Four key steps to fuel a proactive tech and cyber risk function

January 2019

kpmg.com

Organizations—and their technology and cyber risk management (TCRM) functions–are being buffeted by changing dynamics bringing ever-increasing risks: mounting regulatory pressures, innovative new technology, an evolving workforce in need of new skills, and organizational shifts that create cyber and information security challenges.

KPMG's third annual Technology and Cyber Risk Management Financial Services share forum offered cutting-edge solutions, practical guidance and best practices designed to address these critical issues, transform TCRM teams from cost centers to value creators, and elevate the status of the tech and cyber risk function. This report highlights the key insights that were generated:

The TCRM structure should foster a culture of "healthy tension" and collaboration.

KPMG

Get the TCRM structure right

Structure the TCRM function so that it creates a "healthy tension" between the lines of defense. Also, establish a culture where assumptions are continuously challenged in a thorough but collaborative manner.

Obtain good data

Establish a sound data strategy, underpinned by a strong taxonomy and framework to drive and improve information reporting. While companies continually strive to achieve a "golden data source," the underlying data they currently gather often isn't complete, accurate and/or timely. Also, good data is essential for the "risk scoring" process, which enables companies to prioritize areas of risk.

Take a proactive, business-focused approach to risk

Proactively search out and take a business-focused approach to risk; a reactionary-based approach to risk doesn't work anymore. Anticipate where risks are likely to occur and take advanced actions to prevent or mitigate it.

Automation and innovative technology

Develop a risk strategy utilizing innovative digital technologies and advanced machine learning. Few TCRM functions are adequately leveraging automation (e.g., robotic process automation, cognitive/intelligent automation (IA) technologies and data and analytics (D&A)) even when the rest of the organization is.

Let's take a closer look at how leading organizations have integrated these messages into their TCRM process, and offer guidance on how you may be able to adapt them for your business:

Get the TCRM structure right

Coming up with the right TCRM structure takes a lot of planning, critical thinking, and open and honest discussion among stakeholders. And even when you take all of these steps to come up with a sound TCRM structure, it takes time to implement and you may not achieve value from the restructuring overnight. For example, the director of IT Risk & Controls at a major investment bank noted that his firm was in the third year of its journey to restructure and automate its TCRM ecosystem, and is only expecting to generate significant results in the upcoming year.

Building the right TCRM structure encompasses many elements, and it must be customized to fit the needs of your organization. The structure should include at least two separate lines of defense (LOD) working together to identify and monitor acceptable risk levels:

- The first LOD owns the processes and related business risks and appropriate controls needed to prevent or mitigate them. It's also responsible for managing risks, including identifying, measuring, managing, monitoring and reporting.
- The second LOD is tasked with monitoring or challenging the first line's finding or actions. It is responsible for setting standards for risk appetite, tolerance and limits (with business input), assessing risk-return tradeoffs and opportunities, and monitoring risk-levels against established risk appetite and tolerances. For example, the second line may point out where the first line failed to identify or appropriately weight a particular risk, or may suggest that existing controls don't mitigate risk sufficiently in light of the organization's agreed-upon risk appetite and profile.

The TCRM structure should foster a culture of "healthy tension" and collaboration. That is, the TCRM function works best where the various teams can respectfully challenge and disagree with each other, but still communicate and work to effectively and efficiently resolve issues.

In addition, TCRM team members on the second LOD must have the right skill sets to deal with new and emerging risks. For example, forward thinking TCRM second LOD functions are hiring more data scientists, IT personnel, security specialists, and individuals with engineering backgrounds rather than traditional risk professionals.

Obtain good data

Many TCRM functions will continue making decisions based on old and unreliable data, leaving them flat footed and reactionary, unless they change how they gather and analyze data. More importantly, they will come up short in terms of eliminating organizational risk.

A key to ensuring the accuracy and integrity of data is a strong TCRM structure that includes several components—including a risk taxonomy and thoughtfully structured lines of defense. The risk taxonomy establishes the framework for how the organization talks about risk. This taxonomy should be agreed upon by the TCRM function and business units, communicated to all stakeholders, and periodically reviewed and updated as needed. The TCRM structure should also include a risk quantification (or risk scoring) process. This allows TCRM to take the data and prioritize risk based on consistent methodology, thus allowing the organization to allocate resources to the areas of greatest risk.

Also, a team within the TCRM function should independently review the risk data and findings collected by the first line of defense (LOD). This team must manage risk workflow and ensure the integrity and accuracy of the risk information, regardless of where it's located—in the first or second line of defense—or who it reports to (e.g., the chief information security officer (CISO), the chief financial officer (CFO) or another officer). This unit should challenge the accuracy and completeness of the information and point out risk areas that may not be adequately addressed.

Take a proactive, business focused approach to risk

Proactive TCRM teams view risk through a business lens rather than a strictly IT perspective. These teams regularly meet with business units and other key stakeholders to learn about their operations, goals and other concerns, and discuss the most effective means of gathering, using and presenting data. These meetings can also help foster common ground, enhanced working relationships, and the perception that TCRM is a business and innovation enabler, not a roadblock—all important factors in creating a positive risk management culture.

Proactive organizations position the TCRM function to address future critical risks resulting from business decisions, such as the implementation of emerging technologies (e.g., block chain, IA and cognitive computing). TCRM functions need to be flexible and agile enough to seamlessly account for the introduction of these emerging technologies. In addition, they should be able to offer data-backed scenarios that alert the organization to potential risks before they occur. This, in turn, allows the organization to make better informed business decisions.

Forward-looking TCRM teams view risk through a business lens rather than strictly an IT perspective.

Automation and innovative technology

Companies need to equip their TCRM functions with appropriate tools so they can proactively identify, assess and mitigate the new risks that accompany the innovative technology organizations are adopting, including cloud computing, mobile apps, blockchain and IA. These tools can allow TCRM teams to detect, confront and/or eliminate critical risk events before they occur, thus driving business value.

While more mature TCRM functions are leveraging automation, a recent KPMG/Forbes survey found that only 18 percent of TCRM teams currently use automated processes or cognitive technologies even when the rest of the organization does (e.g., sales, marketing, manufacturing, internal audit).

Greater use of innovative technology can also be a key to attaining golden source data. At some point in the future, technology will allow TCRM units to retrieve real time data directly from the source, regardless of the nature of that source, the type of transaction involved, or when it occurs.

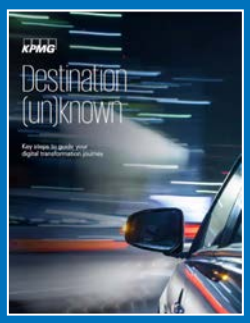
TCRM functions need to make the case to senior management why they need these innovative technology tools to do their jobs effectively. They must demonstrate how these new capabilities will allow TCRM to more effectively gather and analyze data; aggregate and prioritize the variety of risk scenarios the organization is facing; and design and implement mitigation strategies to combat these risks. By educating senior management in this manner, TCRM increases the likelihood of getting the necessary resources and boosting its reputation as a strategic influencer in the organization.

Continuing the conversation

A key goal of KPMG's annual technology and cyber risk management conference is to help build an active, engaged community of TCRM professionals in the financial services space. The forum is a great setting where attendees can share experiences, insights and leading practices, and learn about technology innovations that can help transform the TCRM function.

KPMG looks forward to sponsoring similar forums in the future and encourages more TCRM professionals to participate and continue the conversation with our firm and their colleagues.

For more information on KPMG's tech risk and cyber risk management offerings and thought leadership publications, please click on our TCRM home page or on our TCRM whitepaper, Protect and enable the business with a holistic risk and governance framework.



KPMG

Connect with us:

For more information about how you can benefit from KPMG's technology and cyber risk management services, please go our website, or contact:

Vivek Mehta
Partner
Technology Risk
T: 212-872-6547
E: vivekmehta@kpmg.com

Rob Westbrook
Principal
Technology Risk
T: 804-782-4294
E: rwestbrook@kpmg.com

Luke Nelson
Managing Director
Technology Risk
T: 515-697-1214
E: lnelson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia