KPMG
cutting through complexity

KPMG CROSS-INDUSTRY ITRM SHARE FORUM

Tuning the IT Risk Management Radar

Observations from the event held August 13, 2015

kpmg.com

A common view of IT risk management (ITRM)

is that it has historically focused on information security controls and compliance checks. A modern view, however, holds that **ITRM addresses a rapidly evolving and prioritized company IT risk profile** through smart process design, effective resource alignment, and use of automation to manage IT risk in a fast-changing environment. For example, increased incidence of cybercrime, adoption of disruptive technologies, and tougher regulatory requirements increase visibility to IT risk and reinforce calls for more robust ITRM capability.

ITRM strives to better integrate with business operations, known as the first line of defense, and other company risk functions, collectively known as the second line of defense, to stay ahead of the evolving risk curve. Additionally, agile ITRM process frameworks foster collaborative stakeholder relationships within the CIO's office and beyond. And while disruptive technologies have enabled companies to implement new business strategies, they have also forced companies to begin **fundamentally transforming** their approach to ITRM. Overall, ITRM is changing to become **more proactive, predictive, and automated,** and **companies are now beginning to look at ITRM from a value perspective**.

To discuss the current state of ITRM across industries and the key challenges and innovations needed to sustain effective operations, KPMG LLP (KPMG) convened its first cross-industry ITRM share forum. Participants from the automotive, banking, energy, insurance, retail, restaurant, and technology industries discussed ITRM work "content" as well as emerging and innovative practices. They discussed their organizations' current capabilities, key challenges, and planned improvement initiatives, highlighting the opportunity for ITRM within their own companies, and potentially beyond.

The share forum framed the discussion around the following topics:

- Emerging practices in ITRM
- The IT risk universe, emerging risks, and the interconnectivity of risk
- IT risk assessment practices
- Risk management synergies in the enterprise
- ITRM operating models and operationalizing ITRM
- IT risk sensing and ITRM "ROI"

Key findings

Five observations from the meeting show the following:

1. Emergence of Line of Defense "1.5"
Companies continue to focus on standardizing a three-lines-of-defense model to provide adequate risk management strategy, standards, execution, and enablement. Many companies are building a so-called "1.5" line of defense component function that both enables and challenges the first line of defense and provides effective engagement and integration with the second and/or third lines of defense.

2. An improved understanding of the IT risk universe
Companies are beginning to measure IT risk appetite and impact in a more quantitative and accurate way in order for them to rationalize the IT risk universe and the related ITRM activity set. They are also developing and utilizing solutions that bring new focus to critical IT assets and information.

3. Focused and flexible IT risk inventories
Companies continue to focus on flexible mechanics and fit-for-purpose tools to organize their IT risk inventory. These are seen as providing better transparency and accuracy into risk likelihood and impact, moving beyond mere spreadsheet list management.

4. Alignment of ITRM with other risk functions
There is a common need for integrating ITRM with other company risk functions, with various companies implementing new practices to attain and sustain the right ITRM "seat at the table." This is resulting in a more common risk management language and an increase in the relevance and timeliness of IT input to the enterprise risk view.

5. A focus on managing ITRM talent
Talent management remains an issue, and there is a continuing trend of ITRM functions delivering more with increasingly limited resources. With an almost constant rotation of people and high competition for talent across the industries and services firms, companies are challenged to right-size head count and best deploy skills to operationalize and sustain ITRM.

Emerging practices in ITRM: from reactive to proactive

IT risk is a key topic in most corporate boardrooms, and there is a growing focus on effectively anticipating and responding to related emerging threats. As cyber attacks and information security breaches continue, companies are rethinking ITRM by going beyond a singular focus on compliance and moving toward **enhancing cross-functional integration, proactive threat management, agile process models, automation, and dashboarding.**

A KPMG-sponsored survey[1] revealed that seven of the top ten enterprise risks discussed in the boardroom have direct or indirect linkage to IT. Interestingly, about half of those surveyed said they were spending more on risk management, but only a third felt that their risk management practices were adequate. The majority of survey respondents said regulatory compliance was a large driver of their risk management efforts; however, only a few companies were moving toward a system of unified control compliance. In addition, the survey found that social media and cloud technology continue to weigh on the minds of executives. ITRM, however, has not been seen to have a seat at table when doing large-scale initiatives.

Companies are moving to more predictive risk management, and they are **looking to ITRM to inform a single, comprehensive story of risk in the business context**. They need to leverage data to achieve more real-time IT risk transparency with integrated capabilities that involve infrastructure, applications, networks, and governance, risk, and compliance platforms. In addition to being a risk manager, **they look to ITRM to play the role of consultant to the business and contribute to risk-informed decision-making.**

Mature ITRM models have overcome fragmented knowledge and skills, cumbersome solutions, and limited company and industry context to provide greater risk insights and intelligence, partnering across business lines and risk functions. In a recent KPMG survey, respondents commented on their ITRM maturity according to a scale of five stages: adhoc, reactive, proactive, service, and value. Many companies across different industries are in the proactive stage of maturity

[1]KPMG and Economist Intelligence Unit survey, 2012

"it's not information security anymore, it's really risk management."

and aspire to develop into the service or value stage. While companies across industries define the service and value stages differently, consensus on a specific company's ITRM maturity target is critical to aligning stakeholders on priorities for improvement and innovation. In rethinking their approach to ITRM, companies are focusing more on enterprise risk appetite, linking to IT, and **developing process performance, quality, and scale measures that help sustain the success of ITRM operations.**

A dynamic IT risk landscape demands resource capacity, skills, and automation that are balanced with continuous ITRM improvement. As a set of initial priorities, many companies are focused on the design and implementation of a company-tailored ITRM process model and method for content management and sharing. With the onslaught of emerging risks facing all companies, a typical next wave of ITRM investment provides automation improvements that aid in gathering data, intelligence, and dashboarding for management decisions. Aligning the ITRM organization and people elements is important to effectively and efficiently carry out the ongoing ITRM activity set in collaboration with the business lines as well as other risk functions.

The IT risk universe, emerging risks, and the interconnectivity of risk

The IT risk universe starts with the enterprise strategies and operations, with risks appropriately aligned thereto. In today's environment, **the IT risk universe includes emerging risks and the increasing awareness and management of risk interconnectivity.** Companies must assess whether they have a firm grasp of their risk appetite and key ITRM focus areas, including the sources used to identify and anticipate emerging business or IT risks and the relationships between the two.

A participant from a major oil company discussed how the company's controls-based framework became unsustainable over the years as risks evolved and risk management practices grew more complex. While controls-based frameworks work for small companies or even small operating units of larger enterprises where IT is not at the core of the business, they are too rigid for large companies. He said multinationals must now perform ITRM in a risk-based approach, rather than through the mere application of a controls framework accompanied by periodic compliance reviews. However, an understanding of risk and the methods for risk-based controls may still be inadequate in many companies and industries.

The company started the journey toward a risk-based framework by adding new *modules* of activity to its existing control framework and processes for infrastructure and information security. He noted that this worked for over a decade, but that the company is now struggling with developing and retaining high-quality IT risk analysts and obtaining, let alone maintaining, leadership support.

Given the shortcomings observed with other methods, the oil industry participant argued that "it's not information security anymore, it's really risk management" that is needed, and "the end results are substantiated conclusions on which we can make hard decisions." He said the function in the oil company has improved organizationally, but processes are still too focused on information security. The function also lacks a **standardized process framework to follow that truly enables IT risk management rather than just compliance with a controls standard.**

Nonetheless, he cited examples of risk management models that have achieved varying levels of success in different fields, including insurance models and weather prediction. However, there are still major struggles in economic prediction models, and earthquake or pandemic prediction models still fall short. While many companies refer to ISACA's Control Objectives for Information and Related Technology (COBIT) 5.0 framework as a risk reference, he insists that they still lack in delivering true risk management capability that informs smart investment decisions. The company strives to have the clarity and confidence in estimates of probability and consequence—removing so much of the guess-work and subjectivity that permeates the practice today—to help the CIO, for example, invest $2 this year in order to save $7 over the next several years, converting ITRM into rewards.

"We need to come up with a mechanism to collect data that is flexible, automated, and fairly close to what is happening in the day-to-day activities across companies and industries", he said. He noted that a key goal is to remove the subjectivity from current IT risk models and replace it with parameters that can be calibrated, benchmarked, and updated. By collecting operational data and key risk indicators (KRIs), companies can distill the risk component from them in a consistent and sustainable way that aggregates low-level risks for correlation to high-level risk themes. The vision described includes one day participating in a practical cross-industry standard of practice for quantifying IT risks that is used broadly and aligned with general theory in risk management fields.

Risk management synergies in the enterprise

Companies manage risk through a variety of functional capabilities that include the first and second lines of defense. These include ITRM, internal audit, legal and compliance, and enterprise risk management (ERM). An issue that many companies face is whether **the various risk functions are sufficiently complementary and collaborative to inform and enable one another to provide a reliable enterprise view.** Boards are also calling for increased visibility into

the company's risk position, compliance status, and governance processes, especially when going through major transformation or regulatory reform efforts. Many companies are considering whether a rationalized risk management approach can yield **more assurance at a lower cost and, specifically, what process models, organizational structures, and tools are required to get there.**

Many issues lead to a lack of synergy in a company and make for an ineffective, scattered approach to governance, risk, and compliance operations. Regulatory compliance efforts are often managed independently, resulting in a cumbersome, redundant, and sometimes expensive approach. Control environments are also still heavily manual, despite a trend in increased technology spend. Companies are not taking advantage of enterprise resource planning platforms, with automated controls, integrated and streamlined processes, and central data for a single version of the truth.

Many companies still have not yet achieved a standardized approach for managing risks and operating controls across the enterprise. In response to this situation, risk management practitioners are evaluating options for **better coordination, relationship networks, and information flows across the various company risk management functions.** "There's a level of efficiency that we have to achieve in terms of how we deliver in a more coordinated way," said one participant. "We're communicating our view of risk, but there might be a function that comes in and communicates a whole other view of risk." Timely, or not-so-timely, to risk management processes and related investment decision making, ITRM practitioners—as with all risk management personnel—must have a seat at the table to properly inform the process and support a more inclusive and cohesive model.

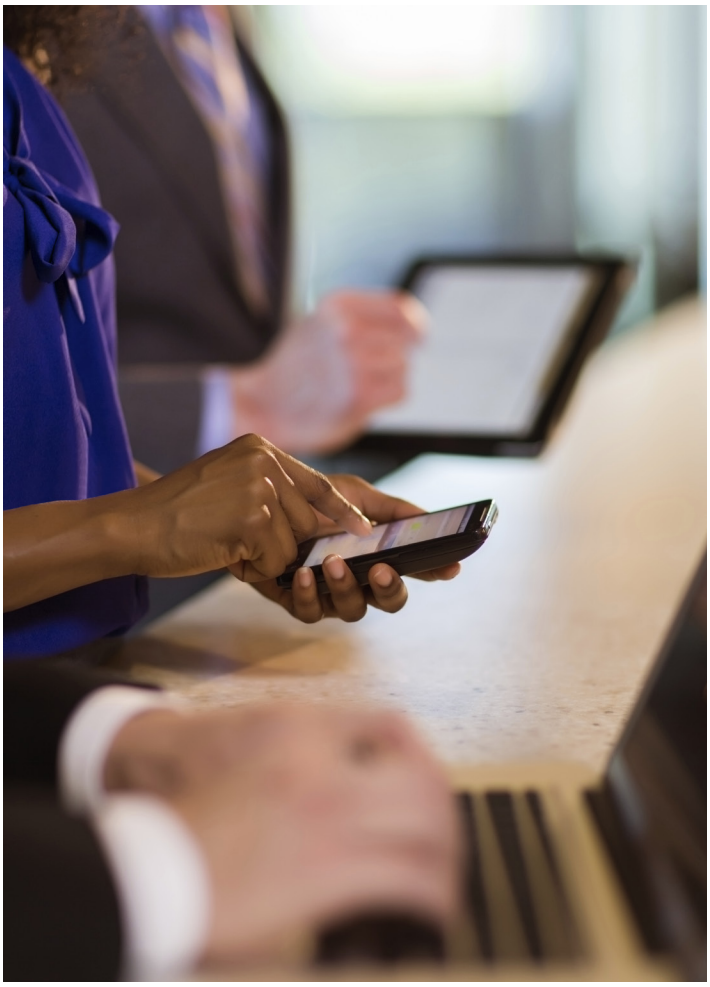
"The integration of business, IT, and players in the third line of defense would be well served working together to understand these impending risks in order to better assess risk in general."

Companies are also facing the issue of effectively thinking through the **signals of impending change** that could impact their industry or their company directly. Cutting across industries, these **disruptive forces can affect company business operations from top to bottom, including IT.** Companies must better anticipate and manage these risks, perhaps developing new ways of undertaking the risk inventory and assessment process in general. One participant said that "the integration of business, IT, and players in the third line of defense would be well served working together to understand these impending risks in order to better assess risk in general."

The participants shared stories in an open discussion about how they are adopting or evaluating new technology to enhance their business, whether for corporate operations or how they engage customers and business partners. Many participants noted the impact of new technology like wearable and digital devices, the online customer experience, and connected devices and sensors in commercial and industrial applications. "We need to be proactive and think about how any of these technologies are going to change how the consumer reacts," a retail participant said. A participant from the restaurant industry concurred and explained the global challenges associated with social media, a major component of his company's "digital risk" inventory. "Digital risk knows no boundaries, and that's what keeps our leadership up at night," he said.

IT risk assessment practices

In the modern company, a vast majority of operational or financial risks are linked to IT. But companies face the issue of **maintaining a representative risk inventory through efficient mechanisms and tools that keep the inventory current.** A participant from the automotive industry discussed how the company started its ERM program in 2009 because of a disconnect in how risk was being managed. The company developed a program to improve its ability to identify significant



risks, implement sustainable and repeatable processes for managing risk, and advise executive leadership and the board on matters pertaining to enterprise and strategic risks. The program has also **successfully advanced and promoted risk management awareness across the company.**

By establishing a risk committee at the board level and an executive leadership team, along with risk officers in all company functions, they "are generating more relevant risk discussions deeper within the company," he said. The company's success is due in part to achieving top-down support for change from the business units up. The top-down and bottom-up approach has helped it to explain risk indicators within the company more effectively, where before "there was nobody connecting the dots who would raise that risk issue to the appropriate level."

Those tasked with ITRM operations are compelled to go beyond their own areas and take an enterprise-wide view of risk, helping to identify "those significant, key, or extraordinary events that could really hurt the company." As part of this task, the ITRM group conducted a survey of open-ended strategic risk management questions to encourage dialogue and inventory these risk areas. In identifying the specific known and emerging risks, the company developed and maintained improved knowledge of several factors: impact, likelihood, speed of onset, response readiness, and control effectiveness.

In addition to informing the company's approach to designing an early warning system for IT risks, the survey revealed opportunities to enhance IT strategy and governance; systems development, acquisition, and maintenance; and IT infrastructure and operations. In combining new information flows—both internally from employees and externally from stakeholders, news reports, or industry trends—with a renewed focus on operations improvement, the company is more prepared to anticipate and respond to the evolving IT risk profile.

ITRM operating models and operationalizing ITRM

Many companies are challenged with **aligning ITRM organizational and operating models, acquiring and staffing talent with the right skills, and scaling the program for shifts in company and industry performance.** One participant from a financial services company shared details of the company's multiyear journey from a controls-focused and reactive ITRM function to a more proactive approach.

As part of the process, the company focused its first year on envisioning, adopting, and implementing a lines-of-defense model; assessing current state and defining target state roles and responsibilities; implementing and transitioning to the line of defense activity set; and developing KRIs. Another significant move at the company involved **realigning resources from the risk department into embedded roles within the business lines.**

The goals for year two were more ambitious around becoming more proactive. The company continued its focus on refining and aligning its ITRM staff model, defining a menu of ITRM services, developing methodologies for key services, and engaging internal audit (IA) for advisory support. The company's monthly reporting dashboard and second line-of-defense role in monitoring high-risk areas have provided important and increased visibility. A perpetual cycle of evaluating process effectiveness and results continues to yield improvements, and in year three the company plans to implement a risk radar to more proactively surveil the risk situation, both known and emerging components.

Another financial services participant noted that the keys to operationalizing ITRM and building a second line of defense for IT were strong commitment from leadership, consistent and repeatable risk reporting, a staffing model with deep functional expertise, and a priority focus on the highest risks. Basing its ITRM foundation on COBIT 5, the company has achieved **reliable accountability and more credibility within the business lines and IT, enabling change for more effective communications and risk management.**

For many companies, perception in the business lines, lack of understanding of value-add, and effective engagement at the necessary levels throughout the company often stymie ITRM operationalization. In efforts to shift the risk culture from a controls and audit issues mind-set to proactive risk management approaches, companies are better delineating roles and responsibilities, attracting and retaining key talent, and investing in behavioral and organizational change management.

A participant from the restaurant industry discussed the challenges of operationalizing ITRM in the global business context and detailed the particular challenges arising from social media. He explained that, like other disruptive technologies, social media generates a lot of data that must be protected. He said the company leverages social media "to get real feedback, but we also have to understand the risk that data is bringing in." Resolving that **social media** is the responsibility of both the first and second lines of defense, the company is addressing it through risk identification and proactive risk management planning. In applying an attitude of risk awareness and ownership, the company has **spurred all lines of defense into action and promoted effective information sharing.**

By applying this attitude to other emerging technologies (such as wearable devices), the company can stay apace of innovation, meeting customer, business operations, and risk management needs alike. Sustaining a consistent strategic philosophy and a core set of operating principles leveraged across assets and data domains, the company's "prescribe-describe-recommend" approach has been very effective in the ITRM content and functional domains.

IT risk sensing and ITRM "ROI"

Companies often baseline their risk profiles on a periodic basis (for example, every one to two years). But with a rapidly evolving landscape, this challenges the viability of yesterday's frameworks, measurements, and thresholds as applied to today's business situation. Companies are designing **IT risk-sensing capabilities to demonstrate the effectiveness of in-place mitigation strategies.** In doing so, they have **visibility into whether ITRM is delivering planned benefits** such as avoiding the cost of what could happen, and enhancing business outcomes by applying a risk lens.

One technique in use by a company in the financial services sector is the risk threshold framework (RTF), which is designed to measure application stability by using a set of available

"... we also have to understand the risk that [social media] data is bringing in."

data inputs and applying metrics to enable management to make risk-intelligent decisions. The RTF's focus on application stability and change risk factors is a move away from spreadsheets. It utilizes central data sources selected on the basis of statistically relevant metrics to drive behaviors around application control, including in particular change management processes where oversight and governance of higher risk changes are warranted.

Models like the RTF aim to **create transparency and consistency in IT risk evaluations, so that companies can then prioritize control efforts and technology investments.** For example, with the RTF enhancement, funding is prioritized for stable applications, but unstable applications receive funding only for risk mitigation. As such, the RTF integrates IT operations, IT portfolio management, and IT risk management, enabling alignment and collaboration in the IT application management life cycle.

Another financial services industry participant corroborated the challenges in characterizing what is considered IT system maintenance and mitigation and what is considered new capabilities. With the key objective being to stabilize the IT risk situation, this company's use of a "kill chain" to **determine the most critical IT components helped it identify opportunities for operational and control improvement.** These included developing IT risk reduction strategies through better testing, implementing additional operational support, minimizing change collision, and rescheduling or canceling releases.

Participants agreed that keys to success center on having a clear value proposition; having key stakeholder involvement, and champions or change agents embedded throughout the company; and connecting to or enhancing existing governance processes instead of building new ones. This means persuading personnel and functions to work collaboratively to a common ITRM goal, as opposed to an "approach by edict" that has shown to yield limited results or scale.

Conclusion

ITRM across industries is changing in response to the evolving risk situation. There are now **calls for more predictive risk identification and effective risk management, streamlined operations and a focus on value (not just compliance), and the ongoing adoption of disruptive technologies.** In response, company ITRM functions are designing new operating models; optimizing resource allocation; and leveraging data, automation, and risk management decision-support tools. While many companies are still on average at a maturity level of two or three (out of five), many have near-term aspirations for level four and beyond.

Contact us

Phil Lageschulte
U.S. Network Leader
Emerging Technology Risk Services, Chicago
T: 312-665-5380
E: pjlageschulte@kpmg.com

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

Vivek Mehta
Managing Director
Emerging Technology Risk Services, New York
T: 212-872-6548
E: vivekmehta@kpmg.com

kpmg.com