CAPCO

NEXT GENERATION CONTROL FRAMEWORK

RETHINKING INTERNAL CONTROLS FOR THE NEW OPERATING ENVIRONMENT

CHANGES IN THE WORKPLACE

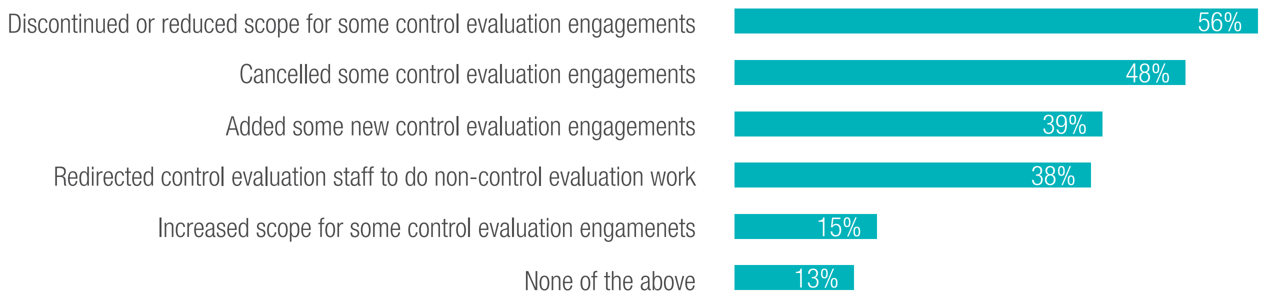
Organizations have been forced to adopt new business strategies to accommodate the considerable operational environment changes in business operations. The new normal and resulting changes in the workplace (e.g., reduced workspace capacity, increased telecommuting) are the catalysts for the shift. While companies have successfully managed the transition to a remote workforce, they may not have considered the impact of transition on to their risk and control profile.

A distributed workforce, with employees either telecommuting or at satellite offices, could present significant and persistent risks to maintaining an effective and functioning operational control environment. Control-centric business communication, deliverables, and control performer/reviewer roles are often dependent on frequent communication and/or co-location. In addition, a distributed workforce presents employees with more opportunities to circumvent and bypass controls as existing processes and tools were designed for a different operating environment.

Organizations will need to strengthen their internal control frameworks to face the specific challenges of a distributed workforce, ensuring that despite physical separation, functions can communicate, perform operational duties and continue to mitigate operational risks. Firms must be prepared for the new challenges of maintaining a robust control environment in a remote setting.

Comprehensive employee training will be a valuable tool in preparing employees for a shift in their control-focused responsibilities and for the potential changes to their business environment. Firms should take this opportunity to build the foundation for their next generation controls framework, which will evaluate the evolving risk and control environments, increased risk velocity, disrupted workforce, and further operations that will shift with the new working paradigms.

A recent survey[1] conducted by the Institute of the Internal Auditors suggests that, control-centric functions are rethinking on-going activities to better meet operational demands



[1] The Institute of Internal Auditors. (April 2020). COVID-19 Impact on Internal Audit: Survey results about risk assessment, audit plans, staffing, and budget, Audit Executive Center Knowledge Brief, Exhibit 12 Page 11.

RISK ENVIRONMENT

As the effects and ramifications of the new operational paradigm become clearer, chief risk officers (CROs) are racing to enable a risk oversight structure that will be comprehensive yet flexible enough to allow for an on-going assessment of internal controls. While some financial businesses, such as trading desk's traders and dealmakers, have shown that they can perform their work duties remotely, it remains to be seen if current practices are reliable and sustainable. To underscore the importance of a functioning control environment, the regulatory authorities have made it clear via a series of recent publications, including 'Dear CEO' Letters and Market Watch notices, that they expect all systems and controls in place pre-operational disruption to remain operational and effective regardless of workforce location.

The right risk oversight structure will keep operational disruptions at a minimum – an essential component in today's environment. Many organizations have been disadvantaged by continuing their operating risk oversight in siloed manners that limit a holistic view of their operational risk profile. Organizations should be addressing risk with a top-down enterprise-wide approach to mitigate the shortcomings of the diffused workforce. In this scenario, risks and the amplification of risks can be aggregated and identified across business functions and geographies. In addition, organizations will need to re-evaluate their risk appetite, risk profile and risk tolerance to allow management and first-line teams to understand the new level of risk exposure, to communicate the exposures efficiently, and control them effectively.

