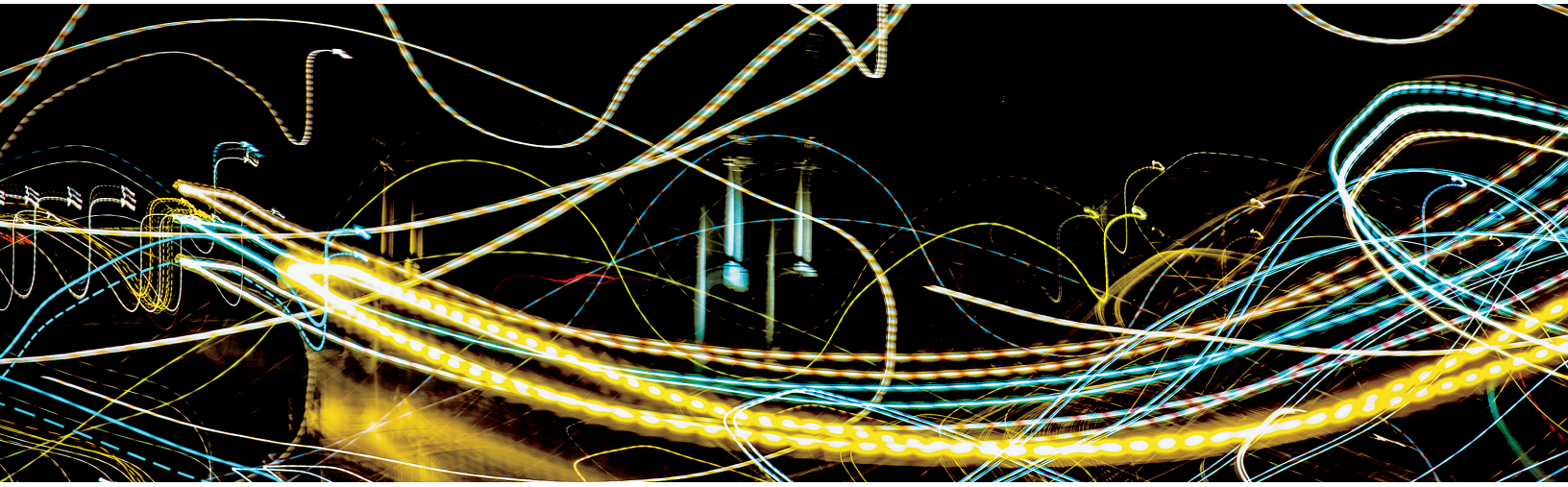
JULY 2016



RISK

‘The ghost in the machine’: Managing technology risk

Technological risks are becoming more prominent—and more dangerous. Six principles can guide banks as they manage them.

Oliver Bevan, Saptarshi Ganguly, Piotr Kaminski, and Chris Rezek

Technology is synonymous with the modern bank. From the algorithms used in proprietary trading strategies to the mobile applications customers use to deposit checks and pay bills, it supports and enhances every move banks and their customers make.

While banks have greatly benefited from the software and systems that power their work, they have also become more susceptible to the concomitant risks. Many banks now find that these technologies are involved in more than half of their critical operational risks, which typically include the disruption of critical processes outsourced to vendors, breaches of sensitive customer or employee data, and coordinated denial-of-service attacks. Cybersecurity alone can account for 10 percent of total information-technology spending, which is now growing at three times the rate of the budget of the technology being secured.

Exposure to these IT risks has grown in lockstep with the rapid increase in digital services provided directly to customers.[1] For example, mobile transactions have expanded exponentially, presenting malicious external actors with billions of new entry points into bank systems. The complexity and growing vulnerability of the underlying IT systems are of equal concern. Big banks must manage hundreds or even thousands of applications. Many are outdated, having failed to keep pace with the radically changed processes they are supposed to support. Even banks that have successfully upgraded their infrastructure face upgrade-related risks—from project and data management to security problems that persist after the migration is complete.

When technology risks materialize, the financial, regulatory, and reputational implications can be severe. If banks lose customer data in a high-profile incident, they face legal liabilities and fleeing customers. Investors sell shares in the wake of cyber-attacks, around 10 percent of which result in a more than 5 percent dip in the stock prices of the companies affected.[2] Regulators penalize firms for noncompliance—from data breach–related fines to mandated remediation activities. Basel II could not be clearer on the topic: one of its seven level-one operational-risk categories is "business disruption and systems failure."

To manage these risks, many banks simply deploy their considerable IT expertise on patching holes, maintaining systems, and meeting regulations. Some have set up specialized teams to cope with particularly acute problems, such as cybersecurity. But these half-measures are unlikely to afford sufficient protection. An IT-oriented approach, furthermore, may be unable to account for wider business implications and operational interdependencies. Institutions focused on compliance could ignore vulnerabilities outside the purview of the regulator and overlook applications critical to the business, with implications for business risk down the road.

Muddling through is no longer an option. The adequate mitigation of technology risk requires a coordinated effort that goes beyond IT-centered remedies. Leading banks are creating specialized teams within the enterprise-risk-management group to manage technology risk, in all its manifestations, across the organization. In this article, we will outline the six principles that these teams use to stay well connected and integrated with the rest of the bank, to develop the skills needed for these complex jobs, and to drive transformation and remediation activities. We conclude with some suggestions for getting these teams off to a good start.

Six principles

These principles are not a step-by-step manual but rather guidance for creating best-practice technology-risk management. By adhering to them, bank leaders will be able to remain in control of the rising levels of risk associated with the digital age.

Adopt a business-first approach

Companies can develop a complete picture of their information needs, uses, and risks only through a dialogue between IT and the business to identify the most critical business processes and information assets. The strongest controls can then be applied to the most valuable IT systems and data, the bank's "crown jewels." Proprietary trading algorithms stored on laptops, credit transaction data shared with third parties, and employee-health information—all may qualify. The IT-risk group should drive the assessment program, but the businesses need to be engaged with it and assume responsibility for the resulting prioritization, as they are the true risk owners. Only in this way will banks make the most effective investments in security. For example, an IT-led prioritization typically focuses too much on securing "big iron" applications while underemphasizing risks from unstructured data flowing through email and stored in collaboration platforms. For the crown jewels, remediation investments might include multifactor authentication, data-loss-prevention tools, and enhanced monitoring and analytics.

Thinking "business first" is especially important in information security. Data leaks, fraudulent transactions, blackmail, and "hacktivism" all pose dangers. Banks should consider their defenses in light of a threat's potential adverse impact on the business, rather than defaulting to blanket security standards that ratchet up after each negative headline. Nevertheless, security and the customer experience need not be approached as a trade-off. Leading banks are finding ways to give their clients

improved digital solutions that are simultaneously more secure and easier to use.

Coordinate across the subdisciplines of IT-risk management

Most banks have established groups to manage some or all of the various realms in which technology risk can pop up. These typically include cybersecurity and disaster recovery—as well as, increasingly, vendor and third-party management; project and change management; architecture, development, and testing; data quality and governance; and IT compliance (exhibit). While such groups are interdependent in many ways, particularly when a new product or service is under development, they often are not formally connected.

Best-practice banks coordinate the work of the subdisciplines to capture significant risk-mitigation synergies. For example, housing crown-jewel data on servers other than those used for the main operational IT systems has implications for security, disaster recovery, and data management. Analyzing these three risks separately could lead to inadvertent gaps in risk management or to redundant overprotection. Coordinating the subdisciplines also avoids duplication of effort, such as a product manager completing a half-dozen overlapping risk reviews before product launch.

Exhibit

Effective IT-risk management covers relevant subdisciplines.

IT-risk subdisciplines	Key risks for banks
Information and cybersecurity	Leakage of confidential customer and internal data, fraudulent transactions, blackmail, “hacktivism”
Resilience and disaster recovery	Recurring or prolonged interruptions of IT services supporting processes that are critical for customers or bank
Vendor and third-party management	Vendors or third parties not delivering reliable and secure service
Project and change management	IT projects not delivering on schedule and within budget, or not at adequate quality
Architecture, development, and testing	Systems not being designed to deliver long-term affordable, reliable, and maintainable service to enterprise
Data quality and governance	Legal/regulatory or transaction-settlement issues as a result of inaccurate, inconsistent, or missing data
IT compliance	Noncompliance of IT systems and process with regulations

Close the gaps in the three lines of defense

Banks have not always consistently applied the principles underlying the three lines of defense—the risk-management approach adopted by almost all financial institutions of any size—to technology risk. The three lines of defense is a more complicated approach for technology risks than for market or credit risk, for two main reasons. To begin with, the first line includes both the business and the IT function that enables it. Second, there are often "line one and a half" functions. In cybersecurity, for example, the chief information security officer (CISO) is responsible for setting policies and risk tolerances, as well as for managing operations to meet those expectations—both second-line activities. Yet the role usually resides in the first line, as part of the organization of the chief information officer (CIO). This blurring of the lines can create potentially problematic situations in which the group is "checking its own homework." Similar boundary confusion can arise in certain subdisciplines, like disaster recovery, where both the first and second lines need real technology expertise.

Banks should carefully clarify the roles and responsibilities in managing technology risk for each line of defense. Increasingly, organizations are asking the IT-risk group to take on the policy, oversight, and assessment roles, while security operations remain within the CIO's scope.

Careful distinctions like these are needed, for example, when institutions launch a new mobile-banking application. While the business sets out its commercial requirements, the IT group will work collaboratively to define the architectural and technical requirements. The second-line IT-risk function should be engaged from the start of such a project to identify risk exposures (such as the possibility of increased fraud or customer-identify theft) and provide an independent view on mitigation actions and feedback from testing results. Risks identified can be mitigated by the CISO and his or her team, through compensatory controls or design changes before the app is launched. This avoids the delays, cost overruns, and organizational tensions that arise from discovering exposures during a security review conducted too close to launch.

Integrate with enterprise risk management

In many banks, technology-risk management is disconnected from enterprise risk management (ERM) and even from the operational-risk team. That inhibits the bank's ability to prioritize the risks that are of critical importance and deploy the resources to remediate them. A contributing factor is often the absence of a common risk-management technology platform shared by both the IT-risk team and the ERM or operational-risk group. Without such a platform, banks struggle to aggregate risk information consistently, and managers are not equipped with the data they need to make decisions.

For example, as banks manage operational risks, they frequently balance the benefits of automation (to reduce opportunities for human error) against operational process controls (to improve behavior). Each option has advantages but also challenges—automation can introduce technology risk while operational controls can make systems unwieldy. Without a unified view of the risks involved, banks must often rely on advocates of particular initiatives when making risk-management decisions, rather than a holistic view of the available approaches and their merits. The bias can thus be to optimize within a risk category rather than to promote the good of the enterprise.

When the IT-risk group is integrated with ERM, on the other hand, real benefits can result—particularly if the technology-risk team comes under the same umbrella as other operational-risk-management teams. Decisions can be made at the level appropriate to the needs of the business and the potential severity of the risk. The business

To prevent the interruption of critical services, IT-risk managers should articulate a risk appetite that reflects the business impact of disruptions.

can make decisions about low-level exposures directly, while the tech- or op-risk group addresses the more significant risks and corporate ERM and senior management address the most significant ones.

Typical decisions with significant but underappreciated risk implications include those affecting a bank's long-term architectural road map and risk-appetite decisions about testing requirements for major IT changes. When it comes to mobile apps, for example, some banks will choose to be early adopters, given the anticipated customer value, while others wait for best practices to develop. Both courses might be sensible, but only senior management should decide between them.

Two domains where ERM integration can yield great benefits are resilience and disaster recovery, and vendor and third-party management. To prevent the interruption of critical services, IT-risk managers should articulate a risk appetite that reflects the business impact of disruptions. Most banks will find that for a small percentage of their business processes, near-perfect IT resilience is essential. These are customer-initiated, time-critical processes (such as ATM withdrawals, brokerage transactions, and point-of-service purchases) with no real-time alternative. Risk investments in resilience and disaster recovery must focus on these specific processes and the relatively small number of systems that support them. For other processes, IT-risk managers should work with the IT function to define the needs for supporting processes where the appetite for risk is relatively high and banks should be able to make savings by reducing the level of support required.

IT-risk managers should also partner with the business and IT to establish standards for security, continuity, and disaster recovery for a bank's external service providers. Given the sheer number of vendors that banks use, standards and audits must be applied in a risk-prioritized way. Banks should also consider involving their closest vendors and partners more significantly with internal ERM processes (to improve risk identification, assessment, and control) and also with incident response. Banks that use "war games" to test their crisis-response plans often find that the roles and responsibilities of third parties are outdated or poorly defined in service-level agreements, potentially leading to problems during a live breach.

Change the performance incentives for IT managers

Banks encourage IT managers to deliver projects on time and on budget and to maintain near-perfect levels of system availability. These objectives are obviously important, but overemphasizing them can mean that project managers do not do enough to minimize business-risk exposure. The prevailing culture encourages short-term delivery while underemphasizing long-tail but significant risks. For example, situations arise in which back-end systems are technically operational but the actual customer-facing business process is unavailable as a result of a lost database connection, for example,

or a lost connection with a client and a delay while the backup system kicks in. Infrequent but high-impact outages are almost never mentioned in performance-management systems, which instead feature operational data.

To monitor risk, best-practice banks add forward-looking metrics, such as the time it takes to detect and mitigate cyberincidents, the volume of unknown devices connected to the internal network, vendors out of compliance with security requirements, and employees failing phishing tests. Leading banks also track the number of incidents and the actual recovery times for highly critical service chains, including systems supporting mobile banking, ATM services, and electronic trading. Such a performance-management system should work hand in hand with a value-assurance framework, which establishes, for each major IT project, the criteria for aligning stakeholders and the software-development life cycle. Research has shown that a failure to manage these elements is the most common cause of budget and schedule overruns.[3] Aligning business and IT managers with appropriate risk-management mindsets and behavior is critical.

Invest in specialized talent

Technology-risk management requires critical thinking and hands-on experience in technology, business, and risk. Individuals with all of these skills are hard to find and command high salaries—but they are indispensable. Only someone skilled in all of these areas can both effectively challenge IT teams and act as a thought partner to guide strategic decisions.

The good news for banks is that they can develop this kind of talent through part-time staffing models, training, and rotational programs. Some banks have succeeded by recruiting experienced IT specialists willing to learn risk-management skills and giving them appropriate training and a ladder for advancement. Banks can thus build a core group of IT-risk professionals with a strong knowledge of functions, technology subdisciplines, and operational-risk practices. These are essential skills for the core work of the group—exercising proper oversight from the second line of defense. They will also help the technology-risk team with other parts of the job. IT-risk managers should define architectural standards, sit on architectural-review committees, establish a consistent software-development life cycle across the enterprise, and monitor test results. They should ensure not only that individual IT changes are delivered efficiently but also that the IT environment is sustainable in the long run.

Independent yet connected

The IT-risk group must be aware of what is happening in all parts of the organization. As a bulwark of the second line of defense, it must have strong insights into the first line (both the businesses and the IT units that support them), have a strong connection to the central IT team, forge connections among the various subdisciplinary teams, and integrate its work with the core risk-management team driving ERM.

To accomplish this delicate two-step of independence and partnership, banks can consider two actions. First, they can establish a single unified mission for the IT-risk group, which should enable the core business and be a partner to other functions to improve the overall effectiveness of technology-risk management. The function's activities in managing technology risks should focus on this vision, shared by the board and top management. The function's mission is then to understand the specific risks facing the bank given its core operational processes and organizational structure, to identify the major challenges in remediating or managing these risks, and to allocate responsibility for the specific actions needed.

Second, banks should create effective interaction and communication models that reduce ambiguity and promote collaboration. Clear committee structures, the frequency of meetings, and reporting lines will both help avoid duplication and ensure that key functions are not left undone. In identifying and prioritizing risk, organizations can usually build on existing risk evaluations and analyses and add mechanisms to ensure collaboration.

The expectations of customers, shareholders, and regulators for the resilience of banks will continue to escalate. Recent events have exposed the ghost in the machine—how the failure of technology can cause lasting damage to an institution's brand and reputation. Successful banks will establish an IT-risk group as a second line of defense that engages with the business and IT function while providing effective oversight and challenge. The group will also be staffed with experts in technology and risk management. With the right practices and capabilities, banks can effectively manage technology risk for the digital age.

[1] Michael Bloch, Sven Blumberg, and Jürgen Laartz, "Delivering large-scale IT projects on time, on budget, and on value," October 2012, McKinsey.com.
[2] Alison Smith, "Share prices are rarely hit hard by cyberattacks," *Financial Times*, October 31, 2013, ft.com.
[3] Bloch et al., "Delivering large-scale IT projects."

Oliver Bevan is a consultant in McKinsey's Chicago office; **Saptarshi Ganguly** is a partner in the Boston office, where **Chris Rezek** is a senior expert; **Piotr Kaminski** is a senior partner in the New York office.

The authors wish to thank Salim Hasham and Wolf Richter for their contributions to this article.