Banking on an agile IT risk management

How the financial services sector manages and secures technology risk in disruptive times

kpmg.ca

> Technology risk exposure at financial services organizations is currently high.

The state of IT risk management

In the financial services industry

Disruptive innovations, such as blockchain. Increased regulatory attention on information technology (IT) risk culture. Competition from financial technology (Fintech) start-ups.

At KPMG LLP's (KPMG) recent share forum for IT risk professionals in the financial services industry, IT Risk Management in the Disruptive World, one message came through loud and clear: Technology risk exposure at financial services organizations is currently high, and threats and regulatory pressures continue to mount. In an industry in which a system hack can wipe out millions of dollars and a service interruption can halt an economy, protecting technology infrastructure and securing data and information takes on critical importance.

Technology risk managers in the financial sector are under tremendous pressure. But they also have a prime opportunity to increase their prominence and add value to the organization. With a robust IT risk framework behind it, technology can be let loose to enable the core business and drive new growth.

So what are the key issues confronting financial services IT risk organizations? What tactics are leading companies using to identify and manage risk proactively and align controls and responses to the enterprise's risk appetite and business goals?

To address these questions, we drew together IT risk professionals representing 70 percent of the largest financial services organizations, including investment banks, retail banks, commercial banks, insurance companies, asset managers, and government-sponsored enterprises.

The firsthand experiences and key insights they shared—which we highlight in this paper—shed light on the state of IT risk management (ITRM) in the financial services industry and revealed leading practices in securing technology operations amid unprecedented change and disruption.

According to an IT risk leader from the organization, the continuous monitoring journey allows the organization to rationalize controls and reduce performance cost.

The challenges

Traditional risk management processes are too slow, inconsistent, and opaque.

Leading approaches

As financial services businesses become more digitized and the amount of data and information within them explodes, ITRM functions realize that they need to push the boundaries when it comes to data and analytics if they are to detect risk and compliance issues across increasingly complex financial and operational environments.

One way they do that is with continuous monitoring. The share forum attendees report that continuous monitoring helps financial services companies get a single, consistent, and transparent view of risk and control performance based on data, metrics, and analytics. This enables companies to proactively identify risks, put risks into perspective, compare risks and their impact to the business, and make more strategic risk remediation trade-off decisions when resources are limited.

Continuous monitoring capabilities may not necessarily replace traditional risk measurement techniques, such as risk and control self-assessment or risk assessments, but are increasingly being relied on as the primary tool to identify and manage technology risk.

In practice: Managing the *right* risks

Designed to enable better management decisions about technology risk, the continuous monitoring approach of a large financial services company consists of:

- A second-order control framework that confirms first-order controls are executed with the right quality
- Data storage and processing that aggregates transactional, operational, risk, and control data for analysis
- Executive reporting dashboards that help leaders understand the biggest IT risks and their potential impact.

The business does not understand its key technology-related vulnerabilities.

Leading approaches

Today, most C-level financial services executives understand the criticality of protecting data and systems. They want to stay informed about all aspects of IT risk so they can effectively guide decisions about what risks to control and how to prioritize remediation of issues. In fact, more than three-quarters of share forum participants regularly report on IT risk to the board of directors.

Do you consistently report to your board on all aspects of IT risk (including security)?	
Yes	78.57%
No	7.14%
Don't know	14.29%

However, traditional IT risk reporting metrics and dashboards can overwhelm business leaders and stall decision making. That is why financial services IT professionals say knowing your audience is critical to effective IT risk reporting at all levels, from individual technology units all the way up to the board level.

In practice: Keeping risk reporting simple

At one large financial services company, "the board was having trouble understanding what risks were important and what they could tolerate," according to the head of information security.

So the company transformed its approach to risk reporting, focusing on informing management of only what it needed to know to act. The team currently only reports six total technology risk metrics to the board. Its executive dashboard clearly compares controls effectiveness and risk level so management action can focus on the highest risks in the areas with the weakest controls.

The challenges

Financial services regulatory bodies are scrutinizing risk culture.

Leading approaches

As misconduct and other security missteps continue to make headlines, one of the top focus areas for the largest financial services regulatory bodies is technology risk culture.

In the context of financial services, risk culture refers to behaviors that are exhibited in how risk-based decisions are made, communicated, and measured. These behaviors are critical. If the core is weak, there will be problems with the surrounding risk and compliance processes.

As such, financial services companies are working to formalize how risk is considered when making key business decisions and embed risk-conscious behaviors throughout the organization. Cultural programs take many forms, such as:

- Including risk in formal decision-making processes
- Company-wide compliance training
- Top-down communications campaigns about risk and ethics
- Incentive programs for doing the right thing
- Incorporating risk in the hiring process.

In practice: Can you measure a culture?

What metrics can measure the health of an organization’s risk culture? Some potential methods currently in use at financial services organizations include:

- Tracking policy violations, e.g., when an employee sends nonpublic information outside of the network
- Behavior modeling, which identifies behaviors that fall outside of the norm, e.g., when an employee downloads many more files than usual or accesses a system he or she has never accessed before
- Measuring positive actions, e.g., when an employee self-identifies an issue before a formal audit

Emerging technologies like social, mobile, cloud, robotics, and blockchain present unknown risks.

Leading approaches

New technologies that improve the customer experience or operational performance are a competitive differentiator in financial services. But as businesses go digital, it is increasingly difficult for IT to protect the enterprise.

To balance risk and reward, share forum attendees say they are taking a structured approach to tracking and reporting emerging risks by updating their ITRM policies, standards, and procedures to incorporate emerging technology risks.

For example, mobile and wearable devices can lead to data theft and leakage of internal corporate information. As usage among employees increases, organizations may need to test, validate, and strengthen security settings for wireless and mobile entry points to the network.

Likewise, as the number of customers using digital and mobile payments increases, organizations will need to address vulnerabilities to data privacy and security and continually monitor the availability of mobile apps.

What is riskier: Blockchain or robotics?

Is blockchain getting undue attention in the financial services and risk community? According to one share forum participant, the risks may be similar to those driven by cloud adoption—namely, protecting corporate data.

Meanwhile, another attendee believes the promise of robotic process automation and cognitive technology is actually greater than blockchain, as it presents opportunities to reduce costs by automating middle-office and back-office activities. However, the risk and control implications are also greater. When you are making thousands of decisions with cognitive technology without even knowing you are making them, the integrity of your code has to be higher.

As one share forum participant indicated, "people are tired of the regulatory 'whip' and want to really understand the value proposition of an IT risk function."

As one share forum participant put it, "We're really good at what we do; we just don't write it down. That doesn't help with the value proposition or fly with the regulators."

"The business is always thinking about market risk, and the missing component was technology risk," said another attendee. "We are showing the board they have to be accountable for that, too. Reporting to the board is an obligation because we have to respond to regulation, but we really should be doing it because it's good for our business. It's helping us run more effective and efficient processes."

The challenges

The traditional approach to ITRM of focusing entirely on regulatory

Leading approaches

ITRM organizations are increasingly being required to focus on and articulate their value proposition in addition to just meeting regulatory requirements.

Firms are taking a number of approaches, including forming governance bodies and integrating risk into performance scorecards. Several participants indicated that they have a board-level subcommittee that focuses on technology risk.

Many financial services ITRM functions are focused on correlating technology risk decisions back to the business.

There is a confusion within financial services organizations about who is responsible for managing specific technology risks.

Leading approaches

The industry continues to define clear and consistent roles and responsibilities for the three lines of defense, and increase transparency and coordination between IT risk, IT service management, and business operations.

One driver is to satisfy regulators.

Closing disconnects between ITRM and decisions made on the ground on a daily basis also helps the technology function run more efficiently and effectively.

“We are seeing regulatory scrutiny and pressure to have clear delineation between the first line and the second line; there is no 1.5,” said one ITRM professional. “We need to break-down the silos—if that integration isn’t there, the regulators will catch on to that.”

“As the second line of defense, I’m interested in effectiveness and sustainability,” said another attendee. “But the risk itself has to be owned at the first line, where the risk occurs.”

The challenges

Rapid innovation from the fintech sector is pushing traditional financial services organizations to innovate faster.

Leading approaches

To compete with smaller and less regulated start-ups and maintain market share, traditional financial services companies are experimenting with agile software development and delivery. While most organizations represented at the share forum are still in the experimental stage, this trend is challenging IT to manage increased technology risk driven by a culture of speed and continuous delivery.

"The alternative is that we take six months and we miss regulatory deliverables," says a company IT leader who attended the share forum."

What is the general level of adoption for agile and related methodologies (including CD, DevOps, etc.) within your organization?	
Widely adopted and used (e.g., including core banking transformation)	37.50%
Mostly experimental usage (e.g., methodology defined but mostly pilot implementations)	62.50%

To speed up technology innovation and go-to-market in a responsible way requires a balance between innovation and control. That means as organizations move to agile, they also need to strengthen controls.

For example, they should implement privileged access logging and monitoring, automated controls across all phases of development, peer review of changes, robust code management, segregation of duties or restricted access to critical business functions, and automated reconciliation of system transactions versus developer production edit logs.

In practice: Innovation versus control

Agile development of technology systems is enticing, but many organizations are not ready to take the leap. At one financial services organization, IT is taking a measured approach.

Rather than going fully agile and releasing updates daily or even multiple times per day, the company's IT developers are doing "sprints." Updates are pushed every four to six weeks, giving IT more time to ensure the systems are fully secure but still increasing time to market.

About KPMG's IT Advisory Services

KPMG's IT Advisory Services can help organizations manage IT-related opportunities and risks to enhance operating performance and provide a level of governance and assurance over their IT controls and infrastructure. With deep industry experience and global networks, our professionals provide practical recommendations for complex business problems. We can help our clients enhance the value of their IT investment by advising them on how to use technology to help drive growth; improve business performance; and maintain operational integrity, security, and continuity.

KPMG professionals apply a risk lens when assisting our clients as they navigate new emerging technologies, develop processes to protect information assets, address assurance over third-party systems, and align their IT audit capabilities and governance with their organization's business strategy and complex regulatory requirements. We provide forward-thinking, resilient, and sound advice on timely and complex technology topics to help guide clients toward positive results.

Contact us

Francis Beaudoin
National Leader
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

kpmg.ca

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.