Recent industry insight from CROs suggests the following to be the new focus for emerging risk[2]:

- Process sustainability
- Revenue protection
- Human capital/workforce wellbeing
- Business continuity

Additional feedback from CROs has highlighted the following risk areas of focus as pressing concerns[3]:

- Updates to risk assessments
- Maintenance of on-going control evaluation
- Reassessment of key controls
- Re-evaluation of policies and procedures
- Re-performance of essential first-line tasks and processes

[2] Kretchmar, D.F. (2020). COVID-19 and Internal Audit: Preparing for the New Normal in 2020 and Beyond. COVID-19 Content Series, Institute of Internal Auditors, Page 6.

[3] Kretchmar, D.F. (2020). COVID-19 and Internal Audit: Preparing for the New Normal in 2020 and Beyond. COVID-19 Content Series, Institute of Internal Auditors, Page 3.

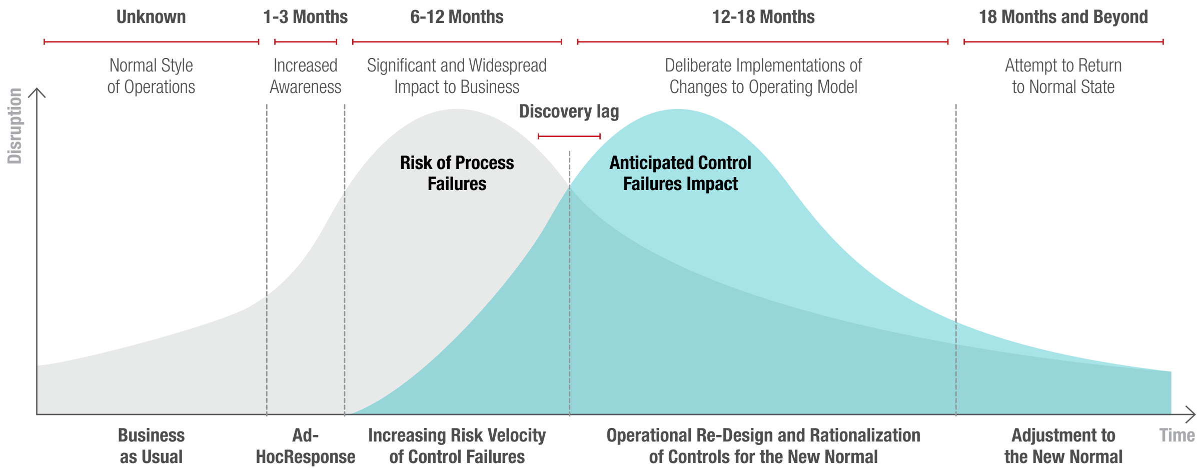
CHALLENGES FOR INTERNAL CONTROLS

Although control monitoring standards remain unchanged through the implementation of a remote workforce, the disruption to operations has created challenges in the assessment of changes in internal controls and the evaluation of evidence. With a remote workforce functioning at a stretched capacity, shifts in responsibility may occur for internal controls towards more junior employees or smaller teams. The transfer of roles increases the odds of a compromised control. Additionally, the standards and requirements of evidence may be loosened, in turn affecting the execution and the testing of controls.

The reality of a prolonged remote workforce has placed employees in a position of greater ethical responsibility, leaving financial institutions with vulnerability in conduct management. Managers need to understand the impact that the rapid shift to a remote working environment has on standard policies and procedures and adopt a more agile, forward-looking approach to risk management. Organizations may find that they need to implement new internal controls or revise existing ones to address the disruption to the normal business processes. Review and approval controls by management stand to face increased impact if individuals are unable to perform control duties due to absence, illness or loss of connectivity. When staff are left to exercise personal judgment, there is a higher risk for inconsistencies in processes and risk responses. Additionally, internal controls that rely on software and technology designed for the bandwidth of an in-office service should be reviewed for their ability to operate on VPNs and home internet connections.

The nature of a distributed workforce can lead to disjointed and inconsistent communication among teammates. This may affect the staff’s ability to effectively operate controls, e.g., when staff working remotely require point-in-time confirmation or authorization from colleagues who are geographically dispersed in different time zones. While the requirement to assess the design effectiveness of controls and determine their operational effectiveness remains unchanged, control evaluation teams must grapple with new challenges that impact the entire lifecycle of control evaluation. Typically, a control evaluation team gains an understanding of internal controls by talking through the details with control owners and operators. However, in the remote environment, it is more difficult to gather multiple stakeholders for a thorough discussion, which may impact critical aspects of understanding the control operation. Even more difficult in a remote environment is assessing operating effectiveness; with social distancing in place, many procedures ordinarily conducted in person (e.g., walkthroughs, observation and inspection) will be increasingly more challenging and time-consuming.

