Technology and cyber risk management

Protect and enable the business with a holistic risk and governance framework
Meet the authors

Charlie Jacco  
Principal, KPMG LLP  
Cyber Security Services  
Charlie has focused extensively in multiple disciplines of the information security field including Security Strategy, Security Transformation, Digital Identity, Enterprise Identity & Access Management, Cyber Defense, and Cyber Risk Management. Charlie’s experience includes designing and implementing a wide variety of technology-based security solutions, which has resulted in a broad background in technology and risk management. Charlie is also an affiliate board member of the FS-ISAC, which allows him to participate in a wide variety of cyber security and cyber risk topics with executives across the financial services industry.

Vivek Mehta  
Partner, KPMG LLP  
Emerging Technology Risk  
Vivek has over 15 years of experience serving F100 clients in the Financial Services industry, including global diversified-financial institutions, broker-dealers, prime brokers, retail banking, private-equity and investment management companies. Vivek’s primary area of expertise is around IT Risk Management, specifically IT Regulatory management, IT Governance & Strategy and IT controls implementation.

Steve Barlock  
Principal, KPMG LLP  
Cyber Security Services  
Steve is a senior business and technology leader with 25 years of experience in consulting related to IT strategy and delivery. With a broad technology background, Steve has deep specialization over the last 15 years in information security and its application in a business context.
Cyber security risk is a business imperative, not just an IT line item

It feels as though technology changes daily in the current ever-evolving digital era, exposing financial institutions to greater risk and deeper regulatory scrutiny. But it also offers new opportunities for value creation through strategic investment. Through a holistic operational risk framework—with cyber security as a foundational component—financial institutions can achieve competitive advantage while securing their most valued assets against cyber threats.

In constructing a comprehensive corporate governance model, financial institutions must first assess and document the level of risk exposure with which they are comfortable when pursuing new revenue streams, meeting regulatory standards, and fortifying the business during periods of economic turbulence.

This new model enables organizations to gain tactical insight, strategic foresight, and granular analytical visibility as they seek to minimize risk exposure while maximizing actionable opportunities.

How do you address the growing cyber risk challenges facing your business? We believe the framework starts with three interrelated propositions:

1. **Isolate the first and second lines of defense.**
Identifying, mitigating, and managing cyber risk should have lines of sight from the Chief Information Security Officer (CISO) as the first line, and the Cyber Risk Management leader as the second line, which elevates the position and puts it at the heart of the business’s decision-making process. This approach establishes a governance model that clearly defines all cyber risk roles and responsibilities as part of the larger operational risk framework (see proposed org structure on page 5). It also empowers the first and second lines of defense to enable the business through risk policies with well-defined owners.

This arrangement, which creates a clear system of checks and balances, is radically different than the traditional Information Technology Risk Management function that has emerged in recent years.

“Cyber security should be baked into the foundational operational risk management framework to enable the business to make timely and strategic risk-based decisions. The CISO can then focus on protecting the enterprise rather than being viewed as too risk averse and inhibiting the business.”

— Charlie Jacco, Principal, KPMG LLP
2. Define enterprise-wide cyber risk appetite and thresholds. This is the cornerstone of the new, comprehensive operational risk framework. Owned by the Cyber Risk Management lead within the second line of defense, this process outlines measurable key risk indicators (KRIs) that inform the overall cyber security policy, as well as an agile, 360-degree “review and challenge” procedure. This is essential not only for meeting regulatory requirements, but also as a metrics-driven, business-led methodology by which financial institutions can actively address and manage risk exposure.

3. Leverage data analytics and other automated tools to support the business by identifying pertinent risk triggers and making them actionable. The goal is to pinpoint these factors before they impact the bottom line, business performance, or the brand. This is achieved by putting in place KRIs that are more closely aligned with overall operational risk, particularly those related to cyber security, which can measure, monitor and manage potential risk exposure against the previously established organizational risk appetite.
First and second lines of defense: CISO and Cyber Risk Management

For too long, many financial institutions relegated cyber security to the world of IT, deeming it an important, albeit niche function intended to protect the perimeters of the organization against potential threats and actual attacks. This structure often positioned CISOs as impediments to the pursuit of new business opportunities, products and services.

By separating cyber security risk from overall operational risk management, financial institutions diminish the granular insights critical to enabling their business objectives.

We envision a more thorough framework for managing risk across the entire enterprise; one in which cyber security risk is just one of the essential components of an operational risk framework. That starts with clearly defined ownership and oversight roles, new governance models, and establishing key metrics.

