Managing IT risk in a disruptive world

Cross-industry perspectives on staying ahead of information technology risks:

Views from a KPMG share forum

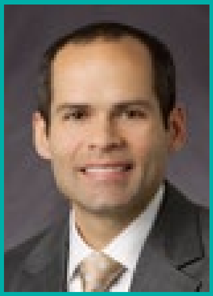
kpmg.com

About the authors

Phil Lageschulte

Phil currently serves as global lead for KPMG LLP's (KPMG) Emerging Technology Risk practice. He is currently focused on emerging technologies—cloud, social media, mobile computing, etc.—and their impact on an organization's strategy. For the past 13 years, Phil also has assisted companies and their boards in managing the business risk related to technology, including IT governance, information security and privacy, strategic sourcing, regulatory compliance, vendor management, and IT audit and audit planning.

T: 1-312-665-5380
E: pjlageschulte@kpmg.com



Joshua Galvan

Joshua helps clients assess, assure, and enhance technologies, operations, and risk management capabilities to assist and improve global business ventures. He leads client service efforts for achieving better IT governance, performance, and integration, helping clients transform and derive more value from IT risk management process frameworks, enabling automation solutions, organizational structures and sourcing models.

T: 1-713-319-2082
E: jgalvan@kpmg.com

The enduring need for ITRM

With the ongoing emergence of new technologies and ever-increasing regulatory requirements, companies across all sectors are seeing a heightened demand for an effective information technology risk management (ITRM) program. But many companies still struggle to establish and sustain a program to help identify, mitigate, and manage the technology risks they face and will face in the future.

KPMG recently assembled a group of ITRM professionals from a diverse cross-section of industries to share better practices and candidly discuss the challenges they are facing with their ITRM programs. The forum focused on five areas of discussion:

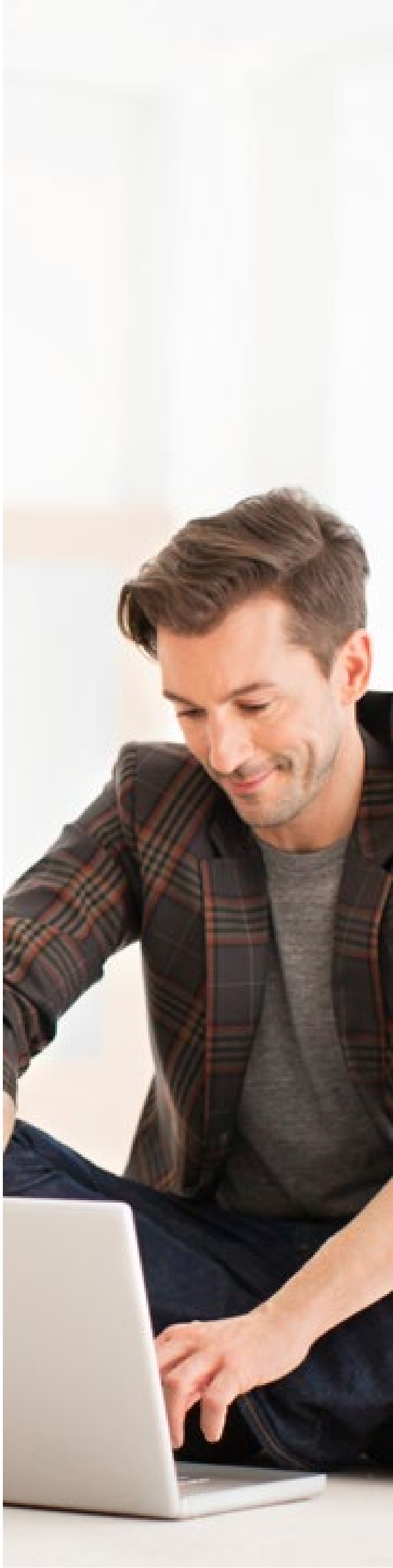
ITRM emerging practices and innovations in the ITRM capability
Participants discussed the challenges and opportunities their companies' ITRM operations are facing, innovations around operating models, and what better practices are emerging across industries.

