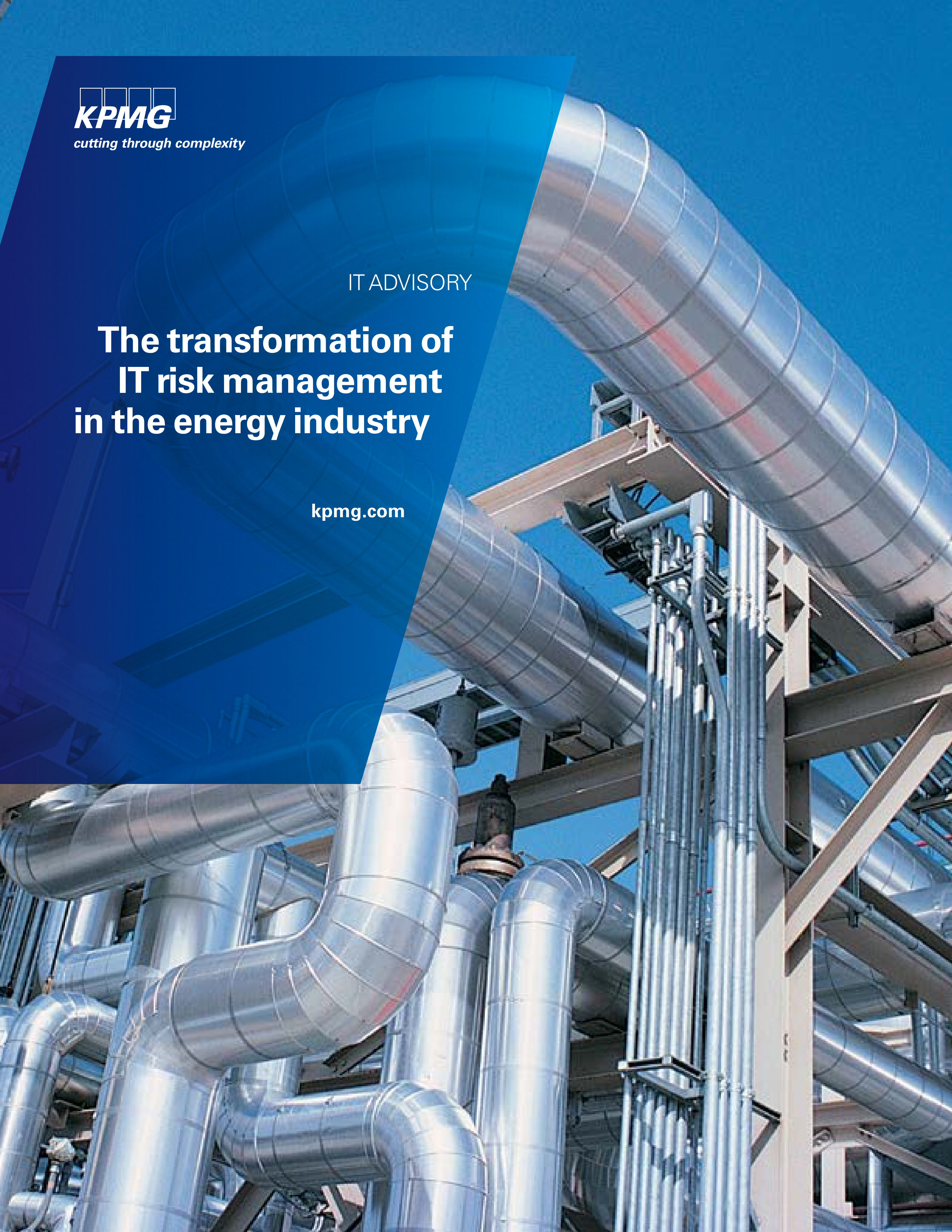


KPMG

cutting through complexity

IT ADVISORY

The transformation of IT risk management in the energy industry

kpmg.com

The transformation of IT risk management in the energy industry

Information technology (IT) has enabled energy companies to enhance operations through solutions that provide, among others, near real-time visibility, data-driven analysis and decision making, and mobility. While these advances have supported and informed a shift in business models across the value chain, they also increase risk exposures and require improved IT risk management (ITRM) processes.

The ITRM function assesses a company's IT system and processes and associated risk landscape to coordinate a tailored risk control framework. ITRM stays apace of a company's evolving risk situation in order to adjust its risk controls and ITRM operating model over time.

By combining a well-designed ITRM operating model with strong business partnerships, energy companies can accelerate innovation while also increasing the ability to identify and manage risk.

However, in the current environment of low commodity prices and pressures to reduce spending, there is a risk of under-investment in ITRM. Instead of waiting out low prices, energy companies should invest in ITRM now in order to be prepared for when prices rebound. Energy companies can do this while also controlling spending by partnering with the business to bring a risk-balanced view on IT solution selection, deployment, and enhancement.

