

fs viewpoint

www.pwc.com/fsi

June 2013

02

Point of view

11

Competitive
intelligence

16

A framework
for response

21

How PwC can help

24

Appendix



It takes two to tango:
Managing technology risk
is now a business priority

pwc

Point of view



Financial institutions rely heavily on technology to support complex business processes and handle critical information. Putting technology risk management on the business agenda today can safeguard and potentially improve your business value, brand, and reputation.

Operating and maintaining technology is inherently risky.

Financial institutions rely heavily on technology to support complex business processes and handle large volumes of critical information. With technology increasingly tied to critical business processes, a technology failure can have a crippling impact on an organization.

Historically, technology risk management functions have struggled to keep pace with this trajectory. This has left some financial institutions exposed to potentially catastrophic technology failures that could impact their brand and reputation.

Existing technology risk programs tend to be unwieldy.

Technology risk management programs are often costly, inefficient, and of limited business value. We believe that technology risk management can be more cost effective and provide greater strategic value.

These programs are not new—by now they should be maturing.

Regulators have required financial institutions to implement technology risk management programs for many years. Heightened regulatory focus on business resiliency and disaster recovery will continue in future examinations. Boards and audit committees

are also demanding greater visibility into the technology risks facing their institutions, and how those risks are being addressed.

Effective technology risk management requires a “top-down” approach.

For too long, financial institutions have viewed technology risk management as a defensive tactic or regulatory compliance activity. However, we see an opportunity to leverage technology risk management to provide strategic business value. We believe that effective technology risk management requires financial institutions to adopt a “top-down” approach that focuses on the objectives of the business, its supporting processes, and critical information assets. By adopting this approach, financial institutions can be better positioned to address technology risk compliance obligations and provide strategic value to the business.

To truly be of value to the business, technology risk management programs should be closely aligned to business strategies and critical business processes.

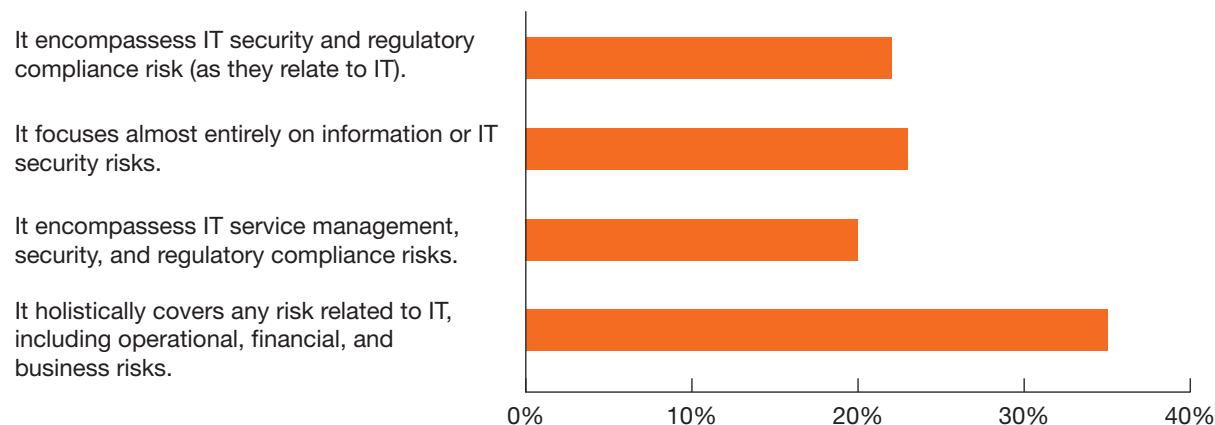
Based on our observations, existing approaches to technology risk management often provide limited value to the business.

Technology risk management often consists of various siloed and fragmented processes working alongside one another to provide a compliance capability that supports technology audits and regulatory examinations. Given today's environment of rapid change and intensifying regulatory scrutiny, these fragmented approaches to technology risk management cannot be sustained.

Without active participation by the business, technology risk management may be poorly aligned with business objectives. A business-aligned approach helps technology risk management support business objectives rather than acting as an impediment.

A survey in 2011 asked business technology professionals about the scope of their technology risk management programs.¹

Survey: Which BEST describes the scope of your technology risk management program?



65% of companies are not holistically addressing their IT risks.

Based on these findings and our own experience:

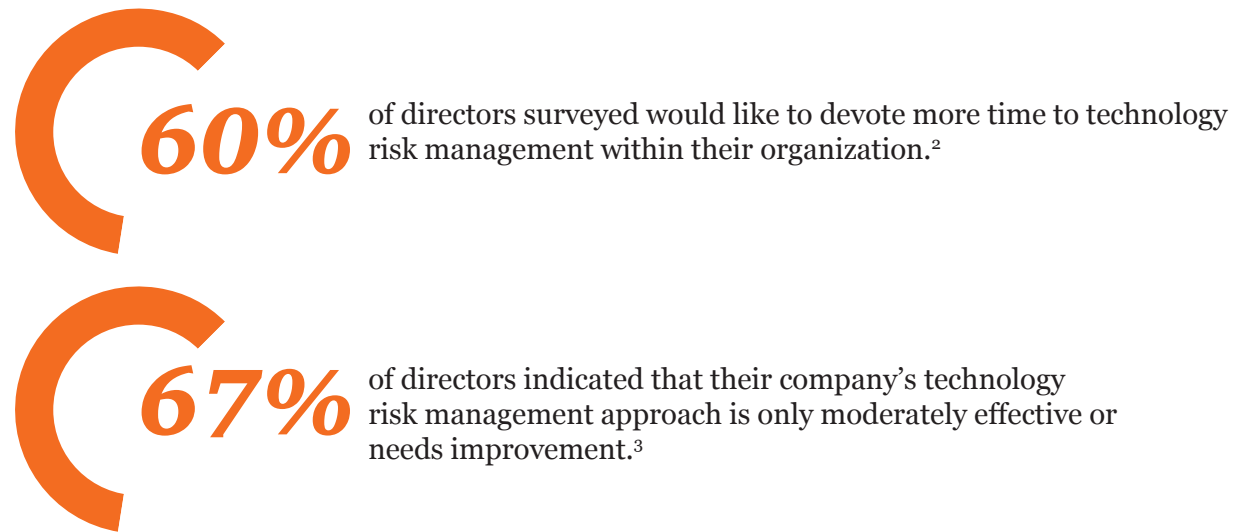
- These numbers are low, given how long institutions have had to mature their technology risk functions. We would expect institutions to have greater confidence by now.
- Technology risk functions have not evolved into something of true value to the business. As a result, technology risks are not considered a business priority.
- Typically, technology risk is focused on information security with little to no consideration for other key areas such as incident, change, and capacity management.
- Technology risk management needs to be more closely aligned to strategic objectives and to establish holistic coverage of business information risks.
- Those responsible for technology risk management require a sound understanding of the business. Technology risk professionals need to be good risk managers, similar to those responsible for areas such as operational risk and credit risk.

¹ Erik Bataller and Gary Alterson, "Risk Avengers: Tenets Of Risk-Oriented Security," *InformationWeek Analytics*, February 2011, www.analytics.informationweek.com, accessed May 4, 2012.

Furthermore, a lack of understanding at the board level has led to a technology risk “confidence gap” at many organizations.

“Many directors want more comfort regarding IT activities so they can sleep better at night.”¹

A survey conducted by PwC in 2012 indicated that many senior managers and board members do not have the level of comfort they would like when it comes to managing technology risks at their organizations.



This “confidence gap” has left many senior management teams wanting to know more about the technology risks that have the potential to affect business objectives, regulatory compliance, and critical business processes.

To address this gap, organizations should evaluate their current technology risk management capabilities, and implement measures to help senior management understand the technology risks and the extent to which they may impact the company’s ability to conduct business.

1 PwC, *Directors and IT: What Works Best*, 2012.

2 PwC, *Annual Corporate Directors Survey*, 2012.

3 *Ibid*

Leading financial institutions are shifting their focus on risk management, moving from a fragmented and reactive compliance approach to a more balanced, business-aligned, and risk-based strategy.

An effective technology risk management program can enable an organization to simultaneously pursue both its strategic business objectives and regulatory compliance requirements. This coordinated approach creates an agile strategy that quickly adjusts to and takes advantage of the prevailing market forces.

When analyzing leading financial institutions that have implemented a strategic technology risk management capability, we see commonalities in approaches they have taken. These include:

- Providing holistic coverage of technology risk domains, such as information security, change delivery, capacity management, and business continuity.
- Knowing the strategic objectives and key risks of the business.
- Developing risk-mitigation strategies that are aligned with business processes, information risks, and business objectives.
- Working collaboratively with the business to agree on mitigation strategies that get ahead of technology risks before they occur.
- Fostering a culture where technology risk management and mitigating controls are an integral part of the business.
- Building technology risk capabilities that balance business objectives with regulatory requirements and audit obligations.
- Hiring risk management professionals that understand the business and can communicate effectively with business leaders.

“Too often, IT risk is treated as an afterthought, possibly even overlooked completely. IT risk and enterprise value somehow have become separated. What is needed is a way of integrating IT risk into enterprise-wide risk and governance models, so the value of IT risk management can be demonstrated.”¹

¹ *IT Risk is Business Risk*, COBIT Focus, April 2012 © ISACA® All rights reserved. Reprinted by permission.

In our view, financial institutions should adopt a technology risk management model that balances the objectives of the business with regulatory compliance requirements.

Understand the objectives of the business

- Identify key stakeholders within the business and work with them to understand the strategic objectives of the company.
- Actively engage members of the business in the formulation of technology risk management strategies to help establish that they are appropriately aligned.
- Develop principles, policies, and standards that enforce the need to manage technology risks in a way that supports the objectives of the business.

Understand critical business processes and associated regulatory requirements

- Work with members of the business to understand the company's critical processes, procedures, and supporting technology.
- Identify technology-related regulatory requirements that impact the business (e.g., IT SOX) based on its critical processes and procedures.
- Determine inherent technology risks based on critical business processes and regulatory obligations.

Enable the business to make informed, risk-based decisions and drive compliance with regulatory requirements

- Gather information about the objectives of the business, its critical processes, and regulatory compliance obligations.
- Assess the organization's technology environment on an ongoing basis to determine its technology risk exposure.
- Inform the business on a regular basis to help them understand the company's technology risk exposure.
- Work with the business to determine its technology risk remediation strategy.
- Track, monitor, and report against the remediation of technology risks across the organization.

In our experience, developing a business-aligned technology risk management model provides a number of key benefits.

These benefits center around improving the risk posture of the business based on its objectives, critical processes, and information risks. Benefits include:

- Aligning the objectives of technology risk management with the strategic objectives of the business.
- Anticipating and avoiding catastrophic impacts to the business that often accompany a technology failure.
- Focusing technology risk management priorities on the needs of the business and its critical processes.
- Engaging the business to be actively involved in managing and owning technology and the associated risks.
- Developing risk assessment and risk mitigation strategies that are driven by business processes and aligned with business objectives.
- Developing the capability to strike a better balance between risk and reward—allowing the business to make informed risk-based decisions and pursue its strategic objectives.
- Achieving a coordinated technology risk management program that balances business objectives with the need to demonstrate compliance.
- Allowing the business to dictate the technology risk management approach based on:
 - The evolving objectives of the business.
 - Key business information risks.
 - Critical business processes.
 - The risk appetite of the organization.

Financial institutions often need to overcome a number of key challenges as they develop their technology risk management capabilities.

Key challenges

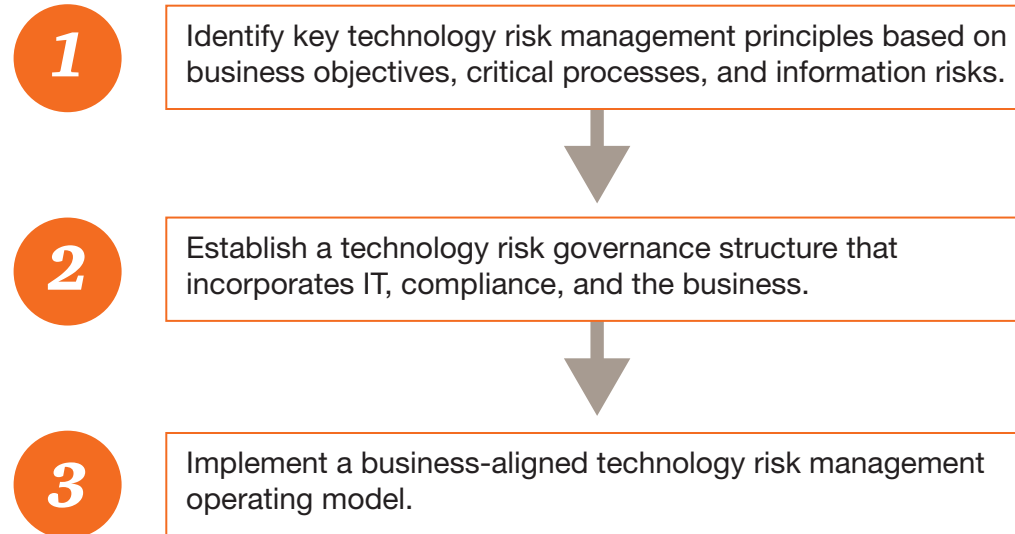
- Providing value to the business.
- Aligning technology risk priorities with the objectives of the business.
- Reaching agreement with the business on its risk appetite.
- Involving business leaders in technology risk management.
- Hiring technology risk management professionals who understand the nature of the business.
- Achieving compliance with the growing number of laws and regulations.
- Developing enterprise-wide technology risk management capabilities, systems, and approaches.
- Implementing a comprehensive operating model that supports proactive technology risk management and addresses the needs of the business.

Potential solutions

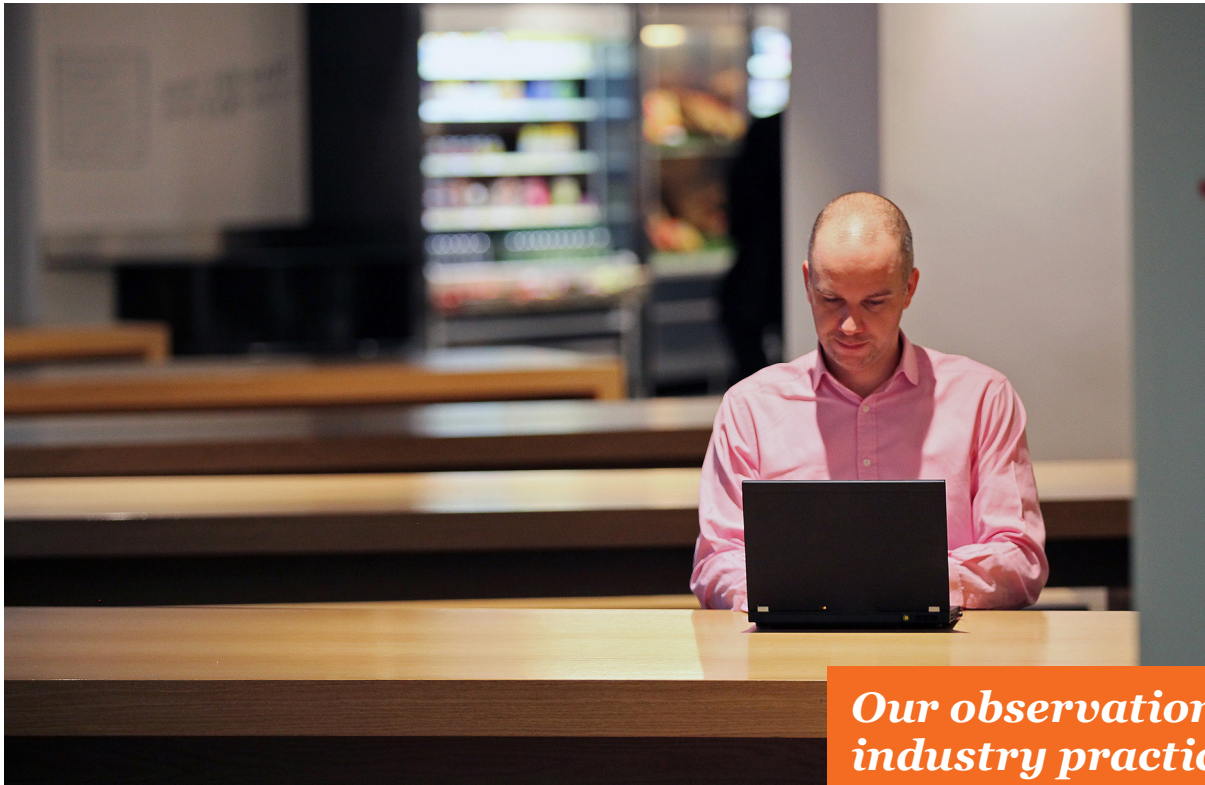
- Build a technology risk management operating model that enables the organization to identify, measure, and manage technology risks against its business objectives, critical processes, and information risks.
- Foster collaboration between business leaders and technology risk professionals to achieve alignment.
- Involve the business in technology risk governance early on to plan and communicate expectations and accountability—going beyond formal policies and procedures to build a corporate risk culture where the right people do the right thing at the right time.
- Hire and train technology risk professionals who understand the strategic objectives of the business and its critical processes and key information risks.
- Prepare for growing scrutiny by the regulators and promote ongoing compliance.

In short, build a risk-resilient organization designed to navigate through regulatory complexity and align with the strategies of the business, its supporting processes, and critical information assets.

We recommend a three-phase approach for achieving strategic technology risk management.



Competitive intelligence



*Our observations of
industry practices.*













We have observed several leading practices that can be leveraged to develop a more effective, business-aligned technology risk management program.


The PwC technology risk management model has been developed to incorporate and build upon these leading practices.

Adopt a risk-based approach	Work with the business to develop IT policies and standards that focus on critical business processes and important information risks.	Support IT policies and standards with effective implementation guidelines.
	Establish consistent risk assessment and compliance processes that help the business understand its technology risk exposure.	Enable the business to measure its own compliance with IT policies, standards, and regulatory requirements.
Think strategically	Adopt a strategic technology risk management approach that balances regulatory compliance needs with the objectives of the business.	Work with the business to identify and resolve technology risks on an ongoing basis.
	Centralize technology risk program management to enable a composite view of risk issues across the organization.	Provide holistic coverage of technology risk disciplines (e.g., information security, change management, supplier risk management).
Support the business	Establish clear accountability between the business and IT for technology risk.	Adapt technology risk management to the evolving needs of the business.
	Leverage business strategies and supporting processes to align technology risk management with key information risks.	Use technology risk management to balance the needs of the business with the need to comply with regulatory requirements.

Financial services institutions are at various stages of adopting leading technology risk management practices.













“Adopt a risk-based approach”

Leading practice	Financial institution 1	Financial institution 2	Financial institution 3
Work with the business to develop IT policies and standards that focus on critical business processes and important information risks.	 A risk assessment was conducted with members of the business prior to the development of an IT policy and standards framework.	 IT policies and standards were developed based on high-level business and information risks.	 The development of IT policies and standards was not accompanied by a formal risk assessment.
Support IT policies and standards with effective implementation guidelines.	 IT implementation procedures were developed to drive compliance with all IT policies and standards across the organization.	 IT implementation procedures had been developed for some, but not all, of the IT policies and standards.	 IT implementation procedures were not in place to help establish ongoing compliance with IT policies and standards.
Establish consistent risk assessment and compliance processes that help the business understand its technology risk exposure.	 An enterprise technology risk assessment framework was implemented to align with the information risks of the business.	 Risk assessments were performed centrally by the organization's technology risk group. However, assessments were rarely performed with members of the business.	 Risk assessment methodologies were fragmented and inconsistent. Departments were responsible for developing their own risk assessment frameworks.
Enable the business to measure its own compliance with IT policies, standards, and regulatory requirements.	 Technology risk and control assessments were performed on an annual basis by information risk managers in each business unit.	 Periodic risk assessments were performed on an annual basis by the firm's central technology risk and compliance group.	 Technology risk and control assessments were not mandatory across the organization. Assessments were performed only following a data breach or incident.

 Leading
  On par
  Lagging













Financial services institutions are at various stages of adopting leading technology risk management practices.



“Think strategically”

Leading practice	Financial institution 1	Financial institution 2	Financial institution 3
Adopt a strategic technology risk management approach that balances regulatory compliance needs with the objectives of the business.	 Risk assessments were scoped to address regulatory compliance needs in light of business objectives, supporting processes, and information risks.	 An organization-wide assessment had been performed to identify, review, and consolidate requirements associated with SOX, GLBA, and Basel II. However, these were not aligned to the objectives of the business.	 Regulatory requirements were not routinely reviewed or documented, and business objectives were not incorporated into the risk management framework.
Work with the business to identify technology risks and resolve technology risks on an ongoing basis.	 A transformation program was initiated to assess and remediate technology risks within all business units on an ongoing basis.	 Compliance gaps were identified during a risk assessment and addressed through individual remediation projects at the business unit level.	 Technology risks and gaps were addressed by individual technology teams following a data breach or technology incident.
Centralize technology risk program management to enable a composite view of risk issues across the organization.	 Technology risks were reported to senior leadership by individual business units on a quarterly basis.	 Technology risks were consolidated by the firm's central technology risk and compliance group and reported to senior leadership on a quarterly basis.	 An escalation process was in place for reporting technology risks to senior leadership when they were identified. However, there was no technology risk reporting framework in place.
Provide holistic coverage of technology risk disciplines (e.g., information security, change management, supplier risk management).	 The organization provided broad coverage of some key IT risk disciplines. However, certain topics were missing (e.g., capacity management, change management).	 The central technology risk and compliance group was organized into multiple IT risk disciplines, providing extensive IT risk coverage across the organization.	 Technology risks were, by and large, focused on information security. There was limited coverage of other IT risk disciplines.

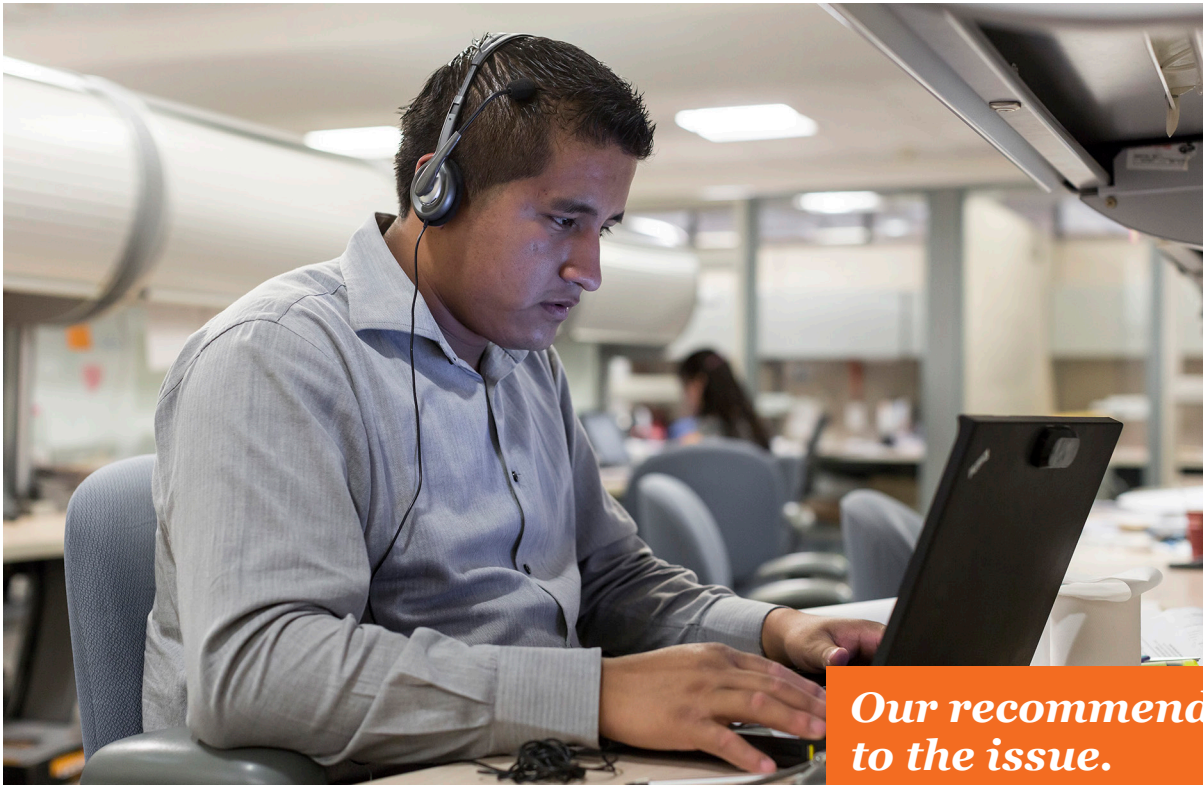
 Leading  On par  Lagging

Financial services institutions are at various stages of adopting leading technology risk management practices.

“Support the business”			
Leading practice	Financial institution 1	Financial institution 2	Financial institution 3
Establish clear accountability between the business and IT for technology risk.	 Technology risk managers were held accountable for the organization's technology and engaged the business on an ad hoc basis. Accountability was not well established for business information assets.	 The technology risk and compliance group was accountable for the organization's technology assets. Business units were accountable for the information handled by those technology assets.	 Governance of technology risk management was not formally defined. Accountability for technology assets and business information was not well understood across the organization.
Adapt technology risk management to the evolving needs of the business.	 Technology risk managers engaged business leaders on an infrequent basis to discuss future plans and technology risk needs.	 The technology risk and compliance group met with business leaders on a frequent basis to understand their evolving strategies and identify new technology risks.	 There were minimal efforts to engage business leaders and align future strategies with technology risks.
Leverage business strategies and supporting processes to align technology risk management with key information risks.	 Technology risk management initiatives were aligned to some key business processes but not all. Some business units experienced challenges maintaining ongoing compliance with risk management requirements.	 Technology risk management initiatives were closely integrated with key business processes to help establish ongoing compliance across all business units.	 Technology risk management initiatives were not aligned with business processes. Business units often found it challenging to maintain ongoing compliance with risk management requirements.
Use technology risk management to balance the needs of the business with the need to comply with regulatory requirements.	 Business leaders engaged the technology risk managers to incorporate regulatory requirements into critical business processes and future strategies.	 Regulatory requirements were assessed in parallel with business technology risks. Where feasible, remediation efforts were combined to address gaps in both areas at once.	 Regulatory requirements were not routinely reviewed or incorporated into critical business processes and future strategies.

 Leading
  On par
  Lagging

A framework for response



*Our recommended approach
to the issue.*

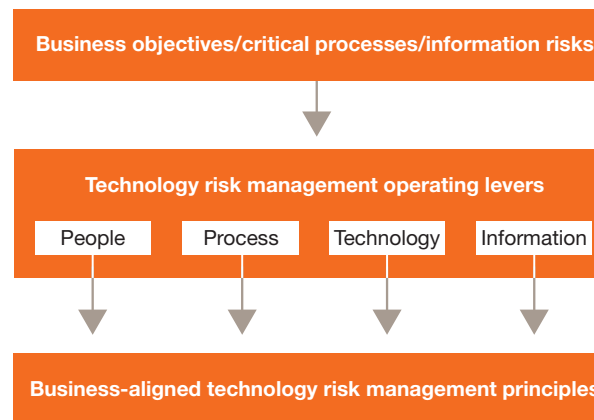
There are a number of next steps that organizations may look to address as part of the PwC technology risk management model.

Phase		Next steps
1	Identify key technology risk management principles based on business objectives, critical processes, and information risks.	<ul style="list-style-type: none"> • Develop core technology risk management principles that are aligned with business objectives, critical processes, and information risks. • Develop risk-based IT policies and standards to enforce the technology risk management principles across the business.
2	Establish a technology risk governance structure that incorporates IT, compliance, and the business.	<ul style="list-style-type: none"> • Establish clear accountability between the business and IT for technology risk management. • Implement a technology risk governance structure that incorporates members of the business and IT. • Centralize technology risk program management to enable a composite view of risk issues across the business. • Provide holistic coverage of technology risk domains (e.g., information security, change management, supplier risk management).
3	Implement a business-aligned technology risk management operating model.	<ul style="list-style-type: none"> • Create an inventory of critical business processes, supporting IT systems, information assets, and information owners. • Enforce IT policies and standards through risk and compliance assessments that focus on business information risks. • Establish consistent risk assessment and compliance processes that help the business understand its technology risk exposure. • Enable the business to measure its own compliance with IT policies, standards, and regulatory requirements.

1. Identify key technology risk management principles based on business objectives, critical processes, and information risks.

We recommend anchoring the approach for IT risk management to a set of core principles; this can help institutions achieve a high degree of consensus on the objectives of technology risk management between IT and the business. It can also facilitate the development of risk-based IT policies and standards through which technology risk management can be enforced across the organization.

Once management identifies its set of principles, it can assess the methods used to execute those principles and find the logical points for integration. To tackle this major undertaking systematically, management should evaluate how the four operating levers, **people**, **process**, **technology**, and **information**, apply to each principle.



Examples of technology risk management principles

- Operating technology is inherently risky.
- Technology risk management is a business mandate.
- Technology risk management is driven by business objectives, critical business processes, and business information risks.
- Technology failures can have a direct impact on critical business processes.
- Effective IT controls will primarily result from technology risk assessments that are focused on addressing the needs of the business.
- The business is accountable for its information; IT is accountable for the supporting technology.
- Technology risk management controls must be proportionate to the information risks defined by the business.
- Effective technology risk management requires the organization to balance business objectives with regulatory requirements and audit obligations.

2. Establish a technology risk governance structure that incorporates IT, compliance, and the business.

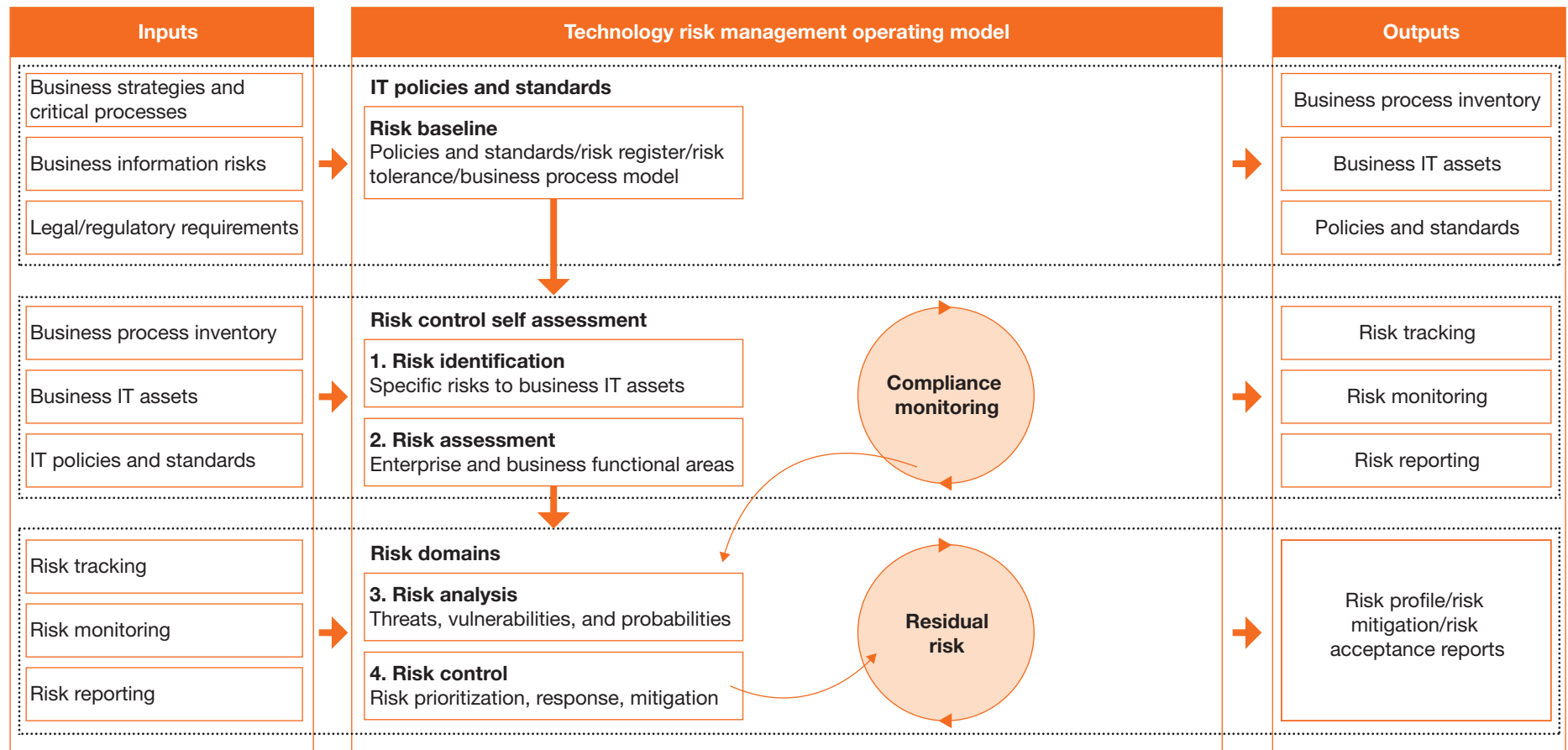
There are four building blocks that can be used to establish an effective technology risk governance structure. These building blocks will help your organization to do the following:

- Establish a leadership function that includes key stakeholders from IT, the business, and compliance.
- Set the technology risk baseline for the organization through interaction with IT, the business, and compliance.
- Focus technology risk management on information assets that are important to the business.
- Deliver a technology risk assessment framework that balances business needs with regulatory compliance obligations.

Risk leadership	Representatives from business and IT					Objective: Involve the business, IT, and other key stakeholders when setting the technology risk appetite across the organization. Establish clear accountability for IT assets and the business information handled by those assets.
	Technology risk and compliance	CIO/COO	Business leadership	IT leadership		
Risk baseline	Risk-based IT policies and standards					Objective: Set the technology risk appetite of the organization, based on key inputs from the business, IT, and compliance groups. This risk appetite is enforced through risk-based IT policies and standards.
	Business information risks	Controls inventory	Legal/regulatory requirements	Risk and control self assessment	Compliance monitoring	
Risk assets	Business and IT assets					Objective: Enable IT and the business to focus their technology risk management activities on critical business processes and supporting information assets.
	Business solutions	Business services	Supporting processes	Supporting IT assets		
Risk assessment	Representatives from business and IT					Objective: Develop tools and methodologies to identify, measure, and address technology risks in accordance with the risk baseline established through IT policies and standards.
	Risk identification	Risk analysis	Risk ranking	Risk control	Risk exposure	
	Technology risk domains (e.g., change management, business continuity, information security, capacity management).					

3. Implement a business-aligned technology risk management operating model.

A business-aligned technology risk management operating model facilitates proactive identification, measurement, and control of technology risks. Ultimately, the business owns its information assets, and IT owns the supporting technology. For technology risk management to be effective, IT requires input from the business regarding its information risks, critical processes, and business strategies.



How PwC can help

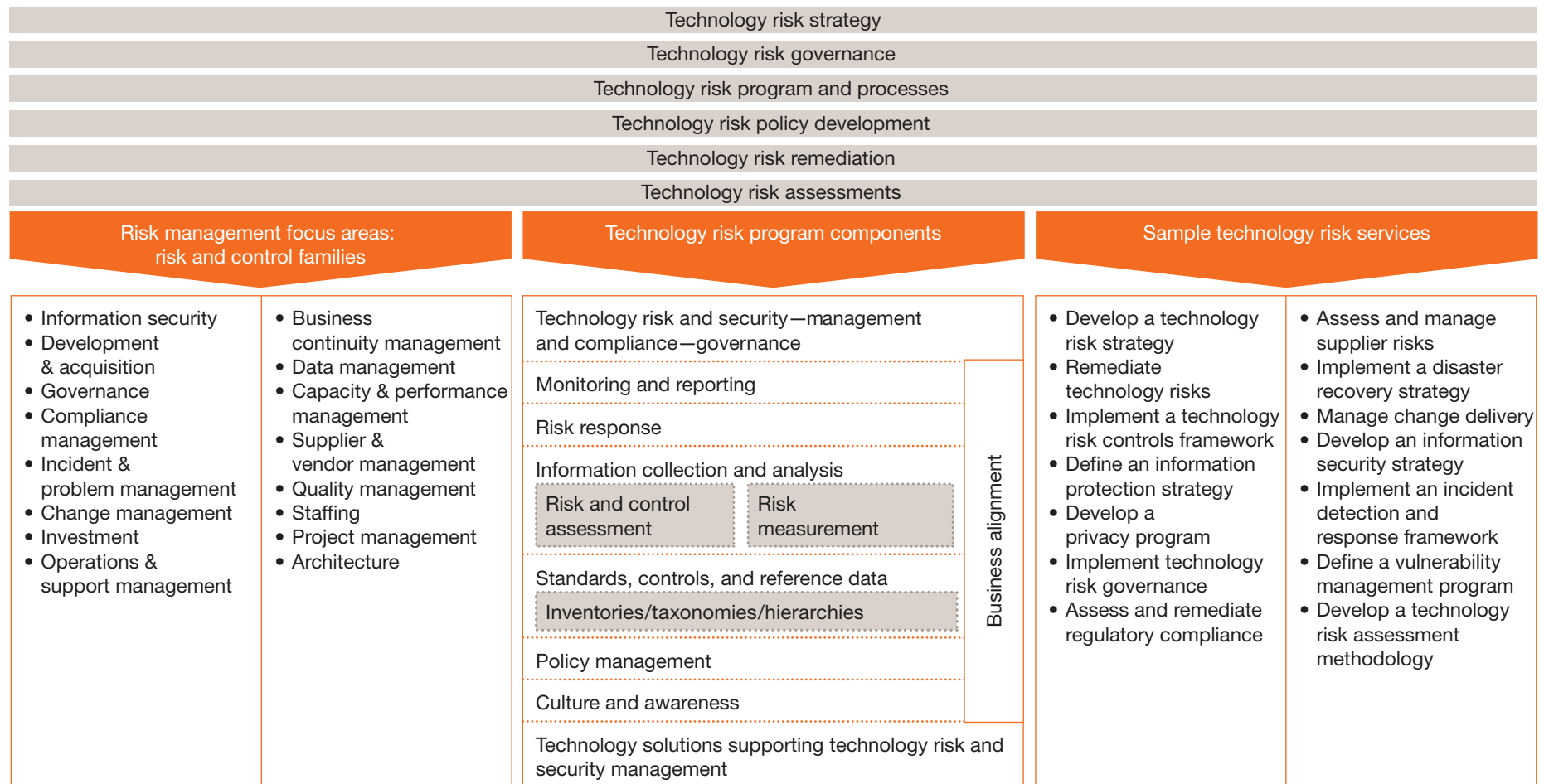


*Our capabilities and
tailored approach.*

PwC's Technology Risk practice employs experienced risk professionals with deep expertise.

- Proven ability to work with IT and business leaders when implementing IT risk frameworks.
- Multiple practice aids and accelerators.
- Knowledge of regulatory frameworks such as SOX and FFIEC.
- Leadership in the formulation of industry standards such as COSO and RiskIT.
- Formal certification by relevant authorities.
- Industry partnerships.

Our most valuable credential is our track record of positive feedback following successful delivery to major clients.



PwC technology risk management aids and accelerators.

PwC has developed a number of aids and accelerators that enable it to deliver its technology risk services more effectively and efficiently.

Aid/accelerator	Description	Value
Technology risk and control register	<ul style="list-style-type: none">• List of risk statements and IT controls addressing technology risk.• Risk mitigation approaches based on leading industry frameworks (e.g., ISO 27002, NIST, COSO).• Industry-standard practices for implementing and operating technology risk management controls.	<ul style="list-style-type: none">• Eliminates the need to formulate technology risk statements from scratch.• Provides a baseline of technology risk controls to build upon.• Greatly simplifies risk mitigation planning.
Risk assessment frameworks and reporting templates	<ul style="list-style-type: none">• Aids for conducting risk assessment activities.• Dashboard reporting templates.• Risk assessment frameworks and methodologies.	<ul style="list-style-type: none">• Decreases preparation time, allowing PwC team members to focus on the assessment of risks.
Risk and control operating models	<ul style="list-style-type: none">• Leading practice alternatives for maintaining the technology risk control framework.	<ul style="list-style-type: none">• Leverages PwC experience in identifying the leading model for each organization.

Appendix



Select qualifications.

Development and implementation of an IT risk framework— Global wealth management company

Issues	<p>The organization had increased its focus on building robust technology risk management processes and practices. It recognized that many business units were not consistently addressing significant risks due to inadequate governance and lack of resources.</p> <p>To support this directive, the client requested that PwC assist with a number of technology risk management areas, including issue assurance, corrective action planning, risk remediation, and program management.</p>
Approach	<p>PwC reviewed previously identified technology risks to understand:</p> <ul style="list-style-type: none">• Adequacy of existing controls implemented as a part of remediation.• Recommendations to address inadequate/inappropriate controls. <p>PwC reviewed the client's risk and issue management processes to help develop the following:</p> <ul style="list-style-type: none">• Governance structure with clear roles and responsibilities.• An issue management playbook with procedures.• Transition planning for the client to undertake key activities such as the control self assessment process. <p>PwC also assisted with the identification and remediation of gaps associated with key process areas such as access control, vulnerability management, and vendor risk management.</p>
Benefits	<p>Following the engagement, the organization realized the following benefits:</p> <ul style="list-style-type: none">• Greater governance and control over technology risk and governance processes.• Improved ability to follow up and resolve risk and control issues.• Implementation of appropriate and sustainable controls within the environment.• A strong target operating model for risk and issue management based on evolving business needs and resource constraints.

***Establishment of an
enterprise IT compliance
framework—
Global insurance company***

Issues

The client had a number of outstanding audit exceptions because IT controls and IT policies were poorly developed, not strategically aligned with the business, out of date, and inconsistent with industry practice. This affected the client's ability to align its IT risk capability with the business and maintain compliance with both internal and external IT control requirements.

Approach

The client engaged PwC to assess the existing IT controls environment and develop a strategy to remediate the gaps identified. PwC leveraged its technology risk and control register to establish a baseline of IT controls and to perform a risk assessment of the client's IT environment. Based on the findings of the risk assessment, PwC helped develop an extensive set of policies and standards, defined a strategic IT risk operating model, and implemented an IT risk governance framework.

Benefits

Following completion of the project, Internal Audit concluded that IT had implemented an effective risk and compliance program. IT was also recognized as the enterprise leader for risk and compliance within the organization.

Development of a technology risk register and information security controls inventory—International bank

Issues	The client's technology risk and control function had established a long-term initiative to develop a technology risk management capability.
Approach	<p>The client engaged PwC to develop a strategy for identifying, measuring, and remediating IT operational risks. PwC helped develop an inventory of technology risk controls, leveraging industry standards such as ISO 27002 and CobiT as a baseline.</p> <p>PwC also assisted in the development of a risk register that enabled the client to document key operational risks associated with its technology environment.</p>
Benefits	The technology risk register and controls inventory developed by PwC were well received by the client sponsor. The client now has a baseline for taking a more comprehensive view of IT operational risks and providing supporting content for risk-based IT policies and standards.

Design and implementation of an IT control self assessment program— Top 5 US bank

Issues	After experiencing many years of recurring and unresolved audit and regulatory issues, the CIO wanted to improve the organization's technology risk management capability. The client wished to increase visibility into the IT controls environment, begin remediating critical issues, and build a capability that would proactively identify technology risks.
Approach	PwC helped to develop a technology risk and control framework based on risks identified by the client's various internal control groups. PwC worked with the client to develop an IT control self assessment methodology based on the new framework and managed a pilot implementation program. PwC helped manage the rollout of the IT control self assessment program and worked with client personnel to progressively transfer knowledge and capability.
Benefits	The client now has a mature strategic technology risk management framework that covers IT operational risks, supports continuous process improvement, and exceeds regulatory and audit requirements. The bank was able to eliminate and resolve all significant IT-related deficiencies within two years. In addition, the client now maintains a culture of compliance while proactively identifying and resolving issues.

www.pwc.com/fsi

***To have a deeper conversation,
please contact:***

Julien Courbe julien.courbe@us.pwc.com
+1 646 471 4771

Stephen Russell stephen.j.russell@us.pwc.com
+1 203 539 3079

Shawn Connors shawn.joseph.connors@us.pwc.com
+1 646 471 7278

Follow us on Twitter @PwC_US_FinSrvc

"It takes two to tango: Managing technology risk is now a business priority," PwC FS Viewpoint, June 2013. www.pwc.com/fsi

© 2013 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

DC-13-0217. Rr.