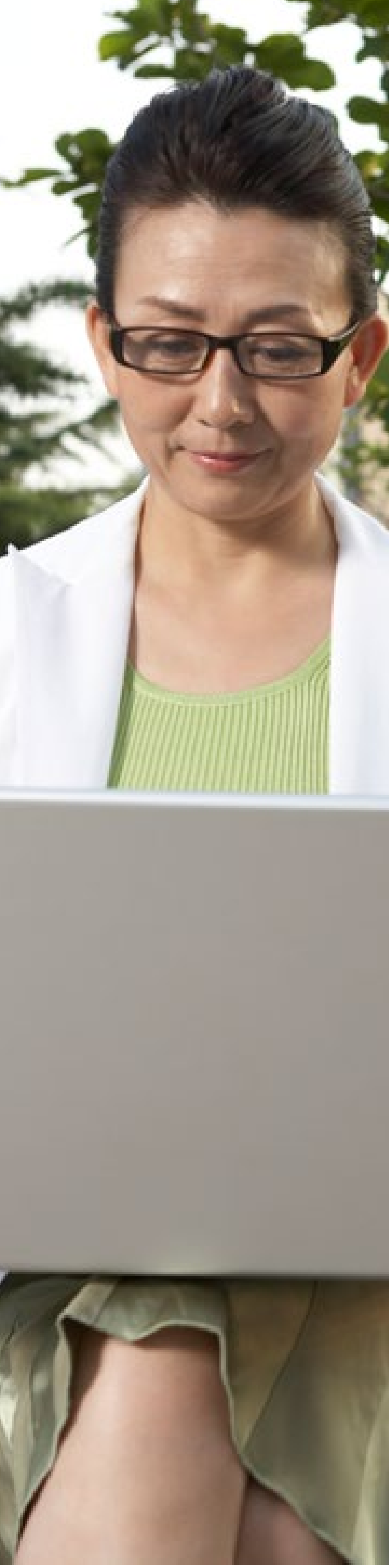
ITRM risk management program development
Participants weighed in on the importance of ITRM, scope of activities, required skills and competencies, the integration of risk management functions, and other supporting activities across the organization.

Third party technology and information risks
Participants explored the advantages and challenges of effectively integrating third party risk management into ITRM, as well as the techniques for identifying and managing related risk.

IT risk management culture
Participants discussed both the benefits and challenges of implementing an effective risk culture for ITRM, noting that it is often hard to define and even more difficult to implement.

IT risk reporting and the boardroom interface
Participants discussed ways to provide boards (and the audit committee) with reliable information and analyses to help make better decisions about what IT risk bets the company is and isn't willing to take.





ITRM emerging practices

An update on innovations

IT risks: More than cybersecurity

Today, when the topic of IT risk comes up, the conversation typically steers to cybersecurity. That is not surprising given the attention the media gives to cybersecurity breaches.

But in fact, cyber is not the most prevalent IT risk experienced by most companies. A KPMG analysis of more than 10,000 news articles related to IT incidents from around the world found that cybersecurity issues accounted for less than half of the total number of incidents.[1] The reality is that avoidable glitches, such as a component failure or human errors, led to more than half of the incidents. These incidents are costly, with each occurrence costing companies approximately $640,000.

$640,000

Approximate price tag for an IT incident.

4 million

Average number of financial accounts (e.g., credit cards) affected by an IT incident.

776,000

Average number of people (e.g., individuals, patients, employees) affected by an IT incident.

