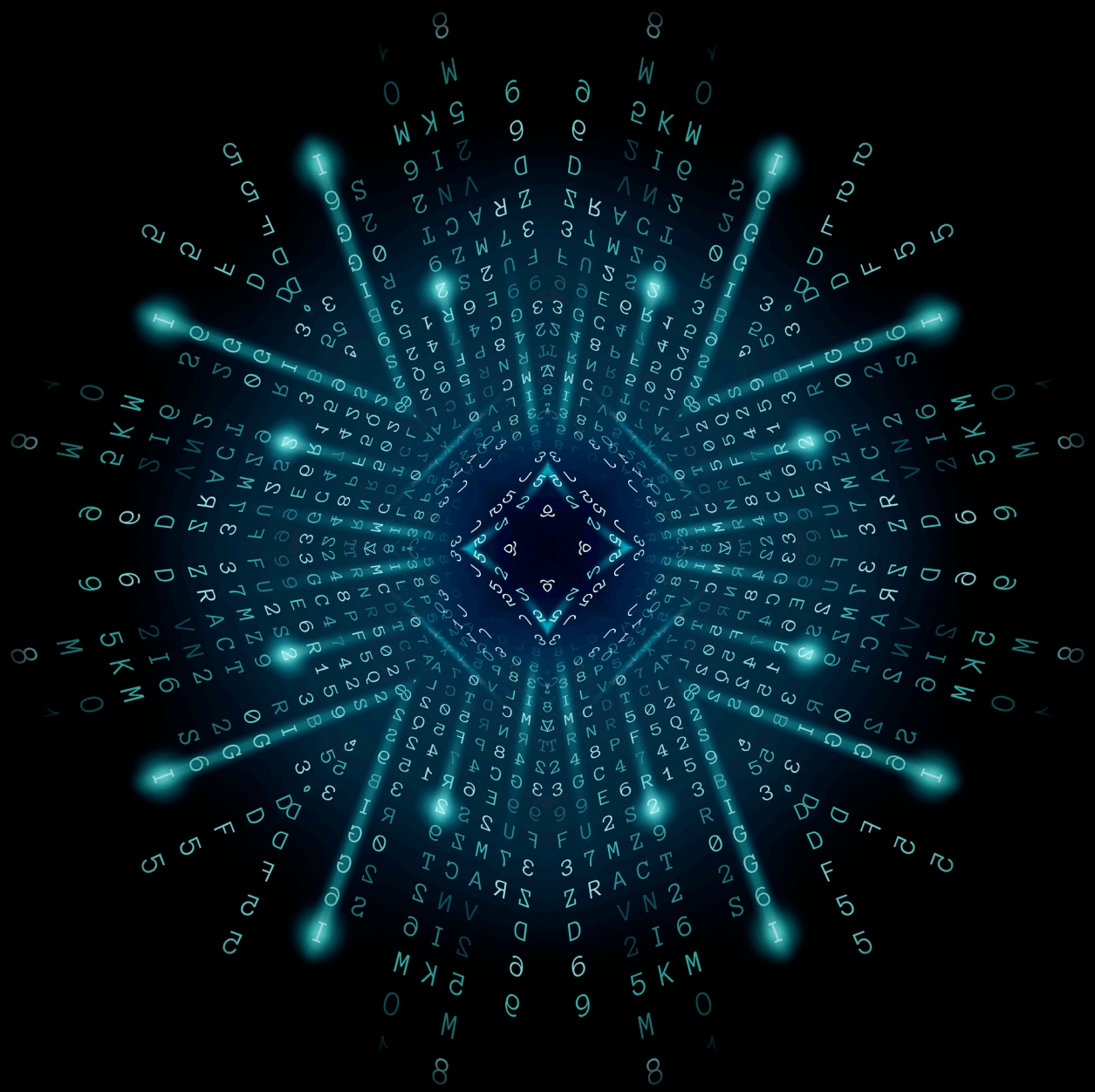
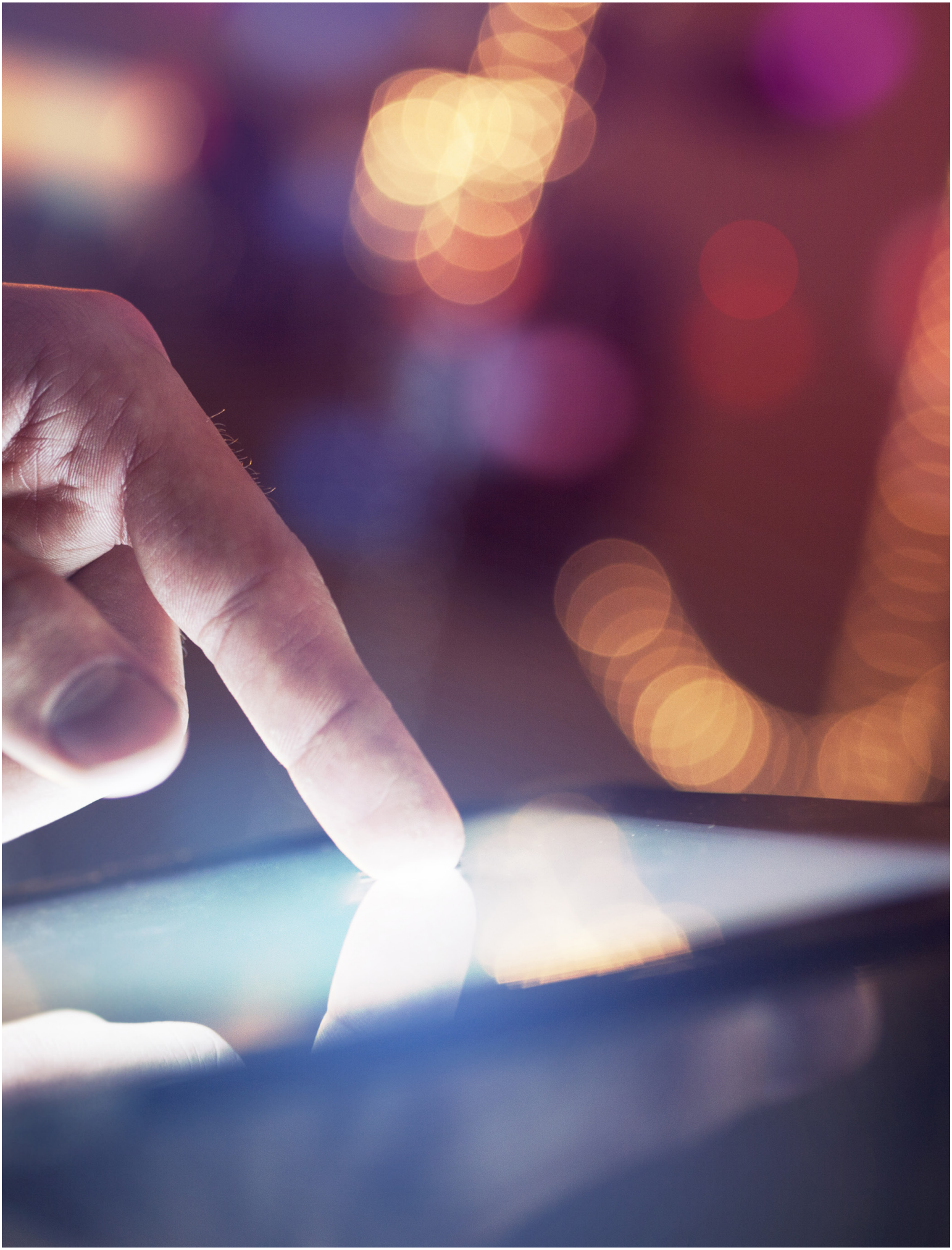
Deloitte.



What board members need to know—*and do*
Information technology risks in financial services:



Boards' risk-related responsibilities at financial services companies have intensified, with governance of Information Technology (IT) risk becoming increasingly critical. Yet IT risk may be the one risk that the typical financial services board member may be least prepared to oversee. After all, few directors are chosen for their expertise in IT, and many think of IT risk somewhat narrowly—that is, in terms of cyber-attacks and system availability—when in fact IT risks permeate the company.

Consider that at the heart of a financial institution lies, in essence, a technology company. Technology enables virtually every activity in financial services and consumes a huge portion of capital investments and operational expenses. A financial institution's performance depends on the reliability and security of its technology. System downtime can hobble an institution and its customers. The business relies on accurate and timely data. The changing technology landscape requires institutions to make strategic decisions on which technologies to adopt, and which to avoid. Weak controls in technology can lead to processing errors or unauthorized transactions. And regulators around the globe continue to focus not only on safety and soundness but also on compliance with country-specific laws and regulations.

Boards are as accountable for overseeing IT risk as they are for other risks. Ultimately, the effective management and governance of IT risk depends on both the senior executive team, including the chief information officer (CIO), chief risk officer (CRO), and chief technology officer (CTO), as well as well as a broad set of accountable managers from across the company. All financial organization leaders must understand IT risk and the levers available to ensure it is being adequately addressed. This paper highlights select IT risks for boards of financial institutions to consider, and suggests strategies they can employ to better oversee them.

The Board and IT Risk

To address technology risks, board members need not become experts in IT, but they do need to understand the IT landscape well enough to oversee and challenge management.

Technology is the great enabler, but it also presents pervasive, potentially high-impact risk. Cyber risk in the form of data theft, compromised accounts, destroyed files, or disabled or degraded systems is "top-of-mind" these days. However, that is not the only IT risk that the board and management should be concerned about.

Financial institutions face risk from misalignment between business and IT strategies, management decisions that increase the cost and complexity of the IT environment, and insufficient or mismatched talent. Financial companies' technology may become obsolete, disrupted, or uncompetitive, with legacy systems hindering agility. Mergers and acquisitions can hopelessly complicate the organization's IT environment—a fact that many management teams fail to budget for and address. Meanwhile, technology-driven startups and disruptive financial technology ("FinTech") solutions are challenging the business models and processes at the core of many institutions, making swiftness of response a requirement for ongoing relevance and viability.

Technology risk holds strategic, financial, operational, regulatory, and reputational implications. To address this, board members need not become experts in IT, but they do need to understand the IT landscape well enough to oversee and challenge management.

Deloitte's IT Risk Management Framework

A good starting point for the board is to understand the framework management uses to manage IT risk. While frameworks vary from institution to institution, an effective one helps drive a practical and consistent operating model across all IT domains to identify, manage, and address risks. As an example, Deloitte's IT Risk Management Framework is shown in Exhibit 1.

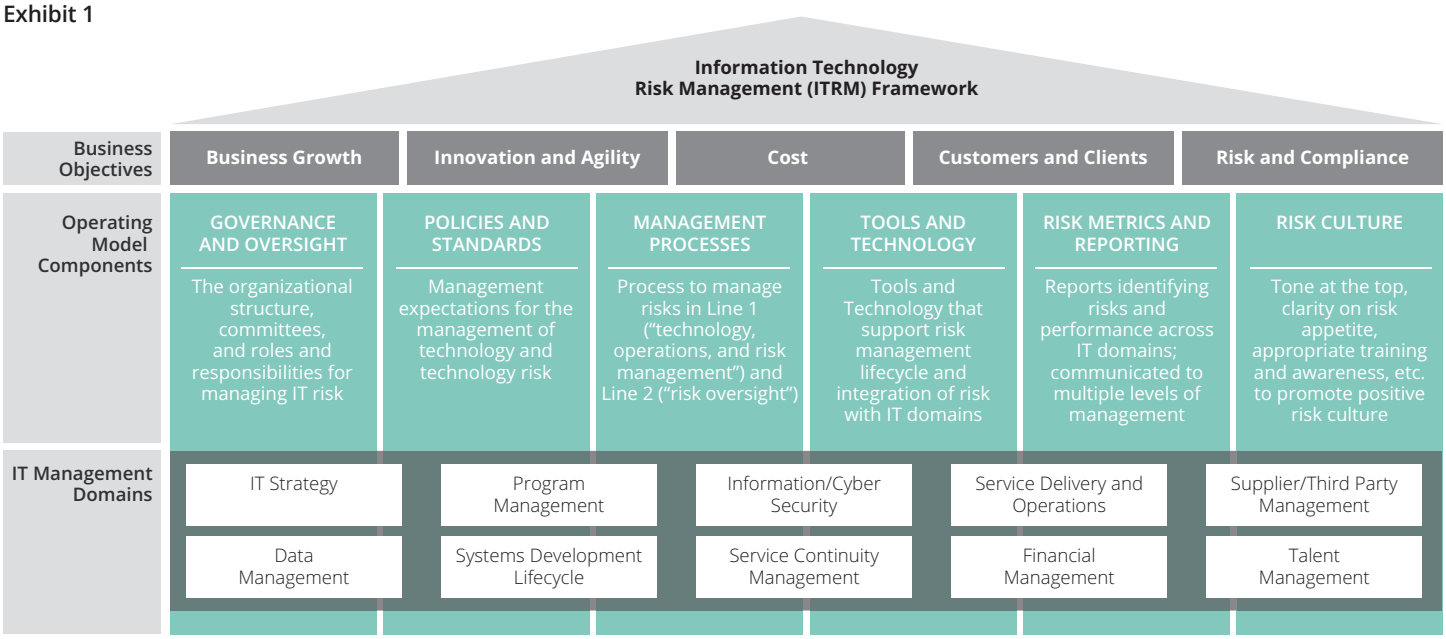
This framework depicts—along the top layer—the key drivers and business objectives of IT in financial services: enabling business growth, achieving technological innovation and agility, promoting cost reduction, supporting a customer and client focus, and solidifying effective risk and compliance management.

The next layer illustrates the six operating model components required to support IT risk management across the company: governance and oversight, policies and standards, management processes, tools and technology, risk metrics and reporting, and risk culture.

The bottom layer identifies typical IT management domains, such as IT strategy, data management, and service delivery and operations. While the names or configuration of these domains may vary from company to company, they are typical of the activities required to implement IT capabilities in an organization.

IT risks can emanate from any layer within the framework. First, risks can emerge from competing priorities among the objectives of achieving business growth, reducing costs, supporting a client focus, and so on. Second, IT risks can persist within or be amplified by an inadequate risk management operating model, i.e., ineffective governance and oversight, policies and standards, management processes, tools and technology, risk metrics, or risk culture. Third, risks can emerge from unsound delivery of any of the 10 IT management domains pictured here, including IT strategy, program management, cyber security, and so on.

Exhibit 1




Technology
Innovation
SYSTEM

Top risks in information technology

To oversee IT risk, boards must understand the risks technology poses to the institution, and have questions for management that drive a real understanding of the risk landscape and set clear direction and expectations.

Some of the most significant risks in technology in financial services include:

1. Strategic risk of IT
2. Cyber security and incident response risk
3. IT resiliency and continuity risk
4. Technology vendor and third-party risk
5. Data management risk
6. IT program execution risk
7. Technology operations risk
8. Risk of ineffective risk management

The following serves as a primer for board members on each of these risks and can be used to drive more meaningful conversations with key stakeholders on IT risk.

Strategic risk of IT

In a rapidly changing world, risk emanating from an ineffective IT strategy stands among the top threats a financial institution faces. Examples of risk emanating from IT strategy include:

Embracing versus watching new technology: Institutions must balance the risk of adopting new technology against that of ignoring it or waiting for things to settle. Cloud solutions hold both immense promise and significant risk. FinTech solutions—a focus of much innovation in financial services—are disrupting the status quo, driving increased competition and important decisions on partnerships and technology adoption.

Run versus build: IT and the business must agree on the appropriate portfolio of investments, specifically on how much to spend to "keep the lights on" versus investing in new technology and capabilities. Overspending on maintenance can crowd out opportunities to adopt new technology and develop new capabilities.

Lack of integration between IT and business strategies: Failure to integrate business and IT strategies can lead to inappropriate investments and misaligned expectations. The IT strategy must support evolving business priorities and operating models, and enable agile responses to market developments.

Legacy technology: Financial institutions continue to struggle to phase out or decommission outmoded technologies including data centers, platforms and applications. Often technology retained to support select geographies, custom products, or unique processes generate increased complexity and higher costs. When this occurs over hundreds or even thousands of applications, the organization can find itself hamstrung by its own technology.

Avoidance of hard truths: Mergers and acquisitions multiply applications in technology portfolios when management focuses on short-term cost savings rather than simplifying and upgrading the IT environment. In many cases, bold investments may be required to address years of having avoided expenditures required for a sound and efficient environment.

Questions for the board to pose:

- What is our organization's IT strategy, particularly as it relates to supporting our businesses, offerings, and customers and other stakeholders?
- In general, do we as an organization want to be an innovator in IT-enabled financial services or to take the more conservative route and be late adopters? What do we need in place to manage the risks inherent in either strategy?
- How do we monitor the marketplace for developments that could pose opportunities or risks for our business?
- What investments are required to remediate and update our legacy IT environment?

Cyber security and incident response risk

The many reports of cyber attacks, data privacy breaches, and misconduct at major companies have pushed cyber security to the top of boards' agendas. Directors need to understand management's view of cyber risks, the potential likelihood and impacts of risk events, and the steps taken to address the risks. It is neither practical nor possible to protect all digital assets equally; in addition to having foundational cyber capabilities across the institution, "crown jewels" should be identified and further protected. Management must be vigilant in identifying emerging threats and implementing effective mechanisms for mitigating them. Finally, vigilance in cyber security—access controls, security protocols, and the like—should not hinder the institution's objective of being easy to do business with. It can be a difficult balance to achieve.

Cyber incident response (CIR) kicks in when cyber security fails, as it almost certainly will from time to time. The high probability of a cyber incident dictates that management must have a solid, well-tested CIR plan ready to launch when an incident is detected. Responses should be proportionate to the incident and cover technical, forensic, communication, and compliance protocols. Priorities might include securing the digital evidence, restoring operations, and notifying senior management, affected stakeholders, and perhaps, law enforcement and regulatory authorities.

Questions for the board to pose:

- Do we have the right accountability model in place for cyber security? Do we have the right funding and talent?
- Have we identified our "crown jewels"? What have we done to protect them?
- Considering the evolving cyber risk landscape, where are our greatest exposures and what investments are required?
- For which cyber scenarios do we have controls in place?
- Have we tested our Cyber Incident Response plan? Are we well-rehearsed?

IT resiliency and continuity risk

With technology enabling virtually every activity in financial services, the organization's IT must be resilient from disruptions and outages. An organization should have resiliency standards so that investments in resiliency capabilities go toward the technology that supports its most critical business processes. Recovery testing, especially for critical technology, must be rigorous and verify that recovery plans will work.

Institutions need an end-to-end view of all technology required to support a particular product or process to validate that all components can recover from a disruption. Often times, institutions perform one-off testing of a particular technology application, rather than comprehensively testing all technology required to support an end-to end process such as clearing or settlement. Finally, institutions relying on third-party providers for critical technology services must understand the third party's resiliency and recovery capabilities as if the technology were owned and operated by the institution.

Questions for the board to pose:

- Have we defined our critical business processes and identified the technology assets—applications, infrastructure, and third parties—most essential to supporting them?
- What scenarios have we planned and tested? Have we planned for extended and/or rolling technology outages?
- Do we understand the single points of failure (SPOFs) in our technology environment?
- Have we experienced any situations where we were unable to respond to a technology outage within our planned timeframes? Why did our testing process not identify this weakness?
- What steps need to be taken to reduce the number and mean time of outages?
- Are we prepared if multiple systems fail at once and do we know which systems are dependent upon one another?

Technology vendor and third-party risk

As arrangements with vendors and service providers, joint venture partners, and other third parties proliferate in financial services, so do the risks. Indeed, third parties' own technology risk can generate operational, financial, reputation, and other risks to the institutions that use their services. A clear understanding of these risks can be obscured by business imperatives and enthusiasm for the relationship, by standard forms of assurance provided by vendors, and by check-the-box due diligence processes.

The financial institution as a whole must develop and implement proper due diligence, contracting, and monitoring procedures for all third parties, including technology vendors engaged by IT. Due diligence must be performed on the third party's reputation, strategic alignment, financial viability, compliance, and other attributes.

In addition, IT must take the lead on assessments of IT capabilities of third parties, whether the third party supports IT or the business. While many institutions have mature capabilities to assess third-party cyber and business continuity risk, they should also understand the effectiveness of the third party's technology management processes. For example, ineffective change management procedures at a third party can increase the risk of a service disruption.

Questions for the board to pose:

- What are the major IT risks associated with the institution's service providers, business partners, vendors, and other third parties?
- What is our process for due diligence—and subsequent monitoring—of third-party IT risks?
- Do we have adequate oversight of vendors with respect to their resiliency and recovery capabilities?

Data management risk

Ineffective data management at a financial institution can open the way to financial fraud, accounting and regulatory reporting issues, and loss of stakeholders' trust. Regulatory agencies are expressing strong interest in data management capabilities, given that risk and capital management depend on reliable, accurate, and timely data. In addition, financial institutions are increasingly combining external data with internal data, adding new layers of complexity to data management and, potentially, new risks.

Rigorous data management capabilities rest on data governance, policy, and procedures that support accuracy, reliability, and timeliness of data, and clarify data ownership, uses and alteration. Controlled creation, transformation, storage, and disposal of data is central to the concept of data integrity.

When institutions retain unnecessary data, they face additional cost, complexity, and risk that it could be breached. Institutions should have policy and standards supporting the sound disposal of data, and assurance that policy is being put into practice.

Questions for the board to pose:

- How effective are our data management policy and standards?
- Are critical data elements identified in key applications?
- How is data quality measured in key services and associated applications?
- How is data governance integrated with IT processes such as the systems development lifecycle, architecture reviews, and the like?

IT program execution risk

At any given time, a large financial institution will have multiple IT programs in development across organizational functions and geographic regions. Examples include enterprise resource planning (ERP), enterprise risk management (ERM), and customer relationship management (CRM) systems. These programs present risks, such as budget overruns, delays, and failure to deliver targeted business results. Generators of risk include programs misaligned with strategic objectives, program charters that fail to address risks, lack of program governance, uneven execution, misallocation of resources, and lack of formal communication. IT program management is also critical to the success of any merger or acquisition that will combine IT systems.

Management needs to focus on the change management, as well as the technical, aspects of a project and minimize optimistic assumptions in project plans. Use of analytics to identify and manage risks, forecast project outcomes, and identify course corrections as projects unfold is an emerging approach. Data-driven decision making methods can supplement or replace the anecdote-driven approach that often prevails in project planning. Testing the waters with a pilot project can reveal how analytics might work and whether to implement that approach on a broader scale.

Questions for the board to pose:

- What key IT programs (purchases, projects, implementations) do we now have under consideration or underway?
- Does our program management framework embed a consistent set of governance processes and tools across the program—and flag risks of project delays, budget overruns, and delivery failures early so they can be addressed?
- Does our IT program coordinate strategic objectives, business processes, and system development over multiyear timeframes? How rigorous are we in our planning, communication, and controlling efforts?
- Have we considered the use of analytics to manage and coordinate our IT programs?

Technology operations risk

Management should ensure that rigorous operational processes are in place to protect the integrity of the technology environment. IT needs to deliver services at levels agreed upon with the business, manage capacity, understand and manage its assets, comply with software license agreements, and effectively manage incidents and problems. Non-standard and complex architectures can hinder the ability to meet service performance objectives. A weak incident management process leads to untimely and inconsistent resolution of issues, and missed opportunities to strengthen processes.

Technology environments are not static but are continually evolving. One of the most significant risks is the release of a change into the environment that renders a technology unusable. Management must ensure changes to technology are tested and released appropriately, and handled with great care.

Questions for the board to pose:

- How many technology changes caused an outage when released or needed to be reversed/rolled back? Which aspects of our current process enabled this situation?
- In what areas do we lack adequate service level agreements between technology and the business, and therefore risk a disconnect between service expectations and performance?
- What are our uptime/downtime statistics for our critical technologies? How could we improve our performance?

Risk of ineffective risk management

Financial institutions traditionally pursue a three lines of defense model to address risk. The first line of defense, product and process owners, identifies and manages risk. The second line, frequently executed by risk and compliance functions, provides a risk management structure and independent oversight of the first line. The third line, usually internal audit, provides independent assurance on the effectiveness of the first two lines of defense to the board and senior management.

Finding the right operating model to enable effective technology risk management presents challenges. The risk function may have the risk management expertise, but lack the knowledge of technology that would enable it to provide sound insights on the IT environment. Conversely, the IT function has the knowledge of technology, but lacks the independence needed to provide an unbiased view of risk.

Considering the importance of technology risk today, organizations need to improve skills development and career paths in technology risk management. In fact, demonstrating skills in both technology and risk management could be an additional criteria for management positions such as the CIO or CRO.

Questions for the board to pose:

- How are we structured to balance the need for technical people who can identify technology risks with the need to be independent and objective?
- What practices do we have in place to monitor major strategic risks in technology?
- How can we prevent the risk management function from devolving into a control testing function?
- Have we created paths to management level positions for those serving in our technology risk management function?

Top actions boards can take to better oversee IT risk

The board can take a number of steps to improve its knowledge of—and its visibility into—the IT risks the institution faces and management's methods of addressing them. The following practices have emerged from Deloitte's experience and research, and include approaches and mechanisms to enable financial services boards to better oversee IT risk:

1. **Form a board IT risk committee:** Consider forming a board-level IT risk committee, a sub-committee of an existing risk committee, or an advisory committee to promote understanding of IT risk. This committee could interact with the IT and risk functions, the CRO and other senior executives, the board-level risk committee, and the audit committee. Beyond the benefits of oversight, such a committee would send a strong message to stakeholders that the organization sets a high priority on IT risk management.

   A committee of this type could include outside board members and members of management with expertise in IT and IT risk. Boards might consider including at least one or two directors with deep, hands-on experience in IT and cyber risk management on this committee. The committee would report to the full board at its regularly scheduled meetings. This committee could be tasked with examining future, as well as current, IT risks and liaise with other board level committees as needed.

   If the board and management do not currently view a board-level IT risk committee or sub-committee as feasible, they may consider establishing an IT risk advisory committee. This advisory committee could include members of management with IT expertise, and perhaps one or two external experts, to provide guidance to the board, board risk committee, and audit committee, as well as to management, regarding IT projects, investments, and risks.

2. **Require IT expertise on the board:** Consider broadening the board's expertise by adding a director with strong technology management skills and leadership experience. This requirement could be added when a board vacancy arises, during the next director nomination process, or even by adding a director to the current board.

3. **Engage internal audit:** Call for internal audit to strengthen its focus on IT risk, and to report on IT risk independently to the board through the audit committee. Internal audit can report on the organization's IT risk management landscape and capabilities, and on opportunities for IT risk program enhancements. The board should ensure that internal audit has the talent and skill sets required to independently challenge IT. In addition, external third parties can be brought in to augment internal audit's capabilities and conduct independent reviews of select technology areas.

4. **Increase transparency:** Encourage management to enhance the quality of reporting on IT to the board, focusing less on traditional IT projects and more on IT risk events, resiliency, and key risk and performance indicators. Boards need insightful, fact-based management reports in order to be assured that the institution is truly managing IT risk and not simply providing "lip service" to the issue.

5. **Set board notification/approval thresholds:** Define thresholds for IT risk situations that must come to the board's attention, including significant IT investments, proposed vendor contracts with significant IT risks, and certain risk events, such as cyber breaches, system outages, or items triggering regulatory notification.

6. **Define the agenda:** The board should ensure that IT risk has a standing space on the board agenda. Topics could include top IT risks and vulnerabilities, emerging risks, risk management culture, IT risk management investments, IT program management initiatives, and career path and talent development.

   In addition, some boards may designate specific directors to take a greater role in IT and meet separately with technology management. In these conversations, directors can ask probing questions, get more detail, and gain a greater level of understanding which they can subsequently share with fellow board members.

7. **Prohibit jargon:** Emphasize to management that the board should not be expected to translate and interpret technology jargon. Set a firm expectation that management must inform the board or board committee of IT risks, programs, and issues in a clear, concise matter.

8. **Ask questions and seek education:** The board should ask technology and risk-related questions of management, such as those suggested in the call out boxes in this paper and gauge which areas are being strengthened by management to support safety and soundness versus simply to satisfy compliance requirements. Consider inviting guest speakers, such as law enforcement officials, academics, regulators, management consultants, and technology experts to board meetings. External experts can provide an independent view of the IT risk landscape, and insights into what other companies are doing, how the organization compares with its peers, and where new capabilities or investments may be needed.

9. **Participate in crisis exercises:** Board members should have a place at the table in preparing for and responding to a technology crisis. By participating in crisis simulations and war games, the board can gain a greater understanding of the institutions real capabilities, communicate how it would like to be engaged in a crisis, and evaluate its own capabilities to help "steady the ship" in the event of a major event.

Beyond the benefits of oversight, an IT risk committee can send a strong message to stakeholders that the organization sets a high priority on IT risk management.

A high priority for financial institution boards

Amid all the challenges and risks to be addressed, senior financial services executives might overlook IT risks. They dwell primarily in the world of financial and regulatory risk and tend to view IT as an enabler of operations and IT risk mainly in terms of cyber attacks and system availability.

The board can broaden that view. While it may first have to broaden its own view of IT risk, the board can immediately commit to invigorating IT risk governance within the organization.

Getting comfortable with conversations about IT risk can take time for directors lacking IT experience. Yet common sense is an excellent guide as well as a tool for cutting through jargon. Readings and briefings from external experts can also help. However a board goes about it, IT risk governance and oversight are among key risk-related responsibilities now and for the foreseeable future.

In addition, IT risk-related challenges in financial services will surely grow in number and importance in the years ahead. Getting ahead of these risks now will pay dividends for the board, their executive teams, and their institutions in the future.

Contacts

Edward Appert
Cyber Risk Services
Deloitte & Touche LLP
eappert@deloitte.com
+1 212 436 7511

Vikram Bhat
Cyber Risk Services
Deloitte & Touche LLP
vbhat@deloitte.com
+1 973 602 4270

Adel Melek
Global Vice Chairman, Risk Advisory
Deloitte Touche Tohmatsu Limited
amelek@deloitte.ca
+1 416 601 6524

Michael Rossen
Global Center for Corporate Governance
Deloitte Touche Tohmatsu Limited
mrossen@deloitte.com
+1 212 492 4531

Dan Konigsburg
Global Center for Corporate Governance
Deloitte Touche Tohmatsu Limited
dkonigsburg@deloitte.com
+1 212 492 4691

Deloitte.