The present environment will likely give rise to the identification of new risks and a transformation of control evaluation procedures. Risk profiles are changing and expanding to include additional dimensions (risk of office closure, employee sickness, extended lock downs, etc.) yet the nature of the underlying risk mitigation remains the same. As a result, a full and nuanced understanding of control mitigation will continue to be important in designing control evaluation procedures in the future particularly where processes depend on manual execution and are time-consuming.



Capco predicts that over the next six-to-18 months' operational controls reliant on manual performance or dependent on third-parties will face a significant risk of operational failure (i.e., front office trading controls, limit review controls, approval and validation controls, compliance controls, etc.).

RISK VELOCITY

The Great Recession can serve as the closest surrogate for the systemic disruption of control environments due to mismanaged and misidentified risks from counterparties. Both dimensions used to quantify risk exposures, likelihood and severity, were incorrectly assessed. As a result, a new dimension of risk management was introduced into Enterprise Risk Management (ERM) based on the concept of 'Risk Velocity,' i.e., how quickly the effects and the impact of cascading failures lead to material impacts.

The tried and true approach embraced by ERM during the past decade has been to identify and prioritize risk through 'heat maps' showing which risks are most likely and which may have the most severe consequences based on the derived scores. However, risk scores are often refreshed and reassessed periodically (often as a result of an audit finding or significant operational incident). The scores are often not compared over time or benchmarked with a peer group; therefore, they do not reflect a point in time risk events. More significantly, the velocity of risks is often not considered as a component of rating risk due to the unpredictable nature of risk events.

However, as experience from the Great Recession shows, black swan events (i.e., mega disruptive events that are thought of as least likely to take place) do, in fact, occur, and the speed of sequential failures magnifies the impacts. To be better prepared, risk managers should be prepared to think 'outside the box' and to expand assumptions about what will happen and where failures will occur. As a result, ERM functions will need to evolve to include new ways of thinking about risks, with more attention paid to areas thought of as immune to the failures.

THE DIGITIZED FUTURE - A SPECTRUM OF RESPONSES

The pandemic environment forced many firms to adapt to a remote workforce while striving to maintain the consistency of process performance and integrity of the control framework. The so-called Fourth Industrial Revolution, i.e., digitization of the workforce, had begun before the pandemic, but the effects will inevitably accelerate the shift and transformation towards automation.

As organizations head further into a digital world, they will explore ways to balance cost considerations and staff skillset gaps with the need to enable rapid use of digitization tools to achieve efficient and effective operations. While the specific needs will vary, the spectrum of responses will range from small-scale implementation to full-scale automation. A digitization enabler, which is seeing increased early adoption by control-centric functions, is Robotic Process Automation (RPA), suitable for rapid adoption and bridging skill set gaps. While the spectrum of adoption varies from implementing proof-of-concept bots for specific tasks to deploying a structured bot program to perform many activities simultaneously, RPA's automation of repetitive tasks embedded within a process allows for rapid adoption and speedy roll out across the operational landscape. RPAs are advantageous in their implementation as no coding expertise is required, and system integration is not necessary.

The main benefit of RPA for control-centric functions is that it can be used to automate the control evidence assessment as part of evaluation activities as well as enable agile risk analytics and data gathering. Traditionally, data comes from a variety of sources and can be time-consuming to analyze, but the RPA consolidates this process. This streamlining of evaluation tasks and analytics can be preprogrammed and help achieve near end-to-end control evaluation and risk assessment automation. Because RPA replaces the structured, time-consuming, and repetitive activities within control evaluation, the process can become more efficient and effective.

RPA is at the forefront of disruptive technologies and has tremendous potential to transform ERM functions as it ties all interrelated areas – governance, methodologies and enabling technology – together.

Illustrative example: Areas of focus for financial services firm

The pandemic and shelter in place working arrangements have brought the themes of culture, behavior and engagement within financial services back into sharp focus. The below risk themes are common areas of great attention to a typical Trading firm during the operational disruption:

Process Sustainability

Continuing IT functioning given demand of the remote workstations; exposure to hacking and malware penetration due to the unsecured Internet/Intranet access.

Revenue Protection

Trigger event management and timely response/attention to the limit breaches.

Human Capital/ Workforce Well-being

Continuing remote working and social isolation that results in reduced morale and declined employee engagement. Rising rates of depression due to the lack of social interaction and the resulting decline in productivity.

Exposure to Fraud

Heightened risk of business communication being done outside of the secure firm medium (WhatsApp, unsecured phone calls). Access to the secure proprietary information by the unsanctioned individuals (roommates, spouses, etc.). Potential interaction with members of rival trading firms and risk of collusion. The decreased velocity of communication that impedes speed and effectiveness of decision making.

Business Continuity

Traditional BCP revolved around localized technology or operational failures and natural disasters, failing to account for the dynamic and indeterminate disruption posed by the most severe scenarios. BCP must be re-imagined to encompass an understanding of all organizational dependencies as the scope of disruptions become increasingly global and traditional siloed approaches fall short.

Updates to Risk Assessments

Update to agile, a forward-looking approach focused on operational resilience of business-critical processes (scale transformation/ change programs, digital integration, etc.) to identify weaknesses/ exposures early and present opportunity to address through strategic business decision making (rather than post-event remediation, aggregation of losses, events, etc.).

Maintenance of on-going control evaluation

Shift from periodic assessment to digitally-enabled “continuous monitoring” within 1st LOD enabled by data-driven insights in real-time through smart analytics tooling (machine learning, RPA, NLP, etc.) Targeted mitigation supported by defined, holistically applicable trigger events criteria and process enabled by the deployment of specialist SME as opposed to generic analysts covering all risk types) and focusing risk manager attention areas of “point-in-time” concern (i.e.. where risk exposure exceeds appetite) rather than on existing, known risks managed within appetite.

STRESS TESTING YOUR CONTROLS

The modern economy is interconnected. The initial and widescale disruption in the supply chain for critical Personal Protective Equipment at the onset of the pandemic is a testament of that interconnectivity. Modern financial services are, likewise, cross dependent on the normal functioning of the financial clearinghouses, financial intermediaries, credit warehouses, counterparties, lenders and increasingly, third-party service providers. Under normal conditions, expected process errors and control failures are identified and mitigated in-house and are managed without significantly impacting other actors. However, in instances of system-wide disruptions, process breakdowns and control failures tend to cascade with identification and mitigation lagging. These failures and breakdowns accumulate, and their effect is amplified far beyond what we could expect in the past. The ultimate impact of third-party controls' failure is hard to predict due to discovery lag and lack of forewarning.

Therefore, to the extent an organization relies on the functioning control environment of other parties, the business disruption issues related to those parties are important to evaluate and to prepare for. One approach to evaluate potential impact is to perform control stress tests, whereby a process is analyzed to determine whether successful and error-free process execution is dependent on a functioning control environment of other parties. Internal controls are rated for exposure, and a heat map of controls likely to fail due to the internal controls failures elsewhere is prepared. While the true impact of the disruption of the past few months, and the lasting changes the industry will experience remain unpredictable, it is clear that firms must find methods to manage and operate control-centric functions more dynamically. This new reality requires a re-evaluation of risk and controls, and a revised playbook that treats changing working environments, disruptive events, and stress scenarios as a given, rather than an exception.

The control stress test enables companies to review processes and controls to perform a dynamic risk assessment focused on areas where controls could be impacted by disruption and operational errors at counterparties, clients, service providers, regulators and industry peers. As CROs consider mitigating point-in-time changes in control environments, they need to revise existing plans or reassess results of risk assessments and control evaluations performed before pandemic-induced control environment stresses since those results may no longer be valid or reliable. Since control evaluations are predicated on obtaining sufficient evidence that controls are operating effectively, new testing may need to be performed either to validate prior results or to test control effectiveness differently based on how controls may have changed.

The evolution of the next generation controls framework paradigm, which has been driven by societal and industry changes as well as a heightened regulatory focus on resiliency, represents a unique inflection point for risk functions. Ultimately, the degree of success in facing these challenges will rely on an organization's ability to adapt and enhance their approaches and practices to continue to be effective and successfully lead the way as an integral risk management function.

LOOKING TO THE FUTURE

The disruption and the resulting widescale business adjustments may not be permanent, but it does represent a paradigm shift in which structural changes will shift the way control-centric functions operate. Given the sudden onset of the changes, the initial chaotic period of time during “Day 0” where companies played catch up with the new reality of operations while normalizing day to day activities has passed and the new reality of ‘Day +1’ requires re-adjustment and a new playbook in response to the structural changes.

Such a response cannot be a point in time exercise given the wide-scale impact and will be manifested as an evolutionary rather than revolutionary development of a next-generation control framework. This will bring an increased emphasis on proactive identification of prospective control failures, rather than the corrective/reactive mode of control failure response. The need to restructure control-centric functions comes at an opportune time, as regulators such as the PRA begin to stress operational resilience as a fundamental component of risk management. Operational resilience emphasizes the importance of firms’ ability to anticipate and prevent disruptions, aligning with the control environment of the future where proactive identification is paramount. This regulatory-driven increased accountability will force senior management to understand and manage the effects of potential controls failures that have been identified and implement a mitigation workbook to address failures as they arise.

AUTHOR

Michael Martinen, Managing Principal
Michael.Martinen@capco.com

Yan Gindin, Principal Consultant
Yan.Gindin@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO