Revisiting Conduct Risk Management in the COVID-19 Era with Updated DOJ Criteria

DECEMBER 2020

Jonny Frank
Partner, StoneTurn
jfrank@stoneturn.com
+1 212 430 3434

Laura Greenman
Managing Director, StoneTurn
lgreenman@stoneturn.com
+1 212 430 3429

by Jonny Frank and Laura Greenman

Introduction

Financial institutions have always managed conduct risk. Over the last ten years, particularly with the 2013 arrival of the UK Financial Conduct Authority (FCA), Conduct Risk Management evolved into its own specialty alongside its siblings, Operational and Regulatory Risk Management.

Coronavirus disease 2019 (COVID-19) continues to impact the financial industry, increasing both the volatility of the financial markets and disrupting normal business operations. In reaction to the pandemic, financial institutions shifted operations, moving most, if not all, professionals to a work-from-home environment. With the COVID-19 health crisis evolving into an economic crisis, financial institutions must revisit the risk and control environment to adapt ethics and compliance programs to mitigate heightened conduct risks.

Simultaneous to the COVID-19 health and economic crisis, prosecutors and regulators are upping the ante on expectations of ethics and compliance programs. In June 2020, for example, the Criminal Division of the U.S. Department of Justice (DOJ) updated its guidance on the Evaluation of Corporate Compliance Programs (DOJ Guidance). The new guidance

StoneTurn

stretches to 20 pages.[1] In July 2020, the Securities and Exchange Commission (SEC) embraced these requirements in the Resource Guide to the U.S. Foreign Corrupt Practices Act that it coauthored with the DOJ (Resource Guide).

The DOJ and SEC take a 'carrot and stick' approach. Financial institutions that meet expectations are rewarded with lesser penalties and no government-imposed monitor. Those who cannot comply, regardless of COVID-19, face enforcement proceedings, higher sanctions and a government-imposed monitor.

Jurisdictions around the world are following suit. Several countries, including Australia, Canada, Finland, Denmark, France and Germany, have or plan to adopt corporate criminal liability. And, the United Kingdom and Italy even imposed criminal liability on companies for failure to prevent corruption and tax evasion.

This paper suggests practical steps to identify and mitigate increased conduct risks arising from COVID-19. Financial institutions can apply the same steps to meet the DOJ Guidance, Resource Guide and local regulatory expectations.

COVID-19 Heightens Misconduct Risk

Regulators, prosecutors and non-government sector stakeholders expect financial institutions to tailor conduct risk according to changing pressures, incentives and new opportunities influencing engagement in misconduct during normal operations. This becomes even more critical in the COVID-19 era. At a minimum, organizations must be able to demonstrate that they have made a good faith effort to identify and address evolving conduct risks.

Financial institutions must adapt to the 'new normal', as COVID-19 spreads globally and disrupts the normal course of business, impacting professionals, business operations, consumers and financial markets. Financial institutions across the globe executed business continuity plans and moved operations to a work-from-home environment to enable them to continue operating while still meeting regulatory obligations.

A work-from-home environment gives rise to increased market abuse and fraud-related risks. Traders and bankers, normally monitored under established surveillance platforms (e.g., voice and electronic communication surveillance) and supervisory frameworks (e.g., supervisors overseeing one's actions on the desk), now work remotely, increasing their ability to engage in fraud and misconduct by divulging confidential client information or using such information to manipulate the market. Firms have limited ability to prevent a trader or banker from taking advantage of the new control environment and must enhance or adapt control functions.

During this time of uncertainty, the financial markets also hit record levels of volatility, increasing the pressure on operations, systems and controls and humans. The pandemic continues to impact staffing at financial institutions. Health risks impact resources and staffing, causing capacity constraints and staff fatigue within a firm's operations and control functions. At the same time, volatility can lead to unprecedented

losses. The pressure to increase revenues can lead employees to rationalize acting unethically. While this may increase a firm's market abuse and fraud risks as noted earlier, it can also increase the likelihood of client-related risks. There may be a drive to engage with clients on unsuitable products to support or disguise performance.

Frame Conduct Risk Management As A Business Issue, Not A Compliance Issue

For-profit organizations exist, well, for profit. Just as humans release antibodies to fight COVID-19, financial institutions innately battle any perceived impediments to profit. At some companies, business leaders and revenue generators snicker at Conduct Risk Management professionals, deeming them 'revenue prevention officers.'

A key first step, particularly during stressful economic times, is to present Conduct Risk Management as a business issue. Conduct Risk Management professionals must transfigure (mis) perceptions that Conduct Risk Management is bad for business and convert detractors into supporters by demonstrating a positive 'return on investment.'[2]

Obtaining top-of-the-house and revenue generator support is not difficult, especially during times of uncertainty and volatility (e.g., during a global pandemic). Step into business leaders' shoes. Ask them to quantify the financial impact of conduct risk and the value of the institution's brand and their personal reputations. Approaching business leaders this way shifts the mindset away from regulatory compliance and towards the business value of Conduct Risk Management.

Connect First And Second Lines Of Defense Business And Infrastructure Functions

Conduct Risk Management spreads across numerous—often siloed—business and infrastructure functions. In the first line of defense (1st LoD), front and middle office personnel serve Conduct Risk Management roles. The second line of defense (2nd LoD) Conduct Risk Management personnel includes risk management, compliance, anti-financial crime, human resources and legal resources.

Financial institutions vary on whether Conduct Risk Management sits within risk management, compliance or even its own space. But, aside from organization charts, it is essential to also include and coordinate key stakeholders.

COVID-19 remote working arrangements can easily exacerbate compartmentalized culture. Conversely, work-from-home tools can help to knock down silos, at least regarding Conduct Risk Management. The business world's adaption of video conferencing makes it relatively easy to gather individuals who otherwise must travel far distances or just between floors or offices in the same building or city, respectively.

Document Every Step

Documentation is essential. If misconduct occurs, all eyes—the government, Board, senior management, investors, plaintiffs' lawyers, media—scrutinize the compliance program in effect during the misconduct. The DOJ Guidance instructs prosecutors to consider the effectiveness of compliance when the misconduct arose as a key

factor 'for purposes of determining the appropriate: **(1)** form of any resolution or prosecution; **(2)** monetary penalty, if any and **(3)** compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).'[1, p.1] Prosecutors examine whether the conduct program was well designed, adequately resourced and empowered, and is operating effectively.

Contemporaneous documentation is more persuasive than information created after the misconduct occurs. Documentation also saves time. It is faster to document the process and rationale contemporaneously than to recreate it later.

Some attorneys worry that documentation creates a trail of what went wrong and counsel against documentation. This attitude demonstrates a misunderstanding or mistrust of the DOJ Guidance that 'existence of misconduct does not, by itself, mean that a compliance program did not work or was ineffective at the time of the offense.'[1, p.14] The DOJ Guidance acknowledges the backward-looking nature of the assessment and instructs prosecutors to examine whether 'the program evolved over time to address existing and changing compliance risks.'[1, p.14]

Documentation remains essential during the COVID-19 era. Financial institutions can protect themselves and potentially decrease imposed fines and actions if they are able to convince regulators that the firm considered the increased risk exposure driven by organizational changes arising from COVID-19.

Reinforce Culture Of Compliance And Integrity

Both regulators[3–5] and the industry[6–7] recognize and emphasize the link between culture and conduct, including the impact of COVID-19.[8] A culture of integrity serves as a backstop against misconduct, particularly for schemes and scenarios impossible to predict.

Cressey's Fraud Triangle

According to Cressey's Fraud Triangle, named after the 1950's criminologist Donald Cressey, three conditions exist whenever misconduct occurs: **(1)** pressure or incentive; **(2)** opportunity and **(3)** rationalization.[9,10] See Figure 1:

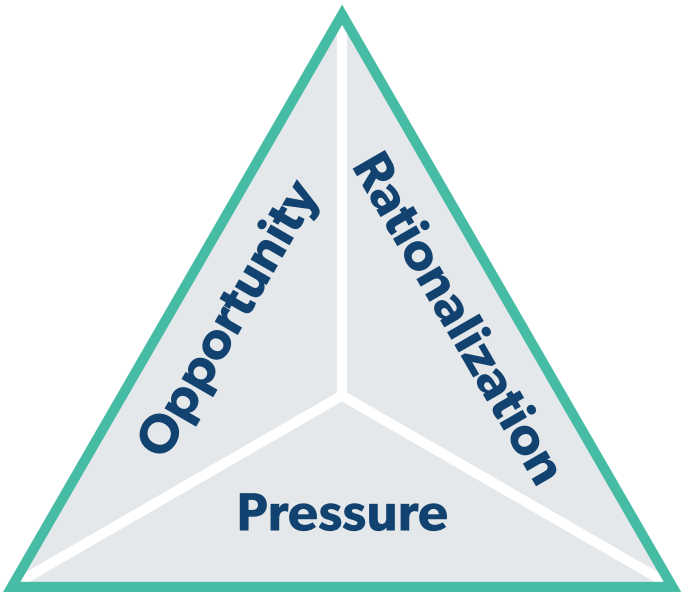

Figure 1: Cressey's Fraud Triangle

Financial institutions tend to ignore the rationalization axis of the fraud triangle and, as a result, forfeit an inexpensive opportunity to

mitigate misconduct risk.[11] If Cressey correctly concludes that offenders need to rationalize misconduct, financial institutions can reduce, if not eliminate, misconduct risk by removing the offender's ability to rationalize. Conversely, financial institutions must understand fostering a cultural environment that allows rationalization leads to an increase in misconduct.

Frequent and Sincere Middle Management Communication

Regulators and thought leaders stress a strong 'tone from the top.' In its update to the DOJ Guidance, the DOJ emphasized that companies must 'foster a culture of ethics and compliance with the law at all levels of the company' and a 'high-level commitment by company leadership to implement a culture of compliance from the middle and the top.'[1, p.10]

It is not difficult, time consuming or expensive for financial institutions to make rationalization of misconduct difficult and meet the updated DOJ Guidance. Frequent and effective messaging and engagement about the importance of ethics are key. Contemporaneous documentation is critical, even if it is just an e-mail memo to the file documenting conversations about ethics.

Communication must be sincere. As employees take cues from their immediate supervisors, it is essential to obtain buy-in and support from middle-management supervisors.

Pulse surveys and focus groups, even done virtually, are effective and inexpensive ways to measure and document the culture of compliance and integrity. Measuring an institution's culture becomes even more important during the COVID-19 era, as employees are under various forms of stress and pressure that may manifest as misconduct. The DOJ Guidance notes the usefulness of surveys and focus groups.[1, p.15] But financial institutions must be prepared to act on the results. This communication becomes even more critical as employees work remotely and do not have the regular engagement of compliance professionals and supervisors.

Refresh The Conduct Risk Assessment

Ineffective risk assessment is a common root cause for financial services and other corporate scandals. Culture alone does not sufficiently guard against significant conduct risk. To be adequately protected, financial institutions must implement preventive and detective policies, processes and controls.

Therefore, prosecutors and regulators emphasize the importance of conduct risk assessments.[12] For example, the updated DOJ Guidance calls risk assessments 'the starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program.'[1, p.2]The guidelines further teach that conduct risk assessment must be dynamic, not static, and kept up-to-date through 'continuous access to operational data and information across functions'[1, p.3] and 'lessons learned from its own misconduct and/or that of other companies facing similar risks.'[1, p.16]

Identify New and Emerging Inherent Conduct Risks

Regulators initially focused on conduct risk of any misconduct affecting customers and the market.

Mature Conduct Risk Management programs broaden programs to include any misconduct including bullying and harassment.

Begin with inherent, not residual risk, to identify new and emerging risks. Residual risk includes only known risks. To meet the threat of COVID-19 and DOJ Guidance, financial institutions must identify and address new, changed and emerging risks.

Cressey's Fraud Triangle, once again, provides a handy tool. Pressures and incentives examine the mindset and motives to engage in misconduct. Job security is paramount. During the 2008 financial crisis, employees lied to cover up mistakes, not for personal financial gain, but to avoid layoffs. Conversely, as business conditions improve, Conduct Risk Management teams must consider the threat of overloaded compliance and operations employees cutting corners to keep their jobs.

The Conduct Risk Management team must consider the organization's role in creating unintended pressures and incentives. For example, drive for revenue can lead employees to circumvent financial crime controls to onboard and retain customers.

And, working remotely creates new opportunities to engage in fraud. An Ethics and Compliance Initiative pulse survey recently found that companies with supervisors perceived to be weak leaders are twice as likely to suffer misconduct than supervisors exhibiting strong leadership.[13] The lesson is clear — even strong supervisors must remain highly visible to the employees they supervise.

It is essential for the 1st LoD revenue generators to participate in refreshing the risk assessment. They, better than anyone, can identify how COVID-19 impacts their business and potential risk areas and misconduct schemes and scenarios. Firms can also look to the industry to identify new and emerging risks that may help to enhance their conduct risk assessment through scenario analysis. This includes identifying events and risks driven by misconduct at competitor firms.

Conduct risk identification also requires consideration of operational risk loss events and near misses. Level of intent differentiates conduct and operational risks. Conduct risk involves intentional conduct; operational risk can occur with an unintentional mistake. Yesterday's accident can give rise to tomorrow's intentional misconduct.

It is important to take note of guidance issued by regulators. In April 2020, for example, the FCA published a 'Dear CEO' letter regarding fair treatment of corporate customers during the COVID-19 pandemic.[14] Institutions should assess whether their Conduct Risk Management program effectively identifies the risks outlined in the FCA letter. The FCA and other regulators issued similar guidance regarding risks during COVID-19, which firms should consider for scenario analysis.[15]

Organizations facilitate conduct risk assessments formally and informally. Some financial institutions hold monthly business nonfinancial risk workshops, councils etc. These meetings provide a useful platform to refresh and identify emerging conduct risks or facilitate informal discussions.

Again, documentation is essential. The DOJ Guidance notes '[t]he failure to prevent or detect the instant offense does not mean that the program is not generally effective in preventing and deterring misconduct' and 'recognizes that no compliance

program can ever prevent all criminal activity by a corporation's employees."[16,17] If a problem emerges, contemporaneous documentation is essential to demonstrate the institution took good faith efforts to identify the risk.

Link New and Emerging Inherent Risks to Control Activities Inventory

Step two of refreshing the conduct risk assessment is to link the inherent risk to the policies, processes and controls (collectively, 'control activities') the financial institution relies on to mitigate the risk. Control activities vary among automated and manual; preventive and detective and entity and transaction-level. Entity-level control activities pertain to the entire organization (e.g., code of conduct).[18 22–24] Transaction-level controls relate to specific processes or transactions.

Mature Conduct Risk Management programs link risks to mitigating control activities through a control activities inventory. A control activities inventory is not difficult to develop. Decentralized, siloed-culture financial institutions, however, can take months, if not years, to organize and implement a controls inventory.

To build a controls inventory, the Conduct Risk Management team asks the 1st LoD and 2nd LoD to identify the key control activities it relies on to prevent and timely detect conduct violations. It is important to identify and document key control activity attributes such as: **(1)** who executes the control activity (i.e., control owner); **(2)** what the control activity does (i.e., control description); **(3)** why the control activity exists (i.e., control objective) and **(4)** when the control activity operates (i.e., control frequency) and **(5)** how the control activity is evidenced (e.g., control output or documentation). Control inventories should also document the type of control as outlined and as seen in Figure 2.

Control Name	Conduct Risk Type	Control Owner	Control Description	Control Objective	Control Frequency	Control Type
Voice Surveillance	*Market Manipulation*	*Compliance*	*Identification of potential instances of misconduct through the surveillance of recorded voice comm's.*	*Detect potential instances of misconduct/ breaches of applicable laws, regulations and internal policies.*	*Daily*	*Detective*

Figure 2: Control Inventory
Note: Excerpt for illustrative purposes only.

Firms must consider how the COVID-19 working environment impacts its key control activities.

Certain controls may no longer mitigate the risk or, sometimes, may no longer exist given professionals are no longer in the office. Firms should identify controls affected under the COVID-19 environment and implement new mitigating controls to manage the conduct risks effectively.

Financial institutions, for example, have had to reduce or eliminate requirements prohibiting trading and sales activities at home, the use of mobile phones or access to video conferencing or chat platforms due to COVID-19. Also, the market experienced an increase in volatility due to COVID-19 leading to more demands on financial institutions' control environments (e.g., profit and loss swings, mark-to-market losses), which puts pressure on both back-office control functions and traders and sales personnel.

Implementing mitigating controls is a critical risk management step during periods of disruption. Institutions should increase surveillance controls (e.g., voice and e-communication surveillance), establish a secure server for video conference capabilities, increase the oversight from supervisors through regular meetings or live video conferences, conduct additional trader certifications (e.g., certification of trader mandates) and increase the interactions between the business and the compliance experts at the firm.

Stakeholders must also be able to understand what control testing the firm performed on its key controls and the results of the testing activities.

Controls Activities Testing

Defective control activities are as, if not more, dangerous than having no control activities. They lure financial institutions to take risks they would otherwise not accept and allow them to lower their guard. Operating with defective conduct-related control activities is like living in a home with broken smoke detectors and deteriorating fire barriers or a city with understaffed firefighters or out-of-date equipment.

Testing the effectiveness of 1st LoD and 2nd LoD controls activities is essential but often inadequate. Also, in a financially strapped, siloed-culture institution, the three lines of defense framework can lead to no testing, as no line of defense has the budget and each regards the other responsible.

Testing considers design and operating effectiveness. Design effectiveness refers to whether the control activities, if they operate as prescribed by persons possessing the authority and competence, mitigate the risk.[18, 42] Operating effectiveness refers to whether the control activities operate as designed and whether personnel performing the processes and controls possess the authority, resources and competence to effectively perform the processes and controls.[18, 44]

Control activities testing must consider the suite of control activities, not just individual controls. Some organizations test only individual controls. That approach is akin to the proverb of not seeing the forest for the trees. Conduct Risk Management requires determining whether the control activities are designed and operating effectively.

Firms must understand how the control activities operate under the new environment created by

COVID-19. Financial institutions should adapt their control testing programs to ensure testing of the current control environment.

Simulation is an excellent way to determine the effectiveness of control activities. Borrowing from the military and cybersecurity, some financial institutions employ red team vs blue team exercises. The red team are the perpetrators. The blue team are the 1st LoD and 2nd LoD personnel charged with defending the financial institution. Red team vs blue team exercises sensitize valuable personnel to the importance of professional scepticism and overcome the 'it's never going to happen to me' naïve optimism bias.[19]

Some financial institutions employ dummy transactions to test preventive and detective control activities. For example, the organization might enter fictitious trades to test the effectiveness of trade surveillance programs.

Documentation again is critical. Firms must document and obtain approvals to engage with specific traders to enter into the fictitious trades, report the results and implement corrective actions to remediate the control deficiencies.

Update Residual Risk Assessment

Conduct Risk Management assesses residual risk by measuring inherent risk against control activities testing results. Organizations typically plot the residual risk assessment against a two-dimensional XY graph as seen in Figure 3. The horizontal axis ordinarily depicts the likelihood of the event within a specified period (e.g., within three years likelihood of the risk occurring is frequent (>70%); likely (40% to 70%); possible (25% to 40%); unlikely (10% to 25%); or rare (<10%).[20] The vertical axis anticipates the financial, legal, reputation and market impacts if the risk occurred (e.g., critical, severe, high, medium, minor).

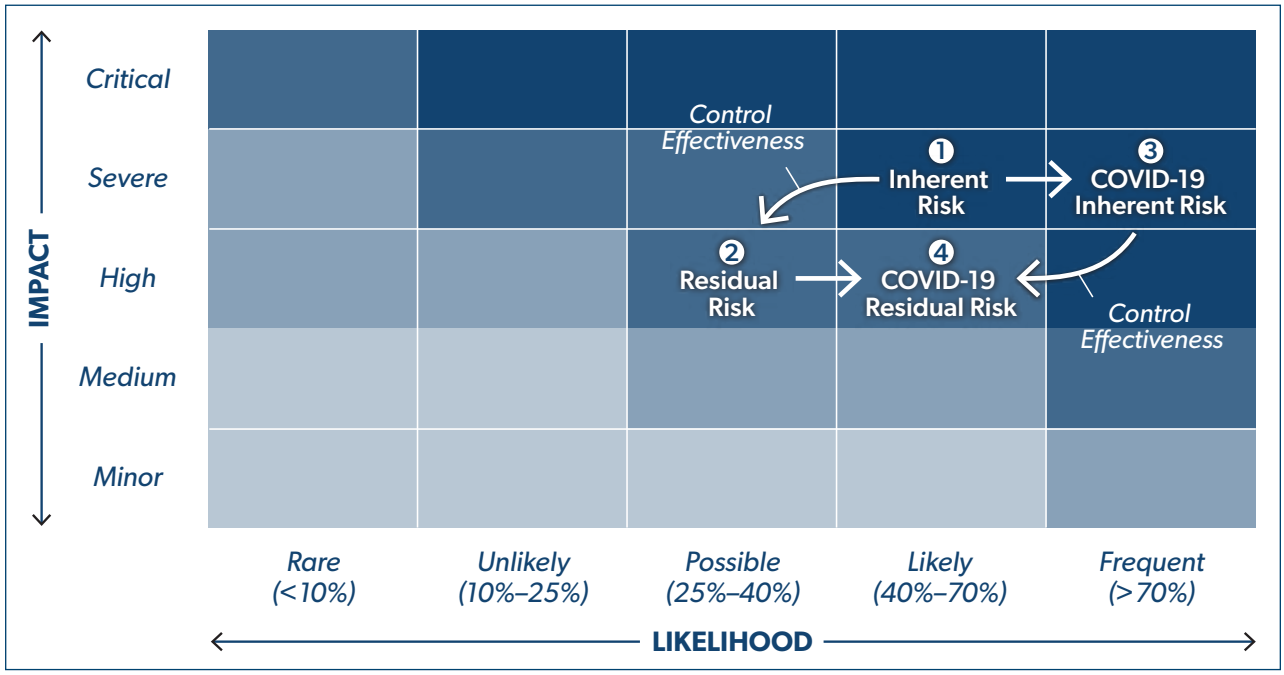

Figure 3: Residual Risk Assessment Grid

StoneTurn

Companies often overemphasize financial impact and understate or ignore legal and reputation risks. In a heavily regulated industry, conduct risk can lead to loss of license or significant business restrictions. Senior management face criminal prosecution and imprisonment. Also, regarding reputation risk, misconduct risk with minor direct financial impact nonetheless can lead to long-term negative media coverage, significant market value decline and material brand dilution.

The residual risk analysis becomes increasingly important during COVID-19. Firms must consider the impact of the health and economic crisis on both inherent risk and control activities effectiveness. Firms should also reassess the impact of COVID-19 on the conduct risk profile. Firms will benefit from the increased transparency of a refreshed risk profile and enable an increased prioritization for control implementation and remediation to mitigate the increased conduct risks.

Scenario analysis is essential. To assess residual risk, the Conduct Risk Management team and 1st LoD, working together, must evaluate how the preventive and detective control activities would match up against specific schemes and scenarios. Also, because conduct risk involves intentional behavior, the assessment must also examine control activities' vulnerability to collusion, management override and other forms of circumvention.[21]

Likelihood And Impact Drive Compliance Risk Strategy

Avoid, Accept, Transfer or Reduce

Likelihood and impact drive the response strategy to emerging COVID-19 era risks. Organizations choose among four options: **(1)** accept the risk as is (i.e., do nothing); **(2)** avoid the risk by eliminating the source (e.g., discontinue products and services); **(3)** transfer the risk (e.g., obtain insurance, outsource the activity) and **(4)** mitigate the risk (e.g., enhance control activities).[22]

Risk avoidance typically applies when, using the heat map in the table, likelihood is 'likely' or 'frequent,' and the impact is 'critical' or 'severe.' Financial institutions, for example, sometimes exit and refuse business in high-risk of corruption geographies because they cannot control the risk.

Risk acceptance is viable only if likelihood is 'rare' or 'unlikely,' or the impact, if the event occurs, is 'minor.' COVID-19 epitomizes a black swan risk[23] of rare likelihood, but 'critical' impact.

For COVID-19, risk mitigation usually is the only practical choice. Financial institutions cannot ignore conduct nor insure against conduct risk. The risk assessment helps firms to develop strategy by allowing prioritisation of resources to respond to the more material residual conduct risks. Risk mitigation is necessary if residual likelihood is 'possible,' 'likely' or 'frequent,' and impact 'medium,' 'high,' 'severe' or 'critical.'

Leverage the Fraud Triangle

Recall Cressey's Fraud Triangle thesis that three conditions exist when misconduct occurs: **(1)** incentive/pressure; **(2)** rationalization and **(3)** opportunity. If Cressey is correct, financial

institutions need to eliminate only one of these three factors to mitigate COVID-19-bred conduct risk.

- *Incentives and Pressure Sharpen Potential Hotspots*

Pressure is often perception, not fact-based. If practical, reduce the anxiety of employees who are not a risk to avoid incentivizing them to engage in misconduct that would, ultimately, cost them their jobs.

Many financial services employees, however, should worry about job security. Revenue generators should fear losing their jobs or suffering large pay cuts for not performing. Non-revenue generators should worry that cost-cutting measures might include widespread layoffs. COVID-19 heightens these pressures as professionals worry about the sustainability and continuity of their jobs while unemployment rates increase.

Institutions can leverage pressures and incentives to focus on whom or what business is at risk. Take trading businesses. What pressures do traders perceive or face? Who particularly is at risk? How might traders at risk engage in serious misconduct? What are the quantitative and qualitative key risk indicators (KRIs)? What additional steps might the institution take to prevent and detect misconduct?

. • *'Good' People Can Rationalize 'Bad'Conduct*

Even 'good people' resort to misconduct to protect their jobs and livelihood. Organizations should continue, if not redouble, efforts to remind employees of obligations and instill a culture of integrity and compliance. Frequent communication is inexpensive, and, if misconduct arises, demonstrates that the organization proactively tried to respond to COVID-19 risks.

Internal communications and small group discussions are easy mechanisms to maintain connection and reinforce firm values. Some companies issue reminders that the COVID-19 pandemic does not justify relaxing legal and business conduct requirements and restate prohibited activities (e.g., sharing confidential information, coordinating with competitors, engaging in inappropriate sales practices). While these communications are useful, it is both unwise and insufficient to rely exclusively on entity-level controls to mitigate conduct risk.[18, 24-26]

Financial institutions should also strive to convince employees they will detect and act on misconduct. Fear of being caught technically differs from rationalization; that is, an employee might rationalize, but refrain from engaging in, misconduct because they worry their employer will detect it. The two concepts are similar because they relate to the mindset and propensity of a potential perpetrator.

. • *Attack Opportunity through Forensic Data Analytics and Surveillance*

Financial institutions need to enhance control activities to mitigate, if not eliminate, the 'opportunity' side of the fraud triangle. Strengthening and expanding forensic data science and surveillance are the most powerful weapons.

Forensic data analytics and surveillance are

growing specialties. As seen in Figure 4, they combine investigation expertise and a forensic mindset with knowledge, skills and experience to: **(1)** conduct risk identification and assessment; **(2)** analyze conduct risk schemes and risk factors and indicators; **(3)** complete computer programming and **(4)** and assess, acquire and analyze data.

Forensic data analytics and surveillance transformed Conduct Risk Management. They allow financial institutions to analyze an entire data population, as opposed to statistical approaches, and increase efficiencies by analyzing more data in less time (e.g., less manual reviews). Forensic analytics and surveillance facilitate more frequent and timely conduct risk assessments, improve the ability to respond to urgent events and enable assembly of risk assessment 'dashboards' that summarize effectiveness of controls for management promptly.

The June 2020 DOJ Guidance devotes a new section to data resources and access. The policy instructs prosecutors to ask

> *Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?*[1, p.12]

The financial services industry has been a long-term leader in using forensic data analytics and surveillance to mitigate conduct risk. The best-known applications are predictive analytics to protect against credit card fraud and transaction monitoring to guard against money laundering, sanctions violations and terrorist financing.

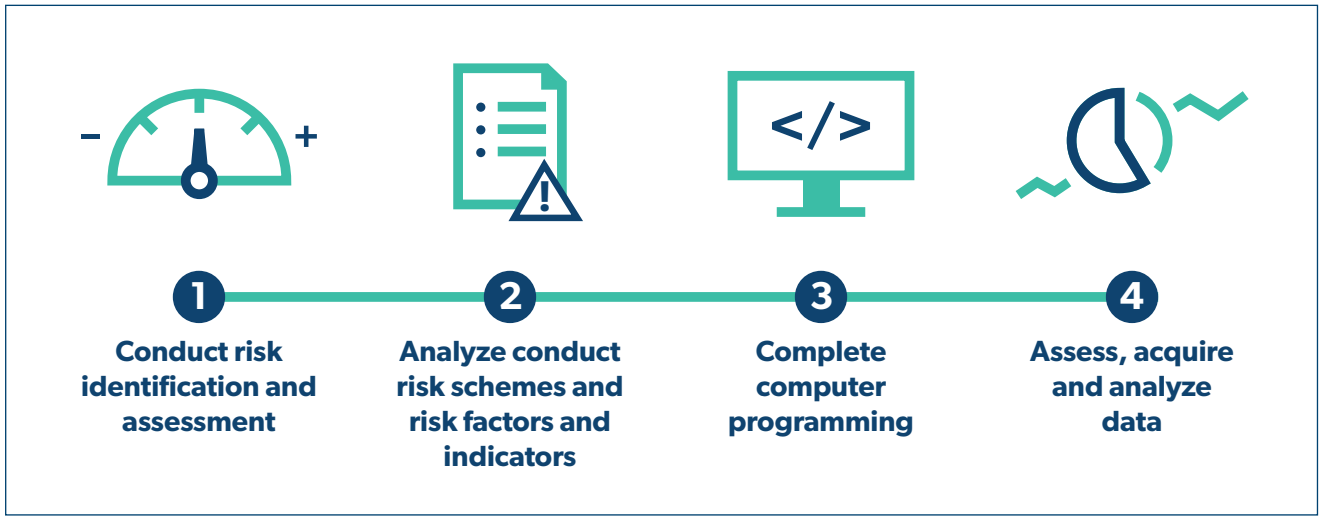

Figure 4: Forensic Data Analytics and Surveillance Process

Over the last decade, financial institutions have developed sophisticated, in-house surveillance groups to build trade, electronic communications and voice surveillance to prevent and detect antitrust violations, conflicts of interest, duties to customers misconduct, market abuse and manipulation, unauthorized trading, misuse of material non-public information and unauthorized trading.

Forensic data analytics builds on KRIs, quantitative and qualitative early signal indicators of risk. Conduct risk and control activities experts play detective to devise KRIs for conduct risk. First, the team disaggregates conduct schemes and scenarios. It then imagines the red flags that would arise in an investigation. Creativity is essential. Advances in forensic data analytics make it possible and practical to compare data from multiple sources. This includes investigating certain KRIs, including looking at correlations between, increases in cancels, corrections or amendments to trades, timing of trades based on location, trades booked to dormant or 'dummy' accounts, lapses in mandatory time away, large changes in volumes of trades booked and changes in trading activity.

The next steps are to: **(1)** acquire and load data into the analysis environment; **(2)** assess data quality, completeness and format; **(3)** transform data (e.g., teach the computer to recognize and translate multiple languages); **(4)** augment with third-party reference data and **(5)** analyze the data by combining quantitative and qualitative risk indicators and trending the information to identify anomalies.[24–25]

Regarding COVID-19 conduct risks, financial institutions should re-evaluate the forensic data analytics and surveillance program. For new risks, they might need to develop a new program just as they would for any other new conduct scheme. This becomes increasingly important as financial institutions must implement new forms of surveillance to monitor their employees in a work-from-home environment.

More likely, institutions will need to expand their use of forensic analytics and surveillance. Many institutions, for example, use voice surveillance to prevent and detect antitrust violations in trading operations. If antitrust risk heightens, in say, mergers and acquisitions, the institution might need to expand voice surveillance to corporate finance.

Conclusion

With a heightened risk of employee misconduct worldwide resulting from the COVID-19 pandemic, proactive Conduct Risk Management is an investment few financial institutions can afford to delay. Fortunately, an effective framework, including robust conduct risk assessments, controls testing and support from middle and top management can assist in mitigating the often overlooked or underestimated conduct risks. Further, when control activities are enhanced by forensic data analytics and surveillance, banks can detect and prevent misconduct. The silver lining is that taking a practical approach to Conduct Risk Management is good for business and can set a financial institution on the right track to reduce fraud, waste and abuse and avoid any related reputational risk.

[1] Department of Justice, Criminal Division (2020)Evaluation of corporate compliance programs [Internet]. The United States Department of Justice, available at: https://www.justice.gov/criminal-fraud/page/file/937501/ (accessed 2nd June, 2020).

[2] Frank, J. (2017) 'Five ways to calculate ROI on compliance,' RANE, available at: https://stoneturn.com/insight/five-ways-calculate-roi-compliance (accessed 2nd June, 2020).

[3] U.K. FCA (2018) 'Transforming culture in financial services,' available at: https://www.fca.org.uk/publication/discussion/dp18-02.pdf (accessed 5th June, 2020).

[4] U.S. Federal Reserve Bank of New York (FRBNY) (2019) 'Education and industry forum on financial services culture,' available at: https://www.newyorkfed.org/aboutthefed/education-industry-forum (accessed 5th June, 2020).

[5] Enria, A. (2019) 'Just a few bad apples? The importance of culture and governance for good banking,' Central Bank of European Central Bank, available at: https://www.bankingsupervision.europa.eu/press/speeches/date/2019/html/ssm.sp190620~f9149fe258.en.html (accessed 5th June, 2020).

[6] U.K. Banking Standards Board (2018) 'An outcome-based approach to assessing organizational culture,' *Journal of Risk Management in Financial Institutions*, available at: https://bankingstandardsboard.org.uk/the-uk-banking-standards-board-an-outcome-based-approach-to-assessing-organizational-culture/ (accessed 5th June, 2020).

[7] The Group of 30 (2015) 'Banking conduct and culture, a call for sustained and comprehensive reform,' available at: https://group30.org/images/uploads/publications/G30_BankingConductandCulture.pdf (accessed 5th June, 2020).

[8] U.K. Financial Conduct Authority (FCA) (June 2020) 'Conduct, culture and COVID-19,' available at: https://www.fca.org.uk/insight/conduct-culture-and-covid-19 (accessed 22nd June, 2020).

[9] Wells, J. T. (2008) 'Principles of fraud examination,' 2nd ed., Wiley, Hoboken, NJ.

[10] Public Company Accounting Oversight Board (PCAOB) (2020) 'Consideration of fraud in a financial statement audit, AS 2401,' available at: https://pcaobus.org/Standards/Auditing/Pages/AS2401.aspx (accessed 5th June, 2020).

[11] Frank, J. (2015) 'Remediation: litigation services handbook: the role of the financial expert,' available at: https://stoneturn.com/wp-content/uploads/2016/02/Remediation_Litigation_Services_Handbook.pdf (accessed 5th June, 2020).

[12] DOJ and SEC (2012) 'A resource guide to the FCPA,' available at: https://www.sec.gov/ spotlight/fcpa/fcpa-resource-guide.pdf (accessed 8th June, 2020).

[13] ECI (2020) 'Are supervisory behaviors linked with misconduct rates?,' available at: https://www.ethics.org/knowledge-center/ethicsstat (accessed 8th June, 2020).

[14] Financial Conduct Authority (FCA) (2020) 'Dear CEO: ensuring fair treatment of corporate customers preparing to raise equity finance,' available at: https://www.fca.org.uk/publication/correspondence/dear-ceo-ensuring-fair-treatment-corporate-customers-preparing-raise-equity-finance.pdf (accessed 22nd June, 2020).

[15] Financial Conduct Authority (FCA) (2020) 'Coronavirus 2020,' available at: https://www.fca.org.uk/coronavirus (accessed 22nd June, 2020).

[16] U.S. Sentencing Commission Guidelines Manual, Effective Compliance and Ethics Program § 8B2.1(a), (2018), available at: https://guidelines.ussc.gov/gl/%C2%A78B2.1 (accessed 22nd June, 2020).

[17] U.S. DOJ (2020) 'Justice manual 9-28.800, principles of federal prosecution of business organizations,' available at: https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations (accessed 22nd June, 2020).

[18] Public Company Accounting Oversight Board (PCAOB) (2007) 'An audit of internal control over financial reporting that is integrated with an audit of financial statements, Auditing Standard (AS) 2201,' available at: https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx (accessed 8th June, 2020).

[19] Shilton, A. C. (June 30, 2020) 'Why you're probably not so great at risk assessment,' *The New York Times*, available at: https://www.nytimes.com/2020/06/30/smarter-living/why-youre-probably-not-so-great-at-risk-assessment.html (accessed 30th June, 2020).

[20] Institute of Operational Risk, Sound Practice Guidance, Risk Control Self-Assessment, (2014), ¶6.1.3.

[21] American Institute of Certified Public Accountants (AICPA), Management Override of Internal Control: The Achilles' Heel of Fraud Prevention (2016).

[22] Committee of Sponsoring Organizations (COSO) of the Treadway Commission, Enterprise Risk Management—Integrating with Strategy and Performance, Principle 13: Implements Risk Response (2017).

[23] Taleb, N. (2007) 'The black swan: the impact of the highly improbable,' Penguin Random House, New York, NY.

[24] Frank, J. (2019) 'How data analytics can weed out college admissions fraud,' Law360, available at: https://stoneturn.com/insight/uncovering-college-admissions-fraud/ (accessed 8th June, 2020).

[25] Frank, J. (2016) 'Data: a hidden gem in the effectiveness of ethics and compliance programs,' Compliance & Ethics Professional, available at: https://stoneturn.com/de-en/data-a-hidden-gem-in-the-effectiveness-of-ethics-and-compliance-programs/ (accessed 8th June, 2020).

About the Authors

Jonny Frank is a Partner at the global advisory firm StoneTurn and serves as U.S. Department of Justice-appointed Monitor to Deutsche Bank, Voluntary Monitor and Remediation Consultant to a Northern European Bank, DOJ-appointed Independent Auditor to a Big Three U.S. automotive manufacturer, and Forensic Audit Adviser to the Securities and Exchange Commission-appointed Independent Consultant of a Big Four public accounting firm. Jonny was previously the Executive Deputy Compliance Monitor of Volkswagen AG, New York State Department of Financial Services Compliance Monitor of Ocwen Financial Corporation, a Big Four partner, Executive Assistant United States Attorney for the Eastern District of New York and among the faculty at the Yale School of Management, Fordham University Law School and Brooklyn Law School.

Laura Greenman is a Managing Director at global advisory firm StoneTurn, where she assists large financial institutions with the implementation and testing of internal control frameworks and compliance programs, advising companies on how to remediate and enhance compliance programs to prevent and detect fraud. Earlier in her career, Laura was with the Goldman Sachs Group, where she focused on financial and regulatory reporting. She also provided financial services assurance to public clients at a Big Four firm.

This article originally appeared in the **Journal of Risk Management in Financial Institutions, Volume 13.**