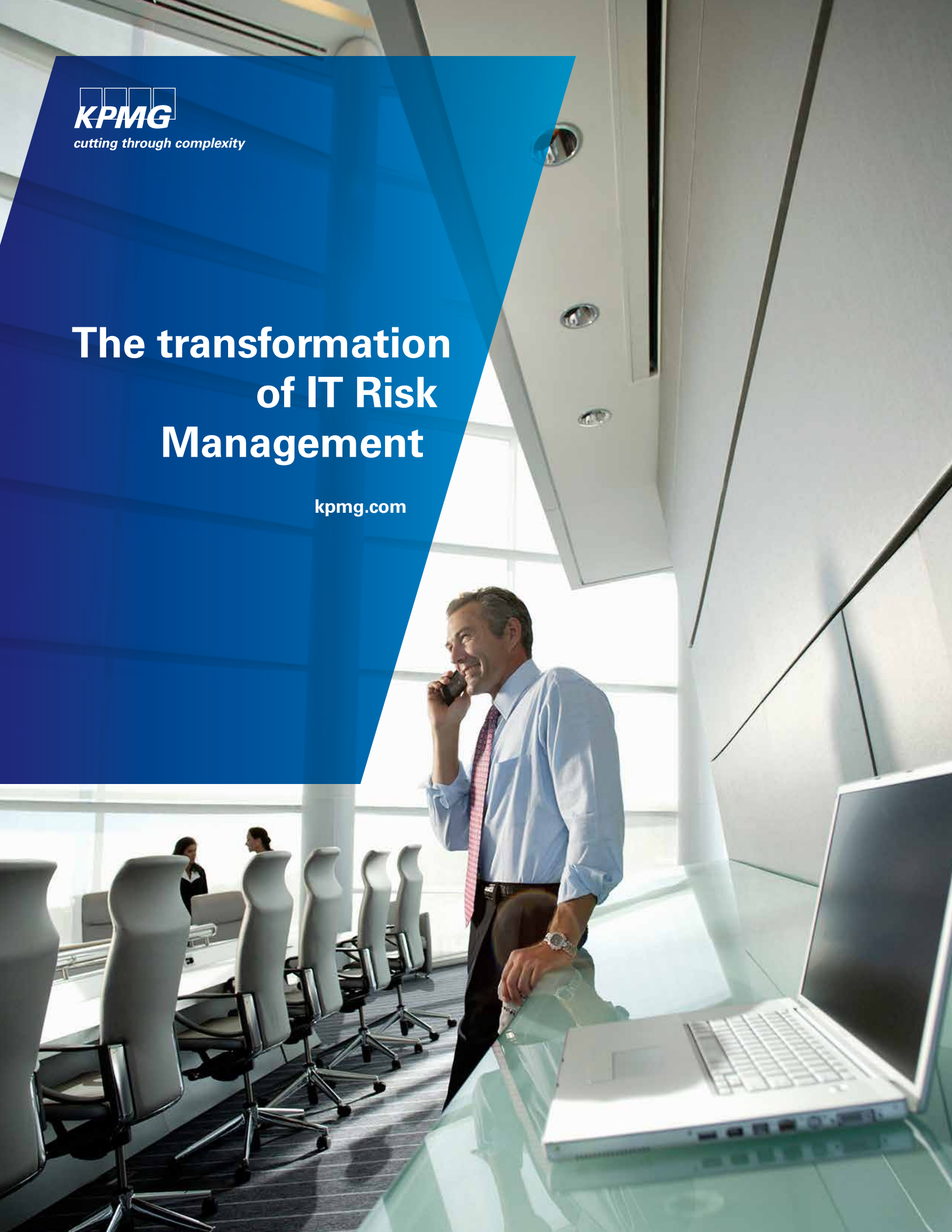
KPMG

cutting through complexity

The transformation of IT Risk Management

kpmg.com



The transformation of IT Risk Management

- The role of IT Risk Management
- Scope of IT risk management
- Examples of IT risk areas of focus
- How KPMG can help
- Case studies

Redefining the role of IT Risk Management in a changing world

Organizations are facing increasing demand to realign their IT Risk Management (ITRM) framework to meet constantly changing regulatory standards. An effective ITRM framework poses many challenges, including maintaining a cost-effective process design and meeting the efficiency demands of company management, while balancing the need to intervene and enabling innovation and the flow of business. This is forcing leading organizations to redefine and transform their traditional ITRM model.

Although cost factors are a challenge for organizations in deriving value from an ITRM function, integrated ITRM operating models can significantly help to improve business decision making and accountability for IT risk. An effective ITRM function can also assist in establishing a risk-aware culture and methods of working and collaborating to take appropriate action, strengthening the first line of defense within the organization.

The role of IT Risk Management

The role of IT in an organization has transformed over recent years and is no longer seen as just supporting the business. IT also allows organizations to differentiate themselves and provides many organizations a competitive advantage. This results in IT being a strategic enabler instead of a cost center. As a result, the view on managing IT risk within an organization has also evolved. Because IT risk covers many aspects of the organization, it is assumed that the functions of internal audit, business operations, and/or technology operations will be able to identify, monitor, and address these risks. However, that is not the case, and often, if these functions are performing an element of IT risk management, the efforts are not coordinated, consistent, or consolidated for an enterprise view.

The ITRM function within an organization operates as a distinct, but integrated, function within IT. It supports the enterprise as a whole addressing the strategic objectives, mission, and business model of the organization. An ITRM function manages the firm's risk posture and appetite for IT risk and security by determining the key IT threats that an organization faces and leading a proactive response to combat these threats. An effective ITRM function ensures a robust and effective engagement with regulatory bodies to determine compliance priorities for each jurisdiction. Furthermore, as an enterprise business issue, ITRM requires an organization to build capabilities that must be embedded and managed across a matrixed organization through a sustainable process to provide transparency and accountability.

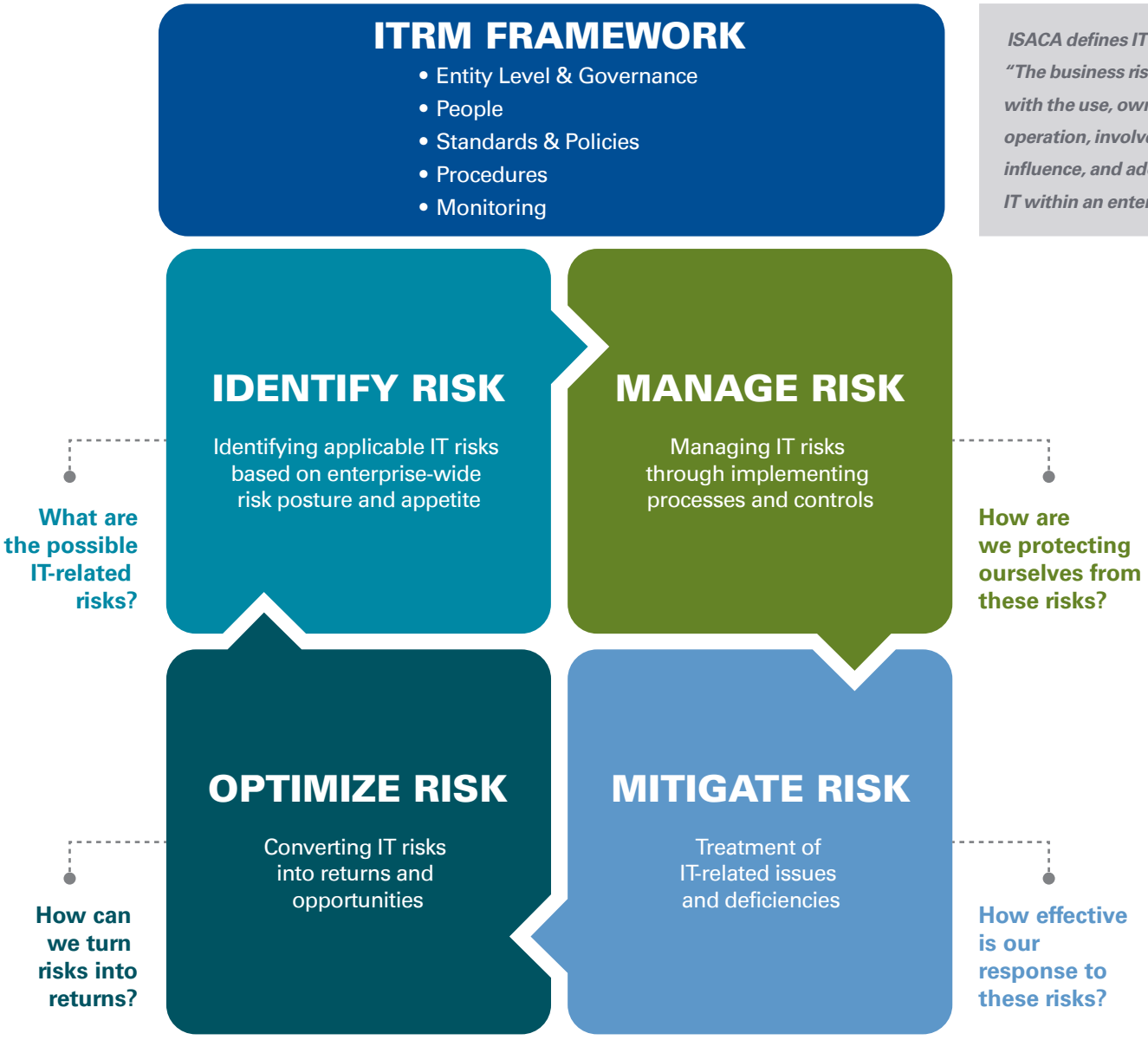
A holistic view and discussion on ITRM helps management to identify, manage and optimize risks—not just mitigate their risks—turning IT risks into advantages and aligning management's risk appetite with a desired return.

ITRM should define a comprehensive view of IT risks; continuously refresh the inventory of IT risks; help create strategies to prevent, mitigate, or accept these risks; and monitor risks against defined tolerances. Through fit-for-purpose design, skills, and competencies, and automation platforms, the ITRM function provides management an opportunity to proactively manage risk and transform its ITRM needs into a capability that plays to the broader enterprise strategy and the critical issues that organizations face.

Aligning the ITRM function with the other risk oversight functions such as internal audit, enterprise risk management, and compliance, as well as with regulatory mandates, is an important element in more effectively ensuring that risks are optimized.

Scope of IT Risk Management

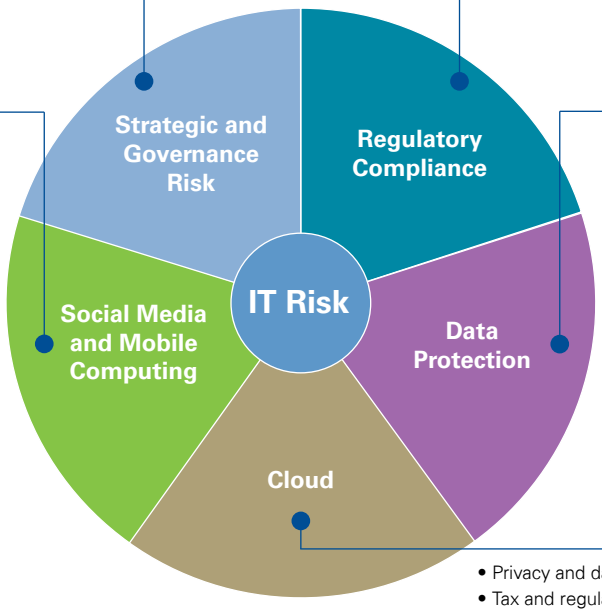
Understanding the complexity of the business environment and changes from within the organization are some of the key drivers in understanding key areas of risk in an organization. These factors are in turn being driven by numerous forces, whether external such as regulatory, geopolitical, or market-driven, or internal such as new products, acquisitions, or IT implementations.



ISACA defines IT risk as "The business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise."

A coordinated approach to ITRM enables information flow and a clear understanding of the risk domains within IT. Organizations need to assess for risk and develop risk optimization strategies by defining and delivering broad risk optimization programs. They also need to establish a measurement program to report holistically on the IT risk posture. But this is not just about measuring and reporting; it is about optimizing the resources dedicated to ITRM on a business impact-prioritized basis, leveraging a defined process, using lessons from history, and applying as appropriate across the landscape of enterprise IT risks.

Examples of IT risk areas of focus



- Alignment of IT risk control framework with business strategy
- IT portfolio prioritization
- Risk posture and key program updates
- Risk assessment rationalization and enterprise alignment

- More rigorous regulations
- Regulatory uncertainty
- Rising costs for compliance

- Security risks and brand protection
- New marketing and business models
- Data leakage and intellectual property protection
- Managing remote access and communications
- Managing diverse Bring Your Own Device (BYOD) environments

- Scale (big data)
- Growth of unstructured data
- Security breaches
- Business continuity and disaster recovery

- Privacy and data security
- Tax and regulatory issues for virtualized business
- New models for data storage, software as a service (SaaS), business continuity, and disaster recovery

How KPMG can help

	Less mature		More mature
IDENTIFY RISK	• Identify enterprise-wide IT risk universe by systems and underlying infrastructure • Develop ITRM strategic direction and framework based on the enterprise's objective capacity for IT-related loss • Map business strategy to IT risk strategy to define appropriate IT risk appetite and tolerance • Assess ITRM resource capabilities and requirements	• Integrate existing ERM framework to include new IT risks (internal and external) • Align IT risk policy based on internal and external risks • Review and assess current ITRM strategy and alignment with regulatory and market events • Develop Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) • Develop communication, training, and awareness	• Enhance the existing ITRM framework to align with new regulatory standards • Develop risk reporting capabilities • Enhance KRIs and KPIs • Develop resource models to include skills/capacity • Quantify IT risk and perform peer analysis of IT risk
MANAGE RISK	• Inventory IT controls by risks and control objectives • Establish the context in which the risk assessment framework is applied to help ensure appropriate outcomes	• Update existing controls inventory and evaluate test of design • Implement controls and monitor operational alignment with risk tolerance thresholds	• Evaluate operating effectiveness of controls (testing and monitoring of controls) • Measure KRIs and KPIs • Enhance ITRM reporting and provide drill down functionality
MITIGATE RISK	• Develop mitigation strategies • Implement mitigation strategies through collaboration with the business • Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis	• Work with the board to define the enterprise's appetite for IT risk, and obtain reasonable assurance that IT risk management practices are appropriate to help ensure that the actual IT risk does not exceed the board's risk appetite	• Embed risk management responsibilities into the organization, helping to ensure that the business and IT regularly assess and report IT-related risks and their impact and that the enterprise's IT risk position is transparent to all stakeholders • Continue maintaining a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis
OPTIMIZE RISK	• Develop and implement tools to assist in monitoring effectiveness of IT controls	• Develop cost benefit strategies to reduce IT cost of compliance through outsourcing/smartsourcing	• Execute resource strategies to develop more cost-effective capabilities (e.g., offshoring) • Enhance existing measurement and monitoring tools

KPMG member firms assist organizations in transforming their ITRM across the entire continuum. Whether working with organizations that want to establish an ITRM function or organizations that are looking to enhance their current risk management function, our services help organizations transform ITRM by proactively building integrated capabilities to identify and manage strategic, regulatory, and emerging technology risks and helping design methods to reduce the associated operational costs through sustainable, repeatable, and insightful processes.

For either mature or early-stage ITRM functions, we consider monitoring to be essential in terms of compliance and operations. Organizations need to consider implementing capabilities to monitor the ITRM function's effectiveness by defining KRIs for managing risks such as number of risks within each risk area, and number of risks mitigated, number of risks by ongoing mitigation effectiveness; determining appropriate collection and reporting methods; and developing tools for reporting on essential measurements for managing risks. KPMG can help design and launch an ITRM function, recommend and implement ITRM function improvements, and support the monitoring of ongoing ITRM performance through "health check" exercises. Our professionals and methods can help transform how companies view and manage IT risk through wide-ranging ITRM design and improvement based upon industry-wide practices and trends.

Case studies

CASE STUDY 1

Large brokerage firm looking to build its ITRM function

Client challenge	The client needed assistance in implementing a formal ITRM framework and strategy that would align with its corporate risk management framework. More specifically, the client needed assistance in addressing the corporate risk management requirements, supporting regulatory and other compliance concerns, strengthening and reviewing their current ITRM processes, and improving IT risk reports to management.
KPMG response	KPMG assisted the client with the following: • Performed an analysis of the current ITRM strategy and developed an ITRM strategy that aligned with the corporate risk management framework • Developed an overall ITRM program that included ITRM processes and procedures. The program was based on a formal methodology for identifying, assessing and responding to identified IT risks—all in alignment with the corporate risk management framework. • Conducted a pilot to validate that ITRM processes and procedures were being implemented. Training for client personnel was provided to help ensure ongoing and sustainable risk management activities.
Benefits to client	• A methodology that has resulted in cost savings for the client while also maintaining a high level of quality • Support from an onshore KPMG team with local industry and subject-matter knowledge • A holistic process for assessing the client's controls and aligning the ITRM function with the client's overall risk management framework

CASE STUDY 2

Global multinational company looking for a cost-effective solution

Client challenge	The client needed a solution that would reduce the cost associated with monitoring compliance and assessing the effectiveness of its IT controls—without compromising the quality of the controls.
KPMG response	KPMG developed an onshore/offshore delivery model for monitoring compliance and assessing the effectiveness of the client's IT controls. Local KPMG staff provided an onshore presence, working with the client to understand the controls and the client's requirements and needs. Offshore resources were provided by KPMG's Global Services team. Together, the two KPMG teams were able to deliver a cost-effective methodology without compromising the quality of the client's IT controls.
Benefits to client	• A solution that has resulted in cost savings for the client, while also maintaining a high level of quality • Support from an onshore KPMG team with local industry and subject-matter knowledge • A tested process for assessing the client's controls and providing reporting to the client

CASE STUDY 3

Global multinational oil and gas company looking to identify and manage business critical infrastructure

Client challenge	The client needed to define, and maintain a process that would identify and categorize risks related to business critical infrastructure components.
KPMG response	KPMG developed a wide-ranging process for identifying, defining, and maintaining business critical infrastructure services. Local KPMG staff then provided a single point of contact to communicate and train the client in understanding the risks associated with business critical services, business critical attributes/definitions, and controls specific to each. In addition, business impact assessments were performed as part of the ongoing management of these assets on an annual basis.
Benefits to client	• A methodology that has resulted in proper risk identification of business critical services • Support from an onshore KPMG team with local industry and subject-matter knowledge • A robust process for assessing the client's business critical assets and the proper maintenance and management of these assets

CASE STUDY 4

Large regional bank reengineering its controls framework

Client challenge	The client had developed an ITRM strategy. However, assistance was needed in developing an IT risk and controls framework that could be implemented as part of the corporate ITRM framework. Additionally, the client needed help in capturing and defining IT risks and controls while also monitoring and reporting compliance to management.
KPMG response	KPMG assisted the client by developing a risk and controls framework that could capture and monitor IT risks. The focus of the engagement was to develop the framework of IT controls and IT risks including the key activities that should be in place to attest to the effectiveness of the IT controls in place. This also included developing metrics (KRIs) that could be used to monitor the effectiveness of the implemented IT controls within the applications at the client, as well as be used for reporting to management.
Benefits to client	• An ITRM framework that is aligned to the client's ITRM strategy and industry practice • The identification of IT risks and the development of IT controls that align with standard practices, as well as used for other assessments with the potential for future cost savings • KPMG professionals who have industry experience and provide insight into how ITRM frameworks and controls have been implemented and monitored at similar organizations

Case studies (continued)

CASE STUDY 5

Global oil and gas company looking for control focused input into process design

Client challenge	The client needed to ensure control designs were being validated and to allow control best practices to be built into the design of its new configuration management and asset management processes.
KPMG response	KPMG participated directly in the project design workshops and provided industry leading control recommendations to the client in the integration of its configuration and asset management systems. KPMG also included a risk-based objective review of the overall project governance, with an assessment on key project risks and recommended actions.
Benefits to client	• Client was able to evaluate its control design for its configuration and asset management process areas • Identified areas of improvement during the design phase around control procedures which were easier to change before the implementation phase • Support from an onshore KPMG team with local industry and subject-matter knowledge

CASE STUDY 6

Global bank looking for assistance to help address regulatory requirements

Client challenge	The client had recently redeveloped its ITRM function so it could be adopted by all regions globally. The client needed assistance in rolling out and performing the IT risk assessments. However, upcoming compliance requirements in one of the local regions meant that risks for a significant number of applications distributed globally needed to be analyzed and addressed in a very short period of time.
KPMG response	KPMG assisted with IT risk assessments across applications that were subject to local regulatory requirements. Upon completion of the assessments, KPMG helped the client to better understand the IT risks that were identified and determine whether sufficient controls were in place to mitigate these risks.
Benefits to client	• Objective evaluation of IT risk assessments for the identified applications • A KPMG team, including member firms of KPMG International advised on a global approach toward the assessment and provided regional/local regulatory knowledge along with experience with financial services

Contact us

To learn more about ITRM, contact one of the following KPMG professionals:

David DiCristofaro
Partner
212-872-3382
ddicristofaro@kpmg.com

Phillip J. Lageschulte
Partner
312-665-5380
pjlageschulte@kpmg.com

Vivek Mehta
Director
212-872-6548
vivekmehta@kpmg.com

Joshua Galvan
Managing Director
713-319-2082
jgalvan@kpmg.com

kpmg.com