Given the number and variety of IT risks that may be present within an organization, participants were asked how their companies identify, mitigate, and manage significant IT risks. Several indicated contracting the services of an external firm to perform an IT risk assessment to help identify, categorize, and prioritize IT risks. Having such an analysis offered several benefits, including creating an overall IT risk management strategy, clarifying leadership about current and emerging IT risks, and estimating the costs to mitigate them. With that understanding, leadership could more easily determine what its risk tolerance would be and allocate appropriate funding for ITRM improvements.

Emerging technologies

Businesses today are embracing emerging and disruptive technologies, including connected devices, cloud computing, mobile computing, robotics automation, and even drones. These technologies reveal new IT risks that may affect the internal business, business partner, customer, and social/community interactions of the company. In addition, companies are employing "agile" business development methods for IT solutions. This presents a major challenge for ITRM: providing adequate risk assurance without impeding innovation.

[1] *Source: KPMG Technology Risk Radar, 2nd Edition—Corporates, 2015.*

As one participant mentioned, sometimes a company will shift the strategy of a technology project midstream based upon ITRM insights in order to avoid undesirable downstream effects. According to the participant, "We were rolling out our network access controls so only our laptops would be able to attach to the company network. Simultaneously, we had another department interested in moving to mobile devices… so we had to adapt our strategy" to consider and address the related risks.

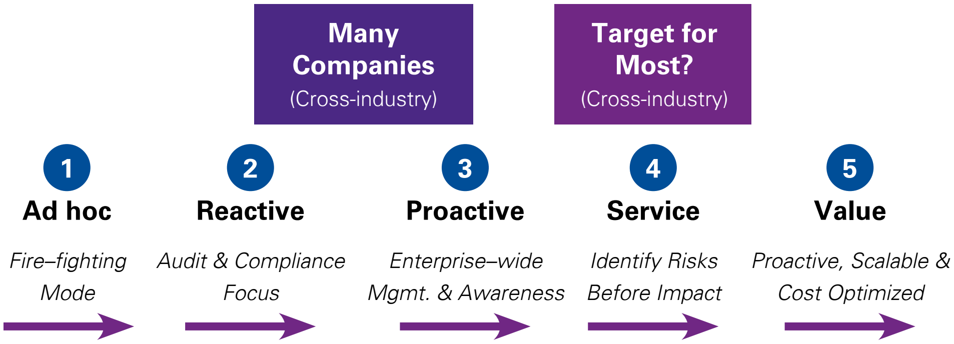
The goal for ITRM, then, is to find that middle ground that spurs, rather than slows, innovation. Ideally, ITRM needs to be able to apply a risk lens that will say "no" less often, and "yes, and here's how" more often.

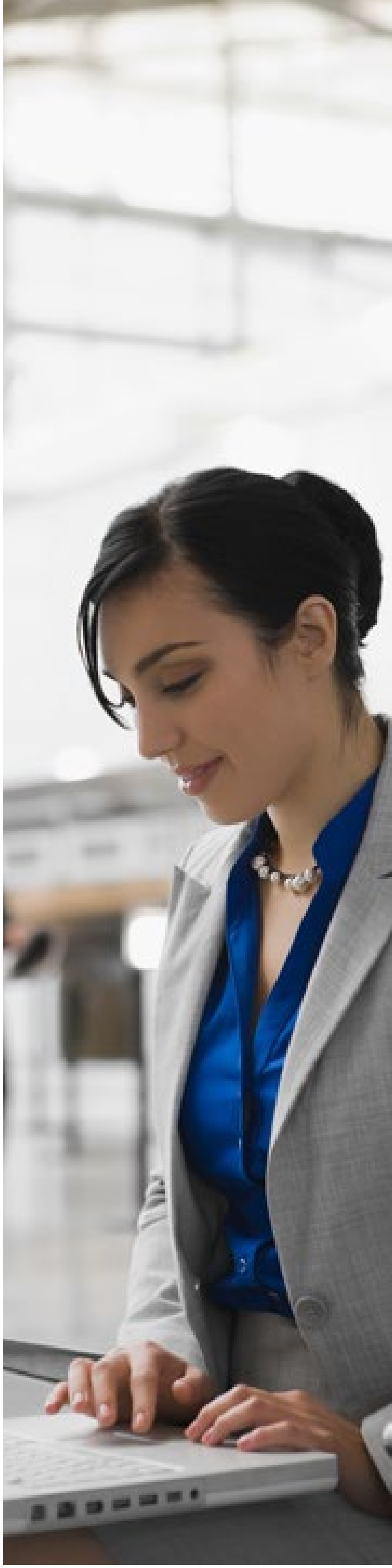
To address the ever-changing IT risk universe brought about by rapid business innovation, company ITRM capabilities must not only align with business strategy and company risk appetite, but also work in partnership with stakeholder groups.