When it comes to cyber risk management oversight and ownership roles for cyber security, financial institutions require two lines of defense: CISO and Cyber Risk Management Lead. The CISO, formerly seen as an inhibiting force when pushing the boundaries of organizational risk appetite at times, should be in the first line of defense reporting to the Chief Information Officer (CIO).

The Cyber Risk Management Lead should report directly to the Operational Risk Management Lead in the second line of defense. Ideally, this role should be responsible for operational and cyber risk management across the entire enterprise. This new second line role, together with the executive risk committee, should focus on the overall governance of cyber risk and incorporate that thinking into the organization's top line operational risk management function. This would entail the establishment of risk appetite statements that will feed cyber security policy and KRI's, and enable the business to make educated and calculated decisions based on its own risk appetite and exposure.

This essentially makes cyber security risk a business-led, rather than a technology-led consideration, and enables the business to move at a much faster pace, with confidence, toward new revenue streams.

In order to effectively enable the business, a risk and control taxonomy needs to be established and governed across the first and second lines of defense. The cyber risk management organization should own the policies that tie to business objectives, external regulations, and external standards, which are then mapped to the control objectives that are owned and monitored by the CISO’s organization.

By separating cyber security risk from overall operational risk management, financial institutions diminish the granular insights critical to enabling their business objectives.

We envision a more thorough framework for managing risk across the entire enterprise; one in which cyber security risk is just one of the essential components of an operational risk framework. That starts with clearly defined ownership and oversight roles, new governance models, and establishing key metrics.

When it comes to cyber risk management oversight and ownership roles for cyber security, financial institutions require two lines of defense: CISO and Cyber Risk Management Lead. The CISO, formerly seen as an inhibiting force when pushing the boundaries of organizational risk appetite at times, should be in the first line of defense reporting to the Chief Information Officer (CIO).

The Cyber Risk Management Lead should report directly to the Operational Risk Management Lead in the second line of defense. Ideally, this role should be responsible for operational and cyber risk management across the entire enterprise. This new second line role, together with the executive risk committee, should focus on the overall governance of cyber risk and incorporate that thinking into the organization's top line operational risk management function. This would entail the establishment of risk appetite statements that will feed cyber security policy and KRI's, and enable the business to make educated and calculated decisions based on its own risk appetite and exposure.

This essentially makes cyber security risk a business-led, rather than a technology-led consideration, and enables the business to move at a much faster pace, with confidence, toward new revenue streams.

In order to effectively enable the business, a risk and control taxonomy needs to be established and governed across the first and second lines of defense. The cyber risk management organization should own the policies that tie to business objectives, external regulations, and external standards, which are then mapped to the control objectives that are owned and monitored by the CISO’s organization.

2nd line of defense

External regulations
External standards
Cyber risk business alignment reporting

Business objectives

Tech & cyber policies
Tech & cyber KRI's & risk quantification

1st line of defense

Tech & cyber control standards
Tech & cyber controls & procedures
Tech & cyber control metrics & measurements

Board of directors reporting

CISO operational reporting

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 766387

Technology and cyber risk management
To help ensure that a cyber security risk management framework operates effectively, institutions can benefit from a governance model that delineates and directs the specific roles that the CISO and Cyber Risk Lead/Operational Risk Lead play around cyber risk. This model can also provide the independent risk oversight mandated by regulatory bodies who are setting standards specific to detailed “review and challenge” processes within financial institutions.

With these two clearly defined lines of defense, financial institutions can effectively manage and mitigate cyber risk, especially given the velocity and rate of technology and business change. The CISO can focus on the critical security issues needed to protect the enterprise based on the decisions the business makes, while the Cyber Risk Management Lead can provide 360-degree visibility into operational risk across the entire institution.
Cyber risk appetite and exposure: Independent oversight and regulatory compliance

The current regulatory environment, especially in connection with cyber risk management in the financial services sector, demands heightened adherence and compliance. In the United States, regulators are pushing industry standards such as the NIST Cyber Security Framework (CSF), which recommends how enterprises should assess and take measurable steps to detect, protect against and respond to cyber attacks.

Dueling requirements
However, especially in financial services, multiple regulators are pushing their own requirements, some that are loosely aligned with the NIST CSF, and others that promote agendas with diverging priorities. The Office of the Comptroller of the Currency and the Federal Reserve Bank seem to have similar, but different, cyber security agendas and reporting requirements. Meanwhile, the Securities and Exchange Commission stepped into the arena recently, and even state governments are getting into the game with the New York Department of Financial Services launching its own cyber security requirements. How are organizations supposed to focus on protecting themselves against malicious attackers while still spending so much time and energy collecting evidence to meet regulatory requirements?

Make it real
It is important that an organization’s operational and cyber risk management framework focuses on compliance, while simultaneously creating a holistic policy that is calibrated to the firm’s cyber risk appetite—which should be more risk averse than the regulators’ “bare minimum” requirement.

“Once a policy is in place, organizations should create appropriate governance and metrics across the first and second lines of defense to measure effectiveness and map the framework back to regulatory requirements, which will make it easier to demonstrate that requirements are being met.”

— Steve Barlock,
Principal, KPMG LLP
First and second line action plan

To put this holistic framework into action, the first and second lines of defense need to layer in the right data to create appropriate metrics for the board of directors and their regulators. The first line should:

Maintain process and asset inventories that tie business processes to technology assets and data classifications, along with assigned asset and data ownership.

Create a control taxonomy that ties the policies and standards owned by the second line to the controls and control implementations owned by the first line, incorporates the firm’s Risk Control Self Assessments, and provides the CISO and board of directors with operational metrics.

Perform periodic scenario testing—such as vulnerability scanning, penetration testing, red team exercises, resiliency testing—and incorporate third-party risk management assessment results.

Most importantly, whether it is for regulatory compliance reasons, or hopefully, to create a better firm wide cyber risk posture, one of the key action items is to create an independent risk management oversight function in the second line of defense under the risk committee and Chief Risk Officer (CRO), ideally as part of the Operational Risk Management function, to:

Develop an independent risk management framework that incorporates the firm’s cyber risk appetite based on industry-standard cyber security frameworks, such as NIST CSF, and performs independent assessments.

Develop limits, thresholds and KRIs obtained via existing data from the first line of defense, but aligned to the new cyber risk appetite statements.

Create new metrics and measurement models that include risk quantification, scenario libraries and Cyber Value at Risk (CVaR) to be reported on a recurring basis to the Risk Committee and the board of directors.

Provide advisory services to the first line, including business, technology risk and information security.

Perform stress testing across standard business operational risk that incorporates cyber security measures.

This ongoing governance framework provides a methodology by which cyber risk management and technology risk can align with the overall risk framework, enabling lines of business and executive leadership to innovate and invest with a foundational understanding of the enterprise’s overall risk appetite.
Intelligent automation for cyber risk management

With predictive data, business intelligence and artificial intelligence driving decision making in real time, these intelligent automation technologies should also play an essential role in measuring operational risk, including cyber risk. Data analytics enable the Operational Risk and Cyber Risk Management leads to frame the organizational strategy around risk. Using operational and metrics data supplied by the first line, the second line can develop models to leverage and augment that knowledge and make it a clear component of their risk appetite statements. This exercise will facilitate the development of measurable KRIs to help the risk team better quantify risks and translate them into business terms more commonly seen by the board of directors.

Extracting true actionable insight
When the CISO reports to the board, the discussion is typically technical, focusing on factors such as the number of vulnerabilities that were closed last month/quarter/year. While that is an important key performance indicator of how well the first line is performing operationally and efficiently, it simply does not answer the real questions:

- Have we reduced cyber risk as a result?
- How many of our vulnerabilities were known to be critical?
- How many of those critical vulnerabilities were on essential business assets?

The ultimate contribution of employing these cognitive technologies vis-à-vis cyber risk management should be to quantify risk across a business's core assets, or “crown jewels,” and put that risk in clear business terms. These tools can also shed light on the level of financial risk that is present across a specific set of critical assets, enabling the board of directors to determine where budget should be directed in the interest of reducing risk.

The CRO, as enterprise owner for risk, can leverage the necessary risk tools to gain unfettered visibility to discover and target potential risks that can increase cyber risk exposure. Through monitoring tools, operating models, automated processes, and cyber security risk assessments, a risk exposure road map can be developed that indicates how every potential revenue-generating or productivity action can either align to the current risk appetite or might expand beyond acceptable risk exposure levels.

Additionally, by collecting, storing, and analyzing data and filtering that data through multiple risk diagnostic lenses, financial institutions can quickly and effectively respond to compliance requests from third-party regulatory groups and agencies.

“A forward-looking tech risk management organization does more than manage risk. It predicts risk and empowers the business to make timely, well-informed decisions.”

— Vivek Mehta, Partner, KPMG LLP
Enable your business with an appropriate risk posture

Taking calculated risks in today’s ever-evolving environment demands a new way of thinking. It also requires investing in and acting upon a thorough operational risk framework that fully embraces and incorporates cyber risk management into its model. By establishing distinct roles for both the CISO and the Cyber Risk Management Lead, financial institutions can comply with regulatory directives while determining how to best innovate and invest within the guiding principles of the organization’s stated risk appetite.

With clear lines of defense for cyber security, dynamic risk governance, independent risk management oversight, an unwavering focus on cyber KRIs, and a movement toward intelligent risk management automation, financial organizations can design and build a risk framework where the enterprise is secure and the business can pursue growth opportunities with confidence.

To recap, we suggest you:

- Update your organizational model to create clearly defined lines of defense with the CISO in the first line reporting to the CIO, and a new Cyber Risk Management Lead reporting to the Operational Risk Lead in the second line for independent risk management oversight.

- Establish cyber risk appetite statements, thresholds and KRIs that align to the operational risk management framework to establish a cyber security policy that is governed in the second line and enables your business to make risk-based decisions.

- Incorporate appropriate intelligent automation tools and reporting to quantify cyber risk across critical business assets, positioning the board of directors and internal business leaders to make educated decisions.
KPMG has established a framework for technology and cyber risk management across the first and second lines of defense that we feel will move organizations towards a most holistic view for managing cyber risks, enabling their businesses, and allowing the business to make better risk-based decisions.

### Strategy & Governance

<table>
<thead>
<tr>
<th>Strategy &amp; planning</th>
<th>Policies and procedures</th>
<th>Ownership &amp; accountability</th>
<th>Sponsorship &amp; funding</th>
<th>Information lifecycle mgmt</th>
<th>Operational risk framework</th>
<th>Awareness and education</th>
<th>Table top exercises</th>
</tr>
</thead>
</table>

### Process & asset inventories

<table>
<thead>
<tr>
<th>Business process inventory</th>
<th>Risk and control taxonomy</th>
<th>Vulnerability scanning</th>
<th>Assessment framework</th>
<th>Risk quantification</th>
<th>Unified control framework</th>
<th>Automated control testing</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Technology asset inventory</th>
<th>Risk control self assessments (RCSA)</th>
<th>Penetration testing</th>
<th>Limits &amp; thresholds</th>
<th>Scenario libraries</th>
<th>Horizon scanning</th>
<th>Risk analytics</th>
</tr>
</thead>
</table>

### Data classification

<table>
<thead>
<tr>
<th>Operational metrics/KPIs</th>
<th>Red team exercises</th>
<th>Resiliency</th>
<th>Key risk indicators (KRIs)</th>
<th>Cyber value at risk (CVaR)</th>
<th>Regulatory mapping</th>
<th>Dynamic risk assessment</th>
</tr>
</thead>
</table>

### Technology hierarchy

<table>
<thead>
<tr>
<th>Continuous controls monitoring</th>
<th>Resiliency</th>
<th>Risk appetite</th>
<th>Board reporting</th>
<th>Content creation</th>
<th>Risk intelligence</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Inventory ownership</th>
<th>Risk attribution</th>
<th>Third party risk management</th>
<th>Business, technology, &amp; cyber advisory</th>
<th>Stress testing</th>
</tr>
</thead>
</table>

### Monitoring & Analytics

<table>
<thead>
<tr>
<th>Evidence collection</th>
<th>Technology enablement</th>
<th>Issue management</th>
<th>Risk remediation</th>
<th>Reporting framework</th>
<th>Business performance</th>
</tr>
</thead>
</table>

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 766387
How KPMG can help

Cyber security is a strategic enterprise risk that goes far beyond IT. Whether we are working with your boardroom, back office, or data center, we seek to provide a jargon-free explanation of your cyber threats, the potential impact to your critical assets, and the recommended response. Ultimately, we view cyber security through a cross-functional business lens, encompassing people, change, financial, and risk management.

Our intelligent automation capabilities were built to help our clients unlock the value of AI to accelerate their strategies for automation and cost management, growth and customer engagement, and risk and regulatory policy. Together with our clients, we leverage intelligent automation across the full spectrum of the value chain, creating solutions that are transforming business and operating models.

Contact us

Charlie Jacco  
Principal, KPMG LLP  
Cyber Security Services  
T: 212-954-1949  
E: cjacco@kpmg.com

Vivek Mehta  
Partner, KPMG LLP  
Emerging Technology Risk  
T: 212-872-6548  
E: vivekmehta@kpmg.com

Steve Barlock  
Principal, KPMG LLP  
Cyber Security Services  
T: 415-963-7025  
E: sbarlock@kpmg.com

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

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 766387