations in a memo to employees[1]. Facing probes from the US Department of Justice, the Securities and Exchange Commission and other government agencies investigating a range of issues including energy trading, bribery in hiring practices in China, and fraudulent sales of mortgage securities, JPMorgan stated that it was devoting 'unprecedented' resources to fixing its risk, legal and compliance operations. Simultaneously, Dimon began meeting with regulators directly to improve relationships and stated his intention to hold 'town hall' meetings twice a year with examiners from the top US regulators.

The company had added 4,000 staff to its control groups and had increased spending on this effort by about one billion dollars. The bank's control group included risk, compliance, legal, and finance, technology, oversight and control and audit functions. Dimon also confirmed that the bank was trying to simplify its operations by getting rid of businesses that were not core to its business model. It had, for example, stopped selling identity theft protection and credit insurance. Earlier that month, the bank also said it was getting out of the student loan business, and was planning to cease physical commodities trading. Dimon went on the say that JPMorgan was conducting a review of its foreign correspondent banking business and paying closer attention to outside vendor

[1] Reuters reporting by David Henry and Lauren Tara LaCapra; editing by Gerald E. McCormick and Nick Zieminski.

partners. Acknowledging the bank's mistakes, Dimon said that he and his employees were 'facing [our] issues and rolling up our sleeves to fix them'.

One by-product of this series of events was the establishment of what Dimon described as a 'state-of-the-art control room' at its corporate headquarters in Manhattan, from which staff devoted to control and operational risk matters could retrieve data from across the firm to spot problems. Dimon called the control initiative an 'unprecedented effort' for JPMorgan: 'Never before have we focused so much time, effort, brainpower, technological power and money on a single, enterprise-wide objective.'

The arrival of the Chief Control Officer

JPMorgan appointed a Global Control Officer to oversee this financial and resource effort – one of many banks that took such a step. The market's move to make such appointments raised a number of questions, scrutinised in the role's foundation years (2014 – 2018) and surprisingly most are still under disruptive discussion today in 2020:

1 What was the mandate of the Control Officer and how could this investment be effectively managed? Could it be quantified in a return on this investment?
2 With regulatory pressures aligned to investor demands and political interference, how would internal supervision, compliance, audit and operational risk collaborate with and not replicate the effort of the 'control office'?
3 How could the Control Officer and their direct and extended team work across the established control functions to drive collaboration and benefit, and avoid potential conflict and duplication of effort?

4 What were the established component parts that the Control Office would own directly? How, with this mandate, could an integrated bank-wide control framework be implemented?
5 What were these established internal control functions? All the control activities performed under the governance and organisational structure established by the bank's board of directors and senior management. Each individual within the organisation was charged to participate in order to ensure proper, efficient and effective performing of the bank's activities in accordance with the management strategy and policies, and applicable laws and regulations, to ensure the integrity and reliability of the accounting system and the timeliness and accessibility of information in the data system.
6 What was the accepted internal control system? All the financial, operational and other control systems carried out by internal controllers, which involve monitoring, independent evaluation and timely reporting to management levels to ensure that all activities are performed by management levels in accordance with current policies, methods, instructions and limits.
7 What constituted the internal audit (inspection) system? A systematic audit process carried out by independent internal auditors as a part of the internal control function and in the form of financial activities and compliance audit independent of the bank's daily activities, considering the management's needs and the bank's structure. This covered all the activities and units of the bank, mainly the internal control system and the risk-management system, enabling the assessment of these activities and units. Assessments were and are made through reporting, monitoring and examination.
8 What would be the internal supervision (control and audit) system? The integrated process consisting of the internal control system and the internal audit system.

9 What would be and is the risk-management system? All the mechanisms relating to standard-setting, reporting, verifying compliance with standards, decision-making and implementation, which are established by the board of directors to monitor, control and, if necessary, change the risk/return structure of future cash flow and, accordingly, the quality and extent of the activities.

Stakeholder management

The subtle art of building a control framework

The Control Officer mobilises the framework outlined above, but other factors also play a part in defining and managing the control framework:

Senior management: the bank's general management, deputy general managers and managers of operational departments who hold signature authority (much more so today in 2020 following regulation that denotes individual accountability such as the Senior Managers and Certification Regime in the U.K.)

Inspector: a staff member who inspects the conformity of the bank's activities with banking law and the institution's internal regulations.

Internal Control Unit: a unit that organises, manages and coordinates the bank's internal control process;

Internal Controller: a member of staff (not an inspector) who is authorised by management to monitor, examine and control the activities of the bank on an ongoing basis;

Risk Management Group: the whole structure that comprises the Executive Risk Committee, Bank Risk Committee, and Risk Management Committees of the individual operational units, centralised or decentralised, established to manage the risks the bank is exposed to in a systematic way.

Asset/Liability Management Committee: the committee assigned by the board of directors with the duties of determining the policies for asset/liability management and mobility of funds, and monitoring implementation of activities, with decision-making executed by relevant units within the framework of the bank's balance sheet management.

Risk Management Staff: staff in risk management committees who are responsible for such issues as defining, verifying and assessing risks to which the bank is exposed through certain criteria, quantitative and analytic techniques. They have knowledge and experience in risk management and work alongside internal controllers in accordance with the provisions and procedure set out by the board of directors.

It is within this melee of established control functions that the Control Officer had to forge a consensus and deliver on the corporate mission (and man y think are still doing so today), starting with the key question:

'What is a Control Office and how do you define its mandate?'

Defining the operating model

The vertical vs horizontal debate

Across the market, a Control Office appeared to be a team established to coordinate all existing control elements into a consistent and logical model. They were tasked with ensuring that future developments in the business would be integrated into this model. This represented a corporate commitment with an emphasis on maintaining and enhancing a robust and effective control framework, not only for meeting regulatory requirements, but also to deliver on the core values and promise to the bank's staff and investors.

In some banks, the Control Office were split into infrastructure and front-office risk and control functions, working independently but in partnership. Other banks used a fully integrated front-to-back and cross-divisional control function. In either model, the role of the Control Officer was to deliver a seamless control framework across the company, with ownership shared by all.

Control had been propelled to the forefront of front-office tasks and responsibilities – the first line of defence (1LOD). However, the role of the Control Officer quickly migrated to being the link for the arteries and veins running vertically through a bank's business functions. Some argued and still do, that these horizontals should remain firmly independent and others that front office should be separate from the infrastructure. Either way, collaboration, communication and making sure that everyone understands the need for a single common objective would help ensure the success of any configuration. This esoteric standpoint would harden, it was hoped, into an unassailable mission if, like Dimon, the bank's Executive would be unequivocal in its commitment to the initiative and the Control Officer was given the budget, the headcount and the mandate to deliver.

Today all the members of the premiership of banking has established such an office with a varying mandate, although some of the smaller banking franchises are still working towards first base. Those that have reached second or third base are now stopping to reflect on the model that has evolved. It does not yet appear clear how any function will operate and divide the task of delivering an integrated approach to control, where it is generally accepted that it must be split into design, behaviour and strategy/forward thinking. A key hurdle to making progress is the complexity of understanding how to define roles and allocate tasks between first and second line, this issue being discussed later. Some have suggested that banks could collaborate in this redesign, to mobilise collective resources, establish market-wide best practices and in so doing so, take great steps towards self-regulation. It would of course need deep rooted support and collaboration from the regulators to do so, where in the short-term direct input by them in interpreting the exactness of the model and responsibilities between the first two lines will help this endeavour.

In the interim, how the Control Officer continues to navigate these risks from within well-established control functions will be key to the success of the position, where much has not changed in the issues facing them since the role's inception in 2014. Notedly, the need to possess well-proven stakeholder, relationship management skills, is becoming increasingly important when chairing committees and change groups and winning the confidence of the business they are appointed to protect.

This complexity in responsibilities and deliverables demands diversity in competencies for any lead member of the Control function. Today they must in part be strategic, understanding the end-to-end process; but they must in equal part have an inquisitive and risk and audit mindset, to be able to identify risks and/or

understand how to link the control function between different sectors of the bank or group.

In no small part due to the demands to restrain, control and regulate the banking sector and its occupants, the banking sector in 2020 has emerged as being better managed and more robust. Signs are promising, as governments and the regulators appear to recognise that the regulatory pendulum may be swinging too far, causing some banks to publicly express their concerns about the erosion of entrepreneurialism and a bank's ability to take risks – factors that must remain at the heart of a thriving banking sector.

However, if the regulators are to make a positive step in supporting and guiding the industry whilst regulating it, building an understanding of the role of the COO and CCO (1LOD) by adding a direct dialogue with this community, alongside the bi-lateral conversations usually held with the head of the business and/or compliance, will be extremely beneficial to all.

Footnote:

Dealing with a historic perception

Winning political, media and public confidence is key to quantifying success

What has made the banking sector such a success – innovation – has also been its downfall. Controls are often designed to deal with historic innovation, not future development. Today's and tomorrow's bankers will find routes to bypass regulations and control measures, and their innovation and entrepreneurialism will ultimately lead to further regulation. The aim of investment in control initiatives is to ensure that such regulation has been anticipated and that the banking sector is seen to be delivering control mechanisms and processes that will prevent disaster rather than respond to it – proactive and anticipatory threat management.

The view of the role of the banking sector remains consistently negative, and this perspective is exacerbated by today's climate of mistrust following on-going events and scandals, where history has an unfortunate habit of repeating itself:

> *'You are a den of vipers! I intend to rout you out, and by the Eternal God I will rout you out. If the people only understood the rank injustice of our money and banking system, there would be a revolution before morning. … If Congress has the right under the Constitution to issue paper money, it was given them to use themselves, not to be delegated to individuals or corporations.'*
>
> US President Andrew Jackson, speaking about international bankers in 1831

It remains the shared responsibility of today's Control Officers and COOs with executive and board-level support, to help change this view, to establish a sustainable banking model that serves its employees and its investors and earns the respect of politicians and the general public. This responsibility is at the heart of the market-wide good conduct effort, inseparable from the control agenda and ultimately the responsibility of the COO fraternity, within which the CCO sits. Even here, however, the moral objective needs to marry with pragmatism and the limitations of the sector to deliver this change with limited resources and capital.

"The command and control framework within the military and commerce are in place to enable effective day-to-day management of resources and to create a framework for enabling and managing change."

CONDUCT AND CONTROL

Leadership as a cornerstone of conduct and culture

At an Armstrong Wolfe COO forum in Q1 2017, there was a united opinion that the present intensive phase of industry evolution is generational, offering no simple, short-term fix to the cultural challenges that can manifest themselves in conduct issues. It was also agreed that today's executive has a responsibility to build on the foundations for control and conduct to ensure success and sustainability for the next generation. There was additionally tacit acknowledgement that cultural change would not be complete until today's generation had exited the sector, taking with them the legacy of previous practices and reference points of bygone days.

Cultural change must be driven and owned by front office, the business, where bridging traditional practices of managerial development with sales and trading staff has proven ineffective and impractical. This gap in need and intent to do the right thing, and the best way to achieve it, were central to the closing comments of the debate.

The markets and its executive talk enthusiastically of embedding a control or risk culture into the industry, repositioning and reinforcing its DNA in the face of on-going scrutiny by the regulators, politicians, public and media. However, we have to approach the transformation of the industry's culture holistically in order to achieve the desired result. The end culture would be based upon an ingrained sense

of individual and collective accountability and responsibility, built on traditional and perhaps until recently unfashionable well-tested values of integrity, value-based professionalism and a defined sense of individual and collective purpose.

A more recent 2020 debate had echoes of the 2017 debate, then pre-positioned with a thought-provoking presentation by Chris Severson, previously of Barclays. Chris, a retired TOPGUN instructor of the US Marine Corps, offered an insight and comparisons in relation to the impact of culture, control and conduct from a military perspective, weighed against his experiences since moving into the banking sector. The basis of the command structure for the USA, the UK and more generally any member of NATO and its armed forces is the operating ethos and practice of 'command and control'.

The US Department of Defense Dictionary of Military and Associated Terms defines command and control as: 'The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called C2.' Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities and procedures employed by a commander in planning, directing, coordinating and controlling forces and operations in the accomplishment of the mission. Commanding officers are assisted in these tasks by specialised staff officers and enlisted personnel. These military staff provide a bi-directional flow of information between a commanding officer and subordinate military units. In this context, the purpose of a military staff is mainly that of providing accurate, timely information that, by category, represents information on which command decisions are based.

The key application is that of decisions that effectively manage unit resources. While information flow toward the commander

is a priority, information that is useful or contingent in nature is communicated to lower staffs and units.

This in itself sounds similar to how any commercial or corporate entity would run its own management and communication structure. The command and control framework within the military and commerce are in place to enable effective day-to-day management of resources and to create a framework for enabling and managing change. Again, similarities exist.

However, it misses one fundamental point. Command and control in the military is a robust, immoveable and pyramidal structure, where training from selection to induction to on-going development underpins this supposition. The very ethos it creates and sanctions is an adherence to absolute leadership. The success of the military, where its risk assessment is quite literally a matter of life or death, rests upon this structure enabling the military to 'march on its stomach' and fight effectively, demands logistical support that also relies on this ethos.

This is not to say that inspirational leadership itself does not play a role, for clearly history shows it does, but inspirational leadership alone cannot achieve the goal. Conversely and very importantly, individual leaders at all levels are given room for thought and decision-making, but all decisions are ultimately tied to the overall mission. With the launch of missions in Iraq and Afghanistan, the military, like the banking community, were under media scrutiny and had to respond to improving practices and, as a de facto public entity, had to work within an increasingly regulated environment. When operational, the command and control ethos, married to a deep-rooted sense of service creates a strong culture of individual and collective responsibility that underpins and supports control.

A CEO of a large company and their managing directorate do not have this absolute structure in place to manage and drive the business. There is, of course, a pyramidal structure, where the chain

of command can be found, but there is not an automatic adherence to the commands that come down these communication channels. All management, irrespective of sector, has to lead by example to maximise performance through respect. In commerce, however, this can be easily fractured if management is poorly executed. To be effective in commerce an executive manager has to possess a box of levers – options to help execute and expedite management's tasks and objectives correctly, invariably using incentives. These can be career advancement and promotion, or relevant to banking, financial reward or, increasingly, the implementation of regulations that create an absolute lever to frame and even quantify individual and corporate conduct.

Importantly and missing in commerce, is one important lever. In the military you have a deep rooted and very well-defined sense of purpose. This purpose is linked to an innate sense of service. This sense is linked to a value being attributed to what you do for society, country and the common good. More so, however, the real strength of the military, when on live operations, comes from the sense of duty and responsibility to your colleagues, your comrades in the trench next to you, where this sense of duty cascades upwards not downwards and is the DNA that delivers operational effectiveness, cultural cohesion and fosters a culture where service men and women go beyond the norm.

With this in mind, the COOs attending asked 'How and what could be done. What additional levers could be provided to management and what could the industry design, implement and embrace market-wide as common managerial levers?' In this context, leadership training was discussed as a medium that should deliver cultural change (*across the industry*). However, all agreed that while such training programmes within the infrastructure or non-revenue departments are manageable and valuable, it was a

challenge if not impossible to implement meaningful programmes in the front office, as loss in associated revenues when taking rising stars and/or established managers off-line was commercially unviable. This in itself appears to be missing the point.

The debate on how leadership can shape culture that effects conduct, took the conversation neatly to that of conduct risk. 'Conduct risk' itself had differing definitions around the table, each bank aligning it differently from an organisational leadership perspective, which in turn characterised its authority and ability to make an impact. A look back and turning the pages of recent history helped, in using as a historical reference Reuters' Conduct Risk Report, 2013: 'Conduct risk is the next step in regulatory evolution. Given the deliberate lack of precise detailed rules and prescriptive requirements from the regulators it might even be considered a revolution.' This proved to be accurate and advance thinking.

Similarly, following its inception in April 2013, the Financial Conduct Authority (FCA) put conduct risk at the top of its regulatory agenda. The 'FCA Risk Outlook 2013' detailed the regulator's approach to analysing the root cause and emergence of conduct risk. At the outset of the Risk Outlook, it was clear that the FCA had opted to purposely not provide any working definition of conduct risk. Instead, it sought to broadly contextualise the risk, indirectly observing that it refers to 'consumer detriment arising from the wrong products ending up in the wrong hands, and the detriment to society of people not being able to get access to the right products.

However, this evolution was not welcomed by all, with leading market protagonist Professor McCormick stating that conduct risk is 'no more than a new term for a part of legal risk' and 'legal risk is a sub-category of operational risk'.

In any event, banks are expected to develop their own 'I know

it when I see it' conduct risk definitions and promote bespoke strategies to meet their specific risks and needs. In other words, there is no 'right' or definitive way for a bank to effectively manage its conduct risk. Simply ticking a regulatory compliance box and not continuously critiquing their market conduct is a recipe for disaster. This approach to risk management is symptomatic of a greater expectation from regulators that banks deliver 'good' outcomes for customers and the industry as a whole. Accordingly, a more holistic approach is needed to examine the scope of conduct risk.

In order to agree how best to lead and embed 'conduct risk' into the narrative of the employees, and therefore become part of the control matrix, it was agreed that conduct risk generally refers to risks attached to the manner in which banks, and their staff, 'conduct' themselves. This incorporates matters such as:

- How are customers treated by banks? Are they getting financial services and products that meet their needs?
- What are the risks of banks prioritising commercial interests over consumer issues? Are innovations in financial products and services in the consumer's best interest?
- How do banks need to behave to restore trust in the industry?
- How does a bank manage its conflicts of interest?
- How does a bank compete fairly with its peers?
- How does a bank ensure that the integrity of markets is at the heart of how it runs its business?
- How do remuneration schemes shape the behaviour of staff?
- How does management's 'message from the top' articulate the right culture or incentivise 'good' behaviour?
- How does the behaviour of a bank and its staff impact on market stability and price information?

Taking the above as gospel, conduct risk therefore marks a regulatory shift from reactive to pre-emptive. With a forward-looking approach you may be able to identify fault lines across the global financial system more quickly and seek early preventive measures. The lack of regulatory guidance on a working definition of conduct risk does have its drawbacks, as it is generally acknowledged that narrow definitions of conduct risk cannot be taken at face value or viewed independently.'

If obtaining an industry-wide definition of conduct risk is a difficult task, it is not surprising measuring a bank's appropriate conduct risk appetite or what a robust conduct risk-management framework should look like is one of the greatest challenges for the banking sector. Conduct risk constantly changes, where leaders are always reviewing their approach to assessing and managing it. Gap analysis is carried out to assess any additional controls that are needed and clear lines of accountability for conduct risk have, in most banks, been established. What responsibility the COO and CCO community may hold in context to forming or managing 'a forward-looking approach' is yet to be determined, but it was agreed it was likely to be a central one and where the principles of command and control could play an important role. This is further investigated when we later discuss the role of the COO and CCO in managing threat. Barring definitional issues, however, conduct risk is a cornerstone of how regulators and banks approach risk management now and into the future. To this end, it will be resident in the COOs in-tray for a generation or more, be this redefined as threat management or not.

A few months after this debate, the worldwide pandemic arrived with devastating social and economic impact. One noticeable shift delivered by the pandemic and the move to an employee base working mostly from home, was debated at a global COO panel

session and symposium in September 2020, attended by over 100 COOs (*see chapter: Surviving, Thriving, Resetting*). This shift has been the change in emphasis from day to day management to leadership and empathetic leadership more specifically. Within a dislocated and distributed workforce, the role of leadership as a principle way to maintain focus, purpose and cultural cohesion, was recognised as an important tool to enhance control and conduct awareness. To be effective, however, and as discussed later, requires this understanding, capital investment and allocation of staff time at all levels to its training).

"The principal dimensions of character are integrity, drive, collaboration, humanity, humility, justice, courage, temperance, accountability, transcendence and judgement."

CHARACTER'S ESSENTIAL ROLE IN ADDRESSING MISCONDUCT IN FINANCIAL INSTITUTIONS

By Furlong, Crossan M, Ganz and Crossan L
Ivey Business School

This article examines one of the critical causes of misconduct that has persisted in the global financial services industry despite the warning flags raised from the financial crisis of 2008–09 and the very public shaming of major financial institutions (FIs) that have violated various regulatory regimes. [1]

The authors argue that many acts of misconduct are consequences of failure of judgement owing to weaknesses in leader character. By doing so, the article pivots away from the prevailing popular wisdom that such acts of misconduct are consequences of the moral or ethical shortcomings of 'bad' people. Rather, it takes the view that these acts of misconduct are usually the result of poor judgements made by people with underdeveloped character dimensions working in organisational cultures that allow or encourage them.

* The views expressed by William Furlong (who is also a Commissioner at the Ontario Securities Commission (OSC)) in this article are his and do not necessarily represent the views of the OSC.

[1] This article is based on the substantial body of research by a team of researchers under the auspices of the Ivey Ian O Ihnatowycz Institute for Leadership.

The article defines character as an amalgam of virtues and values that, individually, collectively and interactively affect the way leaders perceive situations, as well as make and implement decisions. The principal dimensions of character are integrity, drive, collaboration, humanity, humility, justice, courage, temperance, accountability, transcendence and judgement (see Figure 1). The authors' research suggests that character can be assessed and developed, and that leaders with character can infuse character-based decision-making into the culture of the organisations they lead.

When we use the word 'leader', we are not just referring to those in formal, positional leadership roles such as Chief Executive Officer (CEO), Chief Financial Officer (CFO) or Chief Risk Officer (CRO). We also include those who are willing and able to exert influence on leaders. Legal and financial advisers, for example, may not be in executive roles but they can have a substantial influence on the ways in which executive leaders frame and understand issues and make their decisions.

Further, the authors contend that lawyers could and should play an important role in preventing such misconduct if they had a better understanding of the effect that character has on executive decisions. Whether as trusted advisers, compliance professionals, inside counsel or regulators, such understanding would enhance the quality of advice they give or actions they take and would prevent them becoming complicit in wrongdoing. Beyond that, they could become an integral part of building healthy, sustainable organisational cultures that quickly recognise and address potential misconduct even before it happens.

In this article the authors:

- describe the types of poor conduct that have continued to plague the financial industry since the onset of the financial crisis;
- review the media coverage and academic literature that has

tended to analyse and frame misconduct as an ethical or moral issue and why, framing it this way, the solutions designed by regulators, boards and management to address it has been met with only limited success;
- introduce a more complete interpretation of the sources of poor conduct and misbehaviour in the financial industry using the Ivey Leader Character Framework;
- discuss the implications for FIs, regulators and their legal advisers, justifying the authors' position that character must be a legitimate topic of conversation, exploring lines of enquiry related to character, and suggesting criteria by which responses could be assessed; and
- finally, propose how this approach to character might be implemented in ways that will strengthen the business judgement of the leadership, organisational culture, and approach to risk management and regulation throughout financial services organisations.

Poor conduct persists in the financial services industry

Since the 2008-09 financial crisis, there have been numerous and widespread instances of poor conduct continuing to take place within FIs across the globe. Some of the more egregious, recent examples include:

- *Retail fraud*: In September 2016, Wells Fargo had to pay US$185m to settle charges that its employees had fraudulently created more than two million deposit and credit card accounts in order to achieve performance targets and earn bonuses. Wells Fargo employees created personal identification numbers (PINs)

[2] Lucinda Shen, 'Wells Fargo Has Been Fined $185 Million for Opening Unauthorized Accounts' *Fortune* (8 September 2016).

and fake email and phone addresses for the fraudulent accounts.[2] Ultimately, more than 5,300 bank employees lost their jobs, CEO John Stumpf resigned and Wells Fargo now faces an array of new investigations and lawsuits related to the matter.

- *Forex market manipulations scandal*: Global banks will pay more than US$10bn to settle allegations that they rigged the US$5tn daily forex markets. A notable quote from an unnamed trader as written in a 5 November 2010 chat: 'If you ain't cheating, you ain't trying.'[3]
- *Money laundering*: In December 2012, HSBC Holdings plc ('HSBC') reached a US$1.9bn settlement agreement with the United States Department of Justice to resolve charges it enabled Latin American drug cartels to launder billions of dollars from the mid-1990s to 2010.[4] Despite HSBC spending nearly US$3bn annually and tripling the number of compliance staff to around 9,000 people, a monitor overseeing HSBC's compliance with this settlement has found numerous lapses. 'The monitor's findings, which date from 2015, suggest that despite three years of efforts to bring compliance up to U.S. standards, HSBC is still struggling to meet the terms of the deal.'[5]
- *Rogue trading scandals*: There have been numerous rogue trading scandals uncovered in recent years, the larger ones including JPMorgan Chase's 'London Whale' (2012, approximately US$5.8bn loss) and UBS's Kweku Adoboli Equities Trading (2011, approximately US$1.8bn loss).

[3] Lindsay Fortado and Katie Martin, 'Serious Fraud Office drops UK criminal forex probe' *Financial Times* (15 March 2016).
[4] US Department of Justice, 'HSBC Holdings et al Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement' (11 December 2012).
[5] Ese Erheriene and Margot Patrick, 'Iranian Miniskirts, Bags of Cash Raise Doubts Over Controls at HSBC' *Wall Street Journal* (30 March 2016).

In a recently published study by Boston Consulting Group it is estimated that, since 2008, banks have paid fines of US$321bn. In 2016, banks paid fines of US$42bn, an increase of 68 per cent from 2015. Boston Consulting Group believes this amount will increase 'as European and Asian regulators catch up with their more aggressive US peers who have imposed the majority of fines to date'.[6]

What makes these egregious breaches of conduct remarkable is that they occurred or continued to occur *after* the 2008-09 financial crisis; after the multibillion dollar bailouts of the financial services industry funded by taxpayers across the globe; after the extraordinary measures taken by international banking regulators to increase their oversight of financial institutions, including the hiring and placing of staff within the financial institutions and the creation and passage of thousands of new pages of legislation (Sarbanes-Oxley, Dodd-Frank, United Kingdom and European, etc) had been enacted; *after* industry leaders, governments, regulators and the public at large had been sensitised to misconduct that, if not widespread, had led to severe reputational damage to leaders of financial institutions, especially bankers; and after these selfsame financial institutions had committed billions of dollars to the implementation of new governance and oversight programmes, hiring tens of thousands of new audit, compliance and control personnel across the industry. As William C. Dudley, President and CEO of the New York Fed, said: 'I was particularly struck by how the manipulation of foreign exchange rates occurred even after the LIBOR fixing was widely known. The appropriate lessons from the LIBOR scandal did not seem to have been learned. That was both surprising and profoundly disappointing to me.'[7]

[6] Gavin Finch, 'World's Biggest Banks Fined $321Billion Since Financial Crisis' *Bloomberg News* (2 March 2017).

[7] William C Dudley, President and CEO, Federal Reserve Bank of New York, *Remarks at the Culture Imperative – An Interbank Symposium* (11 January 2017).

David Wright, who in 2016 stepped down as secretary-general of the International Organisation of Securities Commissions (IOSCO), was quoted as saying that he has 'no confidence that corporate governance and behavior is improving'. He added, 'My view is that there will be more discoveries of anti-competitive behavior, price fixing and collusion. I hope that I am wrong but I fear that I am not'.[8] In remarks made in June 2015 to the C.D. Howe Institute, Office of the Superintendent of Financial Institutions (OSFI), Superintendent Jeremy Rudin stated that OSFI has 'come to see conduct as a prudential issue'.[9] This position was reinforced by Rudin in an article in which he was quoted as saying, 'Regulators need to make sure harder-to-measure aspects of culture norms and expectations for behaviour are in place to keep the risk-reward balance in check throughout the financial institution'.[10] This lack of progress at improving conduct has been a source of real and intense frustration for managements, boards, regulators, industry stakeholders and the public at large. In the US, it has been publicly stated by regulators that if bad behaviour were to persist then 'the inevitable conclusion will be reached that your firms are too big and too complex to manage effectively. In that case, financial stability concerns would dictate that your firms need to be dramatically downsized and simplified so that they could be managed effectively'.[11]

[8] Chris Flood, 'Cracking down on "megalomaniacs and bullies"' *Financial Times* (24 March 2016).

[9] *Away from the Lamppost: Culture, Conduct and the Effectiveness of Prudential Regulation*, remarks by OSFI Superintendent Jeremy Rudin to the C.D. Howe Institute, 17 June 2015.

[10] Barbara Schecter, 'Canada's bank regulator probing links between risks and "culture" at financial institutions' *National Post* (7 December 2015).

[11] William C Dudley, President and CEO of Federal Reserve Bank of New York, *Enhancing Financial Stability by Improving Culture in the Financial Services Industry*, Workshop on Reforming Culture and Behavior in the Financial Services Industry (20 October 2014).

Poor conduct incompletely framed as an ethical or moral issue[12]

The media, and the public at large, have framed the persistent misconduct issues in the financial services business as ethical or moral problems.

Numerous documentaries (Frontline: '*Money, Power and Wall Street*' aired 24 April 2012, BBC World, The Inquiry: '*Can You Make Bankers Behave Better?*' aired 5 July 2016) and Hollywood films ('*The Big Short*', 2015) have richly portrayed the excesses of the financial services business. Articles from leading periodicals and newspapers support the framing of these misbehaviours as an ethical or moral issue. *The Atlantic* magazine's cover story in its May 2015 issue featured the article 'Can Bankers Behave?'[13] The author cites his own personal experience as an investment banker, interviews other banking professionals, and quotes prominent academics and banking regulators. His concern is 'could Wall Street's deepest flaws be cultural, promulgated over generations by leaders who have chosen to reward those who cut corners, stab colleagues in the back and engage in otherwise unethical behavior?'[14]

Similarly, an article by John Plender in the Financial Times invokes John Kenneth Galbraith's concept of a 'stock of moral capital' present in the financial system at any given time, which rises and falls with market prosperity.[15] However, the author asserts that in addition we

[12] There appears be a broad-based call for improved ethics in all walks of life, including business. Noted columnist and author David Brooks' book *The Road to Character* has been on the *New York Times* Bestseller list since its publication in April 2015. And in the *Harvard Business Review's* April 2015 edition, its 'Idea Watch' section featured the article 'Measuring the Return on Character', summarising the results of a study that demonstrated that CEOs who rated highly on four moral principles delivered better financial results than those that didn't.

[13] William D Cohan, 'Can Bankers Behave?' *The Atlantic* (May 2015).

[14] *Ibid*.

[15] John Plender, 'The crisis shows moral capital is in secular decline' *Financial Times* (9 June 2014).

are witnessing a structural, secular change in this stock of moral capital brought about by an adverse change in ethical values.

There are recent academic studies of human behaviour that strongly support the premise that one's moral fibre is eroded with even minimal exposure to the context of money, financial markets and even banking. According to a study published in the journal Nature, people reminded that they worked for a bank ('identity-primed') were more likely to cheat on a coin toss.[16] This study is consistent with previous landmark studies about 'money priming', which demonstrated that people even only subtly reminded of money were less helpful, preferred solitary activities and more physical space between themselves and a new acquaintance (although apparently were ready to work harder and longer!).[17]

The inescapable conclusion for many is that the financial services industry is riddled with 'bad' people, attracted and empowered by an industry-wide culture that allows and encourages them to exploit the weaknesses and loopholes for their own benefit. Philip Zimbardo captured this dynamic in his description of bad apples, bad barrels (contexts/cultures) and bad barrel makers (managements/boards/regulators), with his classic and unsettling 'Stanford Prisoner Experiment' revealing that 'good' people placed in 'bad' cultures end up doing bad things.[18] It is not a stretch for many to conclude that the nature of the financial industry itself creates its own ethical and moral erosion even affecting 'good' people and efforts to impose rules to codify 'good' ethics, morals, conduct and behaviour are doomed to

[16] Alain Cohn et al, 'Business, culture and dishonesty in the banking industry' (2014) 516 Nature.

[17] Kathleen D Vohs et al, 'The Psychological Consequences of Money' Science (2016) 314 and Kathleen D Vohs, 'Money Priming Can Change People's Thoughts, Feelings, Motivations and Behaviors: An Update on 10 Years of Experiments' (2015) *Journal of Experimental Psychology*.

[18] Philip Zimbardo, *The Lucifer Effect: Understanding How Good People Turn Evil* (2008) Rider.

fail. Yet the financial industry has been under intense pressure to try.

Limited success of solutions trying to address unethical behaviour

Certainly, regulators, boards and management have a much more nuanced view than the general public of the conditions and causes that have led to persistent misconduct and misbehaviour in the financial sector. There is an awareness of the 'bad apples' that need to be removed before they do more damage to their organisations. There is an awareness of the 'bad barrels' that need to be rehabilitated before they inflict more damage on their stakeholders and the system in general. There is an awareness among the 'barrel-makers' of the need to create policy and governance frameworks that also serve the long-term interests of the societies in which they operate who rely on a stable, fair and resilient financial system.

No one seriously advances the belief that morality, although clearly a problem, can be regulated, and even if it could, that it would be a panacea.[19] Nevertheless, regulators continue to try to legislate and regulate what they have defined as morally-driven behaviours. The recognised risk in layering on regulations is that it reinforces the transactional tendency to operate within the letter of the law, rather than exercising the necessary judgement required to both understand the spirit of the law and take actions consistent with it.

> *'Virtue cannot be regulated. Even the strongest supervision cannot guarantee good conduct.'*
>
> Mark Carney, Governor of the Bank of England in a speech in London, Ontario, 2013[20]

[19] 'To regulate for "honest behaviour" and "better culture"… would appear to be fatuous': quoted from Roger McCormick, 'The "Conduct Crisis": Will Banks Ever get in Right?' [May 2015] Business Law International p112.
[20] William D. Cohen, 'Can Bankers Behave?' The Atlantic (May 2015).

The solutions proposed and imposed to date with varying degrees of effectiveness seem to have at their core an intention to install and strengthen ethical and moral sensibilities for the purpose of positive behaviour modification. Examples include programmes that have introduced codes of conduct, ethics and value statements that explicitly include moral considerations as a baseline standard for behaviour. Compensation systems have been substantially adjusted through payout reductions, deferrals and clawbacks in an effort to reduce the incentives that induce or encourage immoral behaviour. Complex and comprehensive compliance programmes have been designed and rolled out that monitor and report key metrics in dashboard formats throughout all levels of an organisation, up to and including the board.

These actions have been taken by legislators, regulators and in some cases, by corporate initiatives in the expectation that sensitising people to a moral code of conduct, redesigning incentive systems to support this moral code and implementing compliance systems that check key performance indicators will lead to more responsible decision-making and fewer instances of misconduct.

However, these approaches have encountered various forms of resistance. Many in the financial services industry object to the notion that they are ethically or morally inferior or flawed, and

[21] It is clear that people within the financial industry do not perceive themselves as morally 'bad'. Tom Hayes, convicted in the UK and originally sentenced to 14 years in prison for his role in the LIBOR scandal, was the subject of an in-depth article in *The Wall Street Journal*. In the article the author writes: 'He was "getting angrier and angrier." His father, Nick Hayes, later told me "The more he gave the interviews to the SFO, the more convinced he was of his innocence." And the more he became obsessed with the notion that his planned guilty plea would haunt him for the rest of his life.' David Enrich, 'The Unraveling of Tom Hayes' *The Wall Street Journal* (13 September 2015).

[22] Tom Osborn, 'Leeson: risk managers should be personally liable for trades' Risk.net (14 March 2016).

programmes that seek to lecture on ethics and morals are often seen as condescending and met with 'flavour-of-the-month' derision.[21] Changes in compensation systems have certainly created better alignment between bonusable employees and their institutions. Yet egregious instances of bad behaviour to preserve bonuses persist, even in situations such as Wells Fargo where the protected bonuses were very modest. Many compliance systems have devolved into 'tick-the-box' exercises where efficiency is more prized than judgement, undermining the effectiveness of the process, and perhaps even engendering a false sense of security. Given the ongoing instances of misconduct it is clearer than ever that simply changing the rules and implementing new processes will not, by themselves, sustainably change culture, and the frame of reference within which people make decisions.

The concern that these approaches have not been as effective as had been hoped is evident in the new programmes that continue to be implemented. In the UK the 'Senior Manager's Regime' (SMR) came into force in March 2016. An article by Tom Osborne on Risk.net described the SMR programme well: 'This regime makes a "reckless" decision that causes a bank to fail a criminal offence carrying a maximum of seven years in prison and an unlimited fine. The rules apply to individuals and banks that fulfil 17 designated senior management functions, ranging from the chief executive and heads of risk and finance to the chairs of the risk, audit and remuneration committees.'[22] In a recent speech Mark Carney, the Governor of the Bank of England, noted: '…codes [of conduct] are of little use if nobody reads, follows, or enforces them'. He praised the SMR as it 'addresses the common refrain of senior management that they weren't aware that misconduct was taking place in their firms. The SMR re-establishes the link between seniority and accountability. Senior Managers now must take reasonable

steps (including training or proper oversight) to prevent or stop regulatory breaches in their areas of responsibility.'[23]

However, even the SMR must rely on fines and incarceration for enforcement. But as the evidence of ongoing misconduct demonstrates, the fear of discovery and punishment has proven to be an insufficient remedy on its own. In the same speech Carney stated: 'So while fines and sanctions have roles in deterring misconduct, they will not, on their own, bring about the cultural change we need... we must move from an excessive reliance on punitive, ex post fines of firms to greater emphasis on more compelling ex ante incentives for individuals, and ultimately a more solid grounding in improved firm culture.' [24]

What is clearly needed now is an approach that impacts and enlightens the individual's conduct at the time conversations are taking place and the choices are being made to activate and exercise the quality of judgement that anticipates the consequences. Such an enhanced level of judgement will be fully aware of the contextual and cultural influences acting on the decision at hand. The individual's judgement is robust enough to not only resist the poor, short-sighted decision, but indeed to exert leadership that will generate appropriate conduct alternatives that positively shape the culture within which future decisions will be made by themselves and others.

[23] 'What a Difference a Decade Makes', p.7, speech by Mark Carney, Governor of the Bank of England, Chair of the Financial Stability Board in Remarks at the Institute of International Finance's Washington Policy Summit, the Reagan Centre, Washington, DC, 20 April 2017.
[24] Ibid, p6.

Poor conduct reframed as a judgement issue

This article proposes that we are much more likely to prevent acts of misconduct or, if they do happen, to mitigate or ameliorate their negative impact, if we begin to reframe, understand and describe them as poor judgements rather than bad ethical or moral actions. Framing the conduct issue as an ethical or moral problem is ultimately incomplete and inadequate, and may indeed create obstacles to identifying the causes of misconduct and effective approaches to resolution. It would be far better to interpret misconduct and misbehaviour in the business sphere as being a failure of judgement. There are two reasons to support this approach. First, focusing on the quality of judgement not only deals with issues of poor judgement but importantly extends to excellent judgement leading to sustained excellent performance.25 Second, while few people self-assess as having deficiencies of ethics or morality, strengthening judgement is something most people aspire to. Viewing misconduct as a judgement issue instead of a moral issue engages audiences who want to improve decision-making but without the judging that is typically associated with moral agendas. Discussions can be had more dispassionately and rationally, and the audience does not feel themselves under attack. Further, a discerning audience will quickly sense an opportunity to improve their own decision-making and performance, making engagement very much in their own self-interest. By explicitly framing the discussion in the self-interest of the listener we can substantially reduce barriers to engagement.

[25] 'In the case of the effects of character, Cameron, Bright and Caza (2004) found that firms whose members possessed more character dimensions outperformed those whose members possessed fewer character dimensions, and in Wang and Hackett's (2016) work, character-based leadership predicted the well-being of both leaders and their followers, along with the performance and citizenship behaviours of employees even after other leadership styles were controlled for.

'Banks should look at culture, and achieving consistent behavior and conduct aligned with firm values, as key to strategic success, rather than as a separate work stream or add-on process to respond to short-term public, regulatory or enforcement priorities'

Banking Conduct and Culture, Group of Thirty, p12, July 2015

This latter point is not to be underestimated. Perhaps one of the most significant challenges to changing organisational culture is that of sustainability. Regulators, boards and management are in agreement that meaningful and sustainable cultural change within large financial institutions has been extremely difficult, and that 'accountability must be seen as a new way of doing business, not as a compliance fad'.[26] To emphasise, improving judgement achieves sustainability in two separate, but self-reinforcing ways. First, measures that enhance individual and organisational performance create their own 'indispensability'. Second, the aggregate effect of improved judgements by individuals, in particular those with formal leadership roles, positively influences the culture of the organisation, solidifying the improvements and making it more difficult and less likely that the culture will regress.

[26] 'Summary Notes: Reforming Culture and Behavior in the Financial Services Industry', p 8, published by the Federal Reserve Bank of New York, 5 November 2015.

Improving judgement using the Ivey Leader Character Framework[27]

The The Ivey Leader Character Framework is intended to create superior performance for both individuals and organisations through sustainably improving judgement and decision-making at all levels throughout an organisation, in particular by focusing on those in leadership roles. Once embedded in an organisation it becomes a strategic asset, driving superior performance, while also raising the standards and expectations for behaviour and conduct, enhancing and developing a robust culture that substantially reduces the risk of catastrophic misconduct. A character-infused culture also provides a degree of protection from the truly incorrigible 'bad apples' that inevitably crop up in any large organisation by making their deviant behaviour easier to identify and more clearly unacceptable, which limits their potential for leadership and organisational influence.

In the past, reframing a discussion on character as a judgement issue has been very challenging because character has always been considered a subjective concept, eluding objective definition, not readily and reliably assessed or measured, and has often been regarded as an unchangeable trait, like the colour of one's eyes, rather than as something that can be developed. However, where there is an accessible, convincing, measureable and reliable definition of, and framework for, character (in the judgement sense), which can be developed, this can be an extremely useful business tool in any organisational/industrial context.

With the development of the Ivey Leader Character model, [28]

[27] This framework has been developed over a period of several years by researchers at the Ivey Business School, Western University, London, Ontario, Canada.

[28] Mary Crossan (Ivey), Daina Mazutis (IMD), Jeffrey Gandz (Ivey) and Gerard Seijts (Ivey), Developing Leadership Character in Business Programs. (2013). This article was awarded the prestigious Academy of Management Learning and Education's Article of the Year.

such a framework is now available. Our fundamental premise is Figure 1: Leader Character Framework that organisations need to elevate character (in the judgement sense) alongside competence for sustained excellence.[29] Doing so requires a rigorous and practical approach to identifying, measuring, developing and applying character in organisations. Research establishes that character is revealed through a set of observable behaviours that support sustained excellence in organisations.[30] Figure 1 depicts the dimensions and elements of Leader Character.

Dimensions are formed of 11 high-level constructs, and elements are the behaviours that represent these dimensions. For example, Integrity is a dimension of Leader Character that comprises more than being principled, including elements such as candour and authenticity, which sometimes make the practice of Integrity difficult, especially when practised in cultures that do not value them. Many organisations identify Integrity as an important value but fail to recognise that simply stating that it is important does not deliver it.

Judgement at the centre of the framework reveals that decisions and actions are predicated on the presence or absence of each of these character dimensions. For example, Judgement that is underweighted on dimensions such as Humility or Temperance runs the risk that decisions will be ego-driven and short-sighted, while those that are overweighted on a dimension such as Drive are likely to be rash and lacking in identification of possible outcomes. Table 1 describes key implications when each dimension of character is present or absent in organisations.

[29] Jeffrey Gandz, Mary Crossan, Gerald Seijts and Carol Stephenson (with research assistance from Daina Mazutis), *Leadership on Trial: A Manifesto for Leadership Development* (2010). See also Appendix 1.

[30] Mary Crossan (Ivey), Alyson Byrne (MUN), Gerald Seijts (Ivey), Mark Reno (Ivey), Lucas Monzani (Ivey/Plymouth) and Jeffrey Gandz (Ivey), 'Toward a Framework of Leader Character in Organizations', (2017) *Journal of Management Studies*.

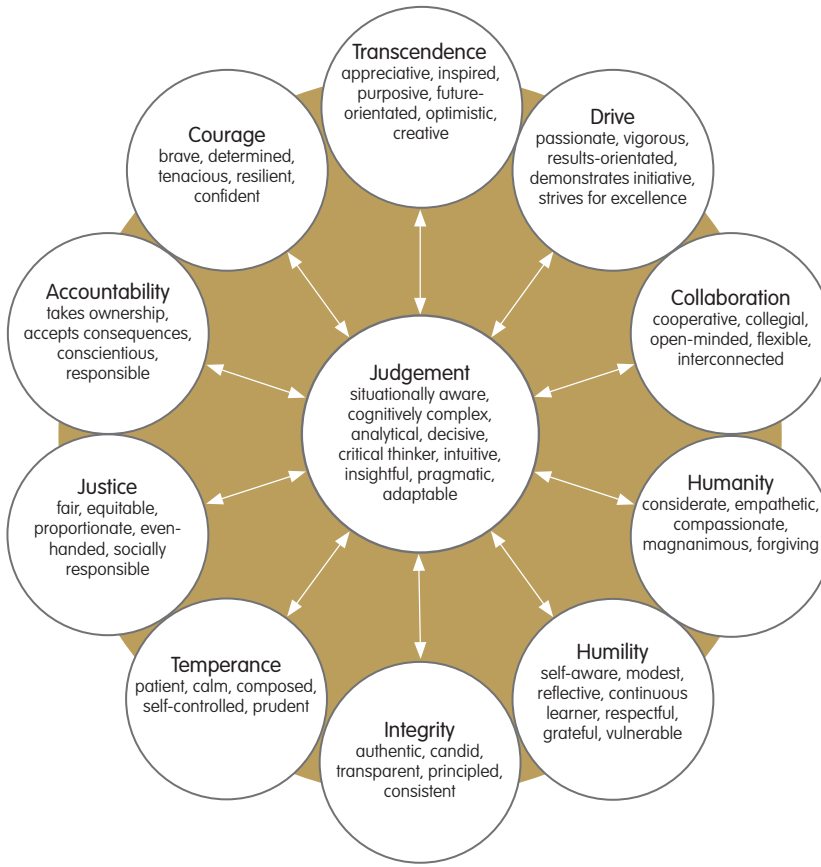


Figure 1: Leader Character Framework

All dimensions can become vices in excess or deficiency. Excess arises in cases where any one or more of the dimensions are overdeveloped or dominant and others are underdeveloped or absent. For example, a high degree of Integrity with low Humility and Humanity results in the type of leader who is certainly

authentic, but ego-driven and self-absorbed and makes decisions that are self-serving instead of those that take into account broader interests.

Humanity that is unaccompanied by Courage or Drive leaves leaders with a great deal of empathy but limited in their capacity to exercise it, resulting in deferred decision-making. A high level of Drive without corresponding capacity for Temperance risks reckless decisions. This lack of balance and integration between character dimensions is analogous to having a sports car with a highly-tuned, powerful engine but a poor braking or suspension system.

Table 1: Impact of character dimensions on organisations

	Present	Absent
Courage	Decisions are made in spite of uncertainty There is opposition to bad decisions Innovation thrives	There is agreement with poor decisions Satisficing rather than maximising is the norm Moral muteness prevails
Drive	There is sustained momentum around focused priorities and high productivity	There is widespread lethargy and low productivity
Collaboration	Effective teamwork enhances productivity There is diversity in teams that contributes to innovation, understanding and appreciation for others' ideas	An 'every man for himself' mentality breeds a hostile competitive climate that alienates potential allies Lack of information-sharing leads to poor understanding of decisions, resulting in friction and conflict
Integrity	There is trust, transparency and effective communication	People operate from a position of self-interest and mistrust, which impairs their ability to make good business decisions

	Present	Absent
Temperance	There is effective risk management governed by reasoned decision-making There is thoughtful consideration (versus impulsive over-reaction) to events that impact the business	Short-term gains dictate strategy Desire for instant gratification trumps a more measured 'what is best over the long term' approach
Accountability	There is ownership of issues and commitment to decisions and their execution	There is failure to deliver results and take responsibility for poor decisions and outcomes
Justice	There is perception of fairness that fosters trust People go above and beyond what is required	Inequities exist that erode trust Widespread favouritism and nepotism exist
Humility	There is a willingness to identify and discuss mistakes The organisation supports continuous learning	Interactions are ruled by arrogance and overconfidence Problems and projects are approached with complacency
Humanity	There is a deep understanding of what is important to stakeholders that fosters unique insights and competitive advantage	There is a failure to acknowledge critical social implications of decisions and actions
Transcendence	There is commitment to excellence There is clarity on superordinate goals and a focus on big picture thinking Inspiration motivates innovation	Strategy is dictated by narrow goals and objectives There is failure to acknowledge, appreciate or strive for excellence People are not inspired to create and contribute
Judgement	There is recognition of key issues relevant to situations Decisions are predicated on excellent understanding, analysis and insight	Lack of comprehensive and balanced assessment of issues leads to poor decisions, confusion and resistance to change

Unfortunately, many financial institutions (and other organisations as well) have inappropriately emphasised and encouraged some dimensions relative to others, creating a culture that overweights and rewards dimensions such as Drive and

Courage and underweights dimensions such as Temperance and Humility. This creates a context for decision-making in which Judgement is impaired.

A fully-developed character, in which all dimensions are present and none dominates, is essential for sustained excellence as it provide the foundation that executives need to make sound judgements in difficult or challenging situations over extended periods of time.

Such character strength enables leaders to resist the pressures that can undermine Judgement, whether they be compensation practices that reward inappropriate behaviours or basic psychological pressures that make it difficult for individuals to take actions that may challenge current approaches. The organisation, industry and societal cultures ('barrels') within which individuals operate both define and challenge Judgement. Speaking at a convention for fraud examiners, Andrew Fastow, the former CFO of Enron, stated: 'Accounting rules and regulations and securities laws and regulation are vague... They're complex... What I did at Enron and what we tended to do as a company [was] to view that complexity, that vagueness... not as a problem, but as an opportunity.' The only question was 'do the rules allow it or do the rules allow an interpretation that will allow it?' Fastow insisted he got approval for every single deal from lawyers, accountants, management and directors yet noted that Enron is still considered 'the largest accounting fraud in history'. He asked rhetorically: 'How can it be that you get approvals... and it's still fraud?'[31]

Consider that rules and regulations are often interpreted as defining 'how the game should be played' and people are often rewarded for creative application of the rules. Fastow claimed he

[31] Peter Elkind, 'The Confessions of Andy Fastow' *Fortune.com* (1 July 2013).
[32] Tracy Alloway, 'Here's a Simple Lesson in Ethics From the Former CFO of Enron' *Bloomberg.com* (2 July 2015).

should actually have been called the 'Chief-Loop-Hole Officer'.[32] The Enron example illustrates the problems that arise from poor decision-making when operating within the letter of the law rather than the spirit of the law. The focus turns to 'creative application of the rules' for personal gain rather than exercising the judgement required to understand the spirit of the law and take actions accordingly.

In addition, rules and regulations typically seek to prevent negative performance outcomes, while values and ethics tend to define expectations. However, they are insufficient to develop the strength of character and resulting judgement that withstands the many forces that undermine sustained excellence. Forces that typically undermine sustained excellence are basic psychological and social forces, such as social comparison, bystander effect, money priming, groupthink and conformity. Compensation and other rewards are often quite transactional and focused solely on results without regard for the quality of the results and the impact that specific results can have on sustainability. Unfortunately, many 'results' have toxic elements or 'ticking time bombs' buried within them that go undetected for long periods of time, as evidenced in many financial scandals. The authors assert that while currently there are few ways to test the quality of the results, deficiencies in character that produce poor judgements are usually implicated. Furthermore, where organisations seek to develop strength of character and its associated culture, it is less likely that those who habitually operate in the lower performance part of the curve will go undetected as they will be more clearly identifiable as outliers (ie, 'bad apples') and be forced to either modify their behaviour or exit the organisation.

Taken together, the implications for the financial services industry are significant. First, character needs to be elevated alongside competence to avert negative substandard behaviour and reap the

benefits of superior performance through enhanced judgement. This is an important pivot away from misconduct viewed as associated with being a good or bad person, but rather as judgement foundational for sustained excellence. Second, many organisations (such as the Enron example cited earlier) have fallen into the trap of overweighting some dimensions and underweighting others, leading to toxic cultures that undermine judgement. The dimensions of character need to work together to support judgement, which acts like an air traffic controller drawing on the dimensions as needed.

Implementing the Leader Character Framework

Character can be defined using the language of the Leader Character Framework. We present the Leader Character Insight Assessment (LCIA), a tool whereby it becomes possible validly and reliably to assess the Leader Character of an individual. The Leader Character Framework also provides the basis to interpret, organise and evaluate the results from more traditional techniques, such as biodata, deep reference checking and interviews.

Organisations are already assessing character (in the judgement sense) using the LCIA offered through Sigma Assessment.[33] It is a reliable and valid survey-based instrument that can be used in self-assessment or 360 format. The results enable individuals and organisations to identify areas of development. Since the Leader Character Framework is behaviourally based, it can be used to select, develop, reward and promote on the basis of character and judgement. Elevating character alongside competence for sustained excellence is in the best interest of organisations and the regulators who provide stewardship.

Character is often (mis) understood as being similar to personality or physical traits, and therefore not subject to meaningful change

[33] See Appendix 2 for sample LCIA report excerpts.

('you either have it or you don't'). However, research suggests otherwise for the following reasons:

- A person's character-driven behaviours change often due to the effects of context or neglect, sometimes because of some intense, crucible experiences, and other times as a result of intervention by others. It can change for the worse; it can also change for the better.
- Character is 'a habit of being'. Change the habit and character change will follow.

There is a substantial body of anecdotal and academic literature that supports the intentional and sustainable development of character. This article discusses three primary approaches to implementing programmes to develop character: feedback and performance management, self-management and stretching, and behavioural modelling and mentoring.[34]

Feedback and performance management

Performance management is an integral part of a comprehensive human resources (HR) system, and feedback is an essential component of this process. The value of the Leader Character Framework and LCIA is that they provide clear language to identify and measure key behaviours that can be used for feedback. In addition, the focus of the feedback is on enhancing individual performance, not providing value judgements, thereby creating a positive, supportive context for the discussion. Specifically,

[34] This section is a summary of elements drawn from the academic paper: Gerard Seijts (Ivey), Mary Crossan (Ivey) and Erica Carleton (Edwards), 'Embedding Leader Character into HR Practices to Achieve Sustained Excellence', (in press, 2017) *Organization Dynamics*.

organisations can incorporate Leader Character and the LCIA into: job or position profiles; leadership assessment; promotion decisions; and conspicuous recognition of character dimensions in communications about key appointments and promotions. A number of organisations, such as Aecon, General Dynamics Land Systems (Canada) and OMERS, have been successfully weaving the LCIA and Leader Character concepts into their HR practices to support performance management and leadership development. FIs, such as TD Bank Group and others, address many of the character dimensions and elements in their leadership profiles and assessments. However, the risk is that some organisations emphasise some dimensions and not others, thereby falling into the serious trap that what they thought were virtues have become vices that undermine performance because they become unbalanced by the character dimensions that have been excluded. Abbreviating the character dimensions to simplify the framework or shorten assessment instruments virtually guarantees this imbalance.

Self-management and stretching

Individuals can take ownership of their character development through self-management and stretch assignments. The Leader Character Framework and LCIA provide a common language to provide each individual with a unique insight into his or her own character, and a reliable guide to leverage strengths and address weaknesses. Each person can intentionally pursue certain assignments or activities in order to develop particular character dimensions, and be more mindful when reflecting upon and interpreting the resultant experiences. This enhanced level of self-awareness is critical to sound judgement and decision-making, in particular in the routinely stressful environments experienced by the leadership of large and complex financial institutions.

Behavioural modelling and mentoring

It is the role of the organisation's HR department to ensure that its employees, in particular its leaders, have access to the necessary educational and human resources to ensure that the lessons learned in these stretch assignments and activities are fully appreciated and absorbed by the individual. Experience suggests that these initiatives will only gain traction if the senior leadership visibly commits to their utilisation and models the appropriate behaviours. The Leader Character Framework, combined with the results of the LCIA, provides individual, targeted character dimensions for focused behaviour modelling. The LCIA also provides a tool for the individual to reassess and measure his or her progress, and suggest new areas for development.

The process of embedding needs considerable and conscientious forethought in order to properly implement Leader Character and avoid organisational disharmony and/or harm. For example, it would be prejudicial to the implementation of the Leader Character Framework if middle management were to judge that the board, chief executive or executive management were disingenuous in their support for it, hypocritical in its implementation or not personally striving to achieve character development in their day-to-day actions.

However, the process of embedding Leader Character in an organisation need not be a high-profile, attention-seeking, dramatic event that disrupts existing HR frameworks, models and practices. Rather the process for successfully embedding Leader Character in an organisation can be much the same as for an individual: a patient, intentional and disciplined process integrated into existing objectives and activitities. Importantly, character should not be treated as a subset of an organisation's existing competency-based HR programmes, but rather as a valuable, seperate and

equal partner that seeks to leverage and empower these existing programmes. In some cases, certain aspects of an organisation's existing leadership framework (eg Integrity) are best transferred to the Leader Character programme, where that specific dimension can be assessed and developed more effectively in tandem with the other dimensions.

Leaders, on their own initiative, perhaps encouraged by regulators, can take advantage of many leverage points to instil character in their organisational cultures. They can use the examples of lack of character in the published experiences of others (Wells Fargo, Volkswagen, Enron, HSBC and others referenced in this article) to answer the question: 'Could this happen here?' They could build the link to character in their internal training and development programmes that deal with risk management (credit, market, operational and reputational, and the 'Three Lines of Defence' risk management framework commonly employed in the industry) as well as wealth management and investor advice.

Implications and application of a character-based approach for regulators

Regulators have long been struggling to pin down the persistent and elusive issues associated with culture, behaviour and, especially, misconduct in the financial industry. In October 2016, the Federal Reserve Bank of New York held its third annual conference on reforming culture and behaviour in the financial services industry. The main message has remained consistent: 'It is ultimately the industry's responsibility to change its culture and behaviours.'[35]

There is not universal agreement that culture and behaviour

[35] Reforming Culture and Behavior in the Financial Services Industry: Expanding the Dialogue, Summary Notes, Federal Reserve Bank of New York, 9 November 2016, p1.
[36] Ibid p9.

are clearly within a regulator's remit. Some industry participants believe that regulators 'should be concerned only with outcomes... that questioning culture is too intrusive, or that regulators lack the expertise to make informed judgements on a bank's culture'.[36]

However, there is arguably a consensus that culture, as evidenced through observable behaviour, is an appropriate factor for risk management and that supervisory assessments might be improved by examining behaviours at financial institutions. A leading example is De Nederlandsche Bank (DNB), the first national banking supervisor to consider culture and behaviour as early stage risk factors subject to supervision. DNB's in-person examinations focused on 'leadership, decision-making and communication and also addressed the group dynamics, behavioural patterns and mindsets of executive and pension fund boards'.[37] DNB uses surveys, interviews and attendance at board meetings to develop its views on an institution's culture and behaviour, and to formulate specific findings.

Whether individuals or groups in organisations engage in misconduct is highly influenced by the culture the system of shared values and beliefs within those organisations. Those cultures are themselves shaped and moulded by the character of organisational leaders who, through their behaviours, decisions and judgements, set examples for others, and influence organisational policies, practices, processes and systems. If regulators actually want compliance, they must address character, before character deficiencies lead to poor decisions, judgements and ultimately risk of loss.

This article proposes that regulators ask a number of questions at the board, senior executive and lower levels in organisations and

[37] Jakob de Haan, Wijnand Nuijts and Mirea Raaijmakers, 'Supervising culture and behavior at financial institutions: The experience of De Nederlandsche Bank' *VOX CEPR's Policy Portal* (5 November 2015).

assess the quality of the responses they get:

- Does the organisation attach importance to the character of its leadership teams? If not, why not?
- If yes, how does the organisation define, assess and develop this character? To what extent have these initiatives or programmes demonstrated improvement with respect to these objectives?
- Do the organisation's code of conduct, mission, vision and value statements, leadership profiles and mandates emphasise the importance of character? In what ways? Is there explicit or implicit overweighting of some dimensions and underweighting of others?
- Does the organisation incorporate character into its decisions related to recruitment, development, compensation, promotion and termination?

Regulators could assess an organisation's responses to each of these on a (four) point scale:

- 0: Organisation does not consider character important to individual or organisational performance.
- 1: Organisation considers character important to individual and organisational performance, incorporates this belief into various organisational materials (e.g. value statements), but otherwise does not incorporate into its human resources policies, procedures and processes.
- 2: Organisation considers character important to individual and organisational performance, incorporates this belief into various organisational materials (e.g. value statements) and incorporates on a largely qualitative basis into its human resources policies, procedures and processes.

- 3: Organisation considers character important to individual and organisational performance, incorporates this belief into various organisational materials (e.g. value statements) and incorporates on a qualitative and quantitative basis into its human resources policies, procedures and processes.

If regulators are going to ask these questions, then legal advisers, whether in-house counsel or external, must ensure that their clients are prepared to address them. In most financial institutions, policies, procedures, performance management systems and training programmes get legal sign-off. If they don't currently address character issues, they should, and legal counsel should be fully engaged in making this happen.

In the authors' view the most important outcome of this approach will be to reframe the discussion away from questionable morality and poor behaviour to a non-threatening, dispassionate and positive dialogue on the nature of decision-making and judgement required for sustained excellence of both the organisation and its leadership.

Conclusions

This article concludes its discussion with three main points:

1. **The continuing misconduct in the financial services industry indicates that the approaches and remedies employed to date have met with limited success.**
It is also clear that the financial services sector is too important to the overall functioning of the global economy for this misconduct to persist. Indeed, key regulatory bodies have signalled that the status quo is simply not acceptable. New approaches, perspectives and initiatives are required.

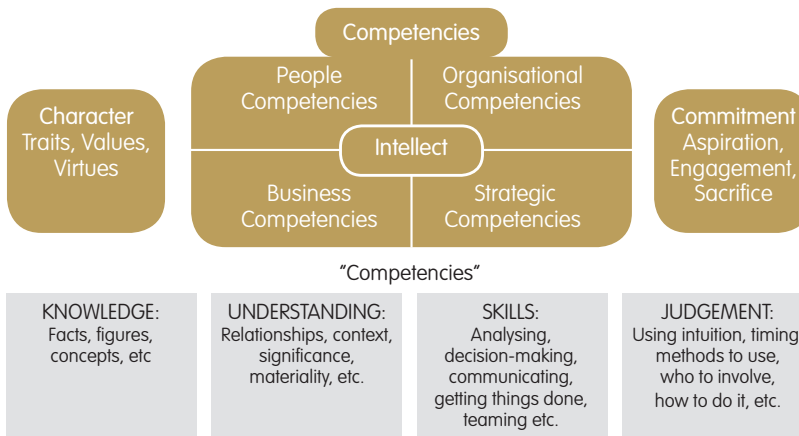
2. **Reframing misconduct in the financial services sector to add character-driven judgement to the moral issue represents a more complete formulation of the problem.**
This reframing has three very significant practical advantages. First, formulating the issue as primarily one of judgement does not meet the same emotional resistance that a 'moral' framing will encounter and allows for a strong alignment of interests among all stakeholders. Second, improved judgement, decision-making and performance that results from a properly implemented Leader Character programme will allow the programme to take its place at the core of corporate strategy, leading to sustained and permanent change. Third, improved character-based judgement will have a positive impact on the context and culture within which decisions are made, fully activating the many measures already put into place, while further improving sustainability and limiting the risk of an incorrigible individual and/or cultural regression.

3. **Embracing and implementing Leader Character represents an opportunity and challenge to the financial services sector.**
Significant sustainable advantages can potentially accrue to the 'first movers' for the leaders in financial institutions who instinctively understand the value that character-based judgement provides in any enterprise that aspires to excellence. Although the challenges of implementing Leader Character may at times appear formidable, the costs and risks of inaction (or simply staying the course) in the current environment are no longer acceptable. The authors strongly encourage leadership across the financial services sector to consider plans, approaches and initiatives directed at embedding leader-character-based judgement as a core element for the long-term prosperity of their organisations. Organisations can start wherever there is a strategic imperative, whether it be recruiting, onboarding, leadership development, compliance,

organisational transformation or the myriad diverse agendas organisations face. All that needs to be done is to consider how character can fundamentally shape the agenda.

Warren Buffet has been quoted as saying: 'Somebody once said that in looking for people to hire, you look for three qualities: integrity intelligence, and energy. And if you don't have the first, the other two will kill you.' This article uses somewhat different language, but the idea is much the same. It doesn't matter how much competency exists, how highly motivated and committed to achieve results the people are, it is character-infused judgement that harnesses competency and commitment to produce sustainable excellence while simultaneously avoiding harmful or even catastrophic outcomes. Developing character and the judgement associated with it provides a practical and meaningful approach to addressing misconduct while also strengthening sustainable organisational performance.

Appendix 1: The three Cs of leadership



Gandz. J, Crossan. M, Seijts. G, and Stephenson, C. (2010). Leadership on trial: A manifesto for leadership development. London, Ontario: Ivey Business School.

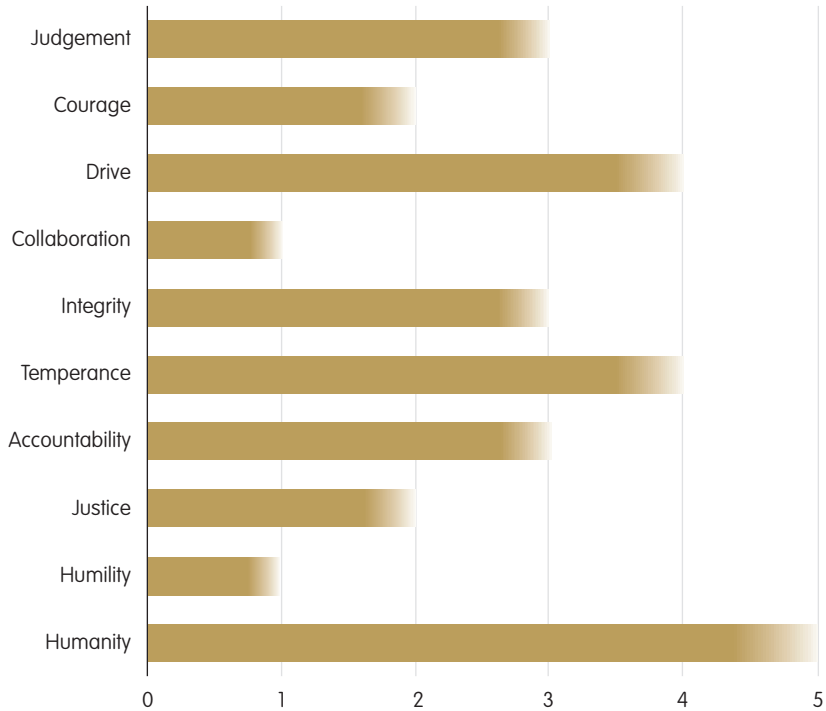
Appendix 2a: Sample LCIA Report Summary

LCIA Results Overview Dimension Scores

In responding to the LCIA items you were asked to identify how likely you would be to engage in various behaviour that reflect the character dimensions and elements described in this report. You responded using the following scale:

1 - Extremely Unlikely, 2 - Unlikely, 3 - Unsure, 4 - Likely, 5 - Extremely Likely.

The graph below shows your score on each character dimension.



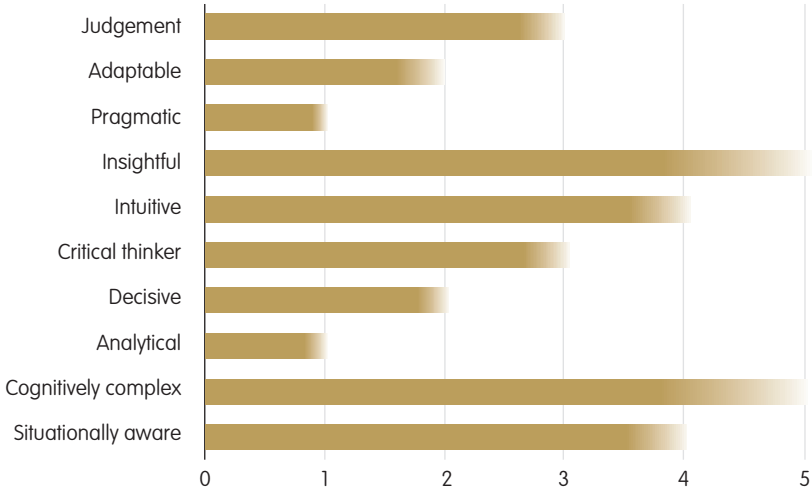
Appendix 2b: Sample LCIA Report Judgement

Makes sound decisions in a timely manner based on relevant information and critical analysis of facts. Appreciates the broader context when reaching decisions. Shows flexibility when confronted with new information or situations. Has an implicit sense of the best way to proceed. Can see into the heart of challenging situations. Can reason effectively in uncertain or ambiguous situations.

Elements

Situationally aware: Demonstrates an appreciation for unique circumstances that may dictate unique approaches.
Cognitively Complex: Analyses, makes clear sense, and draws sound conclusions in uncertain, complex and ambiguous circumstances.
Analytical: Skilfully analyses and employs logical reasoning.
Decisive: Promptly makes astute, level-headed decisions. Shows clear-sighted discernment of what is required.
Critical Thinker: Applies sound analysis and logical reasoning to evaluate ideas, decisions and outcomes.
Intuitive: Understands things without an apparent need for conscious reasoning.
Insightful: Grasps the essence of situations. Sees into the heart of challenging situations.
Pragmatic: Understands, develops and implements workable solutions under varied circumstances.
Adaptable: Modifies plans, decisions and actions to adjust to new conditions.

The chart below displays your ratings for Judgement and its key elements.



"The ability to overcome the stresses and frictions of battle to make the right calls, while remaining within strategic intent and regulatory conduct, are the precise skills and capabilities that businesses need today if they are to survive in a dramatically changing environment."

LEADERSHIP AND DECISION-MAKING

A combat to commercial perspective

By Stuart Tootal

After just over ten years in the corporate sector, I continue to be struck by the number of similarities between the prosecution of military operations and the conduct of business. In both domains planning must be formulated on the basis of acquired data and analysis strategy must proceed tactical application and actual implementation entails risk, and will be uncertain and unpredictable. Best laid plans are unlikely to survive contact with the frictions and realities of execution and, whether on the battlefield or in the marketplace, decision-making agility to respond to unfolding events, at all levels of an organisation, based on sound leadership will be central to determining successful outcomes.

Even before Covid 19 struck and in the wake of the 2008 economic crisis, the pace of global socio-economic and political change has meant that the business environment is becoming increasingly more complex, chaotic, risky, and ambiguous. These are the inherent characteristics of modern warfare, which have been exacerbated by the proliferation of digital weapon technologies, intrusive media coverage, conduct scrutiny, and the emergence of non-traditional battlefield actors, such as insurgent guerrilla forces. In comparison, Black Swan occurrences, dizzying advances in digitisation, artificial intelligence, cyber-attacks and the exponential growth of start-up disrupters and fake news,

combined with increasing regulation and conduct scrutiny, have all fundamentally altered [join to next sentence]traditional business dynamics. As a result, the world of commerce, like combat, has become increasingly more stressful and susceptible to the cognitive biases of emotional human behaviour, which often confound timely and appropriate decision-making and the ability to respond appropriately to unfolding and unforeseen commercial events in highly pressurised situations.

While the context may differ, the military has grappled with the friction of disruption in battle as a core part of its operating concept. First-rate modern armies are well-versed in the phenomenon that no plan withstands first contact with the realities on the ground; or as Mike Tyson put it: 'Everyone has a plan until they get punched in the mouth.' This is because they have spent hundreds of years operating in environments where risk, uncertainty, increasingly complexity, emotional stress and fast changing event are the routine constants. Consequently, a military unit must prevail on the battlefield by exploiting uncertainty, making order out of chaos and reacting and adjusting to events faster than their opponents. Through the evolution of a 'Mission Command' leadership philosophy, armed forces have addressed a seemingly contradictory requirement. This is because it calls for absolute clarity of strategic direction and intent from higher command, while also demanding the empowerment of junior officers to use their initiative to make the right local level tactical decisions to deviate from a plan when the reality of circumstances dictate, in order to achieve an overall mission objective.

It also necessitates an approach that is resilient to the fragility of human behavioural psychology that distorts and impairs sound decision-making under pressure. The ability to overcome the stresses and frictions of battle to make the right calls, while

remaining within strategic intent and regulatory conduct, are the precise skills and capabilities that businesses need today if they are to survive in a dramatically changing environment that is increasingly uncertain and unpredictable. As a consequence, the application of Mission Command offers the potential to provide a powerful schooling for the commercial world.

At its heart, Mission Command is a leadership, decision-making, planning and execution philosophy and methodology. It requires those responsible for tactical delivery of a strategy to operate within the overall direction of their superior commander's intent, in accordance with the unifying purpose of the mission they have been given. Capable of identifying the essentials of a situation, the Mission Command approach sets out the 'why' and 'what' of operational objectives, while devolving the 'how' of decision-making authority to the lowest appropriate level. Consequently, it gives junior commanders the freedom of movement to plan and react as they see fit to unfolding and unpredictable circumstances, while remaining within the boundaries of the overall mission objectives. It is an approach that facilitates independent action and initiative to seize fleeting windows of opportunity in highly fluid and ambiguous situations. Based on a formulaic and well-practised, but highly flexible, structured set of principles, it also provides a mental handrail to guide logical decision-making in stressful conditions, which alleviates many of the biases of human psychological behaviour.

The circumstances of business may be different, but the problem of aligning strategy to execution is not. Modern armed forces have been forced to become fast transients. While they have radically altered their organisation, equipment and critical thinking to adapt to the evolution of a series of revolutions in military affairs, many large companies remain ill-suited to dealing with the fast-moving, increasingly complex and unpredictable commercial environment

they face. Corporate structures, with rigid organisational charts and traditional business concepts, often represent a physical and mental approach that was designed for a slower, more predictable, world.

Today's corporations are full of talented people and the challenge they face is not completely lost on many who lead them. In their survey of 200 of the top global companies, the founders of the 'Balanced Scorecard' stated that nine out of ten strategies fail due to execution.1 Every organisation is capable of formulating strategy, but some are not good at making it happen and the gulf between intentions and actual outcomes, known as the 'execution gap', for over a decade it has been cited as the number one concern of CEOs. Large blue chips buzz with the energy of collective purpose, enshrined in the mantra of mission statements that talk about 'segmentation' and 'capturing market share'. However, many corporations struggle to communicate strategic objectives effectively to all levels of the organisation. If improving customer satisfaction or conduct is central to an organisation's goals, then what this means to employees at all levels of a company needs to be translated in a manner that gets their buy-in and effectively influences their behaviour and performance to achieve it. In reality too many mid-level managers and staff do not understand their firm's strategy, let alone their role in implementing it. Stop and ask any employee of a large corporation about their job and they will be able to tell you about what it entails. However, ask them about how it relates to their company's overall strategic intent and the part they have to play in achieving it, and they may be unable to tell you.

The common corporate response to the execution gap is to invest more resources in control and risk management, in a drive to gain more data and concentrate greater control in the hands of executive leaders. This represents a misplaced faith in the

[1] David Norton and Robert Kaplan – The Strategy Focused Organisation.

detail of a mission rather than its purpose, where the more lines you have on a Gantt chart, or the more 'stakeholder checkpoints' you include in the plan, generates an assumption that they will take an organisation closer to its end state. There has also been a staggering proliferation in the number of committees in many corporations, which tend to create greater bureaucracy, confuses accountability and can paralyse agile decision-making, as it stifles the empowerment of initiative at the lower tactical levels of a company. Business models and tools, such as the Balanced Scorecard, Key Performance Indicators (KPIs), Lean Six Sigma and 'Agile', are often heralded as the answer to providing a way out of this dilemma. However, they are standalone solutions, which lack common currency and do not always enjoy widespread adoption. As one senior corporate leader put it: 'I've been here for over twenty years. There is no focus, these leadership fads come and go, so I ignore them.'

While corporations strive for higher performance and best practice, many suffer a malaise of failing to learn appropriately from failure, which is compounded by inflexible structures and reductionist matrix management practices. Operating in siloes is a common characteristic of big business. Such compartmentalising is a mechanism for dealing with complexity, but it can also militate against the effective capture and passage of information, which inhibits collaborative working across departments. It also generates risk aversion, and a lack of transparency and willingness to learn from mistakes. All of which generate a culture that erodes the initiative of employees at the sharp end to adjust to realities on the ground.

Lack of empowerment, micro control management, rigid adherence to overly detailed plans and an absence of agile decision-making tools, also creates a highly volatile environment that is susceptible to the negative psychological aspects of human

behaviour. All too often businesses remain wedded to false assumptions and stick doggedly to a plan long after reality should have dictated deviation. This is indicative in of a series of recent corporate conduct issues over the last decade serve as examples where cognitive bias, emotional prejudice, pressure and stress-generated behavioural reactions have overpowered appropriate responses and logical decision-making.

As already stated, there are, , significant differences between the military and business environments. No one in the commercial world has the unlimited liability of risking life and limb to achieve their firm's objectives. Additionally, the structural advantage of having a single point of main-gate entry into an organisation, in the form of recruit training depots, senior NCO schools, and officer academies, is not available to corporate entities. However, it would be a misnomer to assume that a modern army gets things done because it has hierarchy; in combat military command structures become flat. A soldier on operations in places like Afghanistan does not risk his life because of rank and rigid adherence to orders. He or she does so because they have faith in their leaders, confidence in their leader's ability to plan a task, trust in their teammates and an innate belief in the organisational culture and ethos of the unit to which they belong. Most importantly, through the application of the Mission Command approach every soldier, regardless of position, has a clear view of his or her role in their commander's concept of operations and an understanding of how what they are being asked to do fits into the bigger strategic picture. In part, this is also achieved by being given a level of involvement in formulating a plan, which is reinforced by a culture where asking questions and calling out challenges is part of the conceptual ethos of mission orientated leadership. In essence permission to challenge in the military is codified in both their doctrine and culture.

While Mission Command is worthy of study for its applicability to business, differentiation in terms of construct and purpose make it impractical to suggest that the military approach represents a simple lift and drop blueprint solution, which can be readily imported and absorbed into the corporate world. However, an increasing number of US and UK companies are beginning to recognise the value of utilising Mission Command skill sets through the employment of ex-military personnel in their organisations. In 2010, we set up the Barclays Armed Forces Transition Employment and Resettlement scheme. Known as 'Barclays AFTER', the purpose of the programme was initially to assist wounded veterans' transition into civilian employment. Although the initial intent was philanthropic, the successful employment of several badly injured soldiers led the company to realise the potential talent flow ex-military individuals can offer to a business. Consequently, the AFTER programme was expanded to encompass all veterans regardless of circumstance, service, and rank. By the end of 2018, Barclays had employed more than 600 ex-military personnel across the firm in recognition of their transferable skill sets in leadership, written and verbal communication, planning, complex problem solving, structured decision-making and an ability to manage risk. Additionally, their behavioural-based attributes of having an ingrained sense of values and exacting standards, a capacity to handle pressure, moral courage, discipline, team-play, and a default for putting collective pursuit of organisational objectives above self, were also highly prized by the company. It was notable that the use of the word 'we', instead of 'I' when being interviewed for a role in the bank is a common practice among ex-military candidates.

Nearly fifty percent of the cohort of ex-military personnel employed through the AFTER programme were from the non-commissioned ranks of the military, which is a reflection of the often-

overlooked talent pool many former Non-Commissioned Officers represent. The fact that former corporals and sergeants comfortably rub shoulders at the same corporate grade as ex-captains and majors is testimony to the collegiate nature and adaptability of the military mindset. As one former junior soldier in the Royal Engineers, who lost both his legs and an arm in Afghanistan, put it: 'I had been used to briefing generals and members of the Royal Family when I was in the Army, so speaking to the Chairman about an issue is not a problem.' In 2015, Barclays began running a military internship scheme as part of the AFTER programme. Candidates of all ranks from the Army, Royal Navy and RAF spend the last three months of paid military service working in different parts of the firm, such as the investment bank, corporate arm and the compliance and conduct functions. Guaranteed only an interview at the end of the process, the internship programme had e a 95% success rate in candidates transitioning to full-time employment: with many going on to promotion to a higher grade in the bank within two years. Barclays was not the only company to recognise the talents veterans can bring to the corporate world. JPMorgan, Jaguar Land Rover, and Amazon, amongst others, also have highly successful ex-military employment schemes. As a ground-breaking company, Amazon has made particular efforts in seizing the initiative in deliberately targeting veterans for their leadership skills and 'can do attitude'.

These statistics are indicative of the added value ex-military can bring to the corporate world. There are, of course, many talented people employed in large corporates who do not have a military background. However, as one financial services hiring line manager put it: 'I can pretty much access all the skills and competencies I need in this company. But I would hire somebody from the armed forces because they bring something different;

they bring a rare perspective that broadens and deepens what I already find here.' This statement emanates from the fact that within months of passing out of their officer or command school training, military individuals in their early twenties are pitched into leadership positions in high-risk situations, which are also complex and uncertain. A young platoon commander or NCO could find him or herself leading others on internal security missions in Iraq, on combat operations in Afghanistan or helping to deal with an Ebola outbreak in Sierra Leone. Within a five-year span of service, they might have held command appointments in all three environments, as well as also completing a staff or training appointment in a higher military headquarters.

Regardless of environment, from the very start of their training, young soldiers are inculcated in an ethos where they will be expected to take independent accountable action and make hard decisions in highly pressurised scenarios. Making a tough call on a difficult day is a central tenet of the decision-making methodology embedded in Mission Command, which cuts across the military at every level of leadership.

It is a corporal to colonel approach, which is underpinned by well-established principles, methodologies and supporting tools. One key process is the 'seven-step Combat Estimate' decision-making and planning tool. Designed to be applied at all levels of military command, it is based on a series of logical sequential questions to analyse a senior commander's intentions and objectives against the essentials of the situational context in and conduct a 'mission analysis' which determines the part the individual junior commander and their team has to play in the senior commander's plan. Consequently, the 'Estimate' process ensures everyone in the organisation has objectively determined task responsibilities, freedoms, and constraints in achieving a mission.

The process also irons out any ambiguity of intent, as it mandates the collegiate engagement of juniors and facilitates a legitimate environment to question seniors to ensure absolute clarity of purpose. The principle that you can disagree with a senior officer and your peers, while remaining loyal to the organisation, team, and mission, is well understood in the military. It is less well-ingrained in the corporate sphere, where poor culture, pressure to conform and concerns about career implications can confound the garnering of the opinions and experience of others to inform the making of better decisions.

When commanding a Parachute Regiment battle group in Afghanistan, I continually advocated to my direct subordinates that intellectual knife-fights were healthy. Debate and challenge strengthened a plan and harnessed the mental horsepower and experience of the collective group. My only stipulation was that challenge had to come from considered thought, logical argument and contain alternative solutions. On one occasion, when issuing quick battle orders to my company commanders, my operations officer disagreed with one phase of my concept of operations; he explained his reasons and suggested an alternative and better course of action. He did so, as tthe junior member of my executive leadership group, when we were under fire and in a highly pressurised situation. The officer in question was a 26-year-old captain and was only two days into his appointment, but his intervention was recognised for the value it added and accepted in a heartbeat; it was also a demonstration of the reason why I had selected him for the role. Today, the decisions I make in the commercial world are also better for open scrutiny and transparent challenge from the team. My role as a leader is to make sure all of the team know that and it is an approach that transitions well into the business sector.

The planning process embodied within the Estimate also frames missions that have a unifying purpose relating to the organisation as a whole. It looks at establishing priorities, identifying the main effort of a plan, and determining the effects that need to be achieved, which are then resourced and sequenced accordingly. The process is reinforced by a specific controls phase that tests the plan in a war game scenario, which asks what has been missed and develops and applies contingency 'what if?' plans and adjustments where necessary. Once the mission and plan is set having completed the Estimate process, the military 'orders' cascade system is used to issue direction in a logically structured fashion using a commonly understood language of command. The 'orders' process ensures that a single unambiguous narrative runs from the top to the bottom of an organisation. It provides the stream of information and direction from which each subsequent subordinate level completes its own Estimate and resulting plan, which extrapolates direction and tasks for their individual teams that aligns to the overall unifying purpose. Embedded in this approach is the use of additional supporting tools, such as 'red team' war-gaming and mission rehearsals to further validate direction given, eliminate confirmation bias and make final refinements and adjustments prior to implementation. Additionally, techniques such as establishing timeline discipline and issuing 'warning orders' can be used to speed up and compress the time needed for decision-making, planning and the issue of direction. This is because they generate anticipatory preparation and concurrent activity, as each level of the organisation waits to receive confirmatory orders.

Although formulaic, the process of Mission Command is also sufficiently embedded in the military mindset to make it highly flexible and applicable to all situations. In combat a battle group might take days or hours to run a cycle of decision-making,

planning and issuing direction to launch a deliberate operation when time permits. However, the same process could be truncated and completed in a matter of minutes when circumstances dictate and when unanticipated events start to unfold during the course of mission conduct. In Afghanistan, the first operation 3 PARA mounted, which we had spent days crafting, nearly collapsed on first contact with the enemy and we found ourselves in an unexpected situation where we were on the back foot and in danger of being outmatched by a large insurgent force. It was compounded by the loss of air support and a breakdown in our radio communications. The weight of resulting psychological stress might have overwhelmed me, but then Mission Command kicked in and provided a default handrail to guide me through uncertainty, complexity, risk, and pressure. Additionally, using their own initiative, my junior commanders were already anticipating what they needed to do to set the tactical conditions for me to apply the 'Estimate' process. Within minutes I was able to reorientate the battle group to new circumstances, decide, plan, communicate and implement a very different concept of operations. The resulting defeat of the enemy force opposing us and our own success came about because Mission Command enabled us to get inside the insurgents' own decision-making loop. Thus, we were able to generate a tempo of decision-making, planning and execution that the Taliban could not match.

As the first UK combat force to be sent to Afghanistan, 3 PARA quickly found itself defending six isolated district centres, which were under relentless attack and in danger of being overrun by the enemy. Each location was separated by hundreds of kilometres and could have consumed the complete battle group and my sole command attention. However, resources were stretched to breaking point and we had to hold individual locations with hastily organised company-

size sub-units of approximately 100 soldiers. My biggest leadership challenge was where to position myself on the battlefield, as I could not be in more than one place at the same time. The solution was to take my remaining battle group reserve forces and to deploy them to where the pressure was greatest, reduce the frequency of enemy attacks and then move on to relieve the next priority district centre in order to prevent it from being overwhelmed and falling to the Taliban. However, when the locations they defended were not the immediate battle group priority, my company commanders were on their own and had to apply the detailed tactical application of our mission within the broad confines of the intent that I had set them. In order to hold their locations, I expected them to be able to take high-risk decisions without reference to me, but I also expected them to do so while remaining within the overall mission objectives. It called for absolute clarity of intent from me as the senior commander and the flexible adoption of Mission Command. It also required for the right application of leadership, accountability, and trust at all levels.

Through it all, leadership was an imperative. It was a function exercised at every command level, from lieutenant colonel to lance corporal. Amongst other things, it required professional competence, example, and moral courage. It also required an ability to know your people, be known by them, have compassion for them and to be able to communicate on a level that made sense to them. Everyone was accountable for their actions, but it was also important to demonstrate that accountability cuts both ways. We made mistakes, but the nature of warfare is a risky business and errors are a common currency of the endeavours of combat, just as they are in business. Ultimately any liability as the senior commander was mine; I was the person who had to write to the families of soldiers who had lost their lives and I was the individual who had to account for their loss in subsequent boards of inquiry

and at the coroner's court. However, it was also critical that we learned from our mistakes, were transparent about the cause and the lessons to be learned. This meant that we avoided becoming risk adverse and continually improved.

We also never spoke about mutual trust, which is a subject often talked about in the corporate world, for in any military unit it is a given. In the armed forces it forms an important part of the ethos and culture, which can be defined as the set of behaviours that a collective body of people default to when they are under pressure. Consequently, who we were and how we were expected to react became a collective point of reference for the entire battle group and facilitated an attitude and ability to adapt, adjust and overcome when the going got tough. Many of the personnel who made up the battle group were not paratroopers and came from the wider part of the Army, Navy and RAF. However, the culture was inclusive, celebrated their diversity and espoused an attitude that everyone brought something to the party and should be valued for it. It was also indicative of the power of culture and ethos that pervades the armed forces as a whole.

Although the context may differ, these are the behaviours and values, that remain deep-rooted in the psyche of ex-military individuals when they transition into civilian employment. They bring the strengths of the Mission Command leadership and the characteristics that underpin it with them. Ex-military are empowered, resilient, accountable, and collaborative by nature. They are also well-versed in having only sufficient necessary detail of strategic intent to allow the departments and functions they lead to develop their own plan and synchronise their activities to meet the overall organisation mission objectives. Veterans are also flexible and time-imperative orientated to remain sufficiently agile to respond to changing situations in compressed timeframes when

a decision needs to be made under pressure. In doing so, they can generate a tempo of activity that reduces risk impact and enables an ability to move faster than a competitor, while reducing the randomness and bias in the decisions they make or inform.

At a time of great national and global challenge, the skillsets and value attributes ex-military personnel offer are precisely what businesses need today if they are not only to survive, but also to thrive beyond complex risk environments.

"The word 'control' could have led us down a rabbit hole, as traditionally the word 'control' had been found attached to operations and back office, where Operations Control was seen by many as the elephants' graveyard of banking operations."

CROSS-INDUSTRY COLLABORATION

Where common sense may not prevail

Back in 2013, my company was asked to undertake two managing director searches, both to report into the Chief Control Officer (CCO). It was the first search we had undertaken for this client and the first for any client with this corporate title. As we do with all searches, before embarking on research and direct market contact, we dissected the technical and behavioural competencies of the position to gain an in-depth understanding of the type of person required and what experiences he/she would have to be effective in this role.

With this in hand you would invariably start most searches by targeting those doing this role elsewhere or possibly those reporting directly into this person, perhaps the number two who would be resident in the department and therefore likely to possess the relevant skills and experience. This would be the starting point of your search and the grounds on which you build your exploration, as you plough this furrow to deliver a shortlist of three to five candidates within four to five weeks for the client.

This did not turn out to be the case in this search, as our client was the only person at that point in the banking sector with this title. The word 'control' could have led us and many potential candidates down a rabbit hole, as traditionally the word 'control' had been found attached to operations and back office, where

Operations Control was seen by many as the elephants' graveyard of banking operations, a process found deep in the back office with little daylight and attractive to few.

Our initial assessment of the role had quickly discounted this group, with our newly found comprehension shaping our research enthusiastically as we sought out talent for this role, embedded in front office. In doing so it partnered the traders and sales people, it was at the forefront of defence of the bank, and, as we later discovered, the industry itself. This was as far from where our initial understanding started as possible and, little did I know, the genesis of my efforts to bring together this evolving community from banks across the sector to address their common challenge and ultimately to seek out areas of mutual interest in which they could cooperate to find mutual benefit and solutions.

How did this happen? Grappling with this search, it was obvious the industry was also struggling with its subject matter. The COO community, those embedded in front office, were unknowingly or knowingly double hatting as the COO and the de facto CCO, executing on the demands of control and conduct in the business from the office of the COO. Control had always been part of the COO's mandate and responsibilities, but the flood of regulation since 2012 had filled the COO's in tray to overflowing and as many control measures and issues were across the business and regional lines, a centralisation of a company's approach to establishing a robust control framework was arguably inevitable. By 2013–14 this centralisation had started at some banks and by 2017 most of the principal banks had an appointed CCO, Head of Non-Financial Risk or at least a Head of Front Office Supervision and Controls.

My journey of understanding started with many replying to my enquiries about the search in 2013. 'CCO, what is this role?', many would ask and I would then do my best, based upon a very limited understanding, to explain it. 'That's my role, I see no purpose to

it as its part and parcel of being a COO' would be the refrain and out of such discussions and comments was born my first article, 'Defining the Indefinable'.

I circulated this paper to my COO community and invited a handful to a dinner at the London club where I enjoy membership, the RAC on Pall Mall, to discuss it. Twenty-five accepted and twenty-seven turned up. In a sector not known for its reliability in turning up at bespoke one-off entertainment, this was remarkable, but what was more remarkable was the strength of debate and the level of engagement on the evening; from it my quarterly forums were born.

Seven years later, this initial event led to these quarterly COO and CCO forums being well established and held in London, New York, Toronto, Hong Kong and Singapore. At the point of writing, this has recently morphed into iCOOC (the International COO Community), with over seventy banks and asset managers represented, where common purpose and interest, a variation of topics, guest speakers and some hard work has bought this community together in a corporate membership committed to serving the interests of the COOs and CCOs worldwide.

It is, however, the output to this endeavour to which we turn our attention. Since 2016, I have concentrated the forum's efforts on identifying and working through cooperate and collaborate ideas and concepts. It is these areas of common and non-proprietary interest on which we will focus.

There are three examples I will use to help demonstrate the common challenges experienced in driving collaborative cross-industry projects. In each case, as a layman and not part of the industry, but an enthusiastic voyeur, common sense appeared to underpin the credibility for each initiative. Admittedly, some of the frustrations I have experienced are due to my naivety and lack of understanding of the complexities of the subjects under consideration and market dynamics. Equally, common sense as a

maxim has become a lost voice in some efforts, being consumed by misplaced understanding, lack of vision, preoccupation with the minutiae – all friends of inertia – or simply, economic and competitive ego. However, at the CCO 1LOD forum's core I found through time a receptive, willing and supportive kernel of intellectuals open to suggestion and testing of the status quo.

There are obviously other aligned reasons for slow progress and failure; where the proposition is not viable, the conceptual broker (me) has failed in my role to mobilise the market participants or timings and other 'here and now' priorities have frustrated the effort. However, even when these are not present, collaborative ventures with hope have fallen and failed to progress, for reasons that still baffle me.

Each example has its genesis at one of my forums, where time will show if common sense and commercial innovation and/or necessity became bedfellows and prevail. Although some, such as the cross-industry lexicon depository have missed their moment, as evolving technologies have already replaced its potential value:

1. Information sharing within Armstrong Wolfe's quarterly COO & CCO forums
2. A cross-industry lexicon depository within surveillance
3. Centralised training within conduct

Before examining each case, what lessons have I learned in my efforts that I believe truly influence the chances of success? What would take us across the winning line when proposing ideas and inventiveness to my CCO community? What must be present to maximise the achievement in the face of betting odds that suggest failure is the likely outcome?

- Common purpose
- Non-competitive/proprietary interests
- Quantifiable benefits (cost, efficiencies, reputational)
- Acceptability to the regulators
- Speaking to the decision maker

With these in place the idea and end user match-maker needs to deliver, foster and maintain the following throughout the process:

- Creativity and innovation
- Drive and ambition
- Excellent administration
- Patience

Lastly, in any such professional venture and in life in general, finding areas of compromise will help the smooth transition from possibility to probability to actuality.

1. Information Sharing Within Armstrong Wolfe's Quarterly COO & CCO forums

The Problem

Information sharing was the basis of why my forums were held initially, and probably remain the primary reason why they are still in place and progressing. Sharing experiences with each other, when facing a common, non-proprietary challenge, can prove as effective as engaging a professional consulting company to tell you what you need to do (and far cheaper!). Each bank is unique in its alignment, regional footprint, business offerings, etc., but at their core they are very similar and share similar challenges, especially in control and conduct and the impact and the role of the regulator.

What started as informal Chatham House Rule discussions moved quickly to meaningful debates, and one subject that the CCO community was struggling with was the organisational design and alignment within 1LOD Control and Conduct. To address this, a masked survey was suggested and agreed upon by sixteen banks. Ironically this is when we brought in the consultancy EY to undertake it, all be it on a pro bono basis, as its professionalism in doing such surveys is well known. The paper it produced was excellent and proved the value of the CCO 1LOD forum in creating value and output to this joint endeavour.

The Vision

With the emergence of the Chief Control Officer (CCO) since 2014, the survey confirmed more than half of the banks surveyed had introduced a CCO position for the dedicated front office control function reporting line. The emergence of this role, distinct from the COO, highlighted the importance attached to risk and control within the business.

By 2018 CCOs had become empowered executives and held responsible for the effectiveness of the control framework within the business, without diminishing the overall accountability of the business leadership for the risk and control environment. At most banks, not just those with a dedicated CCO, the standard and evolving practice had seen an increase in ownership by senior (front office) business management of the overall control agenda, including structure, standards and interactions with the other risk groups.

Whilst no consistent optimum model then (or still now) existed, many global banks Markets' activities had teams of more than eighty, although this is a hard number to qualify, as what direct and indirect headcount sat within and/or were allocated to 1LOD and its tasks were and are very difficult to confirm. This may be because

of a bank's size and its complexity, where drivers of headcount may include variance in specific activities within the function, such as the extent of testing being performed.

Front office control functions had been established as the three lines of defence evolved to have the first line take greater responsibility for non-financial risks.

With this context, we had and still have regulatory and business drivers combining to push direct risk management and control accountability to the front office businesses as 1LOD activities. Specifically:

- Expansion of the 2LOD oversight remit has become a related trend, being a resident point of debate at all forums
- The industry response exhibited a clear trend toward establishing front office control functions as discrete units within Markets businesses, consolidating responsibilities previously dispersed across COO functions and various business roles. These emerging centralised groups provided critical support to senior business management and line of business supervisors, all of whom were and are faced with increased responsibilities.

Exact reporting lines vary, but most front office control teams report into the business executive (e.g. Head of Markets) – either directly or via the COO – to demonstrate authority and stature of the function with desk heads.

The Solution

Whilst no solution per se was sought and/or delivered within the sharing of information, it did frame the community's willingness to work together, aimed at securing some common benefit. The

initial masked survey did bring to the fore recommendations for the industry and for banks to choose which they may seek to adopt.

Then it was argued, despite the progress made by creation of front office control functions, banks would do best to accelerate and optimise their approach in a number of ways:

- By refining the operating 3LOD structure, specifically 1LOD, where banks would clarify the 1LOD accountability model for front office supervisors, staff and control function groups, and would leverage a target operating model that has been rationalised and agreed with second-line functions
- Define key controls within 1LOD. By identifying key controls across disparate lines of business, banks could prioritise testing or other assurance methods applicable to their most important controls
- Invest in tools and embracing technological innovation. Banks would need to continue to develop existing dashboards and MI, control libraries, surveillance, analytics, and workflows with the goal of better evidencing 1LOD control of non-financial risks. As such, key goals were seen to be:
  - Improving data quality and aggregation capabilities to support further automation of monitoring and reporting
  - Increasing use of advanced technology, data analytics, and process automation to improve effectiveness
- Enhance governance. Oversight of non-financial risk, it was argued by many, should include escalation and reporting to senior business management, key committees and independent risk functions, as well as issues tracking related to control remediation.

2. A Cross-Industry Lexicon Depository Within Surveillance

> *'The FCA continues to put a great score on the importance of all market abuse systems and controls, but especially pertinent (for the audience here today) are those related to STRs, particularly fixed income and other non-equity asset classes captured by legislation. Firms should continue to ensure that they have adequate systems and controls to detect suspicious transactions, either through proprietary or client trading in all asset classes and behaviours captured by the market abuse regime.'*
>
> Patrick Spens, Head of Market Monitoring, FCA, 2014

I knew and had heard of the evolution of technologies, designed to address the issue aligned to poor conduct, market manipulation and abuse. It was not, however, until the direct introduction to one of the companies operating in this space, via one of the global CCOs using them, that my appreciation went from acknowledgement to a conceptual understanding of the wonders of technology being developed in an almost Orwellian approach.

'You should meet these guys, RedOwl, as their ex-military pedigree may also interest you,' my contact told me and promised an email introduction to its CEO (Guy Filippelli and COO (Brian White).

I hastily Googled 'Who are RedOwl?' and after initial readings, my attention was caught by an announcement on Blackstone's (one of the world's leading investment firms) website, as follows:

RedOwl Secures $17 Million to Deliver Behavioral Analytics and Insider Risk Management to the Enterprise (Allegis Capital Managing Director Robert Ackerman Appointed to Company's Board of Directors)

San Francisco, CA, July 13, 2015 – RedOwl, a leader in insider risk management and security analytics, today announced it has raised $17 million in Series B funding led by Allegis Capital. The company will use the new funds to continue its expansion, further build out the product development and data science teams, and begin broadening its go-to-market efforts. Reveal, RedOwl's flagship software program for insider risk management, is deployed across multiple verticals and used within many Fortune 500 companies including Blackstone and K2 Intelligence.

This announcement follows a year of exceptional growth for RedOwl, during which the company nearly doubled its team by adding new data scientists and security engineers, and expanded internationally into London. The Series B round includes participation from Blackstone as an investor, as well as previous angel investors including Salesforce Chairman and CEO Marc Benioff, bringing the total funding amount raised to nearly $30 million.

RedOwl also announced today that Robert Ackerman, founder and managing director of Allegis Capital, has joined the company's Board of Directors, further validating that RedOwl's human-centric approach is necessary in addressing today's advanced cyber threats. Existing Board members include Jay Leek, chief information security officer (CISO) of The Blackstone Group, and Elad Yoran, CEO and founder of Security Growth Partners, and a former advisor to the U.S. Department of Homeland Security and the FBI's Information Technology Advisory Council.

"'In 2014, as part of Blackstone's overall security strategy, we set out to tackle the growing concern around insider threats. We reviewed over 15 different insider threat vendors and ultimately landed on

RedOwl for many reasons; most importantly, the company was able to monitor disparate and multiple sets of unstructured data that were being overlooked by other insider threat solutions," said Jay Leek, the Chief Information Security Officer (CISO) of Blackstone. "After bringing them on board to help secure Blackstone we realized that they provided many insights and had a unique value proposition which quickly led us to become a customer, followed shortly by us pursuing an investment in their organization. RedOwl has the potential to truly change the way we think about insider threats and security, focused on moving beyond the perimeter to securing the human-side of an organization."'

RedOwl was acquired by Forcepoint in 2017.This was all pretty clear and added much weight to the business and its credibility, but it was the background of Guy that further intrigued me:

A U.S. Army veteran who spent years working in military intelligence in Iraq and Afghanistan, RedOwl founder and CEO Guy Filippelli recognised parallels between the needs of large enterprises and his work developing first-of-its-kind data analytics software to provide commanders on the battlefield with vital information to make the most informed tactical decisions about the military's biggest asset – people. Upon leaving the Army, Filippelli decided to extend that vision to building software that would give enterprise security the power of "situational awareness". Rather than relying on one channel or data source, large companies in highly sensitive industries like financial services, healthcare and government use RedOwl's software to understand what is happening at the human layer of the business and better manage risk via a multi-dimensional view across disparate data sources.

Through its unique human-centric approach to security, RedOwl allows companies to protect the increasing volumes of sensitive data now being generated and used by employees across the organization

by identifying and analysing changes, patterns and anomalies in user behaviour. Companies use RedOwl to draw from multiple data sources in order to visualize what is happening at the human layer of the business, identify suspicious or risky behaviour in real-time, and proactively identify where unforeseen risks reside within an organization.

"Organizations are responsible for the safety of the data they generate and collect, but each employee with access represents another layer of risk to the organisation, be it through behaviour that is careless, malicious or sloppy," said Filippelli. "Our proprietary behavioural analytics software provides visibility into the human layer of the business, giving enterprise security teams the ability to identify patterns across disparate data streams and create actionable, situational intelligence that drives informed business decisions in real-time."

An initial telephone conversation with Brian White, Guy's COO at the time, led to a lunch in New York with Guy and from the outset from his call and this meeting, I knew I had found a potential willing partner in my efforts to drive collaboration within the control and conduct community.

We had a common purpose, and clearly in RedOwl there was creativity, innovation, drive (aplenty!) and ambition. All these ingredients I had identified as critical to any partner willing to invest in a joint effort to drive collaboration. They needed to be able to marry commercial opportunism with patience, and at second meeting I outlined my thoughts on building an industry portal within lexicons, an opportunity RedOwl grasped and leapt upon.

Market Outline

Q. What is surveillance and monitoring?
The role of the 1LOD control function in surveillance is active and increasing, given regulatory requirements and a shift of these activities from the 2LOD. More than half of banks say surveillance and monitoring are requiring the highest level of effort from their teams. Almost half also cite it as a near-term priority for investment.

Q. What about testing?
At the time, there remained considerable debate as to the future of control assurance activities rising to the level of testing in the 1LOD, and how that related to independent testing currently being performed by, or to be performed by, 2 and 3LODs.

For most banks with first-line testing, testing in 1LOD tended to be focused on enterprise-led regulatory mandates, such as the Volcker Rule and the Comprehensive Capital Analysis and Review (CCAR) attestation process.

However, a few banks had adopted testing as a core 1LOD control function role, establishing extensive first-line testing programmes. Regardless of approach on 1LOD testing, banks agreed that the ongoing migration of control responsibility from 2LOD functions to the 1LOD would result in an increase in second-line testing.

Plans had not yet developed to align testing efforts across the first and second lines, to establish standards for reliance by 2LOD on first-line tests, nor to handle the increased resource implications in the 1LOD from increased 2LOD testing.

Q. What is a banking lexicon?
In simple terms, a bank's compliance department will have a list of words and phrases that it monitors via employees' communications,

such as email and social media, to identify potential fraudulent behaviour.

The Problem

Despite sharing in the same challenges, there did not exist (and still doesn't) an efficient mechanism to share information/experience amongst peers:

- Industry aggressively working to increase effectiveness to better protect their institutions
- Significant expenditure of time and money on low-value add activity that is common across institutions
- Evolution of capabilities is too slow and sporadic to meet the need.

The Vision

- Enable the CCO community to formalise efficient and effective information sharing and collaboration
- Smartly leverage technology
- Build momentum early with high-value initiatives that have little risk/objection
- Over time, identify additional opportunities for collaboration and creation of services in support
- Learn from other successful collaborations in financial services, such as the Financial Information and Analysis Center (FSISAC).

The Solution

The RedOwl Lexicon Sharing Initiative (ROLSI) provides a free,

secure web-based service that enables the controls community to collaborate on lexicon development and efficacy:

- Accelerate lexicon improvement and reduce cost of lexicon development and maintenance
- Membership limited to the control's community
- Governed by a Customer Advisory Board, responsible for governance and vision of collaboration
- Surveillance tool agnostic, import lexicons into any surveillance tool.

The key challenges to advancing this initiative had been the perceived and understandable confidently of such information. However, once the working group's members grasped that there was nothing proprietary in this effort, and indeed sharing lexicons would lead to individual and collective enhanced control awareness, the project moved from concept to possibility.

The next challenge was to secure implicit support of the regulators, ensuring they as a body were aware of and supported this cross-industry effort and would therefore not be viewed as a potential negative or dubious market collaboration. With this in hand the project moved from possibility to probability and then it was a matter of on-boarding the brave few banks that embraced and supported this innovation, moving slowly through a legalistic minefield to arrive at actuality.

Importantly, this initiative was less about the lexicon depository, as important as it, but that as a successful precedent to open the door to further opportunities for collaboration and cooperation within surveillance. How and where technology would aid this collaborative partnership were yet to be determined, but RedOwl had set its stall at the centre, seeking to help the industry identify

ways individually and, perhaps more importantly, collectively to uncover market abuse and criminality that injures all market participants.

The issue that prevented progress was, ironically, the impenetrable wall of compliance. Concerns were raised over such collaboration and despite assurances by the CCOs themselves, some compliance departments saw their lexicons as proprietary and that a centralised depositary would dilute and not enhance effective detection. At this stage of the evolution of the 3 lines of defence, such doubts voiced by compliance were equal to being no-doubts and as they could not be persuaded the initiative died a death far quicker than it had taken to become a defined opportunity.

3. Centralised Training Within Conduct

At one of my early forums, conduct training was discussed and immediately it appeared to me, in a flash of common sense, that the industry would be better served if it centralised this training.

Initial soundings landed on fertile ground, but despite regular watering, the seeds of this idea struggled to find light, but with perseverance, patience and compromise, momentum was finally secured.

My view on my role in this initiative was as the spark, the genesis of the idea and aimed to be the glue and oil in the working group, to take it to the point of actuality, to then step aside and hand the reins to someone more qualified to run what could be a meaningful and global business.

The concept almost found universal support, but I had learnt that where such uniformity exists and is indeed a bedfellow of common sense, this does not necessarily translate into collective action.

The interested party's criteria for inclusion differ hugely, just as does the desire to fully or partly engage in the Conduct Academy

as it set off on its journey. Patience and compromise were needed to carve out individual preferences and innovation around the pilot courses to meet interested party's desires to support and be engaged was a clear necessity.

However, working with diversified training partners and true business innovators, such as Cambridge Judge Business School, the Inspirational Development Group at Sandhurst, EY and, from a truly pioneering perspective, using virtual reality (VR) through Jenson8, joint ambition, drive and responsiveness created momentum and optionality that appeared to overcome detractors.

The Problem

I started by asking the question: 'Why should banks cooperate in this area?' A reply came back from a COO within my network:

> *'I've been thinking about how best to express why, even though conduct risk management creates competitive advantages, banks should still cooperate. This is my outline proposition:*
>
> *Failure to effectively manage conduct risk can lead to significant P&L impact, either directly (rogue trading) or indirectly (LIBOR fines, mis-selling, etc.)*
>
> - *It follows that firms that can better manage that risk class have a competitive advantage versus those that cannot. This advantage*

is either realised directly (avoidance of losses/fines) or indirectly (greater revenue since clients value trading with 'safer' counterparties)

- *However, conduct risk can have systemic impacts (Barings, general loss of confidence in the system, etc.) so it is still in the economic interests of banks to cooperate since that risk means regulators require all banks to hold additional capital*
- *And finally, all significant firms enjoy the implicit support of the financial system (since they are too big to fail) and so, despite the competitive advantage, they have a moral obligation to cooperate in support of that system.'*

It was perhaps the moral obligation and doing what was right for the industry and the clients, investors and society they serve that resonated most.

Background

- Since Q1 2014 the Chief Control Officer Community (CCO 1LOD) had met on a quarterly basis, in London, New York, Toronto, Hong Kong and Singapore, to discuss common challenges and areas of innovation and possible cooperation within the control and conduct sphere, with a particular focus on 1LOD. These were run by my company Armstrong Wolfe,

and moderated on the night by me.

- In the autumn of 2017, six CCOs were invited to the Royal Military Academy Sandhurst, Camberley, U.K.. The aim of the visit was for the Academy to outline its modus operandi: taking raw officer cadets and via a twelve-month leadership course, training them in relation to meeting expectations on behaviour, good conduct, integrity and service.
- This comparison was used to structure the principles for the Conduct Academy for the banking industry, to take the underlying values of how the military works in centralising leadership and conduct training, which seeks to ensure all cadets when passing out from the military Academy are looking through the same lens as to their individual and collective responsibilities at that rank.
- This is then replicated throughout your military career, when being promoted you will attend the officer college for centralised training to ensure that when you are promoted you are fully aware of your responsibilities at that rank, to the armed forces and those you serve. Your specialist training, be it infantry, tanks, engineers etc., is undertaken by each separate division, working in hand with the centralised training.
- In the context of the banking industry, the Conduct Academy sought to provide centralised training to ensure the best and expected highest standards are outlined and taught, but, as with the military, the ultimate responsibility for conduct, individual development and accountability rests with the employer. Attending the Conduct Academy would make it more likely that the attendee would be a good citizen of the industry and an asset to an individual employer. Attending the Conduct Academy, supported by the industry and its participants, will ensure all employees of the sector are exposed to a deeper,

more representative, consistent and higher level of training through this cross-industry collaboration effort.

Note: It is fully understood the military is only a reference point and that, as a public sector entity, there are distinct and unique challenges and differences. This comparison is used as a point of reference and debate, not as an operating model to replicate.

The Vision

The Conduct Academy's long-term vision and objective was and is to provide centralised and accredited conduct training for the banking industry, across divisions, globally and front to bank.

The Academy's role is to be the conduit, the hub of innovation and coordination and the body working with the industry to define and continually develop the collective approach to conduct training and to establish an industry-recognised accreditation aligned to the common purpose of delivering higher and consistent levels of conduct and behaviour across the industry.

The Solution

The Conduct Academy meets multiple objectives:

- To provide annual common and best practice training within conduct for the sector, setting the highest common denominator for good conduct and behaviour for all employees operating within the financial markets front office environment.

- To provide an annual accreditation for conduct that will set the industry's annual standards for training and for promotion – mapped to and approved by key regulators in terms of their

standards, with the accreditation body to be determined

- To provide an accredited promotion course, based upon conduct and leadership expectations, for all those navigating career advancements within the banking industry
- To operate an independent platform solely focused upon reinforcing and enhancing behavioural standards, complementary and additive to existing initiatives – leveraging multiple delivery channels and blue-chip partners to ensure delivery excellence and scalability
- To deliver on a commercial basis with demonstrable cost-effectiveness.

Complementing Compliance Training

The Conduct Academy's training was to be and remains complementary to regulatory driven compliance training. Drawing on present compliance training modules, the participating banks' Chief Control Officers and/or Heads of Conduct, and the Academy defines the content and methodology to deliver cross-industry, best of breed, in-business conduct training, which remains over and above present compliance training.

This was to be delivered through the mediums of online, classroom and visual reality training, embracing technology innovation to bring new life and connectivity to conduct training, and by doing so differentiating the Conduct Academy's offering.

To be effective it would work closely with compliance and their front office business partners to ensure maximum progress is made towards achieving the shared goal of establishing good conduct, exemplary behaviour and ultimately driving cultural change across the industry.

It was envisaged that the Conduct Academy's training would replace component parts/all of compliance regulatory training/

other, whilst it being at the discretion of each bank to decide on this matter.

This approach would deliver a return on investment, a better product for the same cost and align each bank's training to the most up to date and relevant training requirements and innovation within training, further providing a better, more enjoyable, memorable and impactful training experience for employees.

It is important to stress that the Conduct Academy was not and is not to replace all conduct training, such as in-business training by a bank's head of product. As with a parent selecting the best school for their child, with the parent(s) and the home environment remaining ultimately accountable for the child's development and behaviour, the onus of responsibility to ensure any conduct training is taken into the workplace and is established as common practice remains the responsibility of each employer/bank.

One of the principal responsibilities of the Conduct Academy, and an advantage over other training options, is its role in aggregating, centralising and combining ideas and training collateral of the participating banks on a global basis. This draws on their extensive experiences to provide training for the real world, based upon case studies and underpinned by the implied authority that will be created by collecting and combining the intellectual capital of the participating banks to deliver best practice.

The Academy sought to and does provide an exclusive cross-industry approach that delivers excellence and a gold standard. In time, it is hoped that component parts (or more) of individual bank's compliance training will be replaced by the Academy's training, realising some cost and efficiency gains, whilst procuring an enhanced level of training.

Putting it simply, it was recognised and supported by the Conduct Academy's Working Group and the Chief Control Officer and/or

Head of Conduct's representation within it that the industry and its member banks would individually and collectively benefit from working together in this area of common interest, challenge and business criticality.

Individual perceptions and opinions, and those that cut a path with the sharpened knife of common sense, were to find themselves at the end of corporate reigns that limited corporate engagement for some, but allowed them to still voice tacit support for the supporting principles of the Academy.

The shift had been less of the anticipated direct engagement by the banks that had shaped the idea and provided the intellectual training capital, to identifying the key beneficiaries to be those smaller banks that had not been able to invest in developing their own conduct training. Additionally, a regional shift to where there is demand to meet the evolving regulatory agenda aligned to conduct. This was first Asia and post Royal Commission, Australia, where at the point of writing, the Academy is engaged by two Australian banks in location in Melbourne.

Further evolution: *The Regulatory Consideration: The Senior Managers' Regime*

The Senior Managers, Regime ushered in an era of very personal accountability.

Each senior manager is to regularly ask themselves the question: 'what can I do to ensure we are taking 'reasonable steps' to do the right thing and safeguard the bank's interests and reputation, and in doing so mitigate the chances of a significant event or failure?'

Specifically, the SMR seeks to boost personal accountability by putting the onus on senior managers as individuals to demonstrate they are taking reasonable steps to do the right thing. The regime requires a high level of clarity and empowers individuals

to challenge the status quo and debate issues that had previously remained untouched.

Each senior manager needs to be confident with their personal narrative, where the challenges come down to four very fundamental and personal questions:

1. What are your responsibilities?
2. How do you discharge them?
3. How can you be confident in your judgements?
4. How do you trust people to do the things that are done in your name and flow through to your area of responsibility?

The Conduct Academy is linked to the Senior Manager's regime by the need for any senior manager to be able to demonstrate he/she has undertaken all reasonable steps to mitigate incidents and/or failure. Specifically, as a senior manager you must be able to demonstrate you can trust people to do the right things in your name that flow through your area of responsibility. Training is a very simple and effective way to demonstrate in part that such reasonable steps are being taken and to make an impact in making the conduct agenda become a part of the employee narrative.

Conclusion and the Future

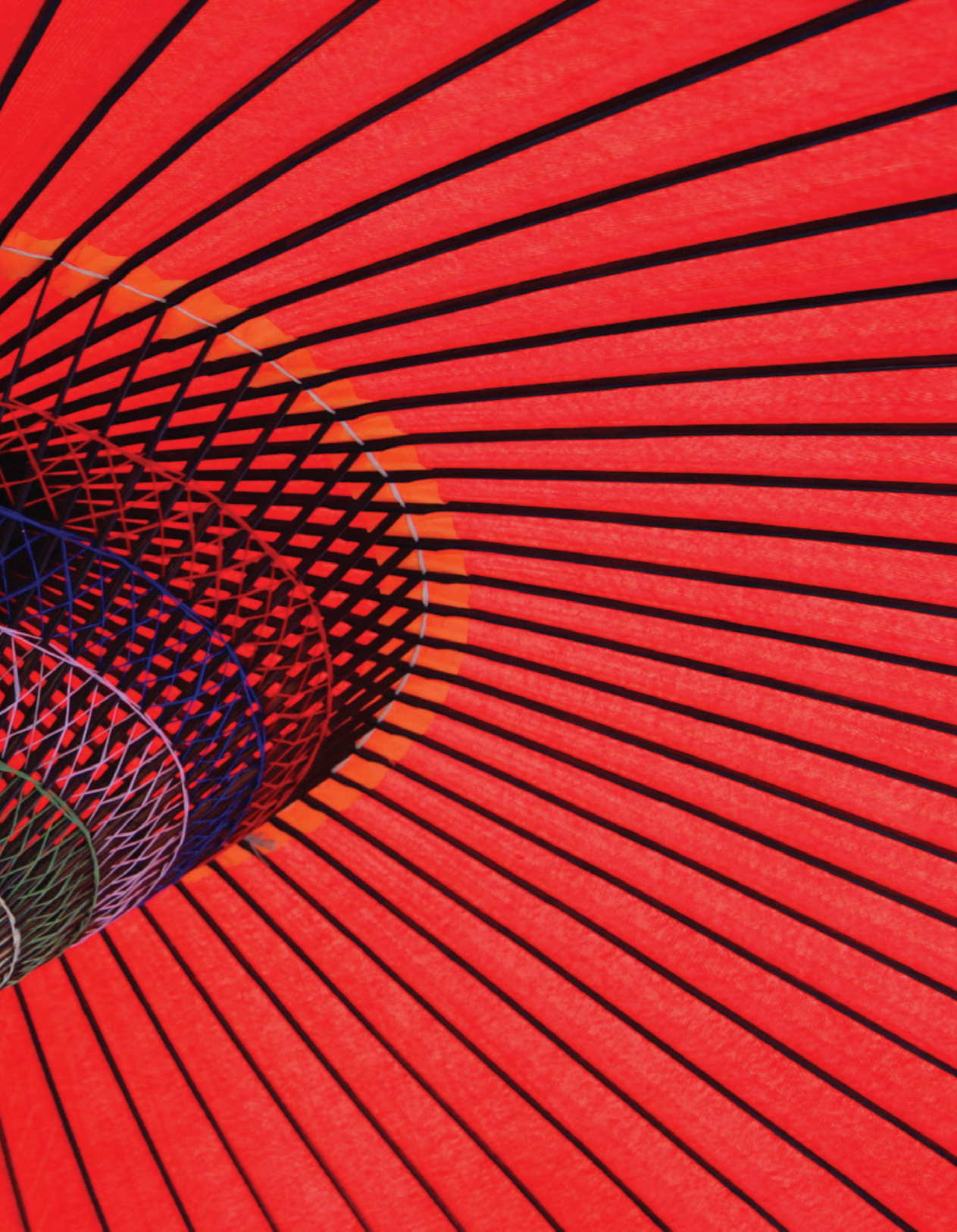
A plethora of studies have shown that collaboration can be a powerful tool towards higher achievement and increased productivity since collective efficacy can significantly boost groups' aspirations, motivational investment, morale, and resilience to challenges.

My experiences show the challenge is not the generation of the idea, nor securing initial interest or the validation process, but ensuring you have the attention of those in the right position of

authority and/or influence to make decisions (for their bank), be it delegated or direct responsibility. Within the area I operate, control and conduct, these contacts must be able to marry commercial acumen and necessity with an altruistic viewpoint and appreciation that it is the collective responsivity of the members of the COO and CCO community to do their best for their companies and to work with industry peers to help the market place overall:

- *to build, sustain and continually look to new horizons to create a robust and impenetrable control structure that will mitigate or even eradicate the chances of failure, abuse or manipulation in the future.*

In doing so, this community can help the industry continue to repair its reputation, to help it return to its position of trustworthiness and reliability and allow it to play its critical role within the global economy.



"Every fraudulent activity can be deemed as a function of two parameters: the person and the situation."

KWEKU ADOBOLI: HOW TO CLONE THE BIGGEST TRADING FRAUD IN THE HISTORY OF BANKING

By Sebastian G. Fritz-Morgenthal and Hagen Rafeld

Introduction

Exactly 1,330 days after Société Générale had to announce the biggest trading fraud in the his-tory of banking on January 24, 2008 with a total financial loss of €4.9 billion, caused by Jérôme Kerviel (Rafeld and Fritz-Morgenthal, 2010), the investment banking arm of UBS re-ported on a material loss of $2.3 billion due to unauthorised trading activities at the bank's Del-ta One Desk on September 15, 2011.

'This was the UK's biggest fraud, committed by one of the most sophisticated fraudsters the City of London Police has ever come across,' commented London police (Simpson 2012). The rogue trader's name was Kweku Adoboli, who was aged 31 when his activities became public. Who was this fraudster?

Adoboli was born on May 21, 1980 in Ghana, the son of a senior United Nations official from the West African country. He grew up in Israel, Syria, as well as Iraq before he was sent to the United Kingdom (West Yorkshire, Ackworth School) in 1991. In July 2003, Adoboli graduat-ed from the University of Nottingham

with an honours degree in computer science and man-agement (Wikipedia, 2018).

At UBS, Adoboli started as graduate trainee in 2003. From 2006 to 2011, he worked as trade support analyst, followed by a senior trader role – with a corporate title of director – at the Ex-change Traded Fund (ETF) Desk of the Global Synthetic Equities (GSE) business in UBS's City of London office. The desk's responsibility was to net delta limits, which was the maxi-mum level of risk the desk could enter into at any given time unless authorised separately.

On September 16, 2011, one day after UBS's announcement of the rogue trading, Adoboli was arrested and later charged with fraud by abuse of position and false accounting dating as far back as 2008. Adoboli was found guilty on charges of fraud by abuse of position, but not guilty on charges of false accounting, by London's Southwark Crown Court on November 20, 2012. He was jailed for seven years, but released after serving half his sentence. There was no additional financial fine (Unknown Author, 2012b).

Similar to the initial reactions from Société Générale to Jérôme Kerviel's rogue trading in which the former CEO Daniel Bouton described Kerviel as computer whiz-kid and as such could not be stopped by anyone, Oswald Gruebel (CEO of UBS) dismissed calls for his resignation and commented on Adoboli: 'If someone acts with criminal intent, you can't do anything (...) That will always exist in our job. If you ask me whether I feel guilty, then I say no.' (Mulier, 2011). Five days after his statement, Gruebel stepped down, and Sergio Ermotti followed as the new CEO; Francois Gouws and Yassine Bouhara (both co-heads of UBS's Global Equities fran-chise) also left UBS after Gruebel's resignation. Carsten Kengeter, the then Global Head of UBS' Capital Market function, was subsequently moved into the internal restructuring unit. On February 12, 2013, his replacement by Jim Molinaro (former CFO of Bear Stearns) and depar-ture from the bank was

announced in an internal memo (Enrich et al., 2013). However, Kengeter returned in 2015 as CEO of Deutsche Boerse (which he left end of 2017 after allega-tions of potential insider trading with own stock and the start of a criminal investigation), simi-lar to the former Head of Capital Markets at Société Générale Jean-Paul Mustier, who was an-nounced CEO of Unicredit in 2015.

Against these personal consequences, and far more severe for UBS, the Swiss Financial Mar-ket Supervisory Authority (FINMA) imposed on February 2, 2012 a range of strict preventive supervisory measures, limiting UBS's operational risk exposure until evidence had been given that the operational control environment was working effectively (Swiss Financial Market Su-pervisory Authority, 2012): (i) any new business initiative in the investment bank which was likely to materially increase the operational complexity of UBS would need FINMA's prior consent, (ii) the investment bank's overall risk weighted assets (RWAs) were capped at specific and declining values for the years ending 2012–15, in accordance with the bank's strategic plan, (iii) the investment bank's RWAs within its London branch were also capped, with the cap declining over time, and (iv) UBS was forbidden from undertaking any acquisitions through its investment bank division.

These measures implied a remarkable external trigger to change UBS's business model. Having said that, the Adoboli fraud needs to be interpreted as a coffin nail for the growth ambitions of UBS's Capital Markets franchise – turning the platform (existing until the Adoboli trading fraud happened) into a low-risk, low-capital-consuming, and consequently, less profitable business for the group. Following that, UBS decided in Q4 2011 to cut 1,575 jobs in the in-vestment bank globally (which represented 9% of 17,265 total employees in UBS's investment bank at the end of 2011). Further restructurings and associated job cuts have been announced since then.

An additional regulatory reaction came from the UK at the

Tab. 1: Unauthorized trading losses caused by rogue traders in banks

Financial Institution						
Year	**Name**	**Country**	**Time to detect [years]**	**Loss [USD bn]**	**Fine [USD bn]**	
Collusive rogue trading (CRT)						
2012	UBS[1]	U.K.	~ 6	N/A[2]	1.47[3]	
	Barclays Bank[1]					
	Deutsche Bank[1]	U.K.			3.75	
	Rabobank[1]	U.S.			1.01	
2012	JPMorgan Chase & Co.	U.K.	0.25	6.2	1.02	
2004	National Australia Bank	Australia	2.25	0.33		
Other						
2011	UBS	U.K.	~3	2.3	0.05	
2008	Groupe Caisee d'Epargne	France	0.6	0.98		
2008	Société Générale	France	2.5	6.9	0.01	
2006	Amaranth Advisors	U.S.	1	6.6		
2005	China Aviation Oil	Singapore	1.2	0.55		
2002	Allied Irish Banks	U.S.	3.6	0.69		
1996	Sumitomo Corporation	Japan	10	2.6		
1996	Morgan Grenfell	U.S.	1.25	0.34		
1995	Barings Bank	U.K.	2.5	1.3		
1995	Daiwa Bank's	Japan / U.S.	12	1.1		
1994	Codelco	Chile	0.5	0.28		
1994	Kidder Peabody	U.S.	3.2	0.08		
1987	Merrill Lynch	U.S.	1/12	0.38		
1982	Drysdale Government Securities Corporation	U.S.	0.25	0.27		

[1] At the time of writing, thirteen financial institutions in total (including two brokers) have been fined by regulatory authorities in light of the interest reference rate manipulation/LIBOR scandal.
[2] For simplicity, we only show imprisoned traders involved in the LIBOR scandal.
[3] An estimated USD 300tn (GBP 192tn) of contracts are based on LIBOR. An exact quantification of the financial loss caused by the LIBOR scandal is not possible.

	Trader			
	Name	**Age when detected**	**Imprisonment (Suspension) [years]**	**Fine [USD k]**
	Collusive rogue trading (CRT)			
	Thomas Hayes[4]	32	14 (3)	1,394
	Jay Merchant[4]	42	5.5 (1)	472
	Alex Pabon[4]	37	2.75 (1.8)	3.64
	Jonathan Mathew[4]	30	4	54.96
	Peter Johnson[4]	57	4	228.89
	Philippe Moryoussef[4]	44	8	
	Christian Bittar[4]	40	5.3	4,448
	Paul Thompson[4]	46	0.25	
	Achilles Macris	50		1,256
	Javier Martin-Artajo	48		
	Bruno Iksil	N/A		
	Julien Grout	34		
	David Bullen	32	3.6	
	Luke Duffy	34	2.5	
	Vince Ficarra	25	2.3	
	Gianni Gray	34	1.3	
	Kweku Adoboli	31	7 (3.5)	
	Boris Picano-Nacci	34	2 (2)	463,050
	Jérôme Kerviel	31	5(2)	
	Brian Hunter	31		30,000
	Chen Jiulin	44	4.25	335
	John Rusnak	37	7.5	1,000 + 691,000 (restitution)
	Yasuo Hamanaka	46	8	
	Peter Young	38	-5	
	Nick Leeson	28	6.6	
	Toshidhie Iguchi	44	4	
	Juan Pablo Davilla	34	8	
	Joe Jett	36		8,400
	Howard Rubin	36		20.4
	David Heuwetter	40	3 + 4 probation	-6

[4] UBS avoided another regulatory fine of EUR 2.5bn from the European Commission because of its expert witness role during the inter-est reference rate manipulation investigation. Source: Authors' representation, based on Hornuf and Haas (2014), Skyrm (2014a), and Wexler (2010: 6), enriched with own research.

end of November 2012 when the Financial Services Authority (FSA) fined UBS $48 million for significant system and control failings that allowed Adoboli to conduct the multi-billion USD loss through unauthorised trad-ing.

It is astonishing, that Adoboli's rogue trading at UBS occurred only three and a half years after Société Générale's trauma caused by Kerviel. Having that in mind, the authors would like to shed some light on two key questions:

(i) Which serious failings in the risk management and control environment at UBS, as well as Société Générale and Barings Bank – the latter of which employed Nick Leeson, the 'Godfa-ther' of all rogue traders (he caused the collapse/bankruptcy of Barings in 1995 due to his fraudulent trading activities) – contributed to the banks' inability to detect or prevent the loss-causing trading activities over an extended period of time and (ii) what mandatory measures are required in financial institutions in order to detect rogue traders earlier in their activities and stop them?

But firstly, what are the specific mechanics and characteristics of the Adoboli fraud.

1. Modus Operandi of Adoboli's Trading Fraud at UBS

Irrespective of Adoboli's actual criminal trades, all rogue trading activities can be reduced to one common characteristic: the rogue trader creates undetected fictitious trades or intentionally mismarks positions, which in turn cover/conceal undetected unauthorised open positions.

Adoboli's loss was incurred on large unhedged Exchange Traded Fund (ETF) index future positions. Approximately $2.1 billion from the total loss was originated by long EURO STOXX 50 and S&P 500 futures positions (peaked at $12.1 billion on August 8 and were sold out on August 11, 2011). The remaining loss incurred on

short S&P 500 and DAX futures, entered after August 11, 2011 (i.e. after the long exposure closure); Adoboli's short exposure peaked at $8.5 billion on September 15, 2011 – the day when UBS discovered his unauthorised positions and unwound them.

As precisely summarised by the FINMA, these are the main facts and findings on the conceal-ment techniques used by Adoboli in order to grant fictitious profit and loss (P&L) and risk ex-posure that concealed the desk's true P&L and risk – all techniques were in use since 2008 and created until the end of 2010 a total fictitious risk exposure of $296 million, plus a fictitious P&L in excess of $40 million, whereby the extent of Adoboli's unauthorised activities in-creased drastically in 2011 (Swiss Financial Market Supervisory Authority, 2012):

- One-sided internal futures trades: These trades were not matched against an internal counter-party, did not require confirmation and were subject to less stringent control processes. The trades were fictitious and generated fictitious risk exposure and P&L.
- Late booking of genuine external futures trades into the front office risk system: The effect of delaying the booking of these trades was to misreport the desk's risk exposure and P&L.
- Fictitious ETF trades with deferred settlement dates: These trades, which were cancelled before reaching settlement, generated fictitious risk exposure and P&L (...). The following variants of these trades were also used:
  - Fictitious ETF trades at off-market prices: The off-market pricing of these trades generated significant immediate ('day 1') P&L and
  - Fictitious ETF trades at off-market prices: The off-market pricing of these trades gener-ated significant immediate ('day 1') P&L and

- Amendments to the prices of fictitious ETF trades: The pricing amendments had the ef-fect of further misreporting the desk's P&L
- Zero-notional bullet cash trades: These were fictitious trades with a quantity and price of zero and an added cash flow (usually used to book cash-settled events such as dividends). The cash flows were used to clear reconciliation breaks generated by the use of other con-cealment mechanisms, and
- Adoboli also developed a profit smoothing mechanism, the so-called 'umbrella' (re-serve/wash account), which was against the existing UBS policy to report P&L when earned. With the umbrella, Adoboli combined several concealment techniques from above. It is remarkable that other desk traders were aware of the umbrella but none of them saw the need to escalate that vehicle to senior management.

When Adoboli and his unauthorised trading activities were discovered by a back office ac-countant, Adoboli sent the accountant an explanatory email of his trading scheme (see full email text in the appendix).

2. UBS's Control Weaknesses and Risk Management Failures

In their summary, the Swiss regulators attested to widespread deficiencies across the UBS's control environment. Front office managers had limited interest in supervising the activities of the traders, while breaches of policies, management instructions and limits were tolerated and not penalised. In addition, control and infrastructure functions were required to reduce person-nel, and requests for new headcount were denied.

In the following, several additional key findings are highlighted (Swiss Financial Market Su-pervisory Authority, 2012):

Tab. 2: UBS's Control Weaknesses and Risk Management Failures

Mismanaged transfer of the ETF Desk (into Global Synthetic Equities business in 2011)	• New desk supervisor was based in New York and therefore unable to supervise the London desk effectively on a day-to-day basis, • No concrete, well-planned, and transparent handover of responsibilities between old and new supervisor took place, resulting in undefined (and hence incomprehensible) responsibilities as well as reporting lines, • No alignment of control and infrastructure functions in accordance to the desk transfer.
Poor supervision	• Too much trust and not enough discipline and control between supervisors and traders, • The desk's trading mandate and risk limits were not formally documented but were communicated verbally only to the traders. Intraday net delta limit was $50 million (overnight net delta limit of $25 million) – limit increase in 2011 to $100 million respectively $50 million. • The desk's net delta limits were breached on at least four occasions between June and July 2011; on one occasion, Adoboli made a profit of $6 million by taking intraday positions in excess of $200 million – Adoboli's supervisor initially congratulated him on his performance before he emphasised the need of abiding by the existing risk limits going forward.
Ineffective control system	• The monitoring of alerts from cancelled or amended future trades and late bookings were not operational until late August 2011, the so-called T+14 Report – to be maintained by an outsourced provider in India – was non-operational from November 2010 to September 2011, without being noticed by management. • Information from the Supervisory Control Portal (SCP) provided only limited trend analysis; the identification of suspicious trading patterns needed to be performed manually. • Alerts on futures trades were sent to the traders rather to their supervisors.

Insufficient understanding and challenge by Operations	• The explanation given by Adoboli for large reconciliation breaks were not adequately questioned by operations staff. • Tendency of operations staff to view their role as supporter/facilitator for the front office trading activities vs. controlling and supervising it.
Inappropriate analysis and challenge by Product Control (PC)	• PC accepted the desk's explanation for the significant increase in proprietary trading revenues, • PC did not have proper infrastructure to review the desk's P&L at trade level, no satisfactory controls were in place to identify trades at off-market prices.
Ineffective Operational Risk Framework	• Reliance on self-assessments by front office as well as control and infrastructure functions. • In 2008, the Operational Risk Management function of UBS reviewed the Société Générale rogue trading event as reported by the bank (Société Générale, 2008) as well as its auditor (PricewaterhouseCoopers, 2008) and potential weaknesses at its own institution; the review identified a number of issues (missing proper control and infrastructure support – caused by significant staff turnover; weaknesses in the cancelled, amended and late booked trade monitoring – but failed to ensure remediation of identified control deficiencies); a follow-up review in late 2010 reported that identified issues had largely been addressed but apparently failed to ensure that identified control deficiencies were in fact sustainably remediated.
Reward and recognition systems	• The financial and non-financial recognition provided implicit incentives for risk-seeking behaviour.

3. Personal Factors, Modus Operandi, Control Weaknesses, and Early Warning Signals

Interestingly, there are many obvious similarities between Barings Bank's, Société Générale's, and UBS's rogue trader (inspired by Gibson, 2008): pto

	Nick Leeson at Barings Bank	Jérôme Kerviel at Société Générale
Personal Factors	High school diploma, followed by joining Coutts & Co, Morgan Stanley, and finally Barings Securities	Decent degree at secondary university; straight to Société Générale after university
	Former trade support/control; knowledge of back office processes and controls key to fraud	Former trade support/control; knowledge of back office processes and controls key to fraud
	No possibility of personal gain except bonus	No possibility of personal gain except bonus
	Aged 28 when arrested	Aged 31 when arrested
Modus Operandi	Mainly trading Nikkei index futures from Barings clients to exploit price gaps between SIMEX and OSE	Mainly trading index-based derivatives; DAX, EuroStoxx, CAC and FTSA index futures, and single stocks
	Took unhedged directional positions	Took unhedged directional positions
	Usage of an 'error' account (88888): Almost 5,000 hidden contracts per end of Jan. 1995 – increase to 61,000 end of Feb. 1995	Created phantom offsetting trades (fictitious hedges based on OTC index futures and ETFs)
	Trade price manipulation (excessive option selling)	Forward trade and settlement dates to help hide
	Unauthorised use of client's margin accounts	Booked fictitious trades against internal counterparties
	Illicit trading started small and became much larger (initial unrealised loss of £20,000)	Illicit trading started small and became much larger (initial unrealised loss of €1.4 billion)
Control Weaknesses	Lack of supervision and no segregation of duties	Widespread failure of risk and control structure and supervision
	Barings' financial reporting systems ('First Futures' in London and 'CONTACT' in Singapore)	Activity dated back three years from discovery
	Insufficient understanding/challenge by back office Controls failed to keep pace with business growth of Barings in Singapore	Concerns about trader also raised three months before discovery
	Doubling down strategy by Leeson, after Kobe earthquake	Société Générale discovered through checking an alleged counterparty

Kweku Adoboli at UBS	Early Warning Signals/Key Risk Indicators (KRIs)
Decent degree at secondary university; straight to UBS after university	• Lifestyle (Gambling and Debt) • Personal Account Dealing • Tracking of Mandatory Time Away/ Adherence to Holiday Policy • Tracking of unusual office hours • Chat protocols/Emails/Bloomberg Messenger/Social Media • Password misuse • Unauthorised use/access of profiles • Code of Conduct Breaches
Former trade support; knowledge of back office processes and controls key to fraud	
No possibility of personal gain except bonus	
Aged 31 when arrested	
Trading index-based derivatives; DAX, S&P 500 and EuroStoxx index futures	• Limit Breaches (VaR, P&L) • Independent Price Verification (IPV) • Trade Confirmations/Outstanding Confirmations • Reconciliation Breaks • Collateral/Margin/Funding Monitoring • Trading Balance Sheet Monitoring • Broker Commission Monitoring • Monitoring of relationships between traders and counterparties/Outsourcing controls • Cancellations, Corrections, and Amendments (CCA)
Took unhedged directional positions	
Created phantom offsetting trades (fictitious hedges based on OTC ETFs)	
Extended forward settlement dates to help hide	
Booked fictitious trades against internal counterparties	
Illicit trading started small and became much larger (initial unrealised loss of €1.45 billion)	
Widespread failure of risk and control structure and supervision	
Activity dated back three years from discovery	
Trader also questioned two months before discovery	
Adoboli admitted it to management following questioning	

4. Consequences

UBS had not learned any lessons from the rogue trading at Société Générale. This is even more surprising when taking into account the level of detailed internal information on control weak-nesses that Société Générale needed to make public three and a half years before Adoboli was detected internally, i.e. Société Générale's Internal Audit Report (Société Générale, 2008) as well as an external Special Investigation Report (PricewaterhouseCoopers, 2008).

UBS needed to learn it the hard way, that a weak control environment and a poor risk manage-ment framework will result in fatal consequences, from the actual material trading loss itself, significantly increased reputational risk, client dissatisfaction/ loss of investor confidence to fi-nally a tremendously changed investment banking business model upon regulatory instructions.

Largely, every fraudulent activity (such as rogue trading) can be deemed as a function of two parameters, the person itself and the situation (e.g. workplace environment). Regarding the lat-ter, the situation, Tab. 2 and 3 provide numerous examples of control weaknesses, risk man-agement failures, and, at the end, suitable targets for criminal offences.

While not everybody who breaches the code of conduct is the next fraudster, it is helpful to be aware of and understand individual behavioural patterns in order to derive early warning trig-gers. Without any doubt, the mechanisms of human behaviour that prevent someone exploiting a favourable opportunity (and vice versa) are complex. Nevertheless, criminological research provides adequate touch points for explanations – also parameters for prediction – of personal risk factors that may trigger deviant behaviour. One of these criminological theories is the Con-trol Balance Theory (CBT) from Charles Tittle (Tittle, 1995 and 2004).

According to Tittle, the amount of control to which an individual is subjected to relative to the amount of control that an individual can exercise determines the probability of deviance occurring as well as the type of deviance that is likely to occur. Imbalances in the control ratio can result in either a control defi-cit (more control is experienced than exercised) or a control surplus (more control is exercised than experienced). Both provide the needed push for corrective action to rebalance control. With that, Tittle interprets deviant behaviour as a device or manoeuvre helping the individual to es-cape from deficits and extending surpluses of control. In summary, motivation triggered by provocation in intersection and favourable alliance with the variables control ratio (in an unbalanced status), opportunity, constraint, and self-control may lead to deviance.

The trigger for Leeson was an initial small loss of £20,000, caused by one of his team members with a so-called fat finger error (e.g. buying a position instead of selling), which he wanted to hide. For Kerviel in turn, it was the desire to become an accepted member of Société Générale's trading department, linked to his non-elite background. Adoboli was a gambler type and moti-vated by risk taking. Since the three fraudsters had superior knowledge of back office control processes – Leeson and Kerviel even still had access to those systems – all three had a clear control surplus. Opportunity was given by the competitive environment combined with a lot of gaps and loopholes in the three banks' control systems (reference to Tab. 2 and 3). Hence, con-straints were limited. All three fraudsters showed a low level of self-control – as entry enabler – when starting their fraudulent activities that increased to a high level during their fraud scheme/fraudulent trading strategy for more than two and a half years (Leeson and Kerviel) or close to three years (Adoboli) (Rafeld et al., 2017a and b).

In our view, the implementation of reliant and robust situative controls to reduce the existence of suitable targets is mission critical for all financial institutions. From the shown risk management failures, mandatory detective measures – such as Key Risk Indicators (KRIs), highlighted in Tab. 3 – need to be designed, implemented, and regularly validated. With that, banks are required to implement effective behaviour risk management and control. Related systems monitor real time trade(r) behaviour, trade patterns, performance outliers (positive and negative), and provide early warning signals for trigger/turning points on individual trader and on trader desk/group level.

However, an effective behavioural risk management and control framework does not only rely on effective KRIs, but becomes integral part of the organisational set-up and is embedded in business and control processes of the institution. Let us take Independent Price Verification (IPV) as an example. This KRI is only effective if (a) it is part of an escalation process, i.e. if a trader and his associated controller cannot agree on the correct price for daily P&L the decision has to be escalated to the next level and (b) when the IPV is coupled with a limit authority sys-tem so that the respective controller an approve only deviations up to a certain amount / thresh-old, while about the threshold, approval from a higher level of authority would be required.

In conclusion, lessons learned from fraudsters such as Kweku Adoboli, Jérôme Kerviel, and Nick Leeson are the following: While we can't change human character, we can control and influence human behaviour and mitigate potential negative consequences. KRIs are helpful in-struments for fraud prevention and mitigation, but only if they are integrated in the organisa-tional structure and operating model of an institution. Such KRIs, as well as associated control processes, need continuous review of their effectiveness.

Appendix

This is the transcript of the email headlined 'An explanation of my trades' that Kweku Adoboli sent on September 14, 2012 to William Steward, an accountant working in the back office, who had challenged Adoboli as to why his trades did not balance (Unknown Author, 2012a):

Dear Will

It is with great stress that I write this mail. First of all the ETF [exchange traded funds] trades that you see on the ledger are not trades that I have done with a counterparty as I have previ-ously described.

I used the bookings as a way to suppress the PnL losses that I accrued through off book trades that I made. Those trades were previously profit making, became loss making as the market sold off aggressively through the aggressive sell-off days of July and early August. Initially, I had been short futures through June and those lost money when the first Greek confidence vote went through in mid-June.

In order to try and make the money back I flipped the trade long through the rally. Although I had a couple of opportunities to unwind the long trade for negligible loss, I did not move quickly enough for the market weakness on the back of the first back macro data and then an escalation Eurozone crisis cost me the losses you will see when the ETF bookings are can-celled. The aim had been to try and make the money back before the September expiry date came through but I clearly failed.

These are still live trades on the book that will need to be unwound. Namely a short position in DAX futures [which had been rolled to December expiry] and a short position in S&P500 fu-tures that are due to expire on Friday.

I have now left the office for the sake of discretion. I will need to come back in to discuss the positions and explain face to face, but for reasons that are obvious, I did not think it wise to stay on the desk this afternoon.

I will expect that questions will be asked as to why nobody was aware of these trades. The re-ality is that I have maintained that these were EFP [exchange for physical] trades to the mem-ber of my team, BUC [the accounts department], trade support and John Di Bacco.

I take responsibility for my actions and the shit storm that will now ensue. I am deeply sorry to have left this mess for everyone and to have put my bank and my colleagues at risk.

Thanks, Kweku

References

Enrich, D., Cimilluca, D., and Das, A. (2013). Senior UBS Banker to Exit. *The Wallstreet Journal Online*, February 12 (available at http://online.wsj.com/article/SB10001424127887324880504578300242536621214.html?mod=wsj_share_tweet – last accessed on January 11, 2021).

Gibson, N. (2008). Will your bank be the next? How to deter your own rogue traders. Chase Cooper Metric (available at https://www.slideshare.net/chasecooper/metric-special-edition-rogue-trading-9426265 – last accessed on January 11, 2021).

Hornuf, L., and Haas, G. (2014). Regulating fraud in financial markets: Can behavioural de-signs prevent future criminal offences? *Journal of Risk Management in Financial Institutions*, 7(2): 192–201.

Mulier, T. (2011). UBS Chief Gruebel Dismisses Calls to Quit After

Unauthorized Trading Loss. *Bloomberg*, September 18 (available at www.bloomberg.com/news/2011-09-18/ubs-chief-gruebel-dismisses-calls-to-resign-after-2-billion-trading-loss.html – last accessed on Jan-uary 11, 2021).

PricewaterhouseCoopers (2008). *Société Générale – Summary of PwC diagnostic review and analysis of the action plan*, May 23 (available at https://www.societegenerale.com/sites/default/files/23%20May%202008%20The%20report%20by%20audit%20firm%20PWC.pdf – last accessed on January 11, 2021).

Rafeld, H., and Fritz-Morgenthal, S. (2010). Breaking down the biggest trading fraud in the history of banking. *Risk Professional*, June: 47–51.

Rafeld, H., Fritz-Morgenthal, S., and Posch, P. (2017a). Behavioural patterns in rogue trading: Analysing the cases of Nick Leeson, Jérôme Kerviel, and Kweku Adoboli. *Journal of Financial Compliance*, 1(2): 156–71.

Rafeld, H., Fritz-Morgenthal, S., and Posch, P. (2017b). Applying control balance theory to the rogue traders Nick Leeson, Jérôme Kerviel, and Kweku Adoboli. *Journal of Financial Compliance*, 1(3): 276–284.

Simpson, E. (2012). Kweku Adoboli jailed for fraud over GBP 1.4bn UBS loss. BBC *News*, November 20 (available at www.bbc.co.uk/news/uk-20338042 – last accessed on January 11, 2021).

Skyrm, S. (2014). R*ogue Traders*. New York: Brick Tower Press, April.

Société Générale (2008). *General Inspection Department: Mission Green* – Summary Report, May 20 (available at https://www.societegenerale.com/sites/default/files/12%20May%202008%20The%20report%20by%20the%20General%20Inspection%20of%20Societe%20Generale.pdf – last access on February 19, 2018).
Swiss Financial Market Supervisory Authority (2012). *Summary report – FINMA investigation into the events surrounding trading losses of USD 2.3 billion incurred by the investment division of USB AG in London*, November 26.

Tittle, C. (1995). *Control Balance: Toward a General Theory of Deviance*. Boulder, CO: Westview Press.

Tittle, C. (2004). Refining control balance theory. *Theoretical Criminology*, 8(4): 395–428.

Unknown Author (2012a). Transcript of UBS trader's 'bombshell email'. *BBC News*, No-vember 20 (available at www.bbc.com/news/business-19902894 – last accessed on January 11, 2021).

Unknown Author (2012b). UBS's rogue-trader trial: The education of Kweku Adoboli. *The Economist*, November 24 (available at www.economist.com/news/finance-and-economics/21567134-swiss-bank-also-has-much-learn-education-kweku-adoboli – last ac-cessed on January 11, 2021).

Wexler, M. (2010). Financial edgework and the persistence of rogue traders. *Business and Society Review*, 115(1): 1–25.

Wikipedia (2018). Kweku Adoboli (available at http://en.wikipedia.org/wiki/Kweku_Adoboli – last accessed on January 11, 2021).

"For those charged with managing risk in the trenches of operational and regulatory mandates, like many COOs and CCOs at financial institutions, it's a constant battle."

THE NEW RULES FOR MANAGING RISK

A primer on understanding and proactively managing risk in today's rapidly evolving landscape

By David Pogemiller, Forcepoint

For some, risk is a thing to be avoided at all costs. For others, like the financial markets with credit default swaps (CDSs), it can be an intangible package and sold for profit. However, for most in business the truth lies somewhere in between; their objective is to manage risk in a way that optimises their ability to make a profit – it's about stopping the bad and freeing the good. Finding this balance is increasingly difficult in a world with a rapidly evolving risk landscape. Across industries, though maybe most prominently in financial services, cyber and reputational risk have risen to the top of today's concerns. Effectively managing risk – and in the best case using it to drive greater success – requires relentless determination, understanding and, ultimately, a proactive posture.

The good news is that businesses increasingly view smart, strategic risk management as way to accelerate performance and create a competitive advantage.[1] Today, leading organisations take a proactive approach to risk and use it to their advantage. For example, at a strategic level, many organisations are actively disrupting their business model before someone else can. This allows them to set the terms of the disruption and effectively

[1] 2017 Fortune risk management survey. https://www2.deloitte.com/us/en/pages/risk/articles/fortune-risk-management-survey.html

capitalise on it, versus being in a constant state of catch-up as they react to the disruptor's actions.

Netflix is a great example of a disruptor that became an incumbent and, ultimately, a leader by evolving beyond its initial strategy. When it began, Netflix capitalised on the perceived inconveniences of Blockbuster's rental model and quickly improved the experience of renting DVD movies. Realising the threat from digital disruption, Netflix shifted its strategy to fully digital distribution. This is just one example of how a proactive risk management approach can drive long-term success.

For those charged with managing risk in the trenches of operational and regulatory mandates, like many Chief Operating Officers (COOs) and Chief Compliance Officers (CCOs) at financial institutions, it's a constant battle. Not only does it directly impact the success of the organisation, but it also increasingly can have serious personal ramifications through regulatory structures, such as the Senior Managers and Certification Regime in the United Kingdom.[2]

This chapter aims to arm the reader with a basic understanding of the current, fast-moving risk landscape and tools for proactively managing risk. For many, it will serve as a healthy refresher on some of the basics of risk management, while hopefully introducing new insights. For others, it will drive new thinking and serve as an impetus to dive deeper into the subject in order to understand how it can benefit them and their organisation on an ongoing basis.

Today's Risk Landscape

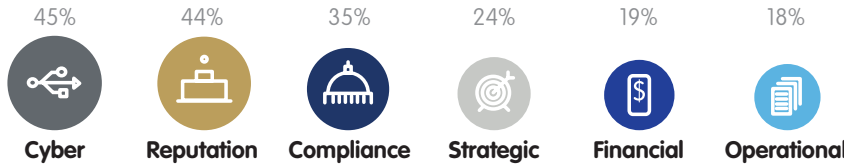
The risk landscape is evolving quickly, and organisations are constantly shifting their priorities to meet newly introduced risk. For many years, the most commonly considered business risks were

[2] FCA Senior Managers and Certification Regime. https://www.fca.org.uk/firms/senior-managers-certification-regime

categorised as strategic, operational, financial and compliance. In today's environment, though, organisations now commonly consider both cyber and reputational risk as first-class categories of their own. As a result, risk professionals are shifting their focus to the human point – the intersection of users and data across all networks. In a 2017 survey of more than 300 US-based executives, both cyber and reputational topped the list of 'urgent' risks; roughly 45% of those polled called them 'very urgent'.[3]

The most urgent risks

% of respondents calling each type of risk "very urgent"



Cyber Risk

Cyber has come out of the shadow of operational risk as its scope, complexity and impact has grown exponentially. The institute of risk management defines cyber risk as 'any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems'. While many factors have driven cyber risk's rise, three particularly stand out.

First, the IT systems that make businesses go are changing faster than ever and organisations are now operating in a zero-perimeter world. Gone are the days where people could focus their efforts on the clearly defined edge the corporation's systems and digital assets lived within. Despite their benefits, the boundless mobility of endpoints (e.g. phones, laptops); infrastructure and data spread

[3] Institute of Risk Management. https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk

across the cloud; sanctioned and unsanctioned cloud applications (e.g. Salesforce, Dropbox); and widely available, cheap or even free applications from the internet present material risk.

Second, technology is lowering the hurdle to threat realisation. Employees no longer have to print reams of information to steal intellectual property. They can interact with data wherever it lives, on any network. Just look at the Uber/Waymo case, where incredible amounts of intellectual property were taken with almost no effort. In fact, the level of knowledge required to execute malfeasance is also being driven down as sophisticated actors and tools arm unsophisticated actors who have nothing of value other than access to a network. In addition to lower barriers on execution, the potential rewards are becoming even greater as increasingly large amounts of valuable information, whether IP or personal, are located in large, centralised databases. The 2017 Equifax breach demonstrated the ability for a malicious actor to commit one hack and walk off with hundreds of millions of people's information. The consolidation of massive amounts of valuable information into 'data aggregators' is increasingly common as organisations such as Yahoo, Facebook, Twitter, Google and many others attract customers on a scale that was previously practically impossible. In addition, once siloed systems are now wired together, further exacerbating the problem.

Third, a significant amount of cyber risk is being driven by insiders. Whether employees, contractors, or third party service providers, these people are rightfully within your walls and network. Warren Buffet once said, 'The fact that people are full of greed, fear or folly is predictable. The sequence is not predictable.' Buffet's statement nicely encapsulates the challenge of mitigating the risk of malicious and accidental/negligent insiders. Not all insiders will be malicious. In fact, most will simply be negligent or cause accidental incidents, and their behaviour is rarely predictable;

only by understanding the context behind users' actions can the industry protect critical data. In Ponemon Institute's 2017 Cost of Data Breach Study, sixty-three firms across sixteen industry sectors within the United States were surveyed after they experienced the loss or theft of protected personal data.[4] Some 52% were caused by malicious actors, 24% by negligent employees and 24% by 'system glitches'. These types of incidents are increasingly meaningful and difficult to mitigate: they cost on average $225 per compromised record and come from a varied set of threats, threat actors and vulnerabilities (we'll define these shortly).

Reputational Risk

Of all the risks organisations face, reputational risk may be the most difficult to plan for and address due to mandates and funding issues. This is, in part, because reputational risk can be very hard to quantify, as it is unclear how a particular event will affect reputation and exactly what its financial impact will be. This is changing, though, as today's boardroom becomes laser focused on reputation; it's now clear how reputation damage translates to financial consequences.

In the past several years, data breaches have been increasingly common. As a result, they have become symbols for how reputational risk can impact an organisation's value through decreased acquisition prices (Yahoo lost ~$350 million after two breaches of user data were revealed in 2016), severe stock price declines (Equifax lost $4 billion in market value in the first week post-breach), or increased customer churn and decreasing customer acquisition. A 2017 Ponemon Institute study showed 31% of consumers who had suffered a data breach ended their relationship with the breached organisation.[5] That reaction is fully justified, as increasing numbers of individuals

[4] https://www.ibm.com/security/data-breach

[5] https://www.centrify.com/lp/ponemon-data-breach-brand-impact/

— 16% in the Ponemon study — suffer a criminal act (e.g. identity theft) because of a breach.

Technology's influence on reputation risk goes well beyond data breaches. One of the most pressing issues businesses face is entirely new threats that emerge based on how our society shares and consumes information about the world. Firms are under intense pressure to manage information flow during this age of 'always on' news, social media channels such as Twitter and Facebook, and web-based reviews from companies including Yelp and Amazon that enable the real-time dissemination of any and all information and inevitably sway a consumer's choices.

Social media management represents one of the greatest challenges. Firms want to support its ongoing use to inform and excite the consumer, but that use exposes them to material risk if employees make purposeful or negligent contributions that reflect poorly on the organisation or potentially expose valuable IP. Some poignant examples include:

- A Chrysler employee was sacked after he accidentally tweeted using the corporate Twitter handle instead of his personal account. The tweet included profanity and was a direct attack on residents of Chrysler's hometown of Detroit.
- In 2011, the CEO of GoDaddy.com posted a video of himself shooting an elephant in Zimbabwe. This invited significant and unwanted negative attention to the brand and resulted in customer churn, including People for the Ethical Treatment of Animals (PETA), who encouraged others to cut ties with the firm.
- One of the original examples comes from 2009, when two Domino's Pizza employees uploaded video that showed them violating numerous health code standards as they prepared food for customers. More than one million people saw the

video and it was widely reported by the media. Both employees ended up facing criminal charges and the company faced a significant reputational crisis.

- In 2013, a Lacoste employee posted his pay cheque on Instagram. He subsequently lost his job for breaking the company's confidentially agreement.

Data breaches and the misuse of social media are just a few examples of the long and growing list of material reputational risks organisations face each day. In addition to the examples above, the list includes such varied things as the mistreatment of employees (e.g. Uber[6]), fraudulent activities (e.g. Wells Fargo[7]), missed earnings and poor product quality. Given the growing number of significant examples of reputational risk within the past several years, it will remain front and centre for senior management and will be an increasingly important component of all well-designed risk management programmes.

Understanding Risk

Today's risks will certainly be prioritised and realised differently than tomorrow's, based on users' behaviour and intent. For that reason, it is critical to have the right framework to understand those risks and then proactively manage them according to that understanding. For many, the adoption of threat modelling provides this framework. The core components of a threat model are defined with examples in Table 1.

[6] www.latimes.com/business/la-fi-tn-uber-sexual-harassment-20170606-story.html
[7] http://money.cnn.com/2017/08/31/investing/wells-fargo-fake-accounts/index.html

Table 1: Risk Model Definitions

Term	Definition
Risk	The probability of a threat occurring and the corresponding harm. (*risk = probability x impact*)
Threat	A negative event that can lead to an undesired outcome, such as damage to or loss of an asset. *Examples: Employee steals intellectual property; an earthquake hits an office location; traders collude to fix markets.*
Vulnerability	The weaknesses in the system that make threats possible and can result in them being more significant when they occur. *Examples: Unpatched servers; poor password management; lack of controls on access to sensitive customer information.*
Harm/Impact	The result of a threat occurring. This can be quantified in any relevant measure including monetary, count of people affected, etc.
Resiliency	The ability of an organisation to effectively resist and reduce the impact of a threat and ultimately rebound.
Threat Actor	The entity (i.e. a person, organisation) that initiates the risk scenario. *Examples: Disgruntled employees, rogue traders, nation state actors and hacktivists.*
Asset	An item, thing or entity that has potential or actual value to an organisation (i.e. data we want to protect).

When discussing risk, many mistakenly confuse 'risk' with 'threat'. The difference between the two is important, as risk is the probability of a threat occurring multiplied by its impact. Therefore, risk is quantifiable whereas a threat is not. Without risk being quantified, it becomes nearly impossible to garner the necessary resources to address it, and difficult to assess whether or not the risk mitigation strategy is appropriate (e.g. are you spending $10 million to avoid a $1 million risk?). The impact will also change as vulnerabilities change. So, while an organisation may never eliminate a threat, it can still significantly reduce the risk associated with it.

One of the most effective ways to work through risk modelling is to write a narrative for each material threat to the organisation (see Figure 1). By explicitly creating these narratives, risk managers can

logically lay out the risks, as well as how they could occur and their potential harm. Doing so is powerful because it enables those charged with mitigation to break down each variable and identify opportunities for risk reduction and improvements in resiliency (both topics covered in the next section). Just as important, these narratives enable a high-quality, rational conversation both up to the board and executive level and down to those actually involved in the processes that expose the organisation to the risks (e.g. employees).

Figure 1: Create the Risk Narrative

To create a risk narrative, specify the essential elements of the risk. Below are two simple examples, but narratives can also include vulnerabilities, assets and other model components that can help provide essential insights on how to mitigate the risks.

Example Narrative 1

A Malicious Insider	**will**	take confidential IP	**resulting in**	$1M loss in costs to recover
Threat Actor		**Threat**		**Harm**

Example Narrative 2

A Negligent Insider	**will**	inadvertently release customer PII	**resulting in**	$3M loss via costs and loss of current/future customers
Threat Actor		**Threat**		**Harm**

Quantifying harm can be the most difficult part of writing the narrative. Over time, as more real-world data and research on the cost of realised risks can serve as reference points, this task becomes easier. Regardless, it is best practice to explicitly document all assumptions made on the cost drivers. For example, when trying to quantify the cost of a data breach, the risk manager should document not just a total harm, but each individual component of that harm (e.g. stock price loss, investigation cost, customer loss, fines) and the

corresponding justification for each. In almost all cases, getting to agreement across all stakeholders on whether the quantification is exactly right will be extremely difficult, but agreeing on the order of magnitude is possible when the assumptions are well laid out.

Managing Risk

Given the above framework for modelling risk, we are able to consider ways to mitigate the risks. There are essentially two broad strategies: reducing risk and increasing resiliency.

Reducing Risk

Because risk is defined as the probability of the threat occurring multiplied by the impact, there are two strategies to reducing it. The first is to lower the probability of the threat occurring. This can be done by fully eliminating the risk or by taking actions that reduce the vulnerabilities inherent in the system. The second is to decrease the impact or harm of the threat. Let's use two real-world scenarios to illustrate these.

For the first scenario, a self-driving car is remotely hacked by a malicious actor and used as a weapon against pedestrians. This is, unfortunately, an increasingly real threat as the promise of self-driving cars intersects with a malicious actor's desire to harm individuals. To reduce the associated risk, auto makers could prevent self-driving cars from communicating with external devices (e.g. Bluetooth, Wi-Fi). This would either fully eliminate the threat or, at a minimum, reduce the vulnerability and, thereby, the probability of it occurring. To approach this scenario from its potential impact (i.e. the amount of harm done), one could imagine defining a policy limiting self-driving to areas that typically have no pedestrian traffic (e.g. country roads) versus those driving in

densely populated areas (e.g. New York City streets).

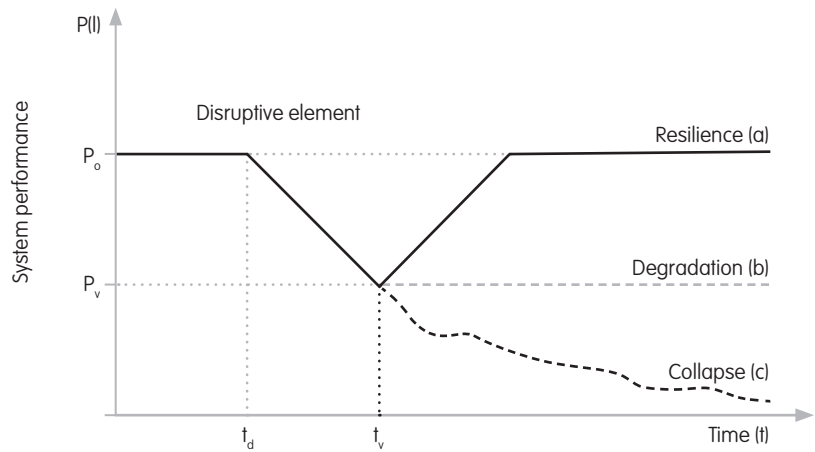
For the second scenario, let's investigate the new European Union General Data Protection Regulation (GDPR)[8] that takes effect in May 2018. The primary goal of this regulation is to better protect EU citizens' personal data by giving them more control of it (e.g. a right to be forgotten, providing more immediate notice of breaches (seventy-two hours), and putting more consequences on organisations that intentionally or negligently handle the data (i.e. fines of up to 4% of their worldwide turnover or €20 million, whichever is higher). Given that any global organisation that holds or processes EU resident data will be subject to the regulation, it is a critical one to put through the risk management process. For non-EU-based organisations, an obvious risk reduction approach is to stop doing business with any EU citizens. Most global organisations view this as an extreme and impracticable approach and are looking for other ways to reduce risk.

Firms are typically taking a two-pronged approach. The first is to improve data systems to have better visibility and control of the data itself. The second is to put new processes and technology – and there is an increasingly sophisticated and complicated set necessary – in place to monitor and understand the context behind the use and movement of the data, in order to ideally stop and, at worst, quickly detect potential misuse of that data. The key to risk reduction is to have effectively modelled the risk scenarios (e.g. threat, threat actors, harm) to be able to pull the right mix of levers.

[8] https://www.forcepoint.com/sites/default/files/resources/files/ebook_gdpr_key_themes_en.pdf

The Importance of Resiliency

In addition to proactive risk reduction, smart risk management programmes will also put significant focus on increasing their resilience. Resilience can be defined as the ability of a system and its component parts to anticipate, absorb, accommodate or recover from the effects of a shock or stress in a timely and efficient manner.[9] For businesses, it is the ability to deal with a realised threat in a way that minimises short- and long-term impacts to its success. Figure 2[10] shows a resiliency curve, where P0 represents the expected revenue of an organisation at a current, steady state. At td, there is a disruptive event (imagine a data breach is announced). This figure illustrates how revenues could follow one of three primary paths. The first path, Resilience (a), represents the business' ability to successfully respond to the breach announcement and quickly recover to its previously expected steady state of revenue. The second path, Degradation (b), represented by Pv, shows a sustained degradation to revenues with



[9] https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7552.pdf
[10] http://mechanicaldesign.asmedigitalcollection.asme.org/articleaspx?articleid=2537152

an insufficiently resilient response to the event. Finally, there is the path of Collapse (c), which represents an absence of any material resilience and leads the organisation to eventual failure. Each of these paths was witnessed in the financial sector during the global financial crisis of 2008, as some banks quickly returned to their previous performance (e.g. Goldman Sachs), some took longer to recover but successfully did (e.g. Bank of America), and others no longer exist (e.g. Bear Stearns).

One of the reasons organisations fail to explicitly design for resilience is that people notoriously assume negative events won't happen. Often attributable to cognitive biases, one's perception of risk can be irrational given known information. For example, optimism bias can cause a person to believe that risks are less likely to happen to them or their organisation than to others. They may irrationally believe that their organisation is at a lower risk for a data breach than a different firm, even though there is no factual reason to support the assumption.

Designing resilience into an organisation is essential, given the inherent challenge in accurately assessing risk and the unfortunate impossibility of eliminating it. No matter how big or sophisticated the company, bad things can and will happen. In the past several years a number of very high-profile outages have demonstrated exactly that: Twitter locked thousands of legitimate global users out of their accounts when they changed a privacy setting; Delta Airlines was forced to cancel 2,300 flights at a loss of $150 million in pre-tax income due to a blown circuit breaker in its Atlanta home office; and Equifax lost more than half of Americans' personal information in one of the most serious data breaches in recent times.

To add resiliency to a system, one should increase both preparation and the organisation's ability to recover. Preparation is done in advance of a threat occurring, and often includes

monitoring to provide early warning of a coming shock. Recovery includes the post-shock plans, resources and processes that enable the organisation to get back to business as usual.

Let's look at the resiliency through the lens of the U.S. banking sector. A bank's access to the Federal Reserve Bank's (Fed) discount window is one of the longest running and truly embedded tools that provides financial stability (i.e. the resiliency of the system). Access to the discount window enables banks to receive short-term liquidity (i.e. loans) to help cover when there isn't enough capital on hand to meet their obligations. The window is meant for day-to-day business, but in extreme times of financial stress, as with the 2008 financial crisis, the Fed can be authorised to act as a lender of last resort to provide liquidity when it has otherwise dried up.

The implementation of the discount window is an example of designing resilience into the system that focuses on response and recovery. In other words, when a financial institution becomes stressed, it can recover by accessing the discount window.

Improved ability to recover is only half of effective resiliency, though; preparedness is the other side of the equation. As noted earlier, in many instances, better preparation will take the form of monitoring and early warning. In the case of financial systems, the Basel II regulations around capital adequacy, planning and economic stress testing are prime examples of improving preparation to improve resiliency. Effectively, the regulations enforce ongoing monitoring and assessment of the financial institutions regarding whether their current capital (i.e. assets that create solvency) is adequate in the event of changes – even extreme changes – to the economic environment. In combination with the continual monitoring of the current economic environment and its likely future path, these regulations enable the financial institutions to be more resilient to any potential shocks that occur, as they will have proactively managed their capital accordingly.

Conclusion

In The Prince, Machiavelli states that: 'All courses of action are risky, so prudence is not in avoiding danger (it's impossible), but calculating risk and acting decisively.' This principle rings true today and should be applied by all organisations. For those ready to take on a more proactive approach to managing risk, here are seven steps to get started.

1. Define your material risks. Ensure you know your business (e.g. what is it built to do, why is it is built that way and what assets are involved in making it happen). Identify the key processes and assets that, if harmed or interfered with, would materially hinder the ability to do business (often termed 'crown jewels'). Remember, your most important assets could be things (e.g. data centres, power plants), people (e.g. employees, customers) or data/knowledge (e.g. intellectual property, like an algorithm for self-driving cars, customer data).

2. Model the risks. It is essential to actively model the risks so you understand not just the impact, but also how they are likely to take effect. Through a deep understanding of the risks, you will be empowered to take a proactive approach to mitigation.

3. Establish the organisation's risk tolerance. While many organisations will share the same risks, not everyone will accept the same level of risk. For example, a large bank with capital reserves to cover fines may be willing to take more sizable financial risks than a local/regional bank with fewer reserves.

4. Proactively manage your risk. The ability of an organisation to proactively manage its risk can be its key differentiator, and is

where winners and losers are made. All material risks should be in your risk register, and you should be actively working to reduce risk and design increased resiliency for each.

5. Be holistic. Remember that managing risk must be done holistically. It is a people, process and technology problem that must be addressed across each dimension. Those organisations that solely focus on one element of risk will fail to be as successful as they need to be.

6. Make it continuous. Given the stakes and the dynamic nature of today's risks, the risk identification and assessment process cannot be ad hoc. When protecting your intellectual property from malicious insiders, you must continually assess the insider's actions and what you know about them in order to make appropriate decisions on how much risk they represent and how much trust to enable them with.

7. Make it adaptive. Continuous assessments need to constantly adjust to varying risk environments. This can be at the macro level, such as adapting the organisation's strategy or the micro level, such as adapting the controls placed on an employee's actions (e.g. what files can they access, what systems can they use).

"Failure, of one sort or another, is inevitable wherever there are people."

THE PEOPLE SIDE OF CONTROL AND THE POWER OF FAILURE

By Bobby Chatterjee and Lucy Phillips

Having worked in and with a multitude of global banks in business partnering, transformation and C-suite coaching roles over 20 years, we bring relevant perspectives.

The expectations on Chief Operating Officers have evolved significantly in considering that a 'change' is no longer seen as an interruption in the execution of routine business strategy, but rather the lever to execute it. This continues to shape the skillsets demanded of Chief Operating Officers where the only constant is business volatility. Further, managing 'operations' requires excelling in multiple roles simultaneously. Back in 2006, Nathan Bennett and Stephen Miles suggested in the *Harvard Business Review* that there were seven 'roles' that COOs may need to fulfil, including: *Mentor, Partner, Other Half* (compliment to others around them), *Change Agent, Executor, Heir Apparent, and MVP* (most valuable player – i.e. given the title for retention purposes).

Given that COOs must increasingly deliver transformations – often repeatedly over their tenures, to execute organisational strategy, they are often wearing several of these hats simultaneously. Further, the operational and strategic facets that a COO must demonstrate to succeed also means that a COO that thrives in one role may not automatically enjoy success in another. This dynamic,

combined with the increasing fiduciary and legal responsibility that Boards and C-Suites now assume for overseeing corporate conduct, means that we are also seeing more companies appoint Chief Control Officers (CCOs) who are specifically responsible for acting as change agents and conduct stewards.

While management guru Peter Drucker is famously credited with stating, "Culture eats strategy for breakfast", as far back as 2000, the sentiment continues to resonate today. This maxim still rings true given increasing pressures on organisations to maximise all operational levers for success, as well as the ease with which the more unsavoury or downright illegal aspects of a company's culture can now be exposed.

So, while this has never been a more exciting time for those CCOs and COOs tasked with managing conduct and culture given its importance at the top tables, this is also a time of ongoing reckoning with culture interventions (and protections) that work... versus those that do not. Our thoughts? We have a series of reflections that we believe should be considered by CCOs and COOs to maximise how they help their people drive change and flourish in its aftermath.

First, Fail fast

On face value, CCOs and COOs and the leaders below them appear to understand that failure, of one sort or another, is inevitable. *Fail fast* is often shorthand for *if you're going to make the mistake, make it once and learn from it*, with the unsaid (but understood) *and don't make the same mistake again*. That said, while there is often a benevolent cultural articulation of *fail fast* in many organisations, few managers would feel comfortable espousing this directly to their people or cheerfully triumphing a fail during their year-end performance review. Unofficially *fail fast* lands on most ears as,

categorically do not fail on my watch.

That said, when we consider our biggest lessons learned whether in the workplace or well, in life… the most profound learnings tend to emerge from our mistakes. Any CCO or COO that truly wishes to serve and protect their organisation by tending to conduct and culture, needs to consider how to engender the wisdom afforded by failure without inadvertently causing operational harm through carelessness or recklessness.

In considering this objective, we believe people broadly fall into two groups when it comes to learning. One group abides by the rules because they are told to do so by those in authority; that perceived extra experience or seniority over them is in itself sufficient for them to comply without question. The other group are those who need to understand for themselves why that rule is in place and the consequences of not following it. For any parents of toddlers, this is the difference between the child who won't touch a hot stove because their parents tell them not to, versus the child who wants to experiment because they won't accept someone else's experience over their own.

We've been intrigued to note another pattern that has emerged during Covid-19 lockdowns. Even otherwise good, rule-abiding, careful people watch to see what others do. If someone else breaks a rule and appears to do so without consequence, it would seem that many of us follow suit, reducing to the lowest common denominator rather than raising the few who choose to break the rules. Case in point: how many people reading this have come onto conference calls with their cameras on – only to shut them off once a majority on the call opt to do the same?

The relevance to CCOs and COOs seeking efficiencies and 'right first time' approach is this: if so many employees effectively learn what to do and what not to do through experience and role-modelling from others around them, how can organisations create

the culture and environment where those people who need to try things out to learn can do so safely? Conversely, how do you best help those who prefer to comply dutifully , to continually think critically about what they are doing and why, to ensure that they are operating in the best way possible too? It's a critical balance to get right as we've seen that even the most successful organisations need the right balance of both rules and governance, as well as critical thinking and vigilance. And as an aside, Managers and HR that get this balance, do a good job of celebrating both people following the rules, as well as using good judgement in the absence of rules... and those who have some lessons learned the hard way.

Our view is that people are spending so much time trying to prove that they are not doing the wrong thing, that they are operating from a mindset of mitigating error and are left with less time to proactively do the right thing. With this in mind, the following provide further illustrations of focusing people towards doing 'right' things... and less around policing them against the 'wrong' ones.

You can put the values in the lobby... as long as you also put them to work

Every bank has values. Increasingly in many banks, these are well-known and visible. In previous years, corporate values were well-intended and visible in marketing materials and perhaps less so in the lived experience of an employee's daily experience. When times were good, there felt less urgency to pay attention to them.

However, given the challenges both caused and experienced by the financial sector, banks must ensure that their corporate values – cornerstones of exemplary conduct and culture – are living and breathing in everyday life. Many banks now induct new employees with a values programme. As a further effort to embed core values,

some are now giving equal weighting to how well employees are executing them against cultural targets and values as part of the year-end review and ratings process.

For this to work effectively however, all leaders need to role-model the right behaviours, take immediate action where any behaviour or conduct falls below clearly articulated standards and be open themselves to such feedback. Any such change requires a mindset and cultural shift to ensure that at all levels, everyone knows, expects and believes that their behaviour and duty of care is as important to the organisation and their personal future career prospects as the results that they tangibly deliver.

Further, for any values onboarding programmes to have teeth, the experience of an employee in the day-to-day job needs to reinforce what they have learned in the onboarding. For example, a new employee may be told "We don't have a blame culture." Yet, if the behaviour of their manager, peer or leader shows a different reality, then those behaviours ultimately are more powerful in both defining the culture in action.

Layered onto that observation is a quick understanding of whether the values sit above individuals in the hierarchy. We are finely tuned to deduce quickly if people are treated equally at different levels for a similar type of issue. If, for example, whistle blowers are promised anonymity, then the CEO should not request any more information about them than anyone else, in the event of a complaint. While managers at lower levels may recognise that they must follow the rules, they are more likely to trust these rules, and the leaders above them, if they see their superiors also honouring these rules. Without shared accountability among all to uphold values, trust can be eroded, and with that loyalty and stewardship of the business.

Engage your people in working through the toughest moments

Not surprisingly, the biggest challenge for many CCOs and COOs is to uphold the values in the face of the expediency of running the business and managing financial pressures. Given that many CCOs and COOs are promoted into their roles due to their ability to execute, be resilient, make tough and (sometimes unpopular) decisions, they face additional scrutiny when companies fall short of either their operational or cultural conduct aspirations. Further, another dynamic we've observed is that often by the time an organisation starts implementing tough decisions, the leaders who have wrestled with the dilemma and made the decision have mentally 'moved on' and are now just focused on the execution.

The same can't be said for those people hearing bad news for the first time; they need time to get to grips with it before swinging straight into execution mode. A common experience is when an operational lead suddenly must cut the budget for a project that is well underway. In our experience these projects are still expected to complete with fewer resources, budget or new accelerated timings. The stresses this puts on the project team is considerable – both in terms of the physical hours needed to be deployed across fewer people, but potentially more perniciously, the psychological burden of suspecting that there is no shared understanding 'on high' of the difficulty in delivering to the same quality. Achieving high standards of conduct is harder when over-stretched. Another example of this breach in trust occurs when additional layers of approval are added into minor decisions, such as requiring two senior leaders to approve a £50 train ticket. Again, the time needed on that task is minimal, but it adds time to get it done and fuels further concerns that top levels are ignorant of the pressures faced in the levels below them.

All too often, there isn't enough explanation as to why

additional processes are required, or project budgets and resources have been cut. Or if financial pressures are cited as the rationale, then bitterness increases when cuts are mandated by teams that are perceived to have little insight into 'what happens next.' For the individual, fear of failure without understanding why often results in an amygdala 'fight or flight' hijack, which clutters the mind, rendering it incapable of finding workable solutions or to make valuable information connections.

While people in banks seem to demonstrate higher levels of resilience than in some other professions, resilience is supported when people have both an intellectual understanding of problems and the ability to shape solutions themselves. Consequently, we've seen some cutting measures and changes play out somewhat better when teams are empowered to consider trade-offs and recommend the savings or changes themselves. We've seen teams and leaders protect sacred cows that are often relatively small-expense areas that play an outside role in boosting morale or team unity. These small victories go a long way to keeping teams engaged through tough times and reinforce solution focus at all levels.

As discussed, fear of failure is a powerful motivator, so it's critical that companies ensure that when they are embarking on cuts and changes, they recognise the need to deliver these messages (and solutions) in a way that doesn't completely eradicate organisational belief in its ability to succeed.

Your time: how much are you wasting fearing failure?

Many organisations make decisions via committee. Waiting for decisions decreases momentum and often disconnects senior levels from the impact of their decisions. The Undercover Boss television series, where senior leaders undertake junior roles to see how the business they run really operates, highlights this disconnect well.

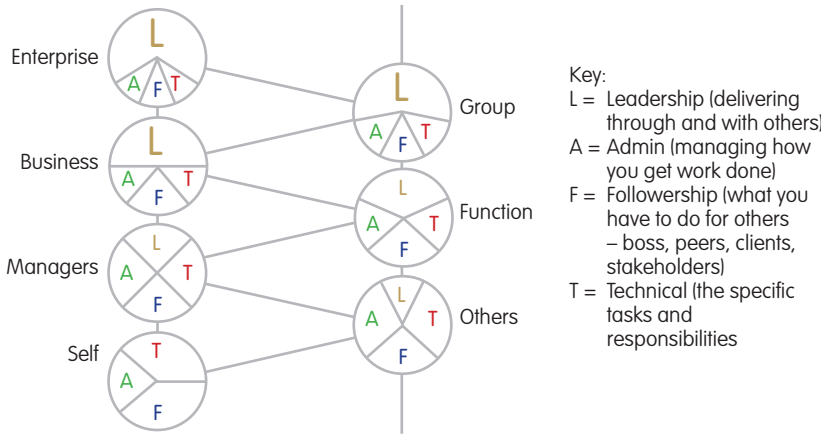
In practice, decisions by committee also mean that if an initiative fails, it is sometimes difficult to pinpoint accountability. The psychology of decision-making tells us that there is a very different mindset when an individual knows he or she will be held solely responsible. When we know that we are accountable we commit and work harder. This is true even for many under-performers. Therefore, it is worth considering having individual or named owners of different topics or individual project elements to get the benefit of accountability.

Another unintended consequence of decision by committee is that everyone with views is included in all the dialogues and corresponding emails. The resulting volume of email traffic for many senior leaders means that emails may go unread, and even if a participant hasn't responded, their inclusion in the email string suggests an implied agreement to a decision when in fact they've been on the sidelines.

Leadership development theory, for example overlaying Drucker's managerial job components with Charan and Drotter's leadership pipeline (shown below), generally tells us that the more senior a leader becomes, the less technical they should be. They should empower those below them and delegate effectively, which further enables their people to develop – and ideally progress in their succession plans. The challenge with this model today is that a leader must both be a strategic, while also being directly responsible for the technical details they oversee.. Carrying the metaphor further, we no longer expect the musical conductors to simply get the best performance out of every member of their orchestras, we expect them to play every single instrument in the orchestra as well.

This way of operating creates a vicious circle causing many banks to allocate too much leadership and managerial time to

Adapted from Charan and Drotter's Leadership Pipeline (2000) and Drucker's managerial job components (1996)



the *Administration (A)* segment of the pipeline. Insufficient time is allocated to *Leadership (L) and Followership (F)* which is where the rubber hits the road in role-modelling, building connections, inspiring and motivating. Administration in turn is viewed as a means to get promoted, which may not inspire the retention of the most dynamic talent.

Regulators add ever-increasing checks and requirements to satisfy themselves that banks are changing and consistently conducting themselves in an appropriate manner, which in part contributes to the emphasis of the *Administration (A)* style.

Further, the fear of scrutiny and being the one that causes a fine or reputational risk means that other management layers or roles are added that supersede what the regulators require. For example, we observed a bank committing to six highly complex and time-consuming deep dives into a topic when the regulator required only four. Additional exertion in areas like this can generate a long list of unintended consequences, many of which can eventually lead

to the kind of high-profile failures the sector has seen far too often. Added to this are the annual performance KPIs which advance relentlessly – yet are often left unchanged, sometimes becoming invalid or irrelevant by year-end. If people feel they are 'set up to fail', they may be less able to focus on good conduct, or less willing to spend time on conduct with many other pressures on their time.

In summary, getting the best out of your people is an artful and scientific balance between having the right controls in place to give them clarity on what not to do... while also showing them how 'good' is achieved through competent leadership and management. A healthy culture is one that is as grounded in good scorecards and metrics as it is in good conduct role-modelling and behaviours. Having coached many senior banking leaders – when people are committed to the organisation's cause, understand the challenges it faces and are targeted in a stretching, fair but achievable way – enhanced productivity and fewer issues are often the outcome, which are key deliverables sought by our CCOs and COOs.

Get the KPIs right

When people are under pressure, they focus on what is being measured. The critical decision every organisation must get right is to ensure that they are focussed on the KPIs that are really powering business growth. The difficulty is that some departmental or divisional KPIs are either conflicting or can inadvertently drive negative or unhelpful behaviours. CCOs and COOs can add tremendous value by challenging conflicting objectives and requiring that all departments challenge themselves if their KPIs are all hitting the bottom line positively.

Further, employee engagement surveys often reveal a low percentage of employees that truly understand an organisation's strategy and vision. This matters; if employees don't know or

understand the strategy, then they aren't using a strategic lens to make decisions or prioritise. What they are likely going to do instead, is to do what they think will best prevent a mistake. While this is a noble aim, the Chartered Institute of Personnel and Development (CIPD) quoted Dutch research in 2020 which found that fear of failure holds back two in five people. So again, the balance for people who are managing people... and by extension COOs and CCOs stewarding an organisation, continually challenge the organisation to clarify the strategy, make sure the KPIs matter and give your people enough guardrails to keep them from a spectacular crash – while letting them go fast enough to learn from a few dents in their bumpers. This type of mindset encourages teams to think about failure as expected in the journey to success, which of course it is.

Provide controls without controlling

While being a controlling leader may appear to have benefits, there are consequences in the behaviours of those who work for these types of leaders. The psychology of continuously being directed results in many individuals becoming lazy, knowing that an instruction will come soon enough, and thus it is not worth attempting to use their own thinking or judgment. No CCO or COO wants an organisation full of human sheep who sit and wait. A manufacturing example highlighted this only too well. A factory worker stamping fresh product was given an incorrect date stamp, thus labelling all fresh product as already out of date before it had left the factory. When this error was highlighted, the individual shrugged and said they had to use the stamp provided by their manager. This potential laziness is completely avoidable with the use of controls rather than being controlling. It does not support the organisation's effort to minimise risk or deliver 'right first time'

in an efficient, ethical and commercially viable manner.

We've also witnessed some divergent behaviours in the midst of the global science-business-social experiment that is Covid-19. We've seen some leaders and managers becoming more micro-managing from the comfort of their home offices to feel a sense of control. They have sought normalcy by seeking to try to increase control. Conversely, we've also seen leaders who previously may have been privately uncomfortable with employees working from home consciously coming around to this new reality by challenging some of their notions about remote working. Their way of leading their people has also adjusted with their finding ways to be more trusting of their people by implementing 'controls' that seek to mimic the rhythms and patterns of the workplace albeit in a virtual setting. As expected, our observations have been that those employees who feel trusted and empowered to get their work done (in a more flexible fashion) have reported better satisfaction, motivation and commitment than those who feel monitored and not trusted. Ultimately, the mass exodus to remote or hybrid (part-home, part-office) working has also demonstrated that again in many companies, delivery is the ultimate KPI, and many companies and employees have noted productivity increases – particularly among those who are equipped and enabled to work remotely.

Serve to lead: lessons from Sandhurst

Sandhurst, the Royal Military Academy where all British Army officers are trained, has a variety of leadership practices that are world-renowned. Notably, leadership is taught first at Sandhurst. Only after leadership training has taken place, is any technical training undertaken. In corporate life, it seems to be technical first then (maybe) leadership later. There is also a concerted focus on the concept of followership as well as leadership to firmly

encourage the leader to be an effective follower and role-model the leadership (and followership) that he or she expects from their team. Standards and consequences are consistently applied.

The Sandhurst values live and breathe and are embedded early in future officers. Discipline is reinforced from the start as attention to even small details matter. In terms of failure, if a soldier cannot run fast enough or needs to be more accurate at shooting, that is considered a training matter and support will be provided. The values, however, are non-negotiable as the cornerstone of good conduct.

In the case of any behavioural issues, the matter is addressed at low-level in most cases, as this is usually sufficient to ensure no repeat occurrence. On the second occasion, if indeed there is one, disciplinary action is provided from a higher level. In practice, there is very rarely a repeat occurrence, but it is notable that demotions are regularly used as an option where multiple issues occur over a period of time. Conversely, demotions are less 'overtly' demonstrated in corporations as a matter of course.

At Sandhurst, feedback is provided, expected and welcomed. There is no bell curve performance distribution, but there is structured, graded verbal and written feedback, transparently discussed with the officer-in-training. Any corrective development plan required is not perceived as a negative or a failure, but as an expected part of learning to become fully competent.

In terms of missions, leaders are instructed to get from point A to B with any critical conditions or boundaries to be aware of, effectively acting as their guardrails. They are then empowered to lead their people to point B in the best way that they can, given whatever situation confronts them. As some missions may have life and death consequences, they ensure that all levels understand what the leaders two levels up from them need to deliver. There are many valuable lessons for the commercial world.

In summary: connecting the dots... for yourself and your organisation

- **Don't encourage people to fail fast... unless you really mean it and will learn from it.** Encouraging your people to fail fast is a tall order unless you are creating an environment that both puts guardrails in place to prevent epic fails... while also making good on having a culture that values learning through mistakes.
- **Make the values matter.** Banks today don't have the luxury of just relegating values to the marketing department. Execution against values must be mandatory; the required behaviours need to be articulated and modelled by the top, and consequences for breaches must be swift, visible and universal across all levels.
- **Give your people the space to hear tough news for the first time.** Deliver requests for cuts and changes during the year with greater explanation and genuine empathy for the consequences to those having to implement that decision. When you can, engage them in finding solutions so that they feel some agency during times of stress.
- **Don't lose time avoiding accountability or 'performing' your anxieties.** Additional scrutiny on the banks is the natural outcome of the failures of 2008 – however, don't add levels of complexity and 'group think' to decision making as a means of skirting accountability. The business environment requires regulation, and it requires agility.
- **Choose the KPIs that deliver the results you intend.** Invest time here. Your people will execute on those areas where they are being measured, so ensure that you've considered how the KPIs will be interpreted, delivered and measured.

- **Having 'controls' encourages people, being 'controlled' demotivates them.** Covid-19 requires many managers find ways to lead, manage, assess, motivate and coach remotely. Given that it's so much easier for employees to 'turn off' if they are frustrated, leaders and managers must apply a more facile touch in enabling their people to succeed in a way that brings out their best.
- **Empower people to help solve the problem.** Empower more people in the consideration of what to change or cut for the smallest impact to business performance and conduct; cuts to the so-called obvious areas like travel budget and training often cause more issues than they solve. Ask employees how best to maintain high standards of conduct and identify when something is not as it should be, rather than launching policies and telling them. People are often far more resilient and innovative if they are actively engaged in solving the problem.
- **Emulate Sandhurst which encourages leaders to *Serve to Lead*.** Foster a mindset in your leaders, managers (and C-suite) that reminds them that as leaders, their role is to enable their people to achieve their objectives as opposed to expecting uncritical execution.

The views expressed in this article are those of the authors and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

KABUKI町
KIRIN BEER
一番搾り
ANRAKUTEI
ANRAKUTEI
ANRAKUTEI
半兵エ
Hanbey
宴会
190席
大座敷
120席
【カラオケ完備】
St.James
湖南菜館
4F
レンタルルーム
エデン
Eden
カラオケ
コロッケクラブ
全店営業中
ゲーム
メンズサウナ
まんが喫茶
BOWLING
ビリヤード&ダーツ
ゴルフ バクス
ANRAKUTEI
HUMAX

5F
天神の宴
完全個室
無料案内所
1F
ラッキー
B1
悪質な客引き注意
劇場通り一番街
1F
2F
DINING BAR
B1 80席
東京豚骨らめん
まんが喫茶
無料案内所
まつ里亭
B1
案内所
無料案内

"There is considerable value in careful preparation and planning for the transition ahead."

TECHNOLOGY AND CULTURE

The cornerstones of control and conduct

It occurred to me early in the investigation into the evolving role of the banking Control Officer that it requires less of a technologist than an informed user of technology, and certainly someone who embraces the future possibilities of technology and how it will fundamentally change the role.

At one of my CCO forums, the question of technology and the vendor landscape within control and conduct arose. 'I find it hard to determine between one company and another,' one CCO commented. 'I find it even more difficult to follow the conversation, which is invariably ambushed by FinTech acronyms, abbreviations and words en route to the Oxford Dictionary,' said another.

This led to a realisation that determining and understanding technological possibilities, and getting to grips with the terminology bandied about by the FinTech sector, would be useful skills for the CCO community. Moreover, it was clear that technology will complement rather than replace the CCO, yet it is absolutely critical to building a robust, defensive and detective framework, aimed at ultimately mitigating and minimising conduct risk.

Let's start with FinTech itself. My understanding is that this encompasses a broad spectrum of companies, technologies and market participants – start-ups, financial services companies,

market infrastructure and technology companies that are set on changing the way financial services are executed. These institutions are influenced by regulators, customers, investors and accelerators, who are introducing new demands, ideas and structure.

FinTech is helping to define new technologies and provide new services, and its companies are changing the financial services sector. 'There is a market-wide recognition and appreciation of its contribution. In my opinion their contribution is timely when the industry is facing unique demands, especially relevant to the control community,' explained one New York-based CCO. It therefore offers opportunities as it seeks to provide cost-effective and innovative solutions to common, market-wide challenges.

As a layman, however, the jargon can be baffling. Accelerators and Incubators, Unicorns and Gazelles, Blockchain and Bitcoin, Robo-advisors or Cloud and Software as A Service (SaaS) ... these are just a few terms I have found hibernating on my notepad, scribbled in haste at interviews and meetings, then largely ignored because I do not fully understand their meaning or context.

In New York recently I sought to address this shortcoming through a contact of mine. 'Can you help?' I asked Brian White, then of Forcepoint, a market leading innovator in cybersecurity and regulatory surveillance solutions. Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries, and through my experiences with many senior people in the control and conduct space I had come to value Brian's opinion on this subject and others. We were embarking on this conversation when we were joined by Guy Filippelli, founder of RedOwl – the FinTech that Forcepoint acquired in 2017.

Guy and Brian make an interesting team; their profiles are noteworthy in themselves and set an expectation on the contribution they would make to any conversation. Guy was schooled in counter-terrorism, worked in the intelligence community and in

2008 was one of four civilians awarded the National Intelligence Medallion from the Director of National Intelligence in the US. This is the highest award for civilians working within the intelligence community and he was the youngest person to receive it by at least a couple of decades. He holds a BSc in Economics and Computer Science from the United States Military Academy (USMA) at West Point and a BA and MA in Philosophy, Politics and Economics from Oxford University. He studied as a Marshall Scholar at Oxford University. His vocational and charitable interest in helping US veterans is a closing soundbite that resonates with me through my own charitable efforts for the British military.

Brian's background is similarly impressive. Prior to RedOwl and Forcepoint, he served at the Chertoff Group and Lockheed Martin. Akin to Guy's governmental experience, Brian served as a senior official at the Department of Homeland Security, was a professional staff member on Capitol Hill and, in his early career, was an associate at Booz Allen Hamilton. He holds an MPA from the Maxwell School of Citizenship and Public Affairs at Syracuse University and a BSc from Syracuse University.

Brian concurrently serves as a senior associate with the Center for Strategic and International Studies (CSIS), is a practice associate at the Institute of National Security and Counterterrorism (INSCT) at Syracuse University, a guest lecturer at the Naval Postgraduate School and frequent speaker on cyber security issues. As if all this was not enough, he was also a German Marshall Fund Manfred Wörner Scholar.

The three of us settled in to deal with the purpose of my visit, and I outlined the common concern within the control community about the perceived over-representation by the sector as to its capabilities. It seemed an honest and simple appraisal was needed. What is feasible today? What is the runway to further developments? What are the milestones for advancement within technology?

Brian walked me through the technology, and remarked on a few things of note, yet what resonated with me is how quickly the field is evolving and is taking advantage of the technologies developed by the military as well as Amazon, Google, and Netflix – and even more intriguing was Brian's explanation that the technology was still improving and we were a few years from the ideal solution. This candour surprised me, especially as many technology vendors claim to be nirvana.

There were other things I wanted to know, and the views of these two qualified men would be invaluable to me.

'Is technology or cultural change the answer to managing conduct risk?' I asked expectantly (antagonistically perhaps). 'Or, what is the weighting between culture and cultural change and embracing technological innovation to deliver a robust and reliable control and conduct framework?'

I am a firm believer that culture defines conduct and is therefore the master of technology. However strong a culture is, there is always a potential seed of bad conduct that might take root. This cannot be prevented by control measures or policies, fear of punishment or disclosure, but technology could provide a defence mechanism against poor conduct that works alongside culture.

Fundamental to the 'three lines of defence' debate is the fact that despite the huge investment in resources into the second and third lines, conduct incidents occur almost exclusively within the first line and they could arguably have been prevented through an unassailable supervisory and surveillance framework or more recently the marriage of behavioural science and technology. It is here that culture, policy and technology meet.

And rather unexpectedly, Brian agreed. He further explained: 'The reality is that technology is merely a solution – and if designed appropriately a very important solution to surface interesting patterns and events, yet it is not a panacea, rather needs to be part

of the broader solution. In my opinion, it should be the foundation, yet it does not substitute for great people, great training, and ultimately a great culture of behaviour. In other words, technology enables you to implement the right program, and uncover problematic behaviour before you have reason to suspect an individual may have violated a rule – this is the very promise and intent of behavioural analytics.'

It is today's capability and technological reality that I am really interested in, so I proposed my third question to Guy and Brian. In, your objective opinion, what is the principal shortcoming of technology today in helping banks address the complexities and demands of the supervisory mandate and enhancing the industry's management of conduct risk? This led to a final question: how long before such shortcomings could be addressed?'

Brian jumped on this question and exclaimed: 'It is the lack of knowledge of this industry. Conduct and control is an expertise and is very difficult to learn or appreciate from afar. I firmly believe that the solutions of the future will be developed in partnership with the leading financial institutions as they seek the opportunity to not just take advantage of technology, but help shape its future to ensure its viable to meet their challenges.'

A leading technologist in this sector would present a valuable opinion on these issues, but not a balanced or objective one. Such objectivity could only be secured through the commentary and observations of those responsible for its application. To this end, I approached my executive contacts in the 1LOD and supervisory field, asking them the same questions. These investigations are summarised as follows:

Q. Is technology or cultural change the answer to managing front office conduct risk?

'Ultimately, both are necessary but neither is sufficient! In particular, firms cannot hope to manage risk by putting all of the best tools in place if the right culture to engage with those tools is not present. We will always have to place some reliance on the first line to appropriately manage and supervise their people, and if we don't have the right culture in place to do that, the framework is built on sand. In addition, though, if we can't deliver the right tools to highlight the risks, supervisors will struggle to identify the relevant events, or their engagement will be harmed by inefficient processes to review data surrounded by "noise".'

GLOBAL HEAD OF FRONT OFFICE SUPERVISION, JAPANESE BANK, MARKETS DIVISION

'Both are required. Whilst technology can help reinforce the message through supervisory tools, and detect conduct risk through surveillance tools, cultural change is essential, as it deals with the way we fundamentally do business and is the best means to prevent conduct risk.'

GLOBAL CCO, US BANK, MARKETS DIVISION

'Both have a role to play. Clearly if the technology existed to create a 100 per cent effective preventative control, then to an extent there would be no need to try and change culture or the behaviour of individuals. Indeed, were this to be possible any sort of background screening, mandatory time away, certification etc. would be rendered entirely unnecessary. Herein lies the problem, insofar as everyone is aware that the creation of 100 per cent effective controls is an impossibility, let alone preventative controls.

' Control environments tend in any event to be detective and this creates a different issue. If you have detective controls which are 100 per cent effective, you still have a problem, as you will be catching the person doing what they should not do just after they have done it. Whilst a regulator always likes to see problems being self-identified, they would still take a dim view if the offence were serious and likely fine an institution where the offence had taken place (albeit at a lower level than had the offence not been self-identified). As a result, the need is for both cultural and technological effort to be combined. Arguably, cultural change is easier to deliver than technological change, and therefore the focus should be there, although

clearly improving control environments through technology and automation has an important part to play.'

GLOBAL HEAD OF CONDUCT AND CULTURE, EUROPEAN BANK, IB AND MARKETS DIVISION

'As one could imagine, it has to be a combination of both. Front office technology and data analytics being developed by FinTech companies has really come a long way over the past two to three years, and continues to develop at a rapid pace. The ability to tie in structured trade data and email/chat messaging will enhance the surveillance capabilities across the control and compliance population.'

FINANCIAL CRIME AND FRAUD OFFICER, CANADIAN BANK

'Cultural change can drive prevention. Technology can drive detection and serve as a deterrent. The answer needs to be a balance of both. Senior management and supervisors should set the right example for their teams to emulate. They need to cascade the appropriate and acceptable behaviours from the top down. Technology can help to identify individual cases of idiosyncratic conduct risk. Technology can

highlight patterns and concentration of risk flags for individuals, teams or business areas.'

GLOBAL HEAD OF SUPERVISION, EUROPEAN IB

'These are not mutually exclusive components; however, I would rank cultural change as the most important, specifically tone from the top, which is aligned with incentives – namely compensation. Technology seems to be more useful as a surveillance mechanism that can identify issues more timely, but not proven as a preventative control.'

AMERICAS CCO, EUROPEAN IB, MARKETS DIVISION

Q. What is the weighting between culture and cultural change and embracing technological innovation to deliver a robust and reliable control and conduct framework?

'As highlighted above, both are important. Technology supervisory tools will take years to mature and require a constant investment. Conduct risk cultural changes already started years ago and we are able to see clear benefits now.'

GLOBAL CCO, US BANK, MARKETS DIVISION

'This is a difficult question. The two need to progress in tandem. They address the same problem from two different angles. The cultural change is something that can be felt, but is difficult to quantify. It is the cultural change that encourages staff to make the right decision for the right reason. However, technological innovation can be quantified. In the ever-evolving regulatory environment, technological innovation helps to demonstrate hard evidence and numerical results.'

GLOBAL HEAD OF SUPERVISION, EUROPEAN IB

'I think the culture probably needs to underpin everything, and is the clearest change to start right away (also doesn't necessarily require much investment), but the tools need to follow.'

GLOBAL HEAD OF FRONT OFFICE SUPERVISION, JAPANESE BANK, MARKETS DIVISION

'Truly embracing a robust control and conduct framework is in itself a cultural change in our industry, essentially brought upon us by our own past misdeeds as an industry, as well as the offsetting response by our regulators. The crisis of 2008 not only called attention to the credit-worthiness of financial institutions, but also how operational risk

can have a profound impact on them. The past five to seven years have seen a dramatic shift and resource allocation into a firm's operational risk framework, both from a technology, process and human-resource perspective.'

FINANCIAL CRIME AND FRAUD OFFICER, CANADIAN BANK

'All equally important. However, the genesis is setting the culture and cultural change in real terms. Not mission statements and aspirational quotes, but translation into how employees are measured in their day-to-day jobs and reflected in how they are paid. Regulators seem to want something to touch and feel, so we cannot ignore the technological aspects – I would say 60/40.'

AMERICAS CCO, EUROPEAN IB, MARKETS DIVISION

Q. In your opinion what is the principal shortcoming of technology today in helping you address the complexities and demands of the supervisory mandate?

'Big data or ability to consume and use data to enable effective supervision. Regulations change rapidly, are increasingly complex, overlapping and sometimes conflicting, which makes it difficult to ensure they are applied consistently. The data is there to support them,

but is challenging to convert this into simple and effective supervisory information and processes.'

GLOBAL CCO, US BANK, MARKETS DIVISION

'The principal shortcoming we face today is not technology in my estimation. It's the data we have to pipe into the different technology platforms.'

FINANCIAL CRIME AND FRAUD OFFICER, CANADIAN BANK

'The single biggest issues are undoubtedly the proliferation of systems that we have inherited and the data-quality issues associated with this – there are far too many disparate systems, all of which create their own format and version of the data for reporting purposes. As a result, when building controls, huge effort has to go into data cleansing – and even after this has been done, system noise continues to be a distraction and leads to a lack of buy-in from control users, who are quick to use data-integrity issues as a reason to ignore or dismiss technologically driven controls.'

GLOBAL HEAD OF CONDUCT AND CULTURE, EUROPEAN BANK, IB AND MARKETS DIVISION

'I'm not sure if this is the principal shortcoming, but one major challenge is that the enormous amount of data it's now possible to gather must also be processed and reviewed. Automated solutions for doing this are still coping with sheer the amount of information.'

GLOBAL HEAD OF SUPERVISION, EUROPEAN IB

'Several shortcomings are noise generated by exceptions, creating extraneous false positives. Technologically driven alerts have not proven to be very definitive regardless of the technology platform offered – at it's core, the alerts are largely predicated on known historical issues – historical fact patterns that have proven to be once problematic tend to form the basis for any alerts; however, these aren't as helpful in predicting future issues. What is helpful is the ability of technology to draw together several tasks, to give the look and feel of a uniform platform and helping evidence supervision.'

AMERICAS CCIO, EUROPEAN IB, MARKETS DIVISION

'The key shortcoming is probably the disparate nature of our technology – multiple, bespoke booking and execution platforms, not all of which

provide the minimum information required to meaningfully aggregate and review data.'

GLOBAL HEAD OF FRONT OFFICE SUPERVISION, JAPANESE BANK, MARKETS DIVISION

In conclusion – and not surprisingly – it is, of course, a combination of both technology and cultural change that will help manage front office conduct risk, but as one of the above sources summarised: 'Herein lies the problem, insofar as everyone is aware that the creation of 100% effective controls is an impossibility, let alone preventative controls.'

This is obvious to all. A 100% preventative model is impossible due to the uniqueness of the central ingredient: the human being.

I would disagree with one summary that 'arguably cultural change is easier to deliver than technological change and therefore the focus should be there, although clearly improving control environments through technology and automation has an important part to play'. Deep-rooted and embedded cultural change takes years to undertake and deliver into a global organisation, and it has to ride alongside changing market conditions and leadership shifts. It is a task that takes patience and must be adhered to in policy, breathed by all and represented especially by a company's leadership, as the ambassadors of its culture.

However, in an age when capital is limited and cultural change costs comparatively little, the following rings true: 'Technology supervisory tools will take years to mature and require a constant investment. Conduct risk cultural changes already started years ago and we are able to see clear benefits now.'

It is rewarding that my research appears to support my view, suggesting in the balance between the two that culture ultimately plays the more significant and influential role, perhaps best summarised by the quote: 'Cultural change can drive prevention. Technology can

drive detection and serve as a deterrent.' However, we must take a measured approach, as bankers and regulators like to quantify results and this is not easy or indeed plausible in relation to culture: 'Cultural change is something that can be felt, but is difficult to quantify. It is the cultural change that encourages staff to make the right decision for the right reason. However, technological innovation can be quantified.'

The clear message from these conversations is that the greatest impediment to technology playing an equal part in a marriage with culture, is data: 'Big data or the ability to consume and use data to enable effective supervision ... is the principal shortcoming we face today [and not] technology in my estimation.'

Within this, the industry is dealing with a legacy of antiquated technologies and lack of capital to invest in their replacement: 'The key shortcoming is probably the disparate nature of our technology – multiple, bespoke booking and execution platforms, not all of which provide the minimum information required to meaningfully aggregate and review data.'

One way or the other the industry must and will address this challenge, capital forces demanding and driving it. Some will lose and fade away, some will be the future, and new entrants will spice up the mix.

My message to the FinTech and broader technology sector, therefore is: sort out the data problem and a world of opportunity will unfold, allowing you to provide a limitless portfolio of innovative solutions to a sector hungry for innovation, to help drive efficiencies, realise cost savings and create, secure and maintain competitive advantage. Do this and you will allow the banking industry to resolve its conduct issue through a cultural revolution, where technology is a partner in this evolutionary process, where the objectives will be achieved and all, including the regulators at large, can look forward to a happy future state.

"How many banks really know whether their culture is effective in reducing misconduct and fraud? The truth is, not many."

IMPROVING BANKS' ORGANISATIONAL CULTURE

A sustainable approach to behavioural change

By Frantz Maurer, KEDGE Business School
and Pierre Pourquery, EY

How much trust should we be placing in our banks?

In the years since the 2007 financial crisis, the question of trust has risen ever higher up the agenda for banks. The crisis exposed numerous weaknesses in the banking industry, not least fragmented approaches to risk management and control. This fragmentation diluted accountability and gave organisations a false sense of protection. It also meant they were unable to adequately predict the crisis, despite a significant focus and a great deal of energy expended on quantifying risks. An abundance of risk and control indicators were creating as much confusion as clarity.

This sense of loss of control was only exacerbated as the banking industry was subsequently rocked by more than USD 100 billion in fines and losses from litigation and fraud. The market tremors from scandals including foreign exchange (FX) and LIBOR fixing are still being felt, and a flurry of fines, prosecutions, and other litigation have followed in their wake.

Yet these crises have been a critical catalyst for change in the banking industry. Banks have invested more than USD 1 billion in restoring public trust and confidence and fixing the weaknesses

revealed during the financial crisis and subsequent scandals. Those fixes, whether driven by new regulations, new market practices or client pressures, have ensured their control environments are now safer and stronger.

So, what's changed to enable this to happen? Several things. Banks have started to take better account of conflicts of interest and other risks. They've reinforced the accountability of their businesses and first lines of defense. They've aligned their policies and procedures with new codes of conduct developed by regulators and through industry standards. They've invested in new technology to better detect fraud or misconduct and they've simplified their business models and control environments by increasing the level of automation.

Necessary though these changes are, they're still lacking in two respects. First, most controls (at least 80%) are still concerned with detection not prevention. This not only significantly increases the cost of those controls, but also does little to stop major issues and crises ahead of time. Second, banks have been insufficiently focused on culture and behaviour. That's especially surprising given that most of their losses in the last ten years have largely been caused by misconduct and culture issues.

To date, most banks have tackled cultural change through staff training. They've explained to employees what misconduct and conflicts of interest really mean in the context of their jobs. The best banks have even created detailed lists of client scenarios that should be avoided. Some have realigned their remuneration structures with a focus on longer-term performance. Others have reinforced their staff management skills, because good managers better understand the negative impacts of misbehaviour on long-term business sustainability. But how many banks really know whether their culture is effective in reducing misconduct and fraud? The truth is, not many. Even when a bank keeps behavioural

data, it doesn't necessarily know how to make the best use of it. In a major study with an investment bank, we have developed a new methodology for measuring culture within an organisation. Called the 'Culture Index', this methodology is based on our practical experiences of working with numerous banks. It explains how to define and codify 'culture' and how to use it to measure a Culture Index for individuals, groups, and entire organisations. Importantly, it enables banks to improve their culture by better understanding the root causes of misconduct and acting on them.

Why is measuring culture so important?

Culture is best defined as a set of expected behaviours. In the past ten years, for example, around 70% of banks' operational losses have been connected to misbehaviour (corresponding to something like a USD 1 billion loss for each bank). There may be further such losses ahead. Potential frauds relating to FX and gold are still under investigation. Martin Wheatley, former head of the UK's Financial Conduct Authority, has said that 'FX rigging is as bad as LIBOR'. Banks have already been fined £2.6 billion, and JPM was the first to settle directly (to the tune of £100 million) with a group of investors. Banks have also experienced large losses (up to USD 5 billion) from large unauthorized trading activities at Société Générale and UBS.

These events have only added to public concerns about banks' potential conflicts of interest. The industry has been under attack from politicians and the media alike. Restoring trust in the banking system – and the reputation of banks whose business relies so heavily on that trust – has become a priority. As a response, banks have developed sophisticated surveillance and monitoring systems to detect abnormal employee behaviour. They're also now trying to integrate trading information with communication information

to identify potential misconduct. This has been combined with an intense focus on training to explain the potential consequences of misbehaviour to employees.

Welcome though these developments are, the results to date have been limited. Banks are still over-reliant on the 'tone from the top' in infusing the appropriate culture. Training is too often seen as a tick-box exercise with little emotional engagement. It does little to understand the root causes of misbehaviour and fails to clearly articulate what kind of conduct is expected from staff. Most banks have no way of systematically distinguishing between the good people doing the right thing and the bad people doing the wrong thing. And they still struggle to detect misconduct early enough to actually do something about it.

Furthermore, by focusing on corporate values rather than behaviours, some banks are putting the cart before the horse. In our experience, values run deep and are not easily changed in a short period of time. Moreover, setting values creates resistance: people don't generally like to be told what to think. What matters far more is clarifying expectations and changing the context in which employees operate. This could include changing remuneration and reward systems, hiring and promotion criteria, the diversity and experience mix of teams, job profiles and rotation, or any other factors that could potentially drive different behaviour. Ultimately, values and mindsets will follow.

Some are now trying a more ambitious data-driven approach to cultural change. They're finding they can successfully identify 'good' and 'bad' behaviour by following a set of simple principles to foster their corporate culture. These banks don't attempt to drive change with a 'one size fits all' approach, instead they look for good practice in their current set-up, and compare and contrast with underperformers, they identify the traits of high-performing people and teams, and they then codify those traits and drive them through

the rest of the organisation. Creating a strong risk culture at an organisational level is no easy task though. Traders, investors, and sales people will always need to balance augmenting their revenues and sales against taking care of their clients' interests. There are three things a bank can do to support their staff as they do so. First, it should formalise the expected culture and communicate clearly what is expected from employees. It should recognize that it's not always possible to capture every single conflict and risk situation – there will always be grey areas that require judgement. But clarifying expected and unacceptable behaviours will help employees take better and more informed decisions. Second, a bank should measure culture at an individual, group, and even organisational level, through a Culture Index. And third, a bank should monitor changes in the Culture Index to help identify the individuals or groups of individuals that could potentially misbehave and favour their interests over those of their clients or the organisation.

Measuring culture – from individuals to organisations

The nature of expected behaviours will depend on each industry and each organisation. But those behaviours (and thus the culture) are still capable of being measured systematically. How? First, by defining the behaviours – both those that are expected (the good) and also those to avoid (the bad). Second, by gathering information about the behaviour of each individual employee and comparing it against those expectations. And finally, by using this information to create a Culture Index at both the individual and organisational level.

When developing a Culture Index in a joint initiative with an investment bank, we began by defining sets of good and bad behaviours, grouped into four main categories: those focused on the long-term interests of the bank and its clients, and the

sustainability of the business; those focused on people accountability and ensuring mandates are exercised responsibly; those focused on rigor and transparency and guaranteeing the reliability of results and operations; and those focused on fostering collective discipline and individual courage. In total, 42 good behaviours and 43 bad behaviours were defined across all four categories. For example, in the first category – long-term interests – 11 good behaviours and 9 bad behaviours were defined (see below).

Good behaviours	Bad behaviours
1. Privileges long-term relationships over transactions 2. Develops a strategic view on client needs with the help of the sales team 3. Are available for sales and client matters 4. Makes clients aware about all the risks 5. Respects suitability and conflicts guidelines 6. Calls attention to existing or potential conflicts of interest (clients/internal) 7. Complies with the bank's Chinese wall rules 8. Acts with the utmost attention to privileged information and confidentiality 9. Ensures appropriate investments have been made to secure the management of the transaction on a long-term basis 10. Treats others with dignity and respect 11. Shares best practices with colleagues and other business lines	1. Compromises relationship interest because of immediate revenues and margins 2. Provides a client with inappropriate products or services 3. Purposely reports wrong prices to clients 4. Enters into transactions not respecting the maximum margin policy without prior authorisation 5. Hides potential conflicts between clients and colleagues and business lines 6. Enters into deals that put the bank's reputation at risk 7. Misuses privileged or confidential information 8. Favours certain brokers to get policy gifts or advantages 9. Fails to inform the bank about potential interests beyond their business line

Having defined good and bad behaviour, a bank can then gather the necessary data about individuals and develop a Culture Index. Behaviour is assessed through a combination of specific observations and a broad judgement about each employee. In this

study, we collected for each employee evidence of bad behaviour the list of 43 bad behaviours. For good behaviour, we relied on a 360-degree assessment performed by colleagues against the list of 42 good behaviours.

With this behavioural data in place, a bank can use the Culture Index to score each employee between 0 and 100 against each behaviour (see Figure 1). A high score means the employee is well aligned with the culture of the organisation. A low score (below 50) means they're a potential risk, and a deeper analysis of their behaviour is needed. Importantly, because the index aggregates scores geometrically rather than arithmetically, it's harder to offset bad behaviour with good behaviour. Every employee's results are then aggregated throughout the organisation's structure. The Culture Index can thus be measured at any line of business, geography, legal entity, or department, and even at the organisational level.

The reason the Culture Index measures both good and bad behaviour is because our observations show that people displaying some good behaviour are less likely to behave badly, even if they're also displaying some bad behaviour. The index also gives different weights to different categories of behaviour. In this study we found it more appropriate to over-weight behaviour related to rigour/transparency and courage/discipline rather than behaviour related to business and client sustainability. Indeed, for this specific organisation, the focus at that time was on reinforcing the culture of controls and transparency and less about client sustainability and accountability. The weighting can, obviously, evolve as priorities change.

Even good employees sometimes display behaviours that fall short of expectations. So it's important to determine a threshold that sets the maximum level of misbehaviour that the organisation

Figure 1: Calculating the Culture Index

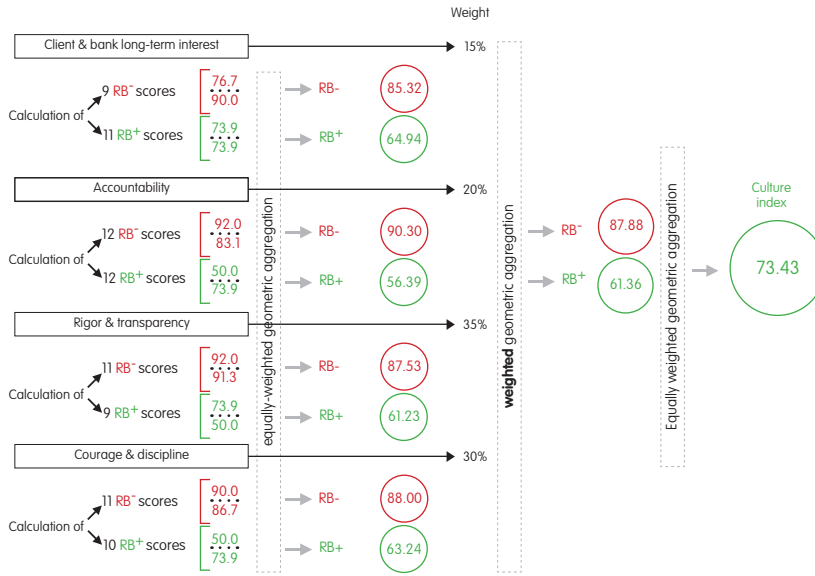


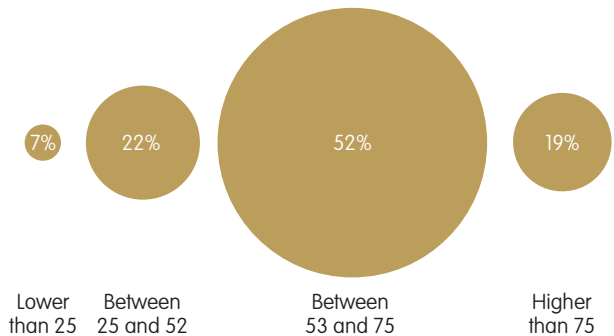
Chart legend
RB: Reference Behaviour
RB⁻: Negative Reference Behaviour
RB⁺: Positive Reference Behaviour

is willing to tolerate. Typically, this should be determined by a peer analysis (what is the average level of misbehaviour, and dispersion in behaviour, for a similar group of people?) and, more importantly, the appetite of the organisation to accept behaviour that falls short. Our observations have shown that, with time, a group inevitably deviates from what is expected of it. In other words, average misbehaviour increases over time, and a group's collective understanding of what is normal changes accordingly. So peer analyses on their own are not enough. Management must set the tone and periodically restate the appropriate threshold.

In this study, we measured the distribution of Culture Index scores for more than 150 sales employees and traders (see Figure

2). The results showed that the vast majority behaved as expected. However, misbehaviour was observed in 29% of those employees. But what did this really mean for their performance and that of the organisation? Had it had a negative impact? If so, what were the causes of this behaviour? Could we change it? This is where a more detailed analysis was required to better understand the impact and root causes of poor culture.

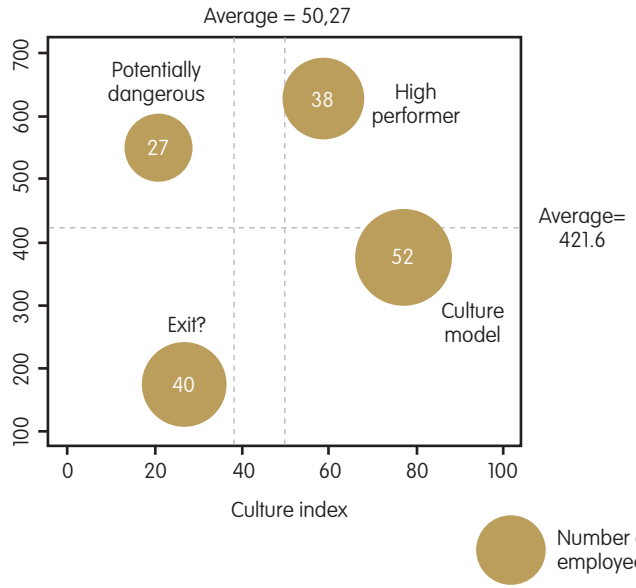
Figure 2: The Culture Index distribution



Understanding the root causes of poor culture

To get to the bottom of this apparent misbehaviour, we used a cluster methodology to group and analyse employees with similar characteristics along two axes: Culture Index and profits generated. This identified four main clusters, from 'high performers' (highest profits and above average Culture Index), through 'culture models' (highest Culture Index with average profits), 'potentially dangerous' (very strong profits but with a low Culture Index), and finally 'Exit?' (very low profits and low Culture Index).

Figure 3: Grouping the employees into four distinct clusters



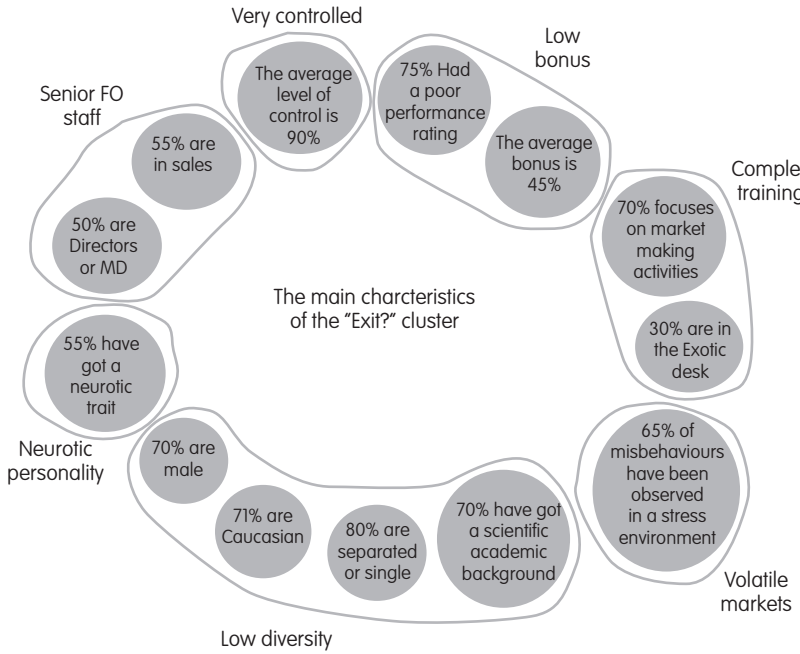
Balancing the development of a strong entrepreneurial spirit with a relatively risk-averse culture is always a challenge. In this analysis, 'high performers' seemed to have found the right balance and needed to be nurtured and rewarded accordingly. They are the role model. 'Culture models', on the other hand, appeared to have fully embraced the organisation's culture, but at the expense of lower profits. They do need some coaching to perform better.

The 'potentially dangerous' cluster represented a real risk for the bank. They were behaving relatively poorly overall, and yet they may well have been seen as role models by their peers (they were generating significant profits after all). If this cluster wasn't managed and coached effectively, their behaviour could well have escalated to more serious misconduct, with the potential for large fines and losses.

The last cluster, 'Exit?', was clearly the most concerning: these were poor revenue generators who were also behaving poorly. We decided a deep-dive analysis was necessary to better understand the root causes of their behaviour. To do so, we enriched the Culture Index and performance data with other factors that we believed could have had a direct or indirect impact on their conduct. We gathered HR data, such as remuneration, end-of-year performance ratings, seniority in the organisation, and personal situation. We asked the group to complete a psychometric survey to reveal individual personality traits. We compiled data on their business activities, including their department/desk, the type of activities they undertook (i.e. market making, proprietary trading, or agency), and the location of those activities. We also tried to capture the evolution of their behaviour the last year in the wider business and economic environment, in both 'stressed' environments (when financial markets are highly volatile) and 'normal' environments (when volatility is average). Finally, we categorised the quality and level of control exercised over their activities by measuring factors like the number and size of losses, the number of audit points, the number of resources dedicated to controls, and the results of any control assessments performed in the preceding year.

The results highlighted some revealing characteristics shared by the 'Exit?' cluster (see Figure 4). They tended to be very well controlled. They received a low bonus compared to their peers. They were often senior sales employees, but they were characterised by relatively low diversity: the group contained a high proportion of males, Caucasians, and employees with similar academic backgrounds. They performed relatively complex trading activities mostly focused on exotic products and market making activities, yet a relatively high proportion seemed to have some type of neurotic personality, and they tended to perform and behave poorly in stressed environments.

Figure 4: Root causes of bad performance and bad behaviour in the 'Exit?' cluster



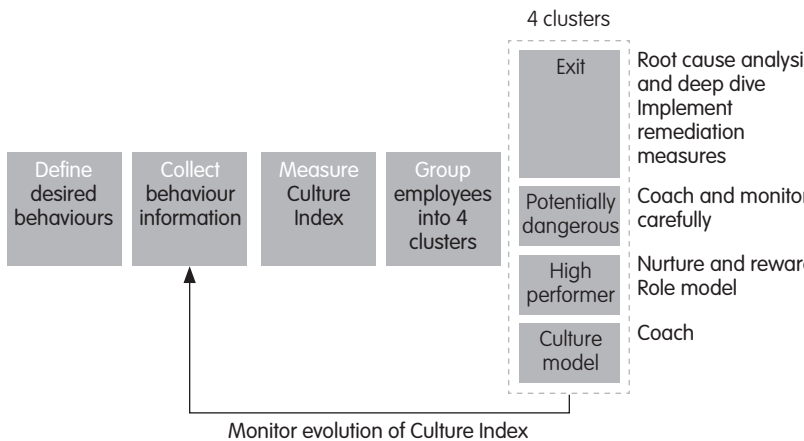
We supplemented this quantitative analysis with one-on-one interviews with members of the 'Exit?' cluster to reveal other factors driving their poor performance and behaviour. This exposed first and foremost a lack of accountability. Because these employees felt they were well controlled, they didn't feel a sufficiently strong individual need to take account of client interests or potential conflicts of interest. They had a false sense of protection, which reduced their sense of personal responsibility in developing a strong risk management culture themselves. This was reinforced by a complex management structure with multiple layers of responsibility. Members of this cluster were unclear who was really

in charge: the country lead, the global business lead, the region lead, or the group management?

They were also unclear about what the organisation really expected of them, and the level of tolerance in risks and controls that was acceptable. Very few could articulate the culture statement and expected behaviours of the organisation. Most felt they were incentivised to generate short-term results at the expense of long-term client and bank interests. They had the ability and the incentives to behave in the way they did. Some also felt that an overly dominant senior leadership led them to compromise their integrity and behaviour. They didn't believe they could really question or challenge decisions openly, and they had to follow the example from the top.

Our overall approach is summarised in Figure 5.

Figure 5: Overview of our four-step approach



Giving people a second chance: creating the right environment to improve culture

The truth is that a combination of various factors contribute to poor performance and poor behaviour. Sometimes it can be explained by an individual's personal situation and personality. For most, it comes down to the working environment. Our objective was therefore to create a different environment and allow the poor performers to show that they could improve.

To do this, we instigated a series of important changes. First, we recommended changing the leadership of certain key desks. We felt that the tone from the top wasn't strong enough, nor was it aligned with the bank's culture. These leaders were not only having a negative impact on their own teams, but also fostering the wrong kinds of behaviour more widely. They were a bad example for the broader population. In addition, we strengthened the proximity of management to employees. That meant putting the desk heads closer to their teams rather than leaving them isolated in their own offices; the principal objective being for desk heads to better understand the difficult decisions their teams were facing on a daily basis. We also created a new coaching and training programme focused on management skills. Most employees had a strong technical background, but many had a poor ability to understand the trade-offs for their business and the potential long-term impacts of their decisions on their clients, franchise, and organisation.

Furthermore, we reinforced the diversity of the desks. Because high-performing desks were characterised by a strong level of diversity in terms of gender, academic background, and race, we added new team members to include more women, more racial diversity, and more people with a non-scientific background. We also changed the reward system to reinforce the importance of

long-term performance versus short-term success. That included incorporating the Culture Index (along with a client satisfaction index for the sales team) in bonus scheme calculations and promotion decisions. Finally, some specific controls were put in place for situations of high market volatility. These included preventative controls to help traders and sales people avoid conflicts of interests with their clients.

Conclusion

These measures were well received by most of the traders and sales teams in the organisation. They felt, in particular, that they had helped clarify what was expected of them and had identified the key organisational weaknesses that needed to be fixed. It should be said, though, that it's still too early to make a definitive assessment of their effectiveness. Time, ultimately, will tell. What's most important now is to monitor how the organisation's Culture Index evolves, and correlate that evolution with the measures implemented. As we gather the necessary data over time, we are highly confident that the cluster methodology we set out in this article will prove to be a robust and effective means of changing banking culture for the better.

THE PANTRY
Sweetheart
TEA, COFFEE & LOVE
Sweetheart
Whittard
Exit

THE EAST INDIA COMPANY
CARAT
THE EAST INDIA COMPANY
THE EAST INDIA COMPANY

"Each individual within the enterprise has a unique intrinsic risk given their own attributes."

THE FUTURE OF CONTROLS SURVEILLANCE

By David Pogemiller, Forcepoint

Introduction

In today's environment, all firms, but especially those in the regulated industries, face increased risk from insiders. The risk continues to grow in frequency and scale as insiders are enabled by new technology and the rewards for successful intrusions are likewise becoming significantly higher.

This changing nature of insider risk poses significant threats to companies that may suffer from compliance failures. Their risks are both reputational and practical, and their senior management teams' risks are significant and personal.

On a reputational level, no firm wants to be known as the company that got breached. No firm wishes to have the same experience as Morgan Stanley – publicly condemned by the Securities and Exchange Commission for an insider breach.[1] Beyond the financial penalties, the damage to the corporate brand has costs that are often just as high yet difficult to quantify precisely.

Likewise, on a practical level, firms that fail to adequately manage insider risk face loss of business, fines and penalties, and

[1] Morgan Stanley SEC Penalty Criticised as Insufficient, https://www.secureworldexpo.com/industry-news/morgan-stanley-sec-penalty-insider-breach-criticised-insufficient

even existential risks. To cite but one example, the Visium hedge fund was once worth more than $8 billion. It imploded because of withdrawals, many of which were directly linked to rumours of insider misconduct (rumours that have since resulted in criminal charges).[2] In today's environment, even the mere hint of an insider trading scandal or data breach can be enough to destroy an industry giant.

Finally, the risks to individual managers are also increasingly significant. The challenges take two forms: at an internal level, firm managers face increased scrutiny relating to their success (or failure) in mitigating insider threats. Often their salaries, bonuses, and even employment are dependent on success. Conversely, from an external perspective, a manager's failure to implement an effective insider threat programme can result in personal liability, which can lead to fines and even jail.[3]

This chapter aims to paint a picture of the future of controls surveillance and how it is responding to the novel risk challenges facing enterprises. We begin by expanding on how we perceive the insider threat to be changing. We then examine the trends that are enhancing the ability of firms to manage and control insider risk (many of them closely related to the trends that enable the threat); and this brief chapter then concludes with a proscriptive description of an idealised holistic insider threat programme.

[2] Rachel Levy, Wall Street Has Been Rocked by $8 Billion Hedge Fund Implosion, www.businessinsider.com/visium-asset-management-closure-rocks-wall-street-2016-6

[3] Several recent instances of American enforcement actions against individual compliance officers are recounted in http://fcpacompliancereport.com/2016/05/close-personal-individual-cco-liability-part
The United Kingdom has a senior managers regime that, likewise, puts managers at personal risk. www.nortonrosefulbright.com/knowledge/publications/122774/criminal-liability-for-senior-bankers

The Changing Nature of Insider Risk

Incidents of insider breach are increasing both in frequency and in magnitude. Why? What factors are contributing to this transformation?

From our perspective, the change is the product of a combination of several factors: social constructs; greater opportunity enabled by technology; and greater economic necessity arising from an uncertain economy. Taken together, these factors are driving a significant change in insider behaviour.

First, let us offer a bit of a theoretical introduction to the problem. Not all insiders are created equal. They differ in motivation; in capability; and in consequence. We have taken to characterising insider threats as falling into three relatively distinct groups (or, if you will, flavours). There are the 'good' employees – these are well-intentioned people who at times may make sloppy or negligent mistakes; the 'tempted' employees, who make decisions every day not to break the rules, but who can be tempted by stress or opportunity; and there are the 'bad' employees who have a malicious intent that can be identified and discovered.

Our view, derived in part from the analysis of Nobel Prize-winning economist Gary Becker,[4] is that people will engage in purposefully bad conduct when the expected benefits to them exceed the expected costs. We use the term 'expected' in this context to incorporate probability estimates of an outcome. For example, the threat of imprisonment might be discounted by the anticipated likelihood of getting caught. Or an individual might ask what the chances are that a theft will net more than $1 million? To express this in a formulaic way, we begin with the assumption that

[4] The most famous early exposition of these ideas is Gary S. Becker, Crime and Punishment: An Economic Approach (1974), https://www.nber.org/chapters/c3625.pdf

a 'tempted' bad actor will consider the cost of the action, the value of the action, the costs of capture, and the risk of capture. When the utility of the action outweighs the disutility of capture, people start to give in to temptation. The sad reality today is that many of these valuation factors are changing in ways that tilt the balance increasingly toward the 'bad' and away from the 'good'.

We assess that change along three axes. An economic climate that is driving temptation; there is a greater opportunity to monetise intellectual property theft, driven in part by technological change; and that same change gives potentially bad actors a greater capability to execute a theft, capabilities that, a few short years ago were much less robust.

Consider first the changing economic climate. No matter how you characterise the economy, it seems undeniable that the last ten years (roughly) have seen a substantially increased constraint on economic success within the financial market. Firms are asking increasingly searching questions about where to find return. The economic downturn, from which we are only now recovering, has put businesses and business executives under great pressure to find higher returns, both for their investors and for their own institutions, yet they are elusive.

This harsh reality is exacerbated by a regulatory environment that is changing in a way that stresses budgets, requiring increases in compliance spending. Significant pressures exist to short-cut compliance measures, making 'bad' actors more likely to succeed.

Meanwhile, financial institutions are systematically reducing employee counts as well as the compensation or bonuses for the employees they retain. In short, that same downturn has had a direct effect on the bottom line for many employees. Some have lost their jobs and others are poorer, even though they remain employed. Uncertainties like this create personal incentives for malicious financial adventurism.

Finally, building on the previous two factors, there is a general sense of uncertainty or, if you prefer, volatility in the industry. Employees, even those who have good prospects, are not convinced that their situation is durable and stable. All of which leads to financial and psychological strains on people that erode the barriers against bad behaviour and allow the 'tempted' to become the 'bad'.

The temptation to go 'bad' is married to technological developments that make it easier to profit from doing so. For example, the Dark Web provides greater opportunity to succeed and to profit from malicious activity. By functioning as a marketplace where one can sell stolen data without consequence, the Dark Web serves as enticement to action.

One can also directly use stolen information to personal benefit in these dark spaces of the network. Here, malicious actors have new (harder to trace) ways of placing orders and taking advantage of insider information by trading ahead in the markets. The Dark Web also helps a potentially bad actor figure out how to accomplish his or her goal. Sophisticated actors on the Dark Web teach newbie, unsophisticated insiders what to do and how to do it. New entrants to the criminal realm can receive instruction and tools to assist in learning how to exfiltrate information, identifying what information is of greatest value and determining how to cover their tracks to avoid capture. These 'skills' reduce the possible costs of malicious insider activity while increasing the possible benefits.

Finally, technological transformation in the financial industry has given potential inside actors greater purchase, if you will, on their ability to engage in theft. They are better able to execute their schemes because the target of their attack has systematically become softer. Consider that, today, all data is now digital and can be readily accessed and moved en masse. Data that, ten years ago, would have required boxloads of paper now fits on a pocket-size USB and can be stolen in minutes. Meanwhile, user interfaces are

simpler, making it easier for less sophisticated people to operate software and manipulate data to their advantage. The same digital improvements that foster efficiency and interconnectedness for the enterprise are also the seeds of its undoing.

In short, the insider threat is growing because economic pressures to act are increasing, because technologies like the Dark Web provide better tools and monetisation for malicious actors and because the systematic growth of firm efficiency enables criminal efficiency in concert. No wonder many think the prospect of insider threat mitigation is grim.

Technological and Analytic Opportunity

Notwithstanding the increased risk from insider threats, the current environment also allows greater possibilities for discovering and defusing insider threats before they occur. In the national security context, it is sometimes said that we live in a 'golden age' of surveillance capabilities. The corporate world can seize a similar opportunity, if surveillance techniques and analytic capabilities are properly applied. The improvement in capability is driven by two factors – one a matter of sociology, the other a matter of technology and technique.

First and foremost, insider threat systems are benefitting from an influx of talent from the national security and law enforcement domains. These new entrants bring with them a holistic view of insider threat surveillance – one that marries new technology with better analytics and a greater understanding of how to assess an overall threat environment. In short, not only do they understand the threat stream but they have experience dealing with it in the high-stakes situations of national security and intelligence investigations.

These new entrants bring with them an improved skill set that benefits the industry. Many have high-level mathematics

skills, enabling superior analysis; others are able to conceive of and develop higher fidelity and more accurate sensors for data collection; and still others are sophisticated analysts – consumers of data who tease out signals of aberrant behaviour. Subject matter experts in all of these areas are rapidly moving from government roles to the controls and compliance area. In part because of their prior experience and in part because of enterprise needs, we are now seeing the professionalisation of control and compliance employees – they are increasingly dedicated to a mission objective and pursue it with vigour.

The other driver of change in the control and compliance field is, of course, technology – in many cases the same technology that enables greater threats also enables a better response. The insider threat field is systematically experiencing technological innovations that enable more efficient and effective surveillance.

First among these changes is the growth in relevant and accessible big data sets. Increasingly, compliance officers have more robust data from which to derive analysis. In fact, many often consider the data available to those in security and compliance to be the richest within the enterprise. The growth is derived from two significant factors: more sensors and fewer silos.

Today, data is richer and comes from more sources than ever. Where compliance systems used to be limited (often, for example, restricted to telecommunications data sets), now their data sets are much more varied. Today's control system will typically review all forms of electronic communication and supplement that information with physical location data and robust interaction information with other individuals in social networks. In effect, one can now observe nearly all aspects of employee activity through the enterprise's digital exhaust.

At the same time, more data is being held in fewer disparate silos.

Instead, modern data aggregation systems are able to house diverse types of data in larger systems. Fewer silos means less work making connections. Data is now collected and stored in central repositories (often called 'data lakes'), making synthesis and analysis easier.

Meanwhile, the total cost of ownership for data storage systems continues to go down. It isn't just that computing power and storage capacity are more readily available – at such low cost they are far more widely accessible. The cost of big data has been so effectively democratised that even the smallest of organisations can afford it.

All the data in the world would be of little use if the capability to analyse it were not up to the task. Happily, technology is also improving in a way that empowers data analysis. Along with better data, sensors compliance and control systems now have, simply put, more computing power. Raw processing speed and power continues to grow (albeit with a slight slowdown from Moore's law), and increasing use of elastic compute within the cloud further pushes the boundaries. Greater processing power means more complex analytics and more data processing capacity.

The analytic capability revolution enabled by computing power is really where surveillance systems' see change is occurring. It is no longer sufficient for an enterprise to conduct threat identification using only basic threshold types of analysis (i.e. 'if someone does more than x of this' or 'if a trade is x% larger than') to identify aberrant behaviour. Analytic systems are capable of a great deal more:

- Anomaly detection through 'baseline' analytics – both for a person and relative to peers – can identify individual deviations from personal norms to discover potentially non-compliant activity.
- Commonly available natural language processing can effectively 'understand' unstructured content such as communications and files with a high degree of accuracy.

- Sentiment analysis can also be applied to communications to understand whether an employee is happy, sad, calm or angry. This type of sentiment analysis is of significant value in assessing risk.
- Even without accessing employee social networks outside of the enterprise, network analysis allows assessment of connections within a corporation. It is now possible to identify thought leaders, social drivers and isolated individuals who might be at greater risk of becoming insider threats.
- Finally, all of these systems improve with use. Contemporary analytics allow for machine learning so that analytic programmes get 'smarter' with the passage of time and the benefit of human judgement smartly captured within intuitive workflows.

Not only are the analytic tools improving, so are their users. The control and compliance field benefits from a growing cadre of analysts who are familiar with these tools and have the sophisticated experience to apply them to compliance problems. There is a larger pool of well-trained and experienced data scientists who know how to get and use data and conduct thoughtful analysis.

Indeed, the discipline is so well entrenched that commonly used/accepted/understood analytic packages are now 'meat and potatoes' to data scientists (a field that simply didn't exist a few short years ago). A broad community has been trained on these packages and has used them since 'college'. By way of example, the field of natural language processing is now so robust that Stanford has a series of YouTube videos available for general consumption as part of its educational library.

Taken together, this combination of factors – more data, more sensors, fewer silos and game-changing analytical methods – are driving a near revolution in our ability to

actually synthesise data. The bar is no longer set at the basic collection and searchability of data. Instead, today's systems are allowing compliance teams to take all of the newly analysed data and integrate it in a fusion layer that effectively synthesises massive streams of information into actionable intelligence.

The Future of Holistic Surveillance

What's next? Looking at growing threats, how should a regulated enterprise develop a response? Here we offer a few thoughts on how best to use new control and compliance capabilities to foster enterprise security.

To begin with, our objective is to implement a holistic approach to surveillance enabled by better technology and a better understanding of how to characterise employees. This allows an enterprise to hire, retain, and develop employees who aid in advancing the enterprise's goals.

But that requires the right technology. Successful surveillance systems must be capable of synthesising all raw person-centric data signals (i.e. communications, physical, transactional, and systems/digital) and incorporating external value-added information to enable rapid discovery of bad actors and empower analysts to quickly investigate and inquire. Holistic surveillance systems recognise that the fusion layer is not a 'bolt on' on top of existing systems. Rather, when properly developed and deployed, they deeply integrate best-of-breed solutions from various previously siloed disciplines, such as trade analytics, e-communications surveillance, voice surveillance and the like. Well-developed technology can also readily incorporate new, innovative techniques as they come online.

Second, this is more than a raw technology problem. The human element is a crucial component; employees are not random collections of people. As such, an enterprise can and should develop

an understanding of each individual as the sum of their complex history, background and nature. Their motivations, capabilities and responses to authority all vary based on individualised attributes. A 'malicious insider' is different from a 'disaffected activist' and both differ from a 'disgruntled manager'.

Each individual within the enterprise has a unique intrinsic risk given their own attributes: what is their role, what information and systems do they have access to, what is their tenure, have they received a good or bad performance review, are they ahead or behind on their portfolio, have they been passed up for promotion, and so on. A full picture allows compliance and control systems to more effectively target surveillance efforts and assess each individual's behaviour in context.

Third, ensure that the programme is implemented within ethical guidelines. While surveillance in the workplace is now essential, if it is done wrong it will backfire. In our experience, an ethical surveillance programme meets five distinct requirements. It is: 1) transparent to employees, 2) surgical in focus, 3) demonstrably intelligent in design, 4) responsible in implementation and 5) above all, lawful (you would be surprised at how some programmes fail to meet this requirement).

Fourth, a continual assessment of outcomes versus goals and progress against that assessment is critical. Systems of this sort either evolve over time or quickly become ineffective and detrimental. They evolve technically as new sensors and data sources are adopted; they evolve analytically as existing techniques are improved and new analytics are developed; they evolve systematically as a better understanding of employee behaviour is dynamically adapted in the face of social, regulatory, legal and ethical change; and, most importantly, they evolve as your organisation does.

Fifth, a holistic system cannot be independent of the context in which it operates. Rather, it leverages the experience and network

effects of other, similarly situated analytic systems in the industry. As discussed more generally in Chapter Six of this book, cross-community collaboration can be effective when the collaborators share a common purpose and have similar non-competitive, proprietary interests. Enhanced effective surveillance is one of those areas where, we submit, there are quantifiable benefits to all participants.

Finally, and most importantly, all of the preceding information is a foundation for engaging your employees and your corporate culture. All the technology in the world is worthless if the enterprise does not create a culture of compliance – doing the right thing because your people want to, not because they have to. Two components to creating that culture are essential:

- First, define the mission of the enterprise in a way that incorporates compliance and good governance. Culture begins at the top of the hierarchy with a commitment from senior level management.
- Second, drive the mission and culture home on a routine basis. Engage employees on the day-to-day experience. For example, when something happens out of the norm, allow the employees to participate in the resolution. Ask them 'was this you ...?' or 'is this right?' Make compliance a daily experience, not a once-per-year PowerPoint check box exercise.

Conclusion

Bob Dylan sang 'the times they are a changing' more as a mournful remembrance of times past than in happy anticipation of a brighter future. At times, enterprises faced with the morphing insider threat seem to adopt an almost Dylan-esque wistfulness about a time when threats were simpler and the systems for ensuring compliance and control were also less complex.

Whether for good or ill, those times now lie behind us. In any regulated community the insider threat is growing, empowered by both social and technological change. But those same factors also enable new compliance and control systems that significantly mitigate the threat. Any enterprise that fails to grow and adapt to this new reality – the reality of a need for holistic surveillance that synthesises native data and value-added components – runs reputational and possibly even existential risks. The future of controls surveillance is now.

ONE WAY
5 AV

PASSENGER
CARS ONLY

"If you don't look ahead, how can you possibly anticipate changes in risk and implement preventative measures to mitigate the risk of causing harm to your customers and stakeholders?"

EMERGING CONDUCT THEMES

By David Long & Charanpal Matharu,
Pall Mall Risk Reduction

The Financial Conduct Authority acknowledged in its FCA Outlook for 2013 that addressing conduct risk was not something that could be implemented overnight by introducing dashboards or implementing remediation plans to address historical events. Rather, the FCA outlined a vision of a journey to be taken by the industry over several years, the progress of which would be monitored closely by the regulator. The FCA Outlook for 2013 also specifically prescribed the requirement for banks to identify and address emerging conduct risks.

For a number of years now, since the formation of the FCA, the banking industry has ploughed a significant amount of time, resources and money into addressing instances of conduct risk. However, as we have seen all too often, those organisations that have not demonstrated sufficient progress have been handed severe penalties.

The Need for a Proactive Approach

The sheer volume of S166 Skilled Independent Persons' Reports, Enforcement Actions and Thematic Reviews issued by the FCA have all directed the industry towards better business practice. With hindsight, it would be easy to argue that banks did not anticipate

the scale of the task ahead, and that they were insufficiently prepared to address conduct risk proactively.

The industry has found itself on the back foot in reacting to regulatory findings, industry reviews, and also internal instances of conduct risk. Banks have employed individuals, in some cases in scale, to address the root causes of the instances of conduct risk with substantial remediation plans. This has often been described as the rear-view mirror approach, analogous to the fact that individuals would not drive a car in a forward direction by solely looking in their rear-view mirror. In addition, working on specific solutions such as benchmark indexes (LIBOR and FX) could mean that the risks have been addressed in isolation. Also, let us not forget the employees working on remediation plans, in that they are sometimes working on addressing conduct risk in addition to their usual roles and responsibilities. They may be exasperated about implementing fixes, sometimes tactical in nature, as opposed to addressing the underlying risk.

For a moment, let us assume a healthy scepticism to this theoretical comparison and question why we need a proactive approach.

Let us also recap on how we define conduct risk. There may be variations in the definition of conduct risk across different organisations, but arguably the core definition is that of the risk of causing detriment (either financial or non-financial) to your customers, and your stakeholders, which includes both the markets and industry that you operate in, the shareholders, regulators and more broadly the community that banks serve, which rely heavily on the services that they provide.

If an organisation only looks back at instances of conduct risk this is likely to mean that it is never in control of the risks that it faces. Addressing historic events means that the detriment has occurred; it is now too late to implement preventative measures

and the damage has been done. The bank's reputation has been damaged, its customers and its stakeholders have suffered, and employees may be subject to employer and regulatory sanctions. The bank is likely to incur a penalty and capital buffers, which will restrict its ability to earn revenue.

If you don't look ahead, how can you possibly anticipate changes in risk and implement preventative measures to mitigate the risk of causing harm to your customers and stakeholders?

Now back to our driving analogy; if we were to add changing conditions such as a twisty road, fog or ice, it would then be natural for a driver to take precautions, perhaps by slowing down and switching on his or her fog lights. Whilst banks look at historic events, often at the request of regulators, they need ensure that they look ahead to identify emerging conduct risks and implement preventative measures.

The Financial Cost

Secondly, there is the financial cost to the banks of the failure to address conduct risk. According to the Conduct Cost Project,[1] the total cost over the last five years to the twenty large global banks was £264 billion, which included regulatory fines, litigation costs and provisions. Mark Carney, Governor of the Bank of England, pointed out in a speech at the Banking Standards Board Panel that bank capital lost to fines could otherwise have supported up to $5 trillion of lending to households and businesses.[2]

The Social Cost

Thirdly, it is important to recognise that there is a social cost. In order to operate, banks need a social licence in addition to their regulatory licence.[3] The social licence is granted by the public,

which is the right to operate in society and is given as long as banks act responsibly. In practice, a social licence is not restricted just to banks, but all corporations. A failure by a bank to conduct itself appropriately, not behaving well in the eyes of the public, will result in society questioning its right to continue to operate. Looking back to the 1980s, a clear example of this occurred with Barclays Bank, which had invested heavily in South Africa at the time of apartheid. University students voted with their feet and boycotted the bank's student accounts.

Having now firmly established the need to be proactive in spotting emerging conduct risks, we now look at mechanisms for how best to achieve this. The most straightforward, obvious way is to keep aware of issues that may currently exist, or anticipate those that could be emerging, by keeping our 'antennae' up. This is achieved in a relatively simple manner, such as discussing themes and trends both with our fellow employees and industry peers. Indeed, many of the following examples have been gathered in this way. The advantage of forming a sense of emerging trends in association with a peer group is the opportunity this gives to learn from a wider group of practices and experiences. It also enables someone to think outside the normal frame of reference of an employer (their own bank), and therefore avoid dismissal such as 'that could not possibly happen here'.

The power of groups and teams to both question and challenge and then arrive at better outcomes than an individual is both obvious and well documented. There is also a more robust route to determining emerging conduct themes, used by Roger Miles' Behavioural Lens approach,[4] which is outlined later in this chapter. This form of horizon scanning is extremely valuable to determining emerging conduct themes.

Let us start by looking at the current inventory of the themes that we have discussed and reviewed with industry peers. Together,

these conduct risks have been validated and they should be considered and addressed before they crystallise into instances of conduct risk.

Emerging Theme 1: New Communication Technologies

Banks have long-standing policies on communication, but most have retained a frame of reference to a time before the proliferation of social media. Furthermore, the social media apps that we use today are rapidly refreshed and replaced by newer platforms. Banks are also largely yet to solve what is referred to as the 'WhatsApp challenge', which is how to control the use of encrypted social media platforms. The UK regulator has already alerted us to this problem, when in March 2017, the Financial Conduct Authority fined an investment banker for sharing confidential client information via WhatsApp.[5]

The industry has yet to form a consensus on an appropriate policy to implement that would address these challenges. According to one September 2017 survey,[6] fewer than half had formal written social media policies for employees to follow. Some banks have banned the use of mobile phones altogether on the trading floor. At least one other bank has banned the use of personal devices and instead supplied staff with mobile phones installed with technology that limits the availability of apps when on the floor. It should also be noted that banks supplying mobile phones to trading floor staff are contrary to the now common practice requiring staff to use their own personal devices, which was established to save costs. Until the development of new technologies, it may be appropriate to evaluate the risk and consider the need to reverse this as an industry in order to lock down the technology available on the trading floor.

Of course, the flaw with all these controls designed to protect the integrity of communications on the trading floor is that they can be easily circumvented by simply stepping off the floor to make the call or send the message. This raises the question of whether there is a boundary for banks, and if so where is that boundary? Is it restricted to the trading floor, or would it be in line with other policies that consider the conduct of an individual outside the workplace as well?

Banks are also taking different approaches to the social media platforms themselves. Many banks report that they have blocked certain specific platforms, for example, Twitter. It then becomes difficult to reconcile this with the need to access social media platforms that banks have themselves employed. There is no doubt that this will become increasingly challenging. There is much valuable information available for traders on Twitter, to the extent that it is now a force in the world of finance, with studies finding correlations between tweets and financial markets.[8] Chinese economic data is officially released via the WeChat app,[7] which is a ubiquitous social media platform in China. So, in summary, trading floor staff have become reliant on consuming data from social media.

The situation when staff post comments on social media may be more ambiguous. The question for us to consider is whether or not such comments represent the firm. An employee's comments on Facebook expose the bank to both conduct risk and reputational risk. In some corners, it may be considered that staff are not representing their bank unless they mention the name of their institution, or otherwise purport to represent it. Other organisations consider personal social media could be indicative of the bank.

Individuals in the front office receive conduct risk training. This should make those staff aware of the risks involved with making

comments on social media, and at least act as a helpful start in attempting to ensure that such comments are within acceptable levels of conduct. However, there are many staff beyond the front office, and as yet, the focus on conduct risk training has not been on them. How are these staff currently using social media, how are they getting their information on acceptable practices? To conclude this section on communication technology, we can summarise the themes as:

- Social media contains information that front office staff need to access in order to successfully perform their roles.
- Policies on the use of social media, to the extent that they exist, need to keep up with the changes in technology, trends and usage. These policies should also be reviewed and refreshed more frequently than what would be the norm for other policies.
- Staff need to be continually trained on social media and new technologies for conduct risk and reputational risk, and also to consider the risk of cyber threats from these new technologies. Conduct risk training should be extended to all staff, beyond the front office.

Emerging Theme 2: Growth in Electronic and Algo Trading

Banks have experienced a dramatic change in the pace and scale of electronic trade flow, with algorithmic (algo) trading being at the forefront of growth over recent years. A 2017 FX survey suggested that 78% of an institutional trader's volume would be conducted electronically, with 12% being executed via algos.[9] On the sell side, within banks, the algo penetration is even higher. Anecdotally, flow in G10 spot FX at major FX banks is reported as being predominantly executed by algo. The question this raises for our introspection on

conduct risk is: what new risks does this bring? The first point to note is that electronic and algo trading needs to be brought fully into the conduct risk framework. There is a current need to have the second line of defence (2LOD) algo trading departments and functions following the same behaviour and conduct processes and operations as that for the general front office. We need to ensure that there is sufficient first line of defence control over the algos. The algos are machines executing transactions requested by users. However, the algos are programmed by technologists, who obviously introduce risks into the system. We need to examine how those algo programmers are trained in conduct risk matters, how they are supervised and how we monitor the effectiveness of their actions that could give rise to conduct risk. In addition, these business lines frequently have employees that have high degrees of access to trading systems and the nature of this trading means that a competitive edge has required higher levels of confidentiality. These areas would benefit from openly demonstrating how they address and mitigate conduct risk.

The broader observation here is the range of staff within the organisation that receives conduct risk training. This needs to be expanded beyond the current scope, which is usually restricted to front office. For example, quants, risk, operations, technology, and middle office functions should all be subject to conduct risk training as well. Most importantly, compliance should be fully engaged in processes, which would include the design and operating model of algos. This requires having appropriately qualified staff who can effectively review and challenge.

Having ensured that all the staff involved in the algo creation process are suitably trained and aware of conduct risk, we also need to ensure that there is adequate second line of defence understanding too, in order that they can provide the satisfactory

challenge and control necessary in this arena.

Secondly, we should be mindful of who exactly has access to the algos (and eTrading in general). There is obviously potential for great damage to be done via algos, and this could be caused accidentally, as in the case of the demise of Knight Capital,[10] maliciously as an act of sabotage, or even from a new-style 'Algo Rogue Trader'. Front office staff are registered with the FCA, and are subject to background checks and continuous screening. Human resources plays a large part in the selection and screening of front office staff. Where exactly are the staff who run the algos? Are the algo staff subject to similar scrutiny by HR? Many sensitive employees are no longer based on the trading floor. Are they in IT? Do they work offshore? Are they working from home right now running the algo? Are we sure we even know these staff? Do they even work for the bank or are they part of the significant IT outsourcing that the industry has undertaken? Is there even the possibility that the person running our algo is at a company that the bank has no relationship with at all, but has been outsourced by the firm we have outsourced to – surely not! There would appear to be a prima facie case for co-locating the algo processes, from design through operation, with the front office to ensure that common standards of conduct are understood and applied, but needless to say, this should be applied to all risks.

Thirdly, an additional layer of complexity of algo trading is the new element of social media use in algos. Data from social media is used as an input to automated, high-frequency algo trading. Feeds of data are taken from social media platforms such as Twitter, Facebook and LinkedIn and used by the algos as a basis for their trading strategy and execution patterns. We need to consider how we control and supervise the data being used. Conduct risk is defined as actions and behaviours, or conduct of business, that

can cause harm to clients, cause the firm reputational damage or risk undermining the integrity of the financial markets.[11] With the magnifying effect of algo trading due to speed and automation, does fake news now have the propensity to alter prices and trading patterns via the algos at levels never previously observed? How would the actions of our algos be judged? The Financial Conduct Authority CEO Andrew Bailey has expressed his views on algos recently: 'It's very important to focus on how algos are used. It's one thing having a badly programmed algo. I think from experience a bigger issue is the inappropriate use of algos.'[12]

Finally, banks have already found issues with algos that have resulted in actions that have comprised clients in relation to the directive of treating customers fairly.[13] The new element here is that these conduct actions are now written into the code of the algo, and not only can they potentially cause harm, but they are also discoverable.

So, the task for banks is to create an inventory of all their algos, classifying them by purpose; for example, whether they are for market making or routing orders. Then a detailed code review should be undertaken to i) consider conduct and ethical requirement, ii) test how they behave in various conditions, and iii) implement an appropriate surveillance programme. In other words, algos should be treated as if they were humans, monitoring them to ensure we know what they are doing and that it is acceptable behaviour. In the event that there are deviations from the expected outcomes these should be subject to a governance review programme that understands the course of events and incorporates modifications, as deemed necessary.

Emerging Theme 3: Use of Data

The final emerging theme for us to think about in this chapter is the way banks use data. Theme 2 highlighted that social media data is already used in bank algos. Taking data and drawing out information from it – performing correlation analyses for example when looking to spot patterns in trading or markets – is something that banks would find very useful. Such an example could include highlighting when a particular event or action occurs, and reviewing the subsequent correlated transactions or market movements. If the data analysed is publicly available, then presumably banks have the same ability as all market participants to take that data into account.

There needs to be an awareness of situations where the use of such data creates an asymmetry of information. For example, where the situation becomes less clear is if banks were to perform such analyses on data to which only they have access. There is a lot of internally available data for banks, the question is whether it is acceptable and indeed ethical to analyse and use this internal data. What about client data? Banks may have custody data of a client or market participant, which potentially shows the position of the customer or counterpart. Transaction history data can highlight trading patterns, such as regularly occurring transactions, or the profitability of trades – their winning nature. Use of such data in an algo could allow a bank to guess the likelihood of the transaction requested by the customer to be a buy or sell. It could allow the algo to 'trade along' with perceived customer winning strategies. The FX Global Code[14] contains useful guidance on this matter, instructing that access to such confidential information should be limited. It requires that confidential information should not be disclosed, including to internal parties, except to those who have a valid reason. It also explains that confidential information obtained

from a client or prospective client is only to be used for the specific purpose for which it was given.

Banks should examine the controls that they currently have in place to monitor and address these issues. They should review the governance around data and data groups. The banks need to have self-awareness of their data usage cases and demonstrate that it is in line with regulations, guidelines and best practice.

The Behavioural Lens

Having noted some of the emerging conduct themes within the industry, it would be appropriate to return to the Behavioural Lens approach as outlined by Roger Miles.[4]

Capturing Emerging Conduct Risk Themes

Conduct risk has proven to be highly dynamic and upon discovery the magnitude of an issue often crystallises into a larger issue that has on more than one occasion involved several individuals and sometimes reached across many organisations.

Banks would benefit from having a dynamic inventory of emerging conduct themes. Existing processes, such as governance forums (new business, reputational risk reviews, product reviews and conduct risk working groups) should be reviewed and enhanced to both adequately consider and capture emerging conduct risk themes.

Other sources of information such as regulatory reviews, industry findings and peer group forums should also feed into this inventory.

The Behavioural Lens should be added to the toolbox in order to assist creating and maintaining such an inventory. At this point it is also important to recognise that the public perception

of these risks has a direct impact on the bank's social licence.[16] The crystallisation of these risks will raise public alarm in five different factors:

LOAD	There is an imposed **LOAD**, for which there is no personal control
NEW	There is a **NEW** aspect and its workings are not understood and is considered to be game-changing
DREAD	It feels scary, causes disruption, which leads to **DREAD**
FAIR	It may not feel **FAIR**, as it is unclear who benefits. It could also imply a 'cover-up' for an alternative motive
SOCIAL	There is a **SOCIAL** impact. 'Normal people' are adversely affected and disagree with the action

Therefore, the task for banks is to continually frame their questioning around these five factors:[17]

- **LOAD**: Are you gaining a volume, a presence, a dependency or significant exposure? Are you denying control to others? Could it be perceived that you are denying control to others?
- **NEW**: What aspects are new? Are there new systems and/or products? Who is watching now?
- **DREAD**: Could you be causing alarm and/or fear to your stakeholders, which includes your own employees? Could you be accused of changing the game around them without their buy in?
- **FAIR**: Is it fair? Who carries the burden and who is rewarded with the benefit?
- **SOCIAL**: Do customers and regulators approve of your approach? How do your customers benefit? Fundamentally, is it socially acceptable?

Now to see the usefulness of this approach, the Behavioural Lens[4] is applied to the emerging conduct risk themes that we have identified:

Emerging Theme 1: New Communication Technologies

LOAD: *Are we gaining volume/presence/dependency/exposure? Are we denying control to others?*
Yes. Social media is becoming ever more prevalent in banks. Banks also use the data and technologies themselves, as we described, Chinese economic data is officially released via the WeChat app.[7]

NEW: *Are we using new systems/products? Who is watching now?*
Yes. The new element is the direct integration of social media and its data feeding into trading decisions. New communication systems and technologies are being rapidly implemented.

DREAD: *Are we alarming anyone (including our own people)? Are we changing the game?*

Yes, as discussed in this paper, the use of social media and the inability to align controls to other forms of communication provided by the banks, such as dealerboards or mobile telephones, causes alarm.
The WhatsApp challenge (encrypted communications) presents another significant challenge.
The inability to control the risk of inappropriate posts on social media platforms causes alarm as it could damage the bank's reputation and unnecessarily expose it to conduct risk.
The DREAD is that currently there is an absence of being able to control these risks.

Emerging Theme 2: Growth in Electronic and Algo Trading

LOAD: *Are we gaining volume/presence/dependency/exposure? Are we denying control to others?*
Yes, algo and automated e-trading trading is prevalent, continues to grow and in some instances now forms the overwhelming majority of all transactions. Banks have become dependent upon it as it operates at a speed that humans cannot replicate.

NEW: *Are we using new systems/products? Who is watching now?*
Yes, new systems are delivering different mechanisms to trade products. There has been rapid growth and some of these systems may not have the transparency of traditional click and deal methods.

DREAD: *Are we alarming anyone (including our own people)? Are we changing the game?*
Yes, employees (your own people) may feel lack of clarity.

The competitive edge of algo trading has often been the secretive code that seeks to identify trading opportunities. The competitive edge of automated e-trading lies in the speed of transacting within milliseconds. The underlying data associated with algos and automated e-trading provides banks with an opportunity to use that information for its own competitive advantage, trading ahead of customer transactions. Banks could utilise this data for their own gain. However, banks could overcome this DREAD by openly demonstrating their compliance and best practices with conduct rules.

The geographical fragmentation of staff to support algo and automated e-trading, due to offshoring and outsourcing presents a number of risks (conduct risk, cyber risk, staff not appropriately

qualified and so forth). Collectively, this presents the risk that banks can no longer manage these individual risks unless they are in close proximity of each other. Instead reliance is placed upon individuals, which in some cases are not even employees of the bank.

Banks could overcome this DREAD by reviewing their operations and evaluating the benefits of cost-saving strategies against these emerging risks.

Emerging Theme 3: Use of Data

LOAD: *Are we gaining volume/presence/dependency/exposure? Are we denying control to others?*
Yes. The use of internal confidential data is growing. Banks are increasingly looking at Big Data initiatives, in many cases to seek revenue opportunities.

NEW: *Are we using new systems/products? Who is watching now?*
Yes, new systems are being developed to use data in innovative ways.

DREAD: *Are we alarming anyone (including our own people)? Are we changing the game?*
Yes, as discussed in this chapter, employees may feel a lack of clarity over the use of data. The use of data would need to consider reputational risk, conduct risk and ethical risks.

Banks can also expect that its employees use innovation to seek new ways to monetise the use of data.

FAIR: *Who is bearing our risks and who benefits?*
Banks could take the information from transactional data and use it to their advantage.

Banks could essentially benefit from the burden (the risks) taken by customers.

It can see that the Behavioural Lens approach flags themes worthy of inclusion in the inventory of emerging conduct themes.

Conclusion and Summary

Addressing Historic Issues

Conduct risks have proven to be very dynamic, and have often quickly materialised into issues that have required regulatory investigation. Whilst addressing conduct risk was spearheaded by the FCA, it has now been firmly established on the agenda of the other regulators.

Whilst banks have frequently employed significant resources to address these issues through the implementation of remediation plans, as previously discussed, this has been a rear-view mirror approach to addressing conduct risk.

Little or no resource has been dedicated to emerging conduct risks, despite its very dynamic nature. As a result, penal sanctions have been subsequently applied by regulators globally.

There is no ambiguity that the conduct risk agenda has been firmly established and further issues may materialise in the foreseeable future.

Implementing Conduct Risk Frameworks

Some banks have implemented conduct risk programmes that have developed a taxonomy of conduct risks and examined inherent conduct risks within their business lines and processes. This has led to the implementation of remediation plans in order to reduce the residual conduct risk to acceptable levels within an

entity-based risk appetite statement. However, as has been seen in the press, those banks that have not implemented such steps have been subject to material sanctions issued by regulators.

The Solution – Moving Conduct Risk Programmes to Phase Two

It would be prudent for banks to anticipate further issues materialising in the future. With this in mind, there remains a need to address these findings by developing and implementing remediation plans. Banks will need to continue to resource this effort.

However, as conduct risk has proven to be very dynamic, banks will need to do more than implement conduct risk frameworks and address regulatory findings. They need to establishes mechanisms for early identification and prevention in order to avoid detriment to customers and stakeholders. Whilst this may sound obvious, in practice few if any banks at all have developed their approach to conduct risk where they could either i) demonstrate prevention, or ii) upon discovery of instances of bad conduct show they addressed those matters and then critically, show how they compensated their customers and stakeholders for the detriment that they have suffered.

Moving to Phase Two is only a matter of time. There is no doubt that the FCA and other global regulators charged with addressing conduct risk are working extensively on developing their approach, requiring banks to adopt a more sophisticated approach.

Also, we should not ignore the fact that there is the political reward of being seen to punish those banks that compromised their social licence, particularly as the financial crises of 2007–08 remains firmly in the memory of customers.

Phase Two, an Integrated Approach to Addressing Conduct Risk

Banks require an integrated approach that can adapt quickly to changes in conduct risk and where that has crystallised into an instance of conduct risk that impacts the industry, they should be able to move rapidly to address the findings.

An integrated approach would require banks to implement the items below. However, this is not an exhaustive list.

1. Continue to work with regulators to address their findings and contribute to industry reviews. As surprising as it may seem, a quick review of the details behind the sanctions applied by regulators will often reveal a lack of cooperation from individuals.

2. Individual banks need to review their inventory of governance processes to ensure that they are:

- Formally charged and qualified to capture conduct risk, specifically including emerging conduct risk themes. For example, is it included on the terms of reference of those governance processes? Is it a formal agenda item? Does it get discussed and are those discussions documented? Is there active, meaningful and valuable discussion around emerging themes? Can they demonstrate that good conduct is rewarded?

- Modified to incorporate the Behavioural Lens approach to identifying emerging conduct risks, particularly in new business, reputational risk and product suitability and appropriateness governance forums. Banks need to review their activities more broadly through this lens and attempt to detect additional issues worthy of surveillance, and address the associated emerging risks before detriment occurs. This would

include those issues unique to their own organisation. Banks need to institutionalise this approach to make it a continuous and dynamic process, one that allows an organisation to be persistently scanning for, and tackling the emerging conduct themes whilst they are still nascent.

3. Metrics alone will not help an organisation address conduct risk. However, they have a useful place and purpose if they are incorporated into a programme of meaningful review and action. For example, conduct risk metrics based upon a business line or individuals, which include instances of conduct risk, inherent conduct risks and emerging conduct risks, would be helpful to identify hotspots and emerging risks, both of which can be proactively addressed.

4. Ensure that staff are engaged within industry forums and peer groups to remain vigilant (the 'antennae up' approach) to instances of conduct risk and the emerging themes within the industry.

5. Ensure that governance programmes are in place to reward good conduct. For example, can banks demonstrate that they take seriously the concerns of whistleblowers?

6. Review and address conduct risk-training programmes to:

- Ensure that they are refreshed for current themes
- Ensure that they are mandatory for new joiners
- Incorporate the integrated approach for addressing emerging conduct risk themes
- Ensure that they are extended firm-wide, beyond the front office to all employees

- Consider formats that tackle behavioural groups, such as junior traders, trading supervisors, sales persons, and product sets, by providing interbank training sessions.

7. Implement conduct risk scenario stress testing by performing controlled tests to challenge behavioural responses and record the results to determine whether behaviours were adequate.

8. Promote and embed the concept of the social licence and its value to the bank and its stakeholders. Ensure that the concept is widely understood, that a social licence is fragile.

As it can be seen, there is much to do to address conduct risk. Whilst different organisations may be at different stages in their journey, at its core there is a need to develop the approach to tackling and preventing conduct risk. Recognising that it cannot be addressed with the implementation of one or two remedial aspects of a conduct risk programme, banks would do well to revisit their approach and take the opportunity to develop ahead of any forthcoming regulatory direction.

A Note About Pall Mall Risk Reduction

Pall Mall Risk Reduction is a specialist COO practice with extensive risk management experience in wholesale banking and capital markets. Founding members David Long, Nick Wilcock and Charanpal Matharu have more than seventy years of combined experience within Tier 1 organisations.

As skilled practitioners, they have an exemplary reputation both within the industry and with regulators across multiple jurisdictions. They possess a proven track record of delivery and pride themselves on their client focus.

Pall Mall Risk Reduction is committed to reducing operational risk and conduct risk across the first, second and third lines of defence within the industry.

References

1. Conduct Costs Project Report 2017 available at www.ccpresearchfoundation.com
2. Remarks at the Banking Standards Board Panel 'Worthy of trust? Law, ethics and culture in banking' Mark Carney, Governor of the Bank of England, Bank of England Conference Centre, 21 March 2017, available at www.bankofengland.co.uk/publications/Documents/speeches/2017/speech970.pdf
3. Conduct Risk Management by Roger Miles 2017, published by Kogan Page Limited. p158.
4. Conduct Risk Management by Roger Miles 2017, published by Kogan Page Limited. p153.
5. https://www.fca.org.uk/news/press-releases/fine-former-investment-banker-sharing-confidential-information-whatsapp
6. https://www.intelliflo.com/press-releases/facebook-increases-in-popularity-but-linkedin-still-top-social-platform-for-advisers-finds-intelliflos-annual-survey
7. See note 15 on this site: www.stats.gov.cn/english/PressRelease/ReleaseCalendar/201612/t20161230_1448613.html
8. http://traderhq.com/top-50-twitter-accounts-traders-should-follow/
9. https://www.jpmorgan.com/global/fx_e-trading_trends_2017
10. https://www.fca.org.uk/firms/5-conduct-questions-feedback/question-1-conduct-risk-identification
11. http://uk.businessinsider.com/fca-ceo-andrew-bailey-misuse-algos-algorithmic-trading-pound-flash-cash-flash-boys-2016-10

12. https://www.ft.com/content/4afc8ea6-8e09-11e5-a549-b89a1dfede9b?mhq5j=e6
13. http://money.cnn.com/2012/08/09/technology/knight-expensive-computer-bug/index.html
14. HYPERLINK "http://www.bankofengland.co.uk/publications/Pages/news/2017/037.aspx" www.bankofengland.co.uk/publications/Pages/news/2017/037.aspx
16. Conduct Risk Management by Roger Miles 2017, published by Kogan Page Limited. p161.
17. Conduct Risk Management by Roger Miles 2017, published by Kogan Page Limited. p164.

PASSENGER CARS ONLY
5 AV
BUSES ONLY
NYC TAXI

"The job of the CCO is to know which controls work and which don't."

THE CHIEF CONTROL OFFICER: PAST, PRESENT AND FUTURE

Executive Summary

As global leaders in executive search for banking and markets business management, Armstrong Wolfe has a unique insight into the profiles of its leadership. The following is a summary of the skills and experience of this leadership group, as well as the evolution of the function itself. We concentrate on the global leaders of the front office control function for markets within twenty top tier global banks.

Within this group, there is a variety of job titles, including Chief Control Officer, Head of Non-Markets Risk and Control, Head of Business Control, Head of Supervision, Operational Risk, Financial Crime, Conduct and Control, or a combination of these.

The skill sets are varied, with a few accountants and one lawyer, but a front office business management background was predominant. This is unsurprising as the role has recently been separated out from the COO role. The average length of tenure was around two and a half years and there was limited experience of working abroad. About a quarter are women. Only one had a trading background whilst most are graduates, but the lack of a degree is no barrier to rising to these positions. Overall it is clear that an integrated and varied background around the skill set seems

best suited for these roles and typically persists. That ambiguity is reflected in that a majority of people have risen through the front office operational, non-revenue generating ranks themselves.

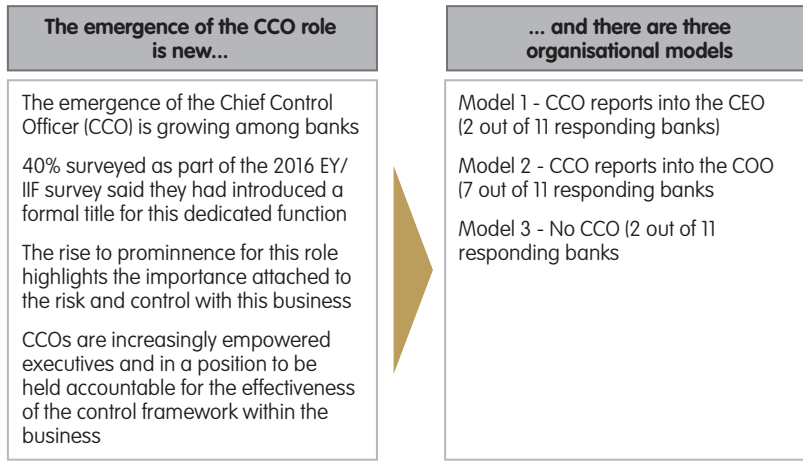
Next, we consider the evolution of the role itself and possible future scenarios. We draw on the EY First Line of Defense benchmark survey of seventeen major banks. This was presented at the Armstrong Wolfe Autumn 2016 Business Risk and Control Forum, and we enclose insets from that survey. It was published as 'Front office control functions, what's next for capital markets banks?' in February 2017.

The Role

The front office COO role evolved after the regulatory response to the financial crisis of 2008. The sheer quantity of administration involved meant that the CEOs of markets businesses leant ever more heavily on this function. It included responsibility for strategy, business development, finance, administration, resilience, and front office risk and control. However, in time, especially with the appointment of Chief Risk Officers, these functions began to fragment. Administration began to be taken over by a CAO, finance sat with a CFO, and the business control function itself began to be taken up by people with a title such as Chief Control Officer. This had always been a significant part of the role, but became even bigger, dealing with the major regulatory issues of each country, region or globally from an operational and conduct risk perspective.

The sheer volume of controls, and the development from manual to technologically based systems, required someone to act as a conduit and take a more strategic approach. The focus became one of risk and control, rather than expansion into new markets or driving efficiencies. This involved major programmes of change

We are seeing three different organisational model for the Chief Control Officer (CCO)



and transformation, including the development and upgrading of surveillance and supervisory systems. Both regulation and ongoing market events drove the need for investment into control measures within the business. This has attracted people with a variety of backgrounds, including legal, finance, audit, risk and change, as well as core front office operational and business management backgrounds, and more recently, traders themselves.

The First Line of Defence

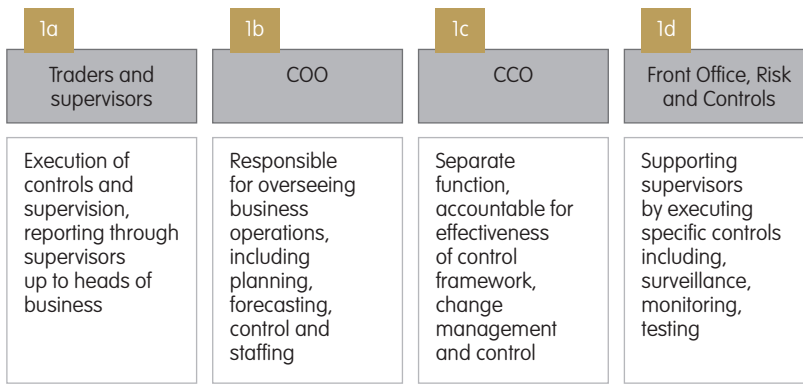
There was a common point of change after the LIBOR and then the FX fix scandals. The question was asked of markets leaders, are you in control of your business, and if so, who specifically is it who owns and leads this business-critical effort?

In addition to what was being booked and how, a framework around behaviour, conduct and activity became an essential part

of management. There was the development of communications surveillance and activity monitoring, such as simple, but potentially important alerts that noticed when people were working late. A rule book was developed to cover all the stages of sales and trading activity. The support functions of compliance and audit were not targeted to examine these activities, and so it became the responsibility of the front line.

In addition, effective supervision required someone who really understood the communication and behavioural signs to monitor. A desk supervisor was the most effective person to do this, especially in terms of pastoral care and mentoring, which the support functions were not really positioned to do, but a framework was required in which to do it. Thus, the first line of defence was established, with control officers setting and managing the implementation of that framework. By 2018, different institutions were at different stages of the establishment of this framework, and had adopted different models of implementation.

The 1st LOD is organised around 4 main functions



Current Status: 2018

These themes are relatively consistent, although a few organisations have maintained the control function within the COO role or even at one leading bank, under the CFO in the front office, with a very strong second line. However, organisations differ by whether the CCO concentrates on the more strategic elements, with a major change agenda, or maintain a focus on pure supervision and governance. Some organisations have the control officers embedded within the individual businesses, reporting directly to the head of desk, with a dotted line to the Chief Control Officer or equivalent. Others have the individual control officers directly reporting to the Chief Control Officer. What is essential is that they must be good at dealing with people, influencing them to adopt the control agenda, and persuading them that it is in the interests of their business.

There is a major job of translation and ambassadorship to be done in applying the demands of the regulator and corporate leadership to the individual desk. The ability to be both a change agent and apply a control mindset requires substantial personal qualities. It can take around five years fully to respond to new regulation,

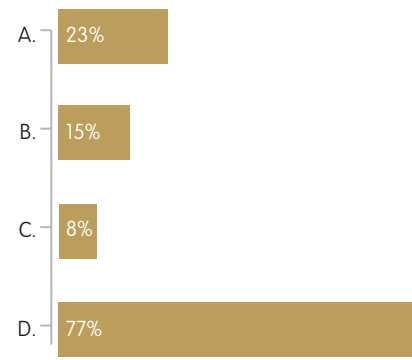
Does the 1 LOD control function perform any testing activity?

A. Yes - performs testing as part of formally or regularly mandated testing and attestation programes (Volcker rules, CCAR CIFO attestation, etc.)

B. Yes - performs testing as part of firmwide internal control initatives (operational risk RCSA, compliance testing, model control and governance)

C. Yes - performs business-line specific testing as part of specific business line reporting and governance (i.e., business-specific quality control processes)

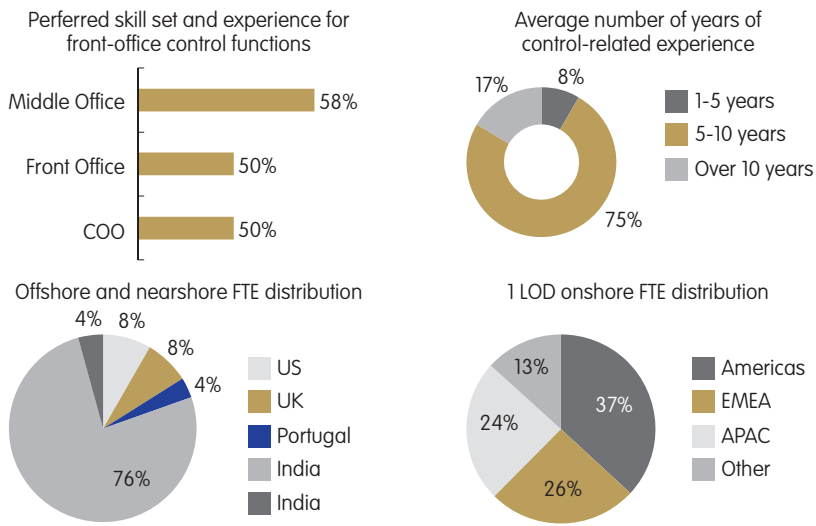
D. - No - at present



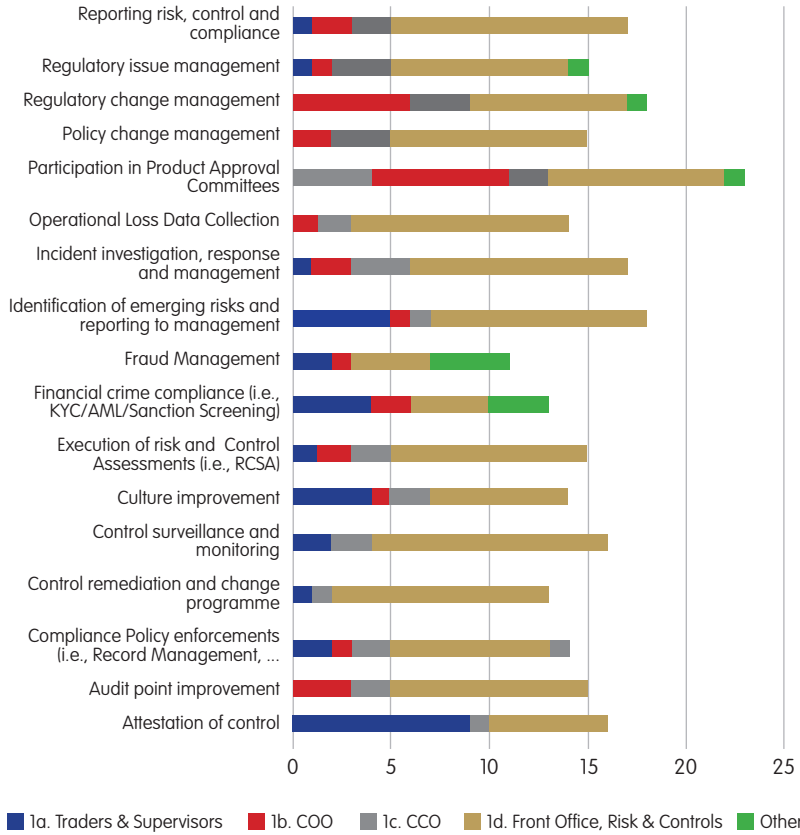
and there will be strong views on how things are done within each jurisdiction. The difference between the US rule-based approach and the UK principle-based approach, for example, presents a challenge to ensure that controls are enforced consistently.

A good control model is one that implements a process of inquiry, testing and review. This may be regarding financial crime or client onboarding, for example, and so may bring in people with a compliance background, and involve a migration from the second to the first line of defence. This also involves significant technological input, providing big data solutions, for example, in first-line surveillance. This, however, requires an experienced eye to distinguish between a whole series of false positive results and a genuine concern. In general, the front-line control function has to take a more integrated approach to overcome duplication, gaps and fragmented solutions.

The 1st LOD is composed primary of FO and MO staff, while offshore capabilities are increasing



The first line ultimately owns the risk and requires a practical solution to its day-to-day management and governance, especially with the implementation of the senior manager regime. Ultimately, there is a need to demonstrate to the regulator that the business has understood its internal risks, and that they have put in place an appropriate control framework. Working across many global locations and jurisdictions obviously poses a challenge in establishing a consistent approach, but this is one the CCO must face.



Whilst there is a formal annual assessment of risk and controls, in practice this is done on a monthly, or more frequent basis. The job of the CCO is to know which controls work and which don't, and to turn an overarching framework into a practical risk assessment and controls framework. This is the work of translation and integration that needs to be done. The practical basis is the one in which the control function helps the business, for example suggesting that five books may be run rather than 95, or that daily closing routines are followed on time. Procedures must be simple, orderly, effective, commercial and compliant, and the ones that don't work must be eliminated. The CCO must be able to understand the different audiences and how they think, working with the other corporate functions front to back, though front office, operational risk and compliance. The front line owns the risk and so must lead this process.

Regarding background, front office experience tends to provide the ability to sell what they are implementing to internal clients and into the business. It is important, however, that this does not just involve taking people who are underperforming, and that this group is constantly refreshed with people who know the current state of the markets and have up to date contacts. Auditors tend to be used to asking difficult questions and dealing with the response, and lawyers have a strong intellectual contribution to make. Ultimately, someone who is comfortable with change is essential.

Future Development

There is some debate as to whether the function will remain separated from the day-to-day role of the COO, or whether it will be reintegrated once the current phase of remediation has been implemented. If the testing is not core to the business then it could revert to compliance, or in part into an operational risk function with an enlarged remit. The alternative is to upgrade the assurance

team with a fully fledged audit, to a Federal Reserve standard. This may involve hiring auditors or people with a finance or legal background, while surveillance may be staffed by security service-type people, technology gurus or ex-traders themselves.

In all cases the industry's capability to manage and use data effectively will define the ultimate solution and the timing of its development and implementation. Whilst technology will deliver this shift, however, it is equally important never to forget the unique and ever changing component in this equation, the human point of contact.

There has been so much regulatory change, there will be more in the future and the demands are so great, that it is not easy to see when (if ever) these control functions and their processes and policies may revert to its pre-existing location, under the direction and ownership of the business COO.

Typically, the front-line function reports through the COO's office into the Head of Markets, Banking or other, who is collectively responsible for all activities within his or her business and will be kept fully up to date with each investigation, and will feel this responsibility more so under the senior manager regime. The second line is viewed in an advisory capacity, one of policing, but while the approaches are very different, the objectives are the same. This fact is very important, as all functions ultimately have the same mission, to ensure the business is protected from poor practice or malice.

Front-line testing and assurance needs to be light touch to avoid unnecessary repetition and bureaucracy, the second and third line tasked to be constructively intrusive. However, as fines increase, problems still need to be solved urgently. Surveillance and engendering a culture of whistleblowing are essential in this regard. The relationship with the regulator is key to the front

office perspective. They need to see friendly faces and have open discussions, but changing the culture remains the long-term objective, to put each bank and the industry on a firmer footing.

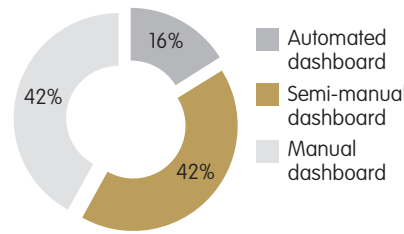
The technological requirements of modern market activity are shaping a need to move towards real-time trade surveillance, especially in conjunction with the implementation of MIFID II in 2018. This depends on the development of external systems and innovation, such as Forcepoint and Nasdaq SMARTS, but also on the development of internal platforms and capabilities. In this

Most of the FO monitoring solutions are still relatively manual and expensive to run

Common metrics reported at granular levels for day-to-day supervision, includes:

- Cancels and corrections
- Fails
- Unsigned confirms
- Regulatory reporting breaches
- Volcker rule metrics
- Risk limit breaches
- Profit and loss (P&L) policy breaches
- Conduct-related metrics (price exceptions, wash trades, and layering and spoofing

Level of automation of FO monitoring:



- Interactive tools and workflow remain limited, but emerge as leading practice
- Very few banks reported any ability of their tools to provide supervisors with trending, drill-through information about the underlying data or pivots by trading strategy, risk book or individual trader, although some leading firms had begun to develop and utilise this capability.
- Workflow capabilities existed in some tools, but this was fairly limited.
- Most metrics were siloed, limited join the dots capabilities at this stage. While banks have aspirations to combine disparate data sources into more sophisticated risk metrics (for example, combining communications and trading data, or risk data with cancels and corrections), these efforts are generally nascent at best and banks typically did not have a clear road map to explore vendor solutions or build out internal capabilities.

context, facing a common non-proprietary challenge, within a cost containment environment, cooperation and collaboration is a viable and valuable route to explore and exploit, enabling the banks to more effectively access and embrace the possibilities being presented by the growing FinTech sector.

Also relevant is the monitoring of chosen trading locations, as well as client suitability. This is further changing the relationship between the first and second line, as is the impact of changes affecting cross-border flows, such as Brexit. This contributes to the need to develop a legal entity level framework as well as a booking level perspective.

Conclusion

The role of the front office CCO is to fulfil the day-to-day execution of the supervision and governance framework, establishing consistency and evidencing for the internal and external requirements of the regulator, compliance and audit. Establishing this on a sustainable basis is crucial, while they must keep a focus on technological innovation and solutions. The activities of this function will continue, but when and if it is reintegrated into the COO role is a moot point, as is the future state of the 3LOD concept itself.

There is some advantage to having someone with a C-Level position who is thus able to carry the authority to implement the front to back change required and to manage the associated investment. Such senior cross-functional executives should be able to secure, even command buy-in, at the highest levels of the organisation, as well as shape that agenda for the future, as human innovation and abilities will continue to test and navigate the controls implemented and poor practices and events will unfold, emerging risks and vulnerabilities now being the primary item on the CCOs' agenda.

'It is time we look forward, get on the front foot, as we have all spent and will continue to spend time and money on mitigating the failures of the past. We must prepare to meet the demands of the future, where many emerging risks are almost certainly things, we as an industry have already done.' (Global Business Controls Officer).

In this context, the role of the CCO and ownership of the control and conduct agenda has years of work ahead. Poor conduct in banking is not a new phenomenon; there is evidence of it throughout the history of the banking industry. Importantly, however, in an era when social media and technology drive communications and perceptions, the CCO's role in maintaining and building a robust control framework and in rebuilding confidence in a beleaguered sector remains central. In part, you could argue, re-establishing the reputation of the industry is reliant on the success of the CCO community.

26
CHAMBERLAIN'S
PIZZAEXPRESS

LUC's
ZZA EXPRESS
THE PE

"I see control as the bedrock of a management structure and hierarchy, where many managers hide behind this structure because they lack leadership."

THE CONDUCT ACADEMY

The end of a road, but not the end of the journey

At one of my forums back in 2015, which was hosted by Penny Tunbridge, the then Chief of Staff to the European CEO of Nomura, the subject of training within conduct was introduced. It quickly became apparent that this was a common subject and challenge, but without a common approach. It is important to remember that at this time, in 2015, the banking industry was at first base as it postured and prepared itself to meet the demands of the conduct agenda.

The debate was full and hearty as ideas and views were exchanged. Clearly, no party had advanced thoughts, no party a silver bullet, and so it remains to this day. I am not sure whether it was that evening or afterwards – there was no epiphany – but it appeared to me strange, if not illogical, that this common challenge was not met head-on by the industry working together. With the thought sown, I enacted follow on conversations within my CCO community in relation to it, referencing my time in the Army and specifically in attending the Royal Military Academy Sandhurst, where conduct, ethics and behaviour are taught, to investigate the suggestion and to answer the question: 'Why can't the banks work together to develop a shared, communal approach to conduct training?'

There appeared no common-sense answer to the question, the most frequent answer advocating or explicitly stating that conduct,

and therefore conduct training, was bank-specific, was proprietary and that collaboration within such a sensitive and business critical area was (most likely) impossible. Initial discussions referenced the implausibility and poor record in bringing banks together in collaborative ventures, precedent indicating it would inevitably fall short of the start line. Facing such strongly-held and defended opinions, it would have been easy to put the idea to one side and let it rest as a 'could have been something', a potentially good idea lost in time. However, the possibility niggled, I simply could not let it be suffocated by an apparent focus on the granular as opposed to the higher valued proposition. I felt strongly that such opinions were misplaced, offering nothing more than parochial protectionism.

The hypothesis and the challenge fascinated me, and resonated with my growing sense of purpose born from the personal challenges experienced since 2008. I concluded that what I needed to do was nurture a debate at this granular level, but reference and carry the concept forward on the higher-valued proposition.

The hurdles were not just the industry and the lack of willingness to make such ventures work, but the perception that this idea was being carried by 'a recruiter'. Throughout the whole period of bringing the Academy into being, you could almost hear the echoes of those not known to me asking: 'Why is a head hunter doing this?' even suggesting in some quarters that I may be using this to gain visibility of a market-wide candidate pool. 'What tosh,' I thought, but their perception was their reality and it was this perception, however misplaced, that I needed to address.

It was understandable perhaps, but I know many accomplished and intelligent people within my profession, those who have dedicated their careers to it, and their opinions are valued by many. Like all industries, however, there are those who give it a bad name, but, as with banking, the very high percentage of those

within the sector are decent people. In the case of an executive search consultant, their privileged position in lending their ear to senior management (of banking) affords them an in-depth and informed insight to the markets and its opinions. My network was established through years in search, and those who trusted me, had created the opportunity for me to bring the forums together. It was to these forums and its participants that I would turn to help validate and drive this initiative.

Through my forums, and therefore as an informed industry observer, I could readily see that culture could and does breed competitive advantage (or dilutes it if a rotten one), but my opinion was firmly committed to not awarding conduct training this accolade. Importantly, a crucial aspect to having sound culture and conduct is that the clients trust the organisations more and are more likely to win business. Good conduct is a long-term play and ultimately wins, despite bad conduct leading to short-term outperformance.

In a conversation aimed at determining the 'why' should banks cooperate, this point was addressed by one of my more erudite clients, learned from his youthful days at Cambridge (I struggled to get into and manage myself through Cardiff University). He had subsequently dedicated himself to a career in banking and held many senior roles. Dominic Cashman had been known to me for more than twenty years, we dined every six months, he would take me to the Oxford and Cambridge Club and I would take him to the RAC, both on Pall Mall. One evening we discussed my question, the next morning his considered thoughts pinged into my inbox: 'I've been thinking about how best to express why, even though conduct risk management creates competitive advantages, banks should still cooperate. How about this for an outline of the proposition:

- Failure to effectively manage conduct risk can lead to significant P&L impact, either directly (rogue trading, regulatory fines) or indirectly (reputational damage leading to loss of revenue).
- Firms that can better manage that risk class have a competitive advantage vs their less capable peers.
- Conduct risk can have systemic impacts, not just through the potential failure of a single firm but also a general loss of confidence in the system, leading to regulators requiring all banks to hold additional capital. So it is in the economic interests of banks to cooperate to reduce the overall risk to the system.
- All significant firms enjoy the implicit support of the financial system (since they are too big to fail) and so, despite the competitive advantage, they have a moral obligation to cooperate in support of that system.

With a small but growing band of conceptual supporters, progress was being made. If you could define the short-to mid-term benefits and marry these to the unquantifiable higher value purpose and allow common sense to prevail, then the Academy could move from concept to reality. Three years later, as I reflected on the journey after the Academy's introductory presentation held at HSBC, I realised what had been needed was patience, perseverance and patronage.

The first I had been gifted by my mother, the second by my father and the third came in the shape of six of my CCO community, who shared the vision or at least agreed to put aside some time to investigate it, and came together in a working group that met quarterly for two and a half years. Its output was a positive validation and support for the notion that the industry should commit to this initiative and defined why it should do it, which led to the next stage of its development of how it would work in practice and be delivered.

Particularly, the initial support of Kevin Sawle, HSBC's Chief Control Officer of its Markets' division, and Toby Billington, CCO for Global Banking at HSBC, were invaluable. Kevin saw the higher valued proposition and was, to a degree, willing to put his name to it on this basis alone. Toby articulated the granular need and benefits to be realised for the industry, although each clearly understood both. Importantly for me, they were willing to give their time and offered their insights to shape my thoughts.

Their support was added to by Nick Lovett, Credit Suisse. I had met Nick some years earlier, when he was working within fixed income business management, alongside David Long. David would come back into the Academy's story some years later, when, having left Credit Suisse and then running his own consulting company, Pall Mall, he helped shape and deliver the first Information Handling pilot course.

Since our first meeting, Nick's career had continued on an upward trajectory and at the point of writing is both Global Chief Control Officer and EMEA COO Markets at Credit Suisse. Nick had supported my forums, hosting many, and his astute and clearly articulated observations had a way of keeping the train on the track, in doing so ensuring the output was always mirroring the input to our efforts.

With these three leading voices interested (I steer clear at this stage of stating fully supportive), next steps were feasible.

The first step was to take this interested group to my spiritual home, the Royal Military Academy Sandhurst. Embedded in Sandhurst is the Inspirational Development Group, a business focused on leadership training and enjoying the commercial licence to work within the hallowed grounds of the military academy. My contact was one of its directors, Lance Gerrard-Wright. Lance and I had gone through Sandhurst together, remained good friends and he was the gateway, some twenty-five years after leaving Sandhurst, for me to return to it.

The supposition, and one that I saw as central to the debate, was that upon entering Sandhurst you were de-badged and detached from your sponsoring unit or regiment. It mattered not whether you were infantry, cavalry, engineers or logistics, your regimental identity was naturalised for your stay at the Academy. You were a witness and a participant to the Academy's training regime and to be faced with the paradox, which is the Academy's motto, *Serve to Lead*, you make your commitment to one of service, putting the focus of leadership where it should be (or rather where Sandhurst feels it should be), when all too often, most people think of leadership as being about the leader, this is the paradox. It's not about you as leader, but about those you lead, those you are committed to serve, not them serving you. The Sandhurst motto embraces the principle that a leader who serves has greater influence, where service and not control,* as many misinterpret leadership, leads to trust and increased influence (and in most cases it could and should lead to enhanced performance of those you serve and lead).

> ** I see control as the bedrock of a management structure and hierarchy, where many managers hide behind this structure because they lack leadership. This would not be so much a good subject for a forum, as to a hearty chat over a bottle of red!*

During the past fifty years the motto *Serve to Lead*, and all it stands for, has been an object of ridicule for some sociologists, psychologists, and social historians. For example, the author of the *Peter Principle*, the Canadian psychologist Professor Lawrence Peter, once queried 'serve to lead' with the question: 'Why should

the ability to lead depend on the ability to follow? You might as well speak of the ability to swim depending on the ability to sink.'

Sydney Jary (MC 18 Platoon (1987), Serve to Lead) takes a counter-position when saying 'Serve to lead is, of course, a paradox, but it is a paradox which should be understood by every officer cadet after each has completed the first command task on Barossa (the principal training ground of Sandhurst). If cadets have not understood the meaning of the paradox, they have no business aspiring to be officers in the British Army.'

When you march up the steps of Old College, throw your hat into the air and grab high for the Queen's commission, you are then handed by the Academy to your parent regiment. You will then be exposed to, be witness to and become proud to be part of your regiment, although you will all look through the same lens as your core leadership responsibilities, those you carry as an officer in the British Army. These were drilled into you whilst at Sandhurst and you will carry them forward into your role as a commissioned officer and into life generally. It was this commonality, this shared and identified responsibility, which I thought was needed in banking and that the Conduct Academy could in part address.

The visit to Sandhurst certainly played its part as afterwards there was an energy amidst the members of what became the Conduct Academy Working Group. For the next eighteen months the six banks met, dissected and discussed the evolving proposition. Strong advocacy from Eric Rabin (Global Markets COO, Société Générale) and Doris Honold (Group COO, Standard Chartered Bank) added weight, substance and purpose to the combined effort, as did the voices of their delegates, Rajeev Mehta and Libby Denchfield respectively. Libby, strong in personality and highly personable, added vitality and often a different perspective and additional colour.

The sixth and final member of the working group, Darren Jarvis, Global Head, Business Control and Supervision, Markets at Citi, was a late entry into the paddock. There was a natural and well-explained cautiousness to Darren's participation. Like all participants and working group members, he was careful not to over-commit, whilst ensuring he offered sufficient commitment. Darren, like all members, appeared to support and believe in the vision, but had a smattering of reality and pragmatism about the challenges ahead.

As the structure and content developed and the proposition took shape, the key and fundamental question as to the justification of why any banks, let alone all banks, should participate, continued to cast a shadow on our energetic and purposeful conversations. Other banks were courted, most took a 'stand and wait' position, waiting to see how things developed. Some were more specific, in stating that until the Academy could prove its training was better than what they already had developed in-house, what justification was there to support the Academy?

This was the key question and one that I viewed as the common purpose, the higher-value proposition and one that Dominic Cashman had stated as a moral obligation. It was with this issue that Darren broke the code when he summarised that it was not whether the content was better than already being used, and that it was certainly not proprietary, but there was a duty, a collective duty of the larger banks to work together to the benefit of the whole banking community. In his case, he saw that Citi had a role to play in driving this collaboration, in sharing its thoughts, in helping to develop a common platform for the whole banking industry to participate and benefit, not just the few. This was to put in place a shared purpose, to develop a cross-industry approach and product that would help address the errors of the past, repair a tattered reputation and build a more sustainable future.

It was becoming apparent that the concept was at the point of open discussion, and to this end Kevin Sawle offered to host a defacto launch evening; his manager, the Head of Markets Thibault de Roux, was supportive of the proposed industry model and agreed to host. This put a line in the sand and set the clock ticking.

To help this short-term increase in the tempo, EY stepped in to work alongside me, having supported my forums throughout the previous year. This gave critical mass and substance behind the proposition and equally, more credibility. However, the question remained for me, and one I had been clear about from the outset, as to who would run the Academy if (or as it appeared, when) it came into being?

I had been open with all that whilst the genesis of the Conduct Academy had been found betwixt my ears, I had set and limited my objective to ratify and prove the point as to 'why the industry should invest in the development of the Conduct Academy'. I was not the man to take it from the 'why' to the 'how'. This demanded a different skill set.

The conduct gods were shining on me at this moment, as the solution came into view almost immediately. Neil Smith had been known to me for many years, principally in the role of the Global COO for Risk Management at Deutsche Bank. Neil had recently left Deutsche Bank and was investigating his options, more specifically he was open to something entrepreneurial and at our first coffee meeting the Academy's concept secured sufficient interest to bring him down to the Cotswolds, where I live, to discuss the idea in depth and the steps needed to take it forward.

I had, in military parlance, secured the beach head, and now needed the follow on troops to take the battle forward. Neil accepted the opportunity to meet the members of the working group and in a two-way assessment of the viability of the opportunity by Neil, and

Neil as a viable leader of the Academy by them, a unanimous vote of mutual confidence saw him being appointed as the Academy's CEO.

Thereafter followed a frenetic and intense period that led to the two pilot courses, one being from the six core modules identified, Information Handling, held in EY's office in Canary Wharf (led by David Long). The second saw a return to Sandhurst and IDG for 22 managing directors to attend the Conduct Ambassador's Course, developed specifically for the Conduct Academy. This married ethics, conduct and behaviour with leadership. Both had their merits, both had room for improvement, both helped accelerate the Academy to its patron evening at HSBC.

There is no question that without Neil at the helm, with his drive, enthusiasm and focus on delivery, standing before the forty executives on the patron evening would have been an uncomfortable experience. Additionally, without the patience of my wife, the evening would not have been quite as successful. We were away for ten days in Cyprus prior to the event, where I spent most it with my face close to my laptop tip-tapping changes and adding ideas to what was to become the presentation at HSBC. My wife's dedication in looking after my three boys while I took shelter inside was by far the harder task!

At the presentation, my role was to explain the 'why', then to hand to Neil to explain the 'how'. Whilst we now know that all went well on the evening and that the Academy has subsequently moved into a period of accelerated progression, with increasing market-wide support and the explicit support of the industry body the FMSB (Financial Markets Standards Board) and its CEO Gerry Harvey, there was no such guarantee as we took the stage that evening.

I summarised the four reasons why we, as a community, should support the Academy:

- The quantifiable – more than $280 billion of fines
- The unquantifiable – reputational damage to the industry
- The obligation – today's leadership to leave their house in better order for the next generation.
- A personal perspective – the impact on directly and to my mother, upon the passing of my father and the consequent loss of the high percentage of his estate due to the 2008 crash.

It was not aimed at being an emotional presentation, it was certainly not a shout for sympathy, but there were real and tangible reasons why I was standing before them. Quantifiable, unquantifiable and an obligation, all reasons resonated. Personally, it was largely, although not solely, the poor conduct of a few bankers leading to the crash that had impacted so many, my family and I included. My father, I outlined, was a retail banker and I further made the point, like the overwhelming percentage of bankers today, despite media representation, was a good man.

To me this presentation was a collection of thoughts, ideas, concepts of thousands of meetings and conversations. It was a journey that started in the dark days post-2008 and an idea that was cared for, cherished and fostered in the interim years. It was in some ways a thesis, or at least an extensive piece of research. It felt like the end of a road, but not the end of the journey. It reminded me of Churchill's famous speech in 1942: 'Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.'

To me the Conduct Academy remains at its core, common sense. And as my father used to say: 'The wonderful thing about common sense is that it is not very common.'

At the time of going to press, the Conduct Academy is now real. It has a tangible identity, bringing together a diverse group of professionals to develop training content for members of the banking community. It is gaining momentum daily. Whilst we are

only at the start of the journey to what I envisaged years ago, I can see the vision becoming a reality, something which gives me great pride. Will the Academy reach the aspirations I hold for it? Who knows. Maybe we can do more together than ever I hoped possible. Only time will tell.

www.conductacademy.com
info@conductacademy.com

"Those banks that have not appointed a CCO arguably have late-entry advantages. They can learn from others who have already invested heavily in this initiative, helping to define 1 and 2LOD."

MARKET AND ORGANISATIONAL SUMMARY 2015 TO 2021

Evolution within the organisational design and construct of 1LOD

2015: 1LOD Organisational Design

Non-financial risk management was critical for top-tier banks, as the impact of getting it wrong became increasingly significant. This was either in quantifiable terms and in regulatory fines or in non-quantifiable terms and the impact of reputational damage and loss in investor confidence.

As a result, banks started to invest heavily to address the second line of defence 2LOD, capturing the internal control and compliance challenges. Most of these institutions were committed to a comprehensive and ambitious 3LOD programme to ensure a consolidated view, consistency and completeness across all different control initiatives. In these cases, each programme's governance had been designed with strong board and bank-wide involvement from the senior management, reporting into the CEOs through the COO's office.

Where banks chose this route, the first step had been to run a pilot (without exception within Fixed Income), to refine the approach and identify control weaknesses, as well as designing remediation and demonstrating the effectiveness of the approach. It became

clear quickly that strengthening the underlying controls required a truly end-to-end activity view and diagnostic of the full scope of non-financial risks. The method of shaping the bank's (principally its Markets' and/or Investment Banking) control functions was guided by the 3LOD key principles to frame and deliver in business accountability, effective implementation, strengthening the control environment and ensuring consistency and continuous improvement.

These principles led to a clear control lifecycle for many banks and its 1LOD, which was principally embedded within front-office sales and trading. This was in turn used to design the control organisation around central, regional and business control units. Almost half of banks surveyed at this time followed this path and by Quarter 1 2016 they were at post-framework design and implementation stage or were in the advanced process of finalising the operating model for the control and conduct organisation.

This was achieved by designing the regional sub-structures and delineating roles and responsibilities between the various sub-components of the organisational design.

The arrival of the CCO and implementation – 2016

In response to the demands of regulatory change and 3LOD agenda, the banking industry experienced an organisational shift in its defined approach to the day-to-day management of 1LOD, with the initial appointments of Chief Control Officer (CCO) being made. This role, embedded in the front office, reported into the Markets' COO and was directly made responsible for the 1LOD. Not all banks embraced the role, but for those that did, the following appointees come from the following backgrounds:

Bank 1: New York (CCO, previously Global COO Cross Product Sales)

Bank 2: London (CCO, previously EMEA COO Markets)

Bank 3: London (CCO, previously Global COO Fixed Income)

Bank 4: New York (CCO, previously Americas COO Markets)

Bank 5: London (CCO, previously COO, Macro division)

Bank 6: London (COO, previously COO Fixed Income division)

Bank 7: Singapore (CCO, previously COO Fixed Income)

Bank 8: London (FO Head of Supervisory and Control, previously Operational Risk)

Bank 9: New York (CCO, previously in-house derivatives lawyer)

This realignment of the approach to 1LOD management was largely (although not wholly) driven by European banks, with the U.S. banks mostly retaining a decentralised approach, in which the principal product COOs retained direct responsibility for the 1LOD control agenda and its execution, supported by operational risk and/or non-financial risk. However, some U.S. banks were reviewing their approach to managing the 1LOD effort and considering the appointment of a CCO as 2016 ran its course.

More so, there existed two distinct models:

a. A centralised model, where the CCO retained all (control) headcount rolling into the CCOs office, including the in-business control officers.

b. Where the CCO was responsible for the centralised reporting and 1LOD framework, but worked with the in-business control officers, that remained reporting into the product and/or business COOs.

Deconstructing the debate over 1 and 2LOD – 2017

As the approach to handling the 3LOD and more specifically the demands of the 1LOD agenda matured, with it came a challenge to the established doctrine of the 3LOD model.

Resident debate existed as to determining the demarcation line between 1 and 2LOD. Compliance (2LOD) had moved increasingly to defining its role as 'advisory', whereas 1LOD saw the inevitable consequence of this definition to be an increase in execution responsibilities within 1LOD itself. With this responsibility came an increase in headcount and additional and understandable questions as to the role and quantifiable results of this investment. These questions more forcibly tabled due to the cost constraint environment in which the industry and most of its participants were operating.

With no clear definition being offered by the regulators to help resolve this debate, inevitably duplication of effort and headcount has arisen, with the common phrase being heard to be 'the checkers checking the checkers'. There are questions being raised as to the operating model and whether, for example, an activity-based approach would best fit the approach to 3LOD as the markets' approach matures, although it is unlikely the regulators will acquiesce on this point (yet).

It is also within the realms of possibility that technology may well circumvent this issue, if it can address the data issue and challenge. Creating a centralised reporting and depository approach to 3LOD may well lend itself to the future use of technologies to break down the 3LOD doctrine, although there will always be the human aspect that needs to be accommodated somewhere in the mix.

2018: Review and Reflection: where now for 1LOD design?

The attitude and methodology coming out of the design and execution of Control and Conduct and the reinforcement of 1LOD have been evolving rapidly since 2015. Those banks that have not appointed a CCO arguably have late-entry advantages. They can learn from others who have already invested heavily in this initiative, working out the best alignment for and helping to define 1 and 2LOD. Furthermore, banks will be able to more readily assign headcount to a centralised function or to that which should be embedded within the business and within this apportionment. In addition, which tasks and responsibilities can be pushed into the infrastructure rather than retaining them within front-office business management are open points for further consideration and debate.

Importantly 1LOD does not mean the task or responsibility must sit within front office, just as there are some 2LOD tasks that arguably would be better placed in front office (and not compliance). This is a point of debate within many banks, where both objectivity and lateral thought are needed to look at each task individually and to frame the 1LOD matrix according to its needs. Such changes in approach to a market-wide effort mean that early leaders in this area may be at a disadvantage. Many banks are reviewing their organisational 1LOD construct, its headcount and task allocation, and many business heads are questioning perceived over-hiring into the front office. This seems particularly true when weighed against the rising pressures from struggling business performance and a focus on costs.

Such investment has been well received by the regulators, who can see in a bank's allocation of headcount a significant real-time commitment to address historic issues. Although there is a sense we are not at the end of this journey yet, as the market's

approach to this issue is not completely resolved or settled. For most, the organisational models are not 100% cent firmed up and it is not yet possible to make precise comparisons on how banks are managing resources to meet this common challenge. Defining what headcount is allocated to a control task or what percentage of a headcount's time is apportioned or aligned is very difficult. One solution is for institutions to share lessons learned, helping to align their efforts and resources to fit individual demands more effectively.

This approach was promoted in 2016 at the Q2 1LOD CCO forum, which led to EY undertaking a masked survey of sixteen banks, aimed at sharing the core data at each as to their organisational constrict and models across 1 and 2LOD.

Collaboration and information sharing is one way the participants in the banking industry could work together to address this common challenge, or at least make their models more efficient and less costly.

2020 No change

2020 was a year that would test the Control community like no other, with the pandemic presenting unique challenges. With the workforce in a dislocated and distributed model, well over 80% of all trading and sales staff WFH, the supervisory demands were tested to the outer realms of the imagination.

Despite this point of effort, the issue the 1st Line had with the inherent challenges in the 3LOD remained. The issue was now twofold: firstly cost, secondly operational efficiencies – the 1 and 2LOD debate had become in many banks a point of contention and in a handful a disruptive matter that was fostering cultural fractures between the business, operational risk and compliance.

To reset the dial, 2 forums with 12 banks in each were run in November 2020. It proposed the following:

Organisational design and governance

Organisational design and governance have defined the industry's efforts to meet the structural and regulatory demands captured within the 3 lines of defence that have defined the operating mantra of the functions that own and manage risk; oversee risk and provide independent assurance. We ask the question 'Is it time to reassess this model, allowing for technological innovation and the industry's investment in this area since the 2008 crisis or has the industry missed an opportunity in failing to ask the question repeatedly 'what problem am I seeking to address and how best do I align my resources to tackle this issue', whilst meeting regulatory interpretation, to succeed? Is it time for a change in thought and execution?

The sessions were as to be expected, with Nick Lovett (CCO, Credit Suisse) noting at close of session 2 "These sessions are great, cathartic, but we have been discussing this point for years, we need to seek to address it."

The 2 forums were followed by a call to arms with 35 banks invited to participate in an industry paper, aimed at presenting 'The view from the 1st Line'.* This issue was becoming an unnecessary distraction to the overriding purpose of the CCO and needed to be addressed. Its initial results can be found in the next chapter.

In parallel to managing the business through the pandemic, many in the CCO community were shifting the perspective on the role towards being a more outward looking, emerging risk and horizon scanning mandate. The evolution of the CCO appeared to be naturally evolving into one focused on threat management, to which end controls and conduct are a key part but not the whole. Threat management would appear to be the next phase of

influence and impact the CCO role embrace as the industry itself moves into a new paradigm.

**email copy sent to 35 bank's COO and CCOs November 24 2020:*

Outline

Armstrong Wolfe has run quarterly 1st line Chief Control Officer and COO forums in 5 financial services centres since 2015.

A common point of debate and challenge has been meeting the demands of the 3LOD model and particularly from a 1st line perspective, the alignment and mandate of 1st and 2nd line.

This led AW to run 2 forums in November 2021 focused on this issue alone and framed by the below statement on organisational design and governance.

Post these forums, a number of banks have requested AW produces an industry paper, focused on 1LOD perspectives on the 3LOD model:

Report: Views from the 1st Line

A commissioned study to deliver a fresh perspective on the inherent challenges in the 3LOD model, with a view to identifying ways to address or mitigate them.

Organisational design and governance

Organisational design and governance have defined the industry's efforts to meet the structural and regulatory demands captured within the 3 lines of defence that have defined the operating mantra of the functions that own and manage risk; oversee risk and provide independent assurance. We ask the question 'Is it time to reassess this model, allowing for technological innovation and the industry's investment in this area

since the 2008 crisis or has the industry missed an opportunity in failing to ask the question repeatedly 'what problem am I seeking to address and how best do I align my resources to tackle this issue', whilst meeting regulatory interpretation, to succeed? Is it time for a change in thought and execution?

Armstrong Wolfe will partner with a consultancy on its delivery

- We believe by partnering with a principal consultancy, it embeds an accepted degree of independence

What will Armstrong Wolfe provide?

- Programme oversight and governance
- Access to the global 1st Line Control and Conduct executive network and representative participation
- Presently the support of 20 global Chief Control Officers/ COO Markets to support and participate in the study (AW anticipates further banks will wish to participate)
- Armstrong Wolfe Partners: content bridge and insights provided by Larry List (previously BNP) and Simon Longden (previously Standard Chartered Bank)
- Perspectives to be delivered to the market:
- To the regulators
- To the industry bodies
- Initial findings presented at Armstrong Wolfe's global Conduct & Culture Summit 2020 (March week 1)
- Study to be presented to the iCOOC members (buy and sell side) in North America, Europe, and Asia
- Invitation by the FCA to present this study and its findings

Outline of engagement

- 20 (+) banks undertake a market survey
- participate in 221 discussions focused on survey output to define activity of the working groups
- 20 (+) banks broken down into 4 working groups of 5, mixed in geographical spread and business size
- Each group to deliver its findings to the other 3 groups for dissection and debate
- Findings of the 4 groups structured into one report and perspective
- Programme oversight provided by Larry List and Simon Longden (Armstrong Wolfe) working with the appointed consultancy
- It is envisaged this will be delivered in 3 months (April 2021)

ABOUT GCF BOSNIA

Goražde Children's Foundation

GCF Bosnia is a UK-based charitable foundation committed to helping rejuvenate the previously war-torn town of Goražde in Bosnia. The charity specifically supports Goražde Primary School and seeks to provide a brighter future for its children.

To date, through the foundation's efforts, an English language teaching centre has been established, and the previously war-scarred playground has been refurbished into an all-purpose Astro Turf for the children to play sportonce again. Future plans include the construction of a fully equipped science classroom and the renovation of six further classrooms in dire need of modernisation.

GCF Bosnia was founded by Maurice Evlyn-Bufton, who was previously a captain in The 1st Battalion Royal Gloucestershire, Berkshire and Wiltshire Regiment (1RGBW). He served with the battalion on United Nations' service, as part of its peacekeeping force during the Bosnian conflict (1992–95) and is currently Managing Director of Financial Services advisory and executive search company, Armstrong Wolfe. GCF Bosnia was set up in memory of four of his comrades, who were killed whilst on operational service as part of the United Nations' deployment in Bosnia.

In the late summer of 1994, the newly-formed Royal

Gloucestershire, Berkshire and Wiltshire Regiment (RGBW) conducted its first operational tour. This was as part of the United Nations Protection Force (UNPROFOR) – the first of three international missions that assisted in bringing peace and stability to this troubled part of the Balkans.

Battalion Tactical HQ, A and B Companies 1RGBW were based in Goražde, one of the three Bosnian Muslim eastern enclaves inside Bosnian Serb territory, south of Srebenica. Their mission was to protect the 60,000 Bosnian Muslim refugees from the Bosnian Serb Army besieging the town. For a number of reasons, due in no small part to UN military intervention, it did not suffer the fate of its neighbours Srebrenica and Zepa. After the fall of these towns, Goražde became the last Muslim enclave in eastern Bosnia.

Defended by UN forces throughout 1994–95, it was not until the ceasefire and Dayton Accord that the roads from Goražde to Sarajevo were opened to civilian and UN traffic. Conditions in Goražde had been harsh, bearing the scars of years of a bitter

struggle. Tragically, during this tour, in September 1994, Privates Ben Hinton, Philip Armstrong, Martin Dowdell and Chris Turner were killed in two separate incidents. In addition, a number of 1RGBW and Corps-attached soldiers were injured and have suffered both short-term and long-term medical and mental effects.

In 2012, seventeen former comrades of 1RGBW returned to Goražde to replace the memorial stones to their fallen comrades, this time dedicated by the battalion's 1994 padre, Patrick Irwin, and the Reverend Andrew Grant. On the last day of this visit, the group was invited to the local primary school and was surprised by the children singing them a song in their language, thanking the British Army for saving their parents and grandparents.

Moved and inspired by this gesture, Maurice asked the school's headmistress what he could do to help. From this discussion was born a commitment to support the school, both in memory of their fallen comrades and as an investment that would benefit the future

generations of Goražde, the Bosnian town the soldiers of 1RGBW had defended many years before.

Through his company Armstrong Wolfe, Maurice has raised over £65,000 to date to help fund the school's ambitions.

In addition to various fundraising activities, in March 2015 Maurice and a number of employees from Armstrong Wolfe ran a marathon starting on the hills above Goražde, to be welcomed by the children cheering them as they crossed the bridge that took them over the river Drina and back to the school. Maurice has now committed to providing a new science classroom to sit alongside the English language centre, which he hopes will be of great benefit to the young children of Goražde.

For more information, go to www.gcfbosnia.org

"Thanks to GCF Bosnia's strong support, my students have been able to make great progress in their English learning process.

Books and teaching materials offered by our English friends helped all of us to teach and learn in far better conditions.

We are so grateful for such a generous gift and hope to have a good cooperation in the future as well."

Zahida Alic – English teacher at Goražde Primary School

ABOUT SIGHTSAVERS

Introducing Sightsavers

Sightsavers is an international development organisation focused on eliminating avoidable blindness and ensuring equality for people with disabilities in developing countries. They believe that no one should be blind from avoidable causes, and that people whose sight can't be saved should live with dignity and independence. Sightsavers works with local partners, focusing on those living in poverty in over 30 of the poorest countries in Africa and Asia.

Eye health

Globally, over 285 million people are visually impaired, including 39 million blind people. Ninety per cent of those affected live in developing countries, and an incredible 80 per cent of all visual impairment is known to be preventable or curable. People affected by visual impairments are far more likely to experience lower incomes, unemployment, hunger, a lack of access to health services and exclusion from education and society.

Sightsavers supports and strengthens local eye care systems to tackle preventable blindness. They provide specialist training for health care professionals, increase public awareness of eye care

and lobby governments to ensure it is universally available as an integral part of wider health care systems.

Working with partners in developing countries, they restore sight or prevent blindness for millions of people each year; from conditions such as cataracts, the leading cause of avoidable blindness, to river blindness and trachoma, two blinding neglected tropical diseases. Treatments for these conditions are inexpensive yet life changing; from just 7p to prevent or treat someone suffering with river blindness or 35p to prevent or treat trachoma, to a sight-restoring cataract operation costing just £28.

The impacts of these straight-forward treatments are enormous; for example cataract surgery can lead to increased economic productivity in the first year equivalent to 1,500% of the cost of the treatment itself. In 2015 Sightsavers supported over 70 million treatments to protect against blinding neglected tropical disease, and carried out over 255,000 operations to restore sight or prevent blindness.

Before Ranin (right) had even turned one, he was diagnosed with cataracts in his left eye. His parents were told that he would lose his sight if an operation didn't take place, but the cost of the operation was too much for them to afford.

Fortunately, Ranin was identified by a health worker trained in eye care under Sightsavers' programme in Bangladesh. His cataract was re-diagnosed and, as his family could not afford to pay, he received surgery free of charge. Following his surgery, Ranin is now a happy and playful boy, looking forward to playing cricket in the future.

Education and social inclusion

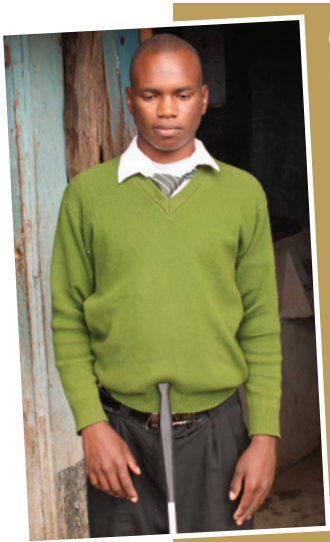
Sightsavers works to make sure disabled adults and children have the same rights and opportunities as everyone else, being treated as equal members of society. They believe that access to education is invaluable in helping people to escape poverty, and they work to make sure children with visual impairments and other disabilities get the chance to go to school.

Over a billion people worldwide live with some form of disability. In the developing countries that Sightsavers works in, people with disabilities such as blindness are often isolated and excluded from their communities. They typically have poorer health, lower educational achievements and higher rates of poverty. The opportunities for children with disabilities to gain an education are dramatically reduced, as they constitute more than one-third of the 57 million primary school age children not currently enrolled in primary school . In Africa in particular, less than ten per cent of disabled children attend primary school .

Sightsavers supports the principle of inclusive education; ensuring that all pupils, including those with disabilities, participate equally and learn together effectively. This teaches them from an early age that they are all equal and valued members of society. They run projects that deliver high quality education for children with visual impairments and other disabilities in their local schools. These projects are both scalable and cost effective, allowing Sightsavers to also use them as examples to lobby governments for change, ensuring that many more children with disabilities can access an education alongside their peers.

We also provide life skills and vocational training for both young people and adults with disabilities, supporting the formation of self-help groups and helping those groups to make the voices of their members heard by those making the decisions that affect

them. Alongside this they directly lobby governments to fulfil their obligations under international conventions for disabled people. In 2015 Sightsavers supported more than 3,600 children with disabilities to gain a mainstream education, and provided life skills and vocational training for more than 16,000 people with visual impairments and other disabilities.



Gideon (left) is one of the students supported through Sightsavers' inclusive education programme in Kenya. He was born completely blind and his parents had little hope of his gaining an education and independence, as the only school they knew of in Kenya that catered for the blind was in Thika, 350 kilometres away.

Fortunately, a local social worker told Gideon's parents about Sightsavers' recently established inclusive education programme in their area. He was referred to the programme and then placed at Korara Primary School, where he began learning alongside his sighted peers. Gideon proved himself to be both a bright student and talented musician, and in 2013 he gained his certificate of primary education, progressing to secondary school.

ABOUT ST. GEORGE'S SOCIETY OF NEW YORK

ST GEORGE'S SOCIETY OF NEW YORK

Patron: HRH The Duke of Gloucester KG GCVO

St. George's Society of New York (founded in 1770) is a membership organisation with a charitable purpose. It provides vital assistance to people of British and Commonwealth heritage in New York who are in need of financial and emotional support. For example, the sick, elderly and disabled as well as students who have the ability to succeed but lack the funds to complete their studies. The Society's vibrant network of influential people and partnerships with key organisations in the British community make it the pre-eminent Anglo–American social and philanthropic group in the tristate area.

Beneficiary Programme

Each year, with the generous support of its community, the Society is able to prevent seniors from losing their homes. Many of the St. George's beneficiaries are referred from housing court in a desperate attempt to stop an eviction. For these people, once they retired, they faced the struggle that their income was not sufficient to pay their rent so once all savings were depleted, the terrifying prospect of losing their homes becomes real. Most are unable to work and so without financial assistance they could indeed be forced into homelessness.

In addition to rent support, the Society provides help with home care expenses, medication, utilities and other quality of life supports. While financial assistance is critical, the St. George's Society's two dedicated social workers also offer much-needed emotional support.

"When I was diagnosed with cancer I struggled with the daily dilemma of whether to pay for medical supplies essential for my care or my housing costs. Thanks to St. George's Society, now I can focus on treatment and getting better without the worry of losing my home."

ENID FROM THE UNITED KINGDOM
ST. GEORGE'S SOCIETY BENEFICIARY

Scholarship Programme

St. George's Society assists British and Commonwealth students who have achieved excellent academic standing in their first three years but due to financial hardship are unable to complete their final year of undergraduate studies. Since 2008, the Society has awarded over $700,000 in scholarships to hundreds of students at Lehman College in the Bronx. Many of the Society's scholars aspire to pursue careers in health services, nursing, education and other professions that give back to the community.

"Thanks to the St. George's Society scholarship I have been able to invest time in studying, volunteering and internships in order to complete my Bachelor's degree in Biology. My dream

is to become a cancer specialist and I look forward to taking the medical college admission test this fall and moving closer to making my dream a reality."

KASHFIA FROM BANGLADESH
ST. GEORGE'S SOCIETY SCHOLAR

Medical and Emergency Relief

In addition to the Society's beneficiary and scholarship programmes, they also respond to appeals for emergency assistance, for people who are facing medical crises. In January 2015, the Society assisted a British couple who were visiting New York when their baby boy arrived 11 weeks early weighing just 3.4lb. The new parents were stranded in America for several weeks while baby Dax was monitored in a Neonatal Intensive Care Unit at Lenox Hill. St. George's Society provided funds to cover food, transportation and incidentals. The Society also offered guidance and paid the application fees for the newborn's passport to enable him to travel back to the UK once he met the minimum weight requirement and was able to breathe and feed on his own.

"When I gave birth to Dax prematurely, it was the hardest thing we have ever faced. Without St. George's it would have been very difficult to cope. They were a massive help and a huge shoulder when we needed it the most."

KATIE, DAX'S MOTHER

These are just a few examples of the life-changing assistance that St. George's Society provides to people in desperate need thanks to the support of its members and friends.

You can join today or donate online at
www.stgeorgessociety.org
St. George's Society of New York
216 East 45th Street, Suite 901
New York, New York 10017
212 682 6110

St. George's Society of New York is a registered non-profit 501 (c) (3) organisation. Tax ID: 23-7426425. The Society receives no government funding and its charitable programmes are primarily funded by membership dues, donations and events.

The value of the role in the new paradigm, post pandemic, will be determined by its ability to look forward, look outward, undertake horizon scanning and focus on emerging risks.

2021 A CHANGE IN DIRECTION FOR THE CCO

Epilogue

I started writing this book without knowing, when in 2015 I penned my first paper on the developing role of the Chief Control Officer. six years later, updated, this article found itself into this book as an early chapter.

In the last 12 months, locked down and tucked away at home amidst the global pandemic, it gifted me time to reset my efforts to complete this book, albeit two others have found their way to print since my first CCO paper was etched.*

In this six-year period, the CCO has evolved, changed and adapted. I have been fortunate enough to have worked closely with this community throughout, this book being completed at a time when the COO and CCO mandates appear to be moving from a steady state to being pushed to think more creatively and to broaden their mandates and responsibilities.

To this end, to frame these emerging themes, five things mark the end of this journey with the CCO and resets the dial for my continued partnership with this community as it enters a new chapter.

- A global community - The International COO Community (iCOOC)
- Maintaining faith - Cultural Surveillance (a POV)
- An emerging theme - Threat Management (a POV)

- Market-wide engagement: Addressing legacy challenges with a 1LoD review of 3LoD
- The Conduct & Culture Summit 2021 (Purpose over Profit) April 19 – 21 2021

In February 2020, Armstrong Wolfe (my company) was facing an exponential crisis, with executive search revenues paused and all 54 pre-booked forums for 2020 cancelled within the last seven days of the month. Our sponsors varied their responses as to what to do, but commonplace was no meaningful discussions on furthering the relationship amidst such uncertainly.

Albert Einstein said, "In the midst of every crisis, lies great opportunity." It was not so much that I saw an economic opportunity in pivoting the business to meet the challenge presented to the banks and asset management communities by the pandemic, but a moment in time when we could add value and prove the worth of the COO community we had established.

The founding principles of our COO community efforts that we had nurtured since our first forum in 2015 had been based upon bringing the COO community together in a round table format to discuss market-wide non-proprietary challenges, hosted by a bank or asset manager and held in a Chatham House Rule environment.

Taking the economic and human tragedy out of the discussion, Covid-19 was exactly this, a market-wide challenge of unprecedented proportions. Taking our product from the physical to the virtual was the first challenge and to meet this test in March 2020 we ran 45 COO calls, webinars and symposiums. Our aim was to offer a platform for COO and CCOs to talk on subjects of granularity, as they grappled with putting their workforce into a WFH configuration and to bring solutions and thought leadership to help them navigate their way through the pandemic.

The human, technological and supervisory demands lay at the

feet of the COO and CCO and to this partnership the eyes of the business turned for guidance. 12 months later in the spring of 2021 they are tasked to plan for a workforce exit from pandemic restrictions and to take their business into a new paradigm. Whatever workforce model adopted, the COO and CCO will be at the heart of decision-making and remain at the centre of operations when the industry moves forward to find a new steady state.

In response to our efforts, in April to May 2020 a handful of banks and asset managers kindly offered to pay us for the work we had been doing in supporting them. We thanked them but requested instead they back us as we sought to change our business model to a paid corporate membership, and to this end by Q1 2021 iCOOC (the International COO Community) secured 37 banks and 26 asset managers as founding members.

In this interim 12-month period much time was spent in debate across the industry as to the significance of mission, purpose and CSR, highlighted by the pandemic and leading a dislocated workforce. Listening, learning and adopting, we sought to practice what we were promoting and preaching in setting our own guiding principles:

All AW employees and partners will commit to and focus on operating within and to AW's mission, purpose and CSR:

Our mission is to bring worldwide COOs into a managed network one degree of separation from each other.

Our purpose is to empower this community by providing thought leadership, promoting cross industry dialogue, and supporting collaboration, design and execution.

Our corporate and social responsibilities focus on addressing inequalities, promoting sustainability, and supporting underprivileged children and early adult education.

Our ability to succeed relies on a global interconnected offering:

Delivering on our mission
The international COO Community (iCOOC) - COO corporate membership scheme

Delivering on our purpose

- AW Institute – innovation hub to create ideas and drive learning for COOs
- AWP - advisory and project execution
- AW Strategic Partners –appointed advisory and technology companies
- AW Ecosystem – trade associations, academic bodies and institutions
- AW Industry Advisors – COO alumni working within professional services
    - Perian – a global executive network of highly respected former COOs

Delivering on our corporate and social responsibilities

- Women in the COO Community (WCOOC) – driving diversity and inclusion
- WCOOC Ambassadors – a global network of voluntary appointed COOs
- The COO Academy – creating opportunities for underrepresented socio-economic communities
- GCF Bosnia – rebuilding a primary school in war-torn Bosnia
- Sustainability – leveraging iCOOC's membership to call to action

Reinvented, repurposed and reset, between March 2020 to March 2021 we established our global community (iCOOC), an execution and project management business (AWp) and the Armstrong Wolfe Institute (AWi), providing training to the business management community. We gathered a group of COO ambassadors committed to supporting us and extended the influence and reach of Women in the COO Community (WCOOC), adding to it the COO Academy, to provide career opportunities for the underrepresented and under privileged. We retained our connection with our charity in Bosnia, diverting some of its funds to provide food boxes to single mothers of pupils from the school the charity supports, in a country where social services and benefits are lacking. We captured what we were doing by launching The COO Magazine, which by April 2021 had a quarterly global readership of over 5000 COOs and business managers. This achieved in equal measure by market-wide patronage, and the hard work and innovation of the employees of Armstrong Wolfe. We focused on the near-term, but our activities were guided by the mid to long-term objectives framed by our mission and purpose. Indeed, amid every crisis, lies great opportunity.

The steppingstones for the future were further set for late April 2021, as we promoted a three-day conduct and culture summit, with a multitude of COO guest speakers and panellists, leading academics and technology and advisory voices committing to support our first conference (see below agenda).

Being committed to using our platform to promote our own thoughts, I retained faith in the role of leadership and its influence on culture as a cornerstone of conduct risk management (see POV Cultural Surveillance) and a belief the COO and CCO mandates can be better used to help manage future events, with the emerging theme of threat management holding court at many forums and given the stage at the summit (see POV Threat Management).

Whilst looking to the future, we paid attention to the echoes of the past. In January 2021, we secured the participation of the global CCOs of 32 banks to undertake a review of the 3LoD, to deliver a paper and conceptual principles to address the and challenges that had become resident in most banks in the inter-relationship between 1 and 2LoD. This effort was not to redistribute or dilute accountability but to enhance efficiencies and as a by-product deliver costs efficiencies and savings. At the point of writing, this report will be presented to the FCA in June 2021, having established a dialogue directly with the regulator. In doing so, our intention is to be the advocate of the COO community, to give it a voice to the regulator, when traditionally the narrative has been set by the bi-lateral conversations held by the regulator with either compliance or the head of the business.

All the above would be captured at the three-day summit, which for me personally draws a line in the sand, a line that can be drawn back to 2008, but also establishes a platform to move forward. The distant events of 2007 – 2009 and how they had shaped my thoughts and set the direction I was to travel professionally, linked intricately to my personal journey, come together on these three days. My father (a career ex-retail banker, who passed away in 2008 see chapter XXX), would hold opinions on the summit's subjects of debate. He was from an age when the bank manager was noted in official documentation as a trusted referee beyond reproach. He carried this responsibility in his professional and personal life, and I hope he would be proud of his son for doing what he could to bring this reputation back into consideration: to be an accepted and embraced responsibility by all those that manage and lead an industry embattled and deeply wounded by the actions and intent of a minority in the past.

"Life is divided into three terms - that which was, which is, and which will be. Let us learn from the past to profit by the present, and from the present, to live better in the future."

WILLIAM WORDSWORTH

*2017 No Place to Hide (the evolution of the Markets COO in the new regulatory era) and 2018 Donkey Mail and Bully Beef (The art of survival: memories of British soldiers in the former Yugoslavia)

CULTURAL SURVEILLANCE

The industry must focus on developing a Cultural Surveillance capability to meet the Conduct challenge
POV provided by Maurice Evlyn-Bufton, CEO, Armstrong Wolfe

Part 1 Asia Conduct Forum Series September 3rd, 2020.

POV: The Industry must focus on developing a Cultural Surveillance capability to meet the Conduct challenge

By revisiting the evolution of the industry's approach to conduct over the years, the Asia COO Conduct Forum's aim, held recently, was tasked to identify specific areas for deep-dive discussions to be held within subsequent forums. These more specifically known as AW COO Cluster Calls (6 – 8 COOs attending), to be undertaken before year end, all held under Chatham House Rule. To drive the conversation to this end objective, the following questions were asked:

"How do you marry technology, process, and training to deliver an effective Conduct Framework? "

"How do you best protect your organisation against insider threat? "

It was not surprisingly concluded it is a multi-faceted reliance on technology, well defined processes, and procedures, which must be married to leadership (at all levels), culture and purpose, that will deliver a robust, reliable, working and value-add Conduct Framework. Easily said, not so easily done.

Technology and the art of the possible opened the debate, where the capture and use of data enabling you to move to a predicative, forward looking line of attack (as opposed to defence) and therefore being on the front foot, was seen as the fundamental adaptation needed to reposition the industry's efforts in grappling with Conduct. In doing so enabling you to undertake material, as opposed to judgemental, horizon scanning and to evaluating emerging risks more effectively. This falling under what we classify as threat management.

The aging debate over in-house as opposed to vendor selection appears to be moving strongly in favour of external innovation and product development, as opposed to the historical reliance to design and build internally, 'there is an irreversible move to accepting that banks are not technology houses and can no longer compete on cost or within innovation with the open (technology) market' one COO commented. The challenge of sourcing and engaging with the FinTech community remains, although this area we believe presents opportunities for cross industry collaboration (within controls and conduct).

The conversation moved from the technical domain to the human, one participant and leading Conduct executive noting 'increasingly our focus is shifting from the technical to the human sphere of influence to meet the challenges presented by Conduct'.

Prompted by this contribution, we outlined our evolving thoughts, to be captured within an academic study, on the concept we have classified as Cultural Surveillance. This is explained at the highest and simplest level as being (literally) the ears and eyes of the business that make up the invisible control and defensive framework of a company, where MI5 was noted as an organisational example where its very existence relies on this cultural necessity being present.

It is our opinion that this invisible supervisory capability is

roused and energised by purpose, effecting a heightened level of intuition and is intricately linked to a philosophy that offers all employees the stage to speak up - speak out on any matter that they, as an emotional stakeholder in the franchise, perceive as being a institutional or material threat to the running of their company. This sense of doing right, of protecting the business and therefore also your colleagues, is a cultural aspiration for many but is achievable and if attained will deliver highly effective Cultural Surveillance.

Supported by technology, process, and procedures (and none in isolation), it was argued it acts (or could act if present) as the primary tool to defend a company against insider threat. Statistics and industry COO and Chief Control Officer opinions strongly support this notion, that colleague disclosure is a far more prolific at detection and uncovering misdemeanour than technological surveillance. The latter, some argue, acts more effectively as a deterrent than as a proven or equal participant in detection or as a discovery capability to human intuition and observation.

This supposition does not account for the potential of evolving technologies that focus on behavioural analysis and predictive analytics, but even with such advancements, such technologies will at best be able to more effectively partner human observation as opposed to replace it. This especially so where human observation has been heightened and become a cultural norm, manifesting itself as a Cultural Surveillance capability.

With conversation flowing, we moved quickly to summarising where the industry is today and that despite the monumental effort and investment of the industry over the last decade, such misdemeanours, poor practices and deceits sadly and almost unbelievably continue.

The question arose therefore, not so much to 'why invest in

the conduct agenda, in developmental and leadership training and technologies' but how do you build a commercial case for doing so, that will enable the industry to continue to invest in, grapple with and resolve its sickness?

This sickness has been controlled via a regulatory lockdown but still requires a preventative vaccine. This vaccine many believe is to be born from a continued evaluation and investment in individual company's and by extension the industry's culture. Ironically, extending the medicinal metaphor, the term 'culture' is extraordinarily relevant*.

It was concluded that you must ask yourself repeatedly, why should we do this?

A point of future debate perhaps:

- It is not because you must do it through regulatory necessity
- It is not to deliver a commercial return on this investment
- It is because it the right thing to do

The right thing to do, why? Simply because the banking industry is the steward of the world's finances, where ethical behaviour is the basic assumption those that entrust this stewardship set their expectations. Therefore, the industry has an obligation to meet these expectations.

Such an investment would liberate the possibility of a working environment where Cultural Surveillance becomes the unseen control framework that enables businesses to operate safely, efficiently and with their employees working to and within a purpose that delivers:

- enhanced productivity and profitability
- meets, exceeds the regulatory requirements

By doing the right thing, you may well, more than likely deliver upon the commercial and regulatory imperatives that have to date have shaped and driven actions undertaken to address the challenge of conduct. However, a decade of investment has shown that whilst the industry's undoubted efforts and accomplishments have taken the patient from ICU into a recovery ward, this patient has not yet been let go from the hospital on the basis of good health and all symptoms cured.

> ** Culture: In microbiology, the propagation of microorganisms in a growth medium. Any body tissue or fluid can be evaluated in the laboratory by using culture techniques to detect and identify infectious processes. Culture techniques can be used to determine sensitivity to antibiotics.*

Actions: It was agreed that Simon Longden and Gordon Grant (Armstrong Wolfe Partners) would engage in 221 follow up conversations with attendees to define the subjects for subsequent debate, oriented to technologies, leadership and reviewing the governance and 3 lines of defence model.

For detailed conversations contact s.longden@armstrongwolfe.com or g.grant@armstrongwolfe.com

For more information and/or to participate in the future debates and COO Cluster Calls (at managing director level) please contact r.reid@armstrongwolfe.com

THREAT MANAGEMENT

Evolving perspectives amidst the pandemic

Defining Threat Management

Entering 'threat management' in the Cambridge Dictionary it will offer you 10 disciplines of management: talent, event, asset, time being four, but threat is not one of them. As an alternative it presents:

> You can also search for 'threat' and 'management'.
> **Threat:** a suggestion that something unpleasant or violent will happen, especially if a particular action or order is not followed.
> **Management:** the control and organisation of something
> (Cambridge Dictionary)

If you complement this with a Google search using 'threat management definition' as your reference, you are taken to a multitude of options and opinions. All, however, see threat management as an umbrella term for the computer security and information security programmes instituted in an organisation. Clearly the concept of holistic threat management has not become common practice. Why is this?

There is a point of view that threat and its many dimensions, come together at the intersection of non-financial, conduct, cyber,

ESG, geo-political and enterprise-wide risk. These established risks have become increasingly overshadowed by climate change, which poses significant risks to the financial system, particularly for the insurance and banking sectors. The question is whether a clustering of this data could be generated allowing value assessments to be made in a broader threat management context?

Additionally, Covid-19 re-emphasised the importance of pandemic risk management. The short-term risks and challenges presented to employers include an unforeseen change in working practices, with industry workers proving they can be just as productive and accountable when WFH. How the industry and its participants will deal with this change in the long-term is to be determined. The importance of getting your positioning right, however, and investing in precise training, tooling, and rewarding of staff (to maximise workforce performance in the new world post pandemic) could materialise into a human capital risk. This risk is important within an industry highly reliant on hiring and retaining the best people, and where workplace options may shift the focus from corporate allegiance and compensation to work placement optionality and culture.

Human Capital Risk in this context is heightened when additionally accounting for the evolving liabilities on mental health and a duty of care towards employees and more materially, the anticipated conduct and cultural challenges that will become evident with the passage of time.

Threat, you could argue, is uttermost when one meets another or triggers another. More so, in the case of the pandemic and like the disease itself, its consequences are contagious, fuelling other risks to become an exponential one.

Threat Management could therefore be defined as is a discipline that is complementary to and encompasses established risks and is best understood in the capacity of horizon scanning and the ability

to detect and determine actions to emerging risks. Its methodology would rely on the integration of established risk data, to be looked at in real-time with its aim being to detect early signs of potentially important developments (that could impact the business) through a systematic examination of potential threats and opportunities, with an emphasis on the use of new technologies, data aggregation and digitisation.

Non-Financial Risk within the continuum of Threat Management

Post Pandemic

An opportunity to change thought and action for the COO?

The pandemic is an interesting case study to apply thought for holistic threat management. All the threats listed above have been surpassed and to differing degrees, stimulated by a lack of pandemic risk management. We have an established understanding that a pandemic is a rapidly spreading infectious disease that may (SARS 2002 and 2004) and could (Covid-19) show a pandemic's ability to create social and economic chaos, severely upsetting business operations and producing disruption in the supply chain. It has further impeded commerce and industry's ability to deliver products and services to customers.

Unquestionably, therefore, managing the threat posed by a pandemic is critical for business survival. To do so we must ask, what is the international community's and individual nation's risk appetite and risk tolerance [in the context of a pandemic]? How much risk management is enough? What are the responsibilities of corporations as well the regulators that monitor them? What expectations should customers have and what liability should banks, asset managers and financial institutions accept in managing this risk? Without addressing these and similar questions, we are likely to end up with poorly conceived, contradictory, and costly strategies that could increase risk.

Policy making is part of the solution, preparedness another, but horizon scanning and looking at this challenge through a forward-looking, threat management lens, could make a material difference to a business and/or the industry's ability to anticipate such events and mitigate damage (when it next happens).

This risk must not be looked at in isolation. Where post-pandemic reviews will point to failures of governments to prepare and meet their obligations and industry-wide failures to prepare for

such an inevitability will also be identified. These failures and lack of preparedness will be better handled in the future if managed as an inevitability, a threat that will materialise, and if planning to meet this inevitability is mandatory. It is a matter of 'when' and not 'if'. If this assumption is accepted, there will be a need to place its influence and impact in a perspective of understanding how it could promote, effect and shape other risks and events.

So what? This question arises when a threat or series of apparently unrelated threats arise at the same time. Who in any company is positioned to guide the CEO and to help set an anticipatory course of action based upon a broader appreciation and understanding of threat management? Presently such guidance is not supported by an aggregated data of all risks and is given in respective quotas by the CRO, the CISO, Legal, Compliance and the COO. What a different approach to threat management could enable the CEO to do is make decisions in confidence and to the best of his/her knowledge and abilities (based upon a uniformed assessment of all risks).

Creativity within Threat Management

The commercial consequences of the pandemic were made worse by the industry having no meaningful pandemic risk management system in place. More so, it was a failure of the imagination. This threat has existed throughout modern mankind's 100,000-year residency on Earth; pandemics having a routine visitation on humanity. Many refer to the Spanish Flu pandemic (1918-1920), although there were three worldwide pandemics and outbreaks of influenza in the 20th century: 1918, 1957, and 1968. The latter two were in the era of modern virology and most thoroughly characterised. All three have been informally identified by their presumed sites of origin as Spanish, Asian and Hong Kong influenza,

respectively. Recently there were two self-limiting SARS outbreaks in 2002 and 2004. The limitation and containment of their impact may in part explain the lack of preparedness for Covid-19. It is clear post SARS incomplete contingency planning was adopted to meet a future pandemic. This has prompted reviews of how Covid-19 should have been an anticipated event. In doing so policies should have been developed within contingency planning to meet this challenge.

Lessons learnt? What is important is the role of creativity and open thought, the active promotion of asking the 'what if', and the right to suggest and assess the improbable becoming possible.

> *"Not thinking it's possible is a failure of the imagination"*
>
> VINOD KHOSLA (CO-FOUNDER OF SUN MICROSYSTEMS)

Is there a role for the COO within Threat Management?

In line with pre-pandemic thoughts on threat management and responding to feedback from the COO community attending our forums amidst Covid-19, we undertook a market survey and set a series of COO cluster calls to discuss the possible benefits and challenges of managing threat holistically.

Some COOs had highlighted an evolving expectation, to have an appreciation, to understand real time operational and non-financial risk, but in a broader context. They were being asked to do so with a fragmented and disconnected view of the overall threat and risk landscape.

Questions arising from these cluster calls set the survey:

- How the COO can establish a better view and understanding of the threat and risk landscape, and what challenges do they foresee?
- How to differentiate between the responsibilities of the COO, CRO and Heads of Legal.
- Compliance, to define a new approach to managing risk and threat that works in the best interests of the organisation.
- What are the areas of support and improvement the COO is seeking in this context to enable them to deliver on their principal responsibility – to protect the franchise.

In conducting the review, Armstrong Wolfe surveyed a representation of COOs from across the community, buy and sell side. The survey was broad in nature, and sought opinions on:

- A view on the maturity and effectiveness of the risk management framework.
- The focus in risk meetings & the extent to which it is "here and now" versus horizon scanning.
- The engagement across the c-suite, particularly with CRO, CISO, legal & compliance.
- The use of risk information within the firm, and the confidence in the quality of data analysis.
- A view on risk systems and process and what they believe could be improved upon.

Survey Output

a. Proactive Identification of Emerging Threat

COOs were unanimous in the view that for their role to be most impactful, they require a broader and more informed view

across risks and threats which impact the franchise. They see the ownership and stewardship of risk as a collective responsibility and are well positioned to support in the translation of those risks into deliverable action plans. There is a challenge, in that the prevalent use of people's time and the focus in risk meetings is on the "here and now". Some firms have invested energy into considering emerging trends and horizon scanning, though this practice could be more robust and where it is conducted is focused more to regulatory change, or cyber, with less consideration given to geo-political events.

b. Efficient Governance Structure with Global Reach

COOs do not see the potential for conflict with the CRO, CISO, legal and compliance, if they were to have a broader view across threats and non-financial risks. There was a consistent message that they must work proactively to make those relationships effective, and to ensure those functions fully understand a local or regional concern and the potential business impact of it. While COOs value the independence and challenge from those roles, there can be issues where there is a strong vertical reporting line for those functions. COOs are looking for the governance structure to enable a more holistic and informed view of the overall risk landscape so they can fully consider its implications.

c. Enable Strategic Decision Making & Operational Control Implementation

Over 70% of survey respondents were not fully aware of the breadth and depth of risk information available within the firm, did not fully understand how it was collated, analysed and distributed, did not believe it was presented in a digestible format and did not have

full confidence in it, nor the analysis that accompanied it.

Risk data and metrics can be very granular, which can be helpful at one level, but can make it harder to identify the material issues quickly. The information packs for risk meetings are often too large, with concerns expressed about the ability to digest them fully beforehand. As it can take time to get to the heart of the real issues, a consequence is that there can be insufficient time spent considering emerging risks and to conduct horizon scanning.

d. Prioritises Leveraging Internal Resources to Focus on Highest Risk Issues

To address this challenge, while there is some tradeoffs that can be made by COOs, including delegation of activities to declutter their inbox, there was a clear message that they see the need to attack the problem of prioritisation with improvements in data and automation.

e. Leverage Technology

When asked to consider how effective risk management was in the context of strategy, governance, culture, business, and operating models and against the use of data & technology, the weakest area by a clear majority was on the use of data and technology. Examples provided included continued use of legacy systems, underinvestment in technology and the ongoing reliance on Excel. COOs want better structure and organisation of the data, particularly regarding the mapping of data into risks to further aid the analysis to enable them to get to the more material issues quickly which will free up time to consider emerging trends and conduct horizon scanning.

2. Bearing in mind this feedback, working with a risk management 3rd party, we sought to demonstrate the range of solutions that could be brought to bear to support COOs across a range of issues of varying scale and complexity. At one end of the spectrum were specific insights into a proven ability to analyse and advise on a specific geo-politically driven event and its ability to severely impact a financial services organisation, namely the imposition of the new Hong Kong national security law. This included:

- **Concerns as to how MNCs might have to flex and structure themselves to** handle an increasingly adversarial sovereign relationship between China and the USA.
- **Determining how well banks in turn understood how their clients** in Hong Kong specifically and Asia generally might be reacting to this worsening relationship.
- **The impact on Hong Kong's reputation** as a place to live and work for professional expats and HK residents.
- **The potential alternatives** to Hong Kong should institutions be forced to relocate in the region, and the risks associated with those options.
- **Impact on back office operations** – For example there has been talk of the US using the threat to cut China off from the global SWIFT messaging and payment settlement platform. While China has its own internal clearing system, it does not yet have the same adoption. If it were to scale up, what does that mean for back office processes, or data security, and for ensuring systems and operations integration to execute seamless processing, transaction monitoring and screening?

3. At the other end of the spectrum, we outlined experiences of designing and helping clients implement programmatic

solutions which explored how institutions tackled the challenge of collating, analysing and disseminating non-financial threat and risk data in a manner which addressed the issues COOs were most concerned about in the survey feedback.

The overarching principles of such programmes can best be summarised below:

MUST:

- Identify high risk scenarios according to rigorous and consistent criteria.
- Inform decisions and controls with risk-focused intelligence assessments.
- Connect dots between siloed analytics and intelligence.
- Focus on proactive indicators and early warnings.
- Involve liaison with other teams on assessment methodologies.
- Conduct targeted multi-source data analytics.

MUST NOT:

- Own risk, but rather be a force multiplier to help lines of business manage their own risk.
- Duplicate or usurp risk-management efforts by other units already under way.
- Overestimate its ability to predict events or influence outcomes.
- Infringe on privacy regulation, national or international law, or adversely impact corporate culture.
- Rely on dragnet analytics or experimental technology instead of human capability.
- Over-spend before establishing a consistent and proven initial capability.

We also discussed the different delivery models that could be used

to deliver such a programme, the roadmap involved and example projects, timelines and indicative costs.

4. What do we seek to understand from you?

a. Does the feedback from the survey resonate with you? If so, how specifically does it impact you in your role?

b. Are you motivated to make change at your organisation and if so, what is the strength of your current interest levels and ability to effect that change?

c. What help do you need to scope the requirement and/or communicate the need internally if any?

By way of guidance re: the above, and from our two workshops with the Markets and Asset Management COO communities, the feedback on this set of questions was:

- Two global brands felt they wanted immediate support with geo-political horizon scanning beginning with China and the trajectory of the future relationship with the USA, and secondly, clarity around the scenarios relating to Hong Kong and the impact of the national security law on their HK operations.
- One global brand seeks analysis on the potential for severe market, economic and societal impact in the USA in the event of a closely contested and disputed election.
- One global brand wanted to discuss how to broaden and deepen the array of high-quality data sources and analysis relating to non-financial threat and risk that they were using to inform their strategic decision making (and subsequent operational controls).

- One Asia focused brand wanted to discuss a full programmatic approach to non-financial threat and risk management.

Case Study: geo-political risk.

What does this mean for the COO?

The next phase of evaluation of how to (or whether we should) operationalise an approach to threat management, will be to take geo-political risk as a case study, and apply collective thought to its management from a COO's perspective.

We will assume that the top of the house, the board, regularly receives geo-political assessments from one or other of the world's leading advisory firms. The question is how this information is distributed and what analysis is undertaken to answer the question 'so what?' We will investigate how this data could be better used to help the COO take anticipatory actions and take the COO from a reactive, on the back-foot position to one that can initiate actions to dilute the potential impact of this risk. We will also look, through lateral thought and dissection, and speculate how this risk could have unforeseen impacts on different parts of the entirety of the business.

This will be timely, as 2021 – 2022 will be challenging on many fronts for companies and investors.

Monitoring risks, developments and trends will be essential in the quest for opportunity; identifying the primary risks and then analysing them through the 'so what' lens will be key to finding a path to progress.

We will present geo-political risk at a series of COO cluster calls, testing the above and debating how the COO (or if not the COO, who?) could play a role in managing threat. Whosoever would need to be armed with the data to interpret and translate

into answers and perspectives to the question 'Threat - so what?" Where notedly the inability to provide data is an emerged problem of an imperative nature and as such, a principal threat.

2021 geo-political risks

All change with a New U.S. President + China & Hong Kong + Cyber Warfare + India-Pakistan + Popular Unrest +

More Difficulties for Western Democracy + Gulf Conflict + Technological Arms Race + Latin American Divisions + Protectionism & Isolationism

BIBLIOGRAPHY

The following publications and websites informed the writing of this book and are referenced as such.

Alloway, T. (2015). *Here's a Simple Lesson in Ethics From the Former CFO of Enron*. [online] Bloomberg.com. Available at: https://www.bloomberg.com/news/articles/2015-07-02/here-s-a-simple-lesson-on-business-ethics-from-the-former-cfo-of-enron

Becker, G. (1974) *Crime and Punishment: An Economic Approach* [online] nber.org. Available at: https://www.nber.org/chapters/c3625.pdf

Carney, M. (2017). *What a Difference a Decade Makes*. Institute of International Finance's Washington Policy Summit. The Regan Centre, Washington DxC

Centrify. *The Impact of Data Breaches on Reputation and Share Value*. [online] Centrify.com. Available at: https://www.centrify.com/resources/the-impact-of-data-breaches-on-reputation-and-share-value/

Cobley, M.(2017). *FCA chief Bailey takes aim at 'greed is good' culture.* [online] Fnlondon.com. Available at: https://www.fnlondon.com/articles/bailey-takes-aim-at-greed-is-good-culture-20170316

Cohan, W (2015). *Can Bankers Behave?* [online] TheAtlantic.com. Available at: https://www.theatlantic.com/magazine/archive/2015/05/can-bankers-behave/389558/

Cohn, A. Fehr, E and Maréchal, M (2014) *Business culture and dishonesty in the banking industry*. [online] Nature.com. Available at: https://www.nature.com/articles/nature13977

Crossan, M., Byrne, A., Seijts, G.., Reno, M., Monzani, L. and Gandz, J. (2017). Toward a Framework of Leader Character in Organizations. *Journal of Management Studies*, 54(7).

Crossan, M., Mazutis, D., Seijts, G. and Gandz, J. (2013). Developing Leadership Character in Business Programs. *Academy of Management Learning & Education*, 12(2), pp.285-305.

Curtis, G. (2008). *The Financial Crisis and the Collapse of Ethical Behaviour.* [online] The Big Picture. Available at: http://ritholtz.com/2008/12/the-financial-crisis-and-the-collapse-of-ethical-behavior/

Dudley, W (2017). *Remarks at the cultural imperative- An interbank Symposium.* [online] NewYorkFed.org. Available at: https://www.newyorkfed.org/newsevents/speeches/2017/dud170111

Dudley, W (2014). *Enhancing Financial Stability by Improving Culture in the Financial Services Industry.* [online] NewYorkFed.org. Available at:
https://www.newyorkfed.org/newsevents/speeches/2014/dud141020a.html

Egan, M. (2017). *Wells Fargo uncovers up to 1.4 million more fake accounts*. [online] money.cnn.com. Available at:
https://money.cnn.com/2017/08/31/investing/wells-fargo-fake-accounts/index.html

Elkind, P. (2013). *The Confession of Andy Fastow*. [online] Fortune.com. Available at:
http://fortune.com/2013/07/01/the-confessions-of-andy-fastow/

Enrich, D. (2015). *The Unravelling of Tom Hayes.* [online] wsj.com. Available at:
http://graphics.wsj.com/libor-unraveling-tom-hayes/1

Enrich, D., Cimilluca, D., and Das, A. (2013). *Senior UBS Banker to Exit*. [online] The Wallstreet Journal Online, Available at:
http://online.wsj.com/article/SB10001424127887324880504578300242536621214.html?mod=wsj_share_tweet

Erheriene, E and Patrick, M (2016). *Iranian Miniskirts, Bags of Cash Raise Doubts Over Controls at HSBC.* [online] The Wallstreet Journal. Available at:
https://www.wsj.com/articles/hsbc-struggles-to-bring-money-laundering-vigilance-up-to-snuff-1459279408

Federal Reserve Bank of New York, (2015). *Reforming Culture and Behaviour in the Financial Services Industry*. [online] newyorkfed.org. Available at: https://www.newyorkfed.org/medialibrary/media/newsevents/events/banking/2015/culture_workshop_summary_2015.pdf

Financial Conduct Authority.(2013). *FCA Risk Outlook 2013*. [online]. Available at: https://www.fca.org.uk/publication/business-plans/fca-risk-outlook-2013.pdf

Finch, G (2017). *World's Biggest Banks Fined $321Billion Since Financial Crisis' Bloomberg News*. [online] Bloomberg. Available at: https://www.bloomberg.com/news/articles/2017-03-02/world-s-biggest-banks-fined-321-billion-since-financial-crisis

Flood, C (2016). *Cracking down on "megalomaniacs and bullies. Financial Times* [online]FT.com. Available at: https://www.ft.com/content/f27c3620-f00d-11e5-9f20-c3a047354386

Forcepoint. (2018). *The General Data Protection Regulation (GDPR)*. [online] Forcepoint. Available at: https://www.forcepoint.com/sites/default/files/resources/files/ebook_gdpr_key_themes_en.pdf

Fortado, L and Martin, K. (2016). *Serious Fraud Office drops UK criminal forex probe*. [online] FT.com . Available at: https://www.ft.com/content/4d4d48d4-eabc-11e5-bb79-2303682345c8

Fox, T. (2016). *Up Close and Personal: Individual CCO Liability - Part I - Compliance Report*. [online] Compliance Report. Available at: http://fcpacompliancereport.com/2016/05/close-personal-individual-cco-liability-part/.

G 30 Working Group. (2015). *Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform*. Washington: Group of Thirty.

Gandz, J. (2010). *Leadership on trial*. London: Ivey School Of Business.

Gibson, N. (2008). *Will your bank be the next? How to deter your own rogue traders.* [online] Chase Cooper Metric. Available at: https://www.slideshare.net/chasecooper/metric-special-edition-rogue-trading-9426265

Goode, M and Mead, N and Vohs, K (2006). *The Psychological Consequence of Money.* [online] Sciencemag.org. Available at: http://science.sciencemag.org/content/314/5802/1154.full

Haan,J., Nuijts, W and Raaijmakers. (2015). Supervising culture and behavior at financial institutions: The experience of De Nederlandsche Bank' [online] voxeu.org. Available at: https://voxeu.org/article/supervising-bank-culture

Hancock, M and Zahawi, N. (2013). *Masters of nothing: How the crash will happen again unless we understand it*. [London]: Biteback

Hornuf, L., and Haas, G. (2014). Regulating fraud in financial markets: Can behavioural designs prevent future criminal offences? *Journal of Risk Management in Financial Institutions*, 7(2): 192–201.

IBM. (2018). *2018 Cost of a Data Breach Study by Ponemon*. [online] ibm.com. Available at: https://www.ibm.com/security/data-breach

Institute of Risk Management (2018). *Cyber risk and risk management*. [online] theirim.org. Available at: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk

Jary, S. (1998). *18 Platoon.* (Durham) Light Infantry Office.

Levy, R. (2016), *Wall Street has been rocked by an $8 billion hedge fund implosion*. [online] Business Insider UK. Available at: http://uk.businessinsider.com/visium-asset-management-closure-rocks-wall-street-2016-6?r=US&IR=T

Maxfield, J. (2015). *25 Major Factors That Caused or Contributed to the Financial Crisis*. [online] The Motley Fool. Available at: https://www.fool.com/investing/general/2015/02/28/25-major-factors-that-caused-or-contributed-to-the.aspx

McCormick, R (2015). *The 'Conduct Crisis': Will Banks Ever Get it Right*. [online] ibanet.org. Available at: https://www.ibanet.org/Publications/business_law_international_may_2015aspx.aspx#

Mitchell,T,. and Harris,K,. (2012). *Resilience: A Risk Management Approach*. [online] Overseas Development Institute. Available at: https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7552.pdf

Mulier, T. (2011). *UBS Chief Gruebel Dismisses Calls to Quit After Unauthorized Trading Loss*. [online] Bloomberg. Available at: www.bloomberg.com/news/2011-09-18/ubs-chief-gruebel-dismisses-calls-to-resign-after-2-billion-trading-loss.html

O'May, N. (2014). *Criminal Liability for Senior Bankers*. [online] Norton Rose Fullbright. Available at: www.nortonrosefulbright.com/knowledge/publications/122774/criminal-liability-for-senior-bankers

Osborn, T. (2016). *Leeson: risk managers should be personally liable for trades*. [online] Risk.net. Available at: https://www.risk.net/risk-management/2450617/leeson-risk-managers-should-be-personally-liable-for-trades

Plender, J (2014). *The crisis shows moral capital is in secular decline*. [online] FT.com. Available at: https://www.ft.com/content/11a3d50e-efba-11e3-bee7-00144feabdc0

PricewaterhouseCoopers (2008). *Société Générale Summary of PwC diagnostic review and analysis of the action plan*. [online] Available at: https://www.societegenerale.com/sites/default/files/23%20May%202008%20The%20report%20by%20audit%20firm%20PWC.pdf

Rafeld, H., and Fritz-Morgenthal, S. (2010). *Breaking down the biggest trading fraud in the history of banking*. Risk Professional.

Rafeld, H., Fritz-Morgenthal, S., and Posch, P. (2017). *Behavioural patterns in rogue trading: Analysing the cases of Nick Leeson, Jérôme Kerviel, and Kweku Adoboli*. Journal of Financial Compliance, 1(2):

Rafeld, H., Fritz-Morgenthal, S., and Posch, P. (2017). *Applying control balance theory to the rogue traders Nick Leeson, Jérôme Kerviel, and Kweku Adoboli*. Journal of Financial Compliance , 1(3)

Rudin, J (2015). *Away from the Lamppost: Culture, Conduct and the Effectiveness of Prudential Regulation*. [online] chhowe.org. Available at: https://www.cdhowe.org/speeches-and-presentations/away-lamppost-culture-conduct-and-effectiveness-prudential-regulation

Schecter, B (2015). *Canada's bank regulator probing links between risks and "culture" at financial institutions*. [online] National Post.com. Available at: https://business.financialpost.com/investing/market-moves/canadas-bank-regulator-probing-links-between-risk-and-culture-at-financial-institutions

Seijts, G., Crossan, M. and Carleton, E. (2017). *Embedding leader character into HR practices to achieve sustained excellence*. Organizational Dynamics, 46(1), pp.30-39

Shen, L. (2016). *Wells Fargo Has Been Fined $185 Million for Opening Unauthorized Accounts*. [online] Fortune. Available at: http://fortune.com/2016/09/08/wells-fargo-credit-card/

Simpson, E. (2012). *Kweku Adoboli jailed for fraud over GBP 1.4bn UBS loss*. [online] BBC News. Available at: www.bbc.co.uk/news/uk-20338042

Société Générale (2008). *General Inspection Department: Mission Green – Summary Report,* [online]. Available at: https://www.societegenerale.com/sites/default/files/12%20May%202008%20The%20report%20by%20the%20General%20Inspection%20

Sturm, R., Vera, D. and Crossan, M. (2017). The entanglement of leader character and leader competence and its impact on performance. *The Leadership Quarterly,* 28(3), pp.349-366.

Skyrm, S. (2014). *Rogue Traders.* New York: Brick Tower Press.

Tittle, C. (1995). *Control Balance: Toward a General Theory of Deviance.* Boulder, CO: Westview Press

Tittle, C. (2004). *Refining control balance theory. Theoretical Criminology*, 8(4)

Unknown Author (2012). Transcript of UBS trader's 'bombshell email'. [online] BBC News. Available at: www.bbc.com/news/business-19902894

Unknown Author (2018). *FCA Senior Managers and Certification Regime*. [online] FCA. Available at: https://www.fca.org.uk/firms/senior-managers-certification-regime

Unknown Author. (2017). *Fortune risk management survey.*[online] Deloitte. Available at: https://www2.deloitte.com/us/en/pages/risk/articles/fortune-risk-management-survey.html

Unknown Author. (2016), *Morgan Stanley SEC Penalty for Insider Breach Criticized as Insufficient*. [online] Secure World. Available at: https://www.secureworldexpo.com/industry-news/morgan-stanley-sec-penalty-insider-breach-criticized-insufficient

Unknown Author (2012). *UBS's rogue-trader trial: The education of Kweku Adoboli*. [online] The Economist. Available at: www.economist.com/news/finance-and-economics/21567134-swiss-bank-also-has-much-learn-education-kweku-adoboli

US Department of Justice. (2012). *HSBC Holdings et al Admit to Anti-Money Laundering and Sanctions Violations, Forfeit $1.256 Billion in Deferred Prosecution Agreement.* [online] Available at: https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations

Vohs, K (2015). Money Priming Can Change People's Thoughts, Feelings, Motivations, and Behaviors: An Update on 10 Years of Experiments. *Journal of Experimental Psychology*. 144, pp 86-93.

Wexler, M. (2010). *Financial edgework and the persistence of rogue traders.* Business and Society Review, 115(1)

Wikipedia (2018). *Kweku Adoboli* [online]. Available at: http://en.wikipedia.org/wiki/Kweku_Adoboli –

Yodo,N and Wang,P.(2016) *Engineering Resilience Quantification and System Design Implications: A Literature Survey*. [online] ASME. Available at: http://mechanicaldesign.asmedigitalcollection.asme.org/article.aspx?articleid=2537152

Zimbardo, P. (2008). *The Lucifer Effect: Understanding How Good People Turn Evil*. London:Rider.