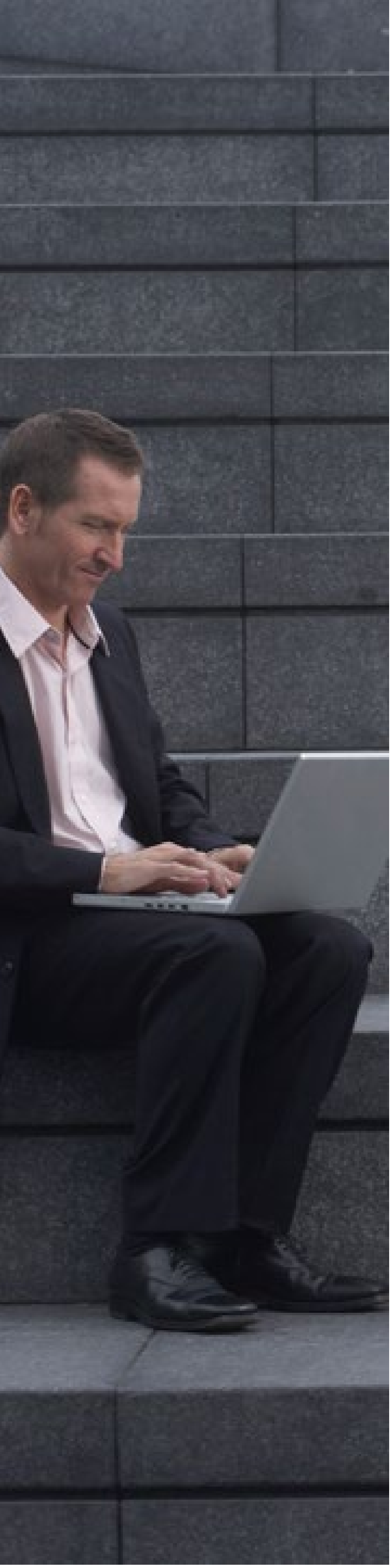
But implementing an ITRM function that engages all stakeholders can be a challenge. Said one participant, "It's so reactive. When we talk to other risk partners in the organization—like insurance, legal, security, internal audit—we're on different pages. We don't even talk the same language. And when we wanted to look at common objectives for the year, we could not align calendars. There were too many other commitments."

Still, a strong ITRM function can act as a catalyst for unifying risk management activity across the organization. For example, risk committees can help drive a common company language for risk and elicit key dialogue about risk management, emerging risks, and reaching a consensus on the company's risk tolerance.

Unfortunately, external market forces and business decisions can affect the priority of investment in ITRM over time. Share forum participants agreed that companies should build and embed ITRM capabilities throughout the company that deliver sustainable value, are cost-effective, and avoid being sacrificed unnecessarily in a down market.







ITRM program development

Putting the pieces together

What is the scope of an IT risk management function? And how can companies build an ITRM function from the ground up that will efficiently and effectively serve their organization's business needs?

Share forum participants discussed those questions, reflecting on where each company represented is in their ITRM journey, what capabilities they need to implement or improve, and how they prepare for the demands of disruption.

In addition to the usual IT risks in an enterprise, companies today now face a slew of new challenges from emerging technologies. Organizations can be susceptible to malicious external threats, such as cyber attacks, data breaches, and espionage. They can also succumb to operational failure or performance degradation if emerging technologies are not properly configured, managed, and maintained. With this, there are also new regulations requiring companies to better identify and protect customer and employee data. And as companies strive to prevent negative social media buzz from eroding brand and reputation, the business demands increasingly more agile solution development, release, and enhancement.

With the right competencies, capacity, and relationships, an effective and integrated ITRM function not only helps a company anticipate and address these risks, but also provides valuable insights for business decision making and results. This sort of ITRM program assists in establishing a risk-aware culture and the associated methods of working and collaborating to take appropriate, proactive action to strengthen the company's lines of defense.

Outline of a modern ITRM program

To achieve those goals, the ITRM program works to identify, manage, optimize, and mitigate the IT risks facing the company. Put another way, ITRM aims to answer these five questions:

- ***What are we responsible for?*** *To which ITRM answers by defining and executing delivery domains, such as assurance and compliance, evaluations and testing, and consulting and advisory.*
- ***What is our scope?*** *To which ITRM answers by identifying applicable content domains subject to ITRM activity performed mainly at the first line of defense.*
- ***What are our priority IT risks?*** *To which ITRM answers by defining a risk universe and risk hierarchy or decomposition.*
- ***How do we get our work done?*** *To which ITRM answers by defining and executing tailored functional domains.*
- ***What outputs do we deliver?*** *To which ITRM answers by developing tailored audits, assessments, dashboards, research, and recommendations for current and future benefit.*

A more flexible and yet integrated approach

But for all the design and implementation of ITRM capabilities, the function must be responsive to shifts in company demand, business priorities, and risk appetite. Solutions developed today must be introduced swiftly, without sacrificing effectiveness to face tomorrow's challenges. In this regard, companies are forming stronger relationships within internal risk management functions, as well as externally with third party suppliers and vendors (software, hardware, and services), driving enhancement of related offerings forward and co-investing in capabilities to anticipate and act in the face of challenges around the corner.

An effective ITRM program requires a company to build capabilities that are embedded and managed across the organization through a sustainable process to provide transparency and accountability. Consequently, aligning the ITRM function with other risk oversight functions, such as enterprise risk management, internal audit, and business continuity management, is critical to speaking a common language, right-sizing risk management efforts, and measuring performance to agreed upon improvement plans.

Third party technology and information risk

Companies are increasingly outsourcing technology, finance, and other core functions to third parties as a way to streamline business processes and reduce costs. While the use of the third party providers (including cloud and software-as-a-service vendors) offers practical benefits, it can also introduce previously unaddressed IT risks.

Organizations utilizing third parties should have a formalized program to evaluate related risks, helping to anticipate and mitigate operations, security and other failures for which a company's investors, customers, business partners, and the media often provide little forgiveness. They want to be assured that the company has its "house" in order and accountability for third party-related risk lies with the company itself.

Common challenges to effectively managing third party risk include:

- Roles and responsibilities have not been appropriately defined to manage third party risks
- A formal third party risk management strategy has not been developed
- Due diligence and procurement processes do not include information security and system integrity considerations
- Third parties are not defined appropriately and are subsequently excluded from related management processes (i.e. long-term contractors operating in a third party capacity)
- Current methods and tools are unable to provide management information on current third parties
- Limited visibility of third party access to IT systems and data.

An effective third party risk program

Companies implementing or improving their third party risk program should consider adopting several key practices, such as:

- Predefined and default contractual language in third party agreements
- Ongoing technology and information security public domain surveillance of prospective third parties
- Ad hoc review of existing third parties
- Integration with existing systems development life cycle (SDLC) processes for internal development teams
- Regular or continuous scanning of internal devices coupled with monitoring of all outbound connections.

Some participants described their companies' efforts to embrace a more holistic approach to information security, including the involvement of the CFO, COO, general counsel, and other executive-level stakeholders in the enterprise risk management committee. Another said that his company has designated privacy advocates. "These are the individuals who have access to a lot of customer information, so they are very privacy aware. They can give us their insight and perspective."

A third described his company's plan for evaluating third parties, "We have a line to us from procurement and legal, and they sit in on our leadership meetings. We have also tried to centralize IT purchases … to get more visibility. But it's still a challenge."

Many companies also struggle to address the issue of unauthorized use of services, given it is not uncommon for some employees, either unknowingly or deliberately, to engage with a third party without involving IT or ITRM (for example, in the use of freely available software or even cloud services, which may be against company policy).

Ongoing evaluation of third parties

Once established, every third party relationship should come under a periodic assessment. But since not all vendors are of the same importance, companies can deploy different levels of assessment depending on potential risk.

To sustain relevance and effectiveness, third party evaluation approaches should be reviewed periodically to help deliver targeted outcomes and align to future ITRM program goals. (See sidebar)

Key questions related to program evaluation:

- Is the third party risk assessment kept current?
- Has the understanding of the third party information security processes and controls increased?
- Has the program improved third party relationships?
- Did the program achieve targeted ROI?
- Has key stakeholder involvement increased over time?
- Are the process improvements identified through the program being addressed?
- What roadblocks still exist related to adoption of the program?

IT risk management culture

With respect to risk management culture, "tone at the top" is essential. But it takes more than this to create a corporate environment that effectively manages a company's risk exposure, including IT.

Risk culture refers to the behaviors exhibited by companies in making risk-related decisions. It is an important component to fulfilling an overall risk strategy and encompasses a number of elements, such as risk appetite, communication, measurement, and training.

Share forum participants discussed the importance of risk appetite in particular. Representing the amount of risk a company is willing to accept, risk appetite must be defined and communicated across functions and organizational levels.

Steps to achieving an effective risk culture

The traditional method of building risk culture from the top with a commitment from leadership involves a strong directive from the C-suite and discipline and communication around the consequences of noncompliance. While this is an essential component, it is only the first step. Advancing the program requires a "bottom-up" approach to spread the culture across functions, including IT. Share forum participants discussed the manner in which effective risk culture is often embedded through peer pressure, rather than by pressure from above, resulting in risk management practices being integrated in the way tasks are performed day to day.

One participant also advocated a "middle out" approach in which risk leadership at the team level is strategically placed to influence and lead practices, champion standards, build talent, and generally represent an example in the company's risk culture. This "managing up, managing down" arrangement puts the right leaders in the right place and requires strong support from functional leaders and the C-suite.

Enabler and differentiator

As company risk culture matures, resulting ITRM practices and approaches become assets within the organization. With more proactive ITRM practices, a company promotes improved risk transparency, which can clear the path to business results and innovation of differentiated products and services. It transforms the way risk is viewed and addressed, moving the company away from effort spent on managing exceptions and merely responding to audits and compliance checks.

Key related questions

Third party technology and information risk program evaluation

According to conventional wisdom, risk appetite is determined in the boardroom and cascaded throughout the company. In actuality, the process often occurs more in the middle, with risks assessed at the division or function level, then communicated up to leadership. This upward feedback assists companies in keeping a finger on the pulse, continuously evaluating the risk situation, and monitoring risk appetite thresholds over time.

To perform its role, ITRM must have linkage across the company, including an effective process for reporting to the board. IT risk reporting must align with company priorities, have support across stakeholder groups, and demonstrate clear steps for ITRM maintenance and enhancements over time. In this way, IT risk reporting not only contemplates the key IT risk categories of the company, but also seeks to justify and secure sponsorship for ITRM innovation.

Yet companies face a challenge in gathering the right information in a timely manner and aggregating it into an effective senior leader message that not only identifies current IT risks but also outlines a vision for better ITRM practices.

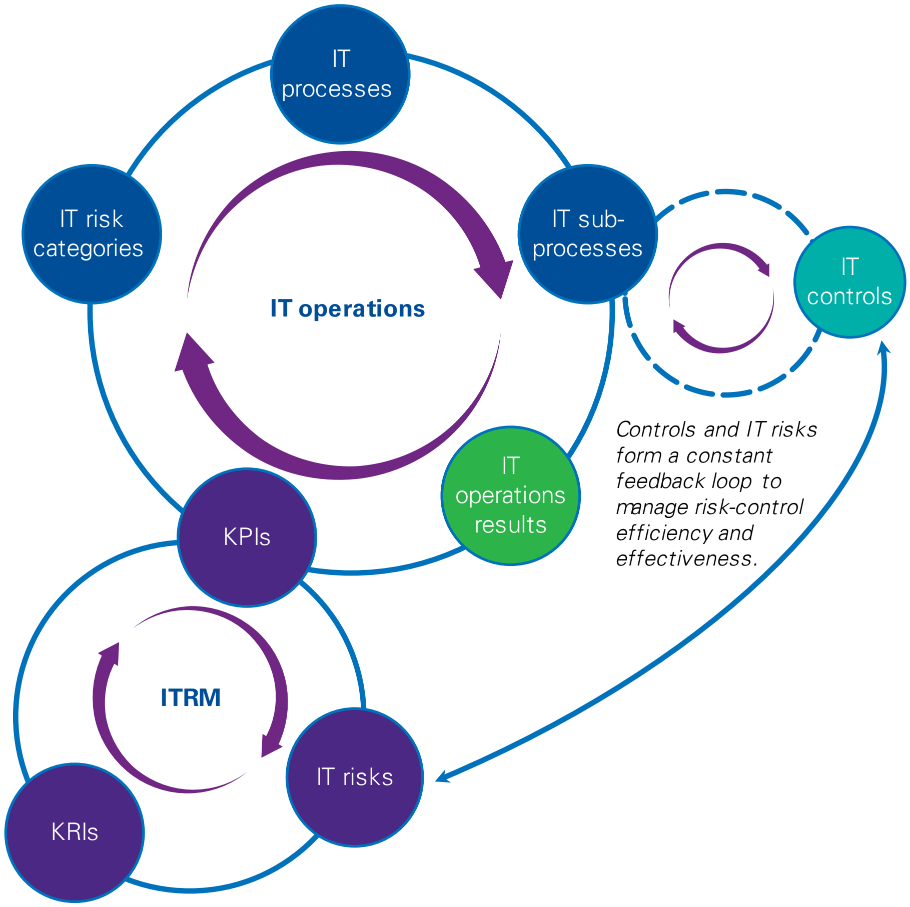
Share forum participants discussed a few principles for effectively building an IT risk-reporting model. By understanding the company's current IT operations process model and leveraging existing data sources for IT risk measurement, ITRM experiences a lighter burden in supporting IT risk reporting. Related relationships improve through this design, mitigate the common impression of ITRM being "a police force," and encourage accountability and responsibility for risk identification and management in the front lines.

The KPI and KRI relationship—an opportunity for efficiency

A popular method of reporting to the board involves dashboards with data and analysis displayed in easy-to-understand graphs and charts. A number of participants expressed frustration with the reliability and timeliness of source data, let alone the development of analysis and relevant and understandable messages for senior leader decision insights.

Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) together are an effective basis for relevant data in developing a risk dashboard. Activities in IT operations and ITRM combine to provide data on operational performance and risk management. IT operations performance is measured and monitored with KPIs. Risks in IT operational processes are identified and used to develop a company's tailored set of KRIs and thresholds.

Not unlike IT operational process, ITRM operational activities also have KPIs, and combined with KRIs, provide the data necessary for delivering a combined efficient and risk-focused activity set.



Controls and IT risks form a constant feedback loop to manage risk-control efficiency and effectiveness.

Key elements of risk dashboarding

IT risk dashboards enable review of ITRM KPIs and KRIs, eliciting recommendations and actions that both sustain good practices and improve practices over time. Key elements of risk dashboarding thus include:

- **Risk Appetite:** It is essential to determine if the company is taking on too much risk or not enough. Risk appetite allows companies to balance strategy with performance.
- **Risk Thresholds:** Risk thresholds represent risk appetite and are recalibrated as conditions change. Measured quantitatively and often aggregated at the risk category level, they help a company determine when the risk situation may be trending towards or exceeding risk appetite.
- **Metrics:** Measurement of the risk appetite and operational performance using reliable and timely source data compared to established thresholds.
- **Top Risks:** Analyzing KRIs and KPIs helps highlight risks that pose the highest threat to achieving the organization’s strategic and operational objectives. Top risks help focus leadership attention and resources in the company.
- **Reporting and Dashboards:** Communicate the risk situation (health and performance) at various levels of IT and the business to facilitate effective decision making.

Company boards are continuing to deepen their involvement in business strategy, including execution. To achieve effective risk management, board members want to understand what key risks they should be aware of and monitoring. They also want to know how well the company is prepared to react and recover if something goes wrong. That means communications with the board must be a two-way street, enabling leadership to make decisions that balance strategy and risk.

Integrating IT reporting with internal audit

If IT risks are being identified through an enterprise risk assessment, they are likely to be among the highest ranked risks of those identified by internal audit. Share forum participants observed that there should be a freer flow of information between internal audit, ITRM, and ERM, driving efficiency in review and consensus on needed action at the board and audit committee level.

Final thoughts

As companies face increasing disruption in the marketplace, changes in regulatory requirements, and adoption of emerging technology, threats to IT will continue to multiply. ITRM will continue to be a critical capability for managing related risks.

Our forum explored some of the key issues facing ITRM professions today: emerging ITRM practices, building an ITRM program, managing third party technology and information risk, fostering an effective risk culture, and IT risk reporting. At the end of the day, the following key points emerged:

- Balancing risk with reward, ITRM professionals are called upon to inform technology adoption strategies, without hampering key business efforts and programs that drive and sustain growth.
- As enablers of IT solution development and innovation, ITRM professionals apply a risk lens so the answer is less often, "no," and more often, "yes, and here's how."
- Modern ITRM models overcome fragmented knowledge and skills, cumbersome solutions, and limited company and industry context through an investment in a full operating model involving people, process, and technology.
- Third parties represent a growing and significant area of risk for many companies and the need to effectively assess and monitor IT risk relative to third parties requires focus from ITRM as well as other key stakeholders within the company.
- Effective ITRM culture starts with leadership buy-in and a framework of standards with clear rewards and consequences. A top-down ITRM organization and bottom-up process model together enable a sustainable risk management culture.
- IT risk reporting must strive for effective executive team and boardroom interactions. Successful IT risk reporting requires open information flow and development of a trustworthy and current IT risk story for timely decision-making and action.

Employing these concepts, IT professionals continue to evolve ITRM from a support role to a truly value-adding function that helps companies successfully meet the challenges of tomorrow's disruptive business environment.

How KPMG can help

KPMG works with companies that want to establish an ITRM function, as well as those that wish to enhance their current risk management function. Our services help organizations transform ITRM by proactively building integrated capabilities to identify and manage strategic, regulatory, and emerging technology risks, and helping design methods to reduce the associated operational costs through sustainable, repeatable, and insightful processes.

Contact us

Phil Lageschulte
Global Lead
Emerging Technology Risk
T: 312-665-5380
E: pjlageschulte@kpmg.com

Joshua Galvan
Principal
Emerging Technology Risk
T: 713-319-2082
E: jgalvan@kpmg.com

kpmg.com/socialmedia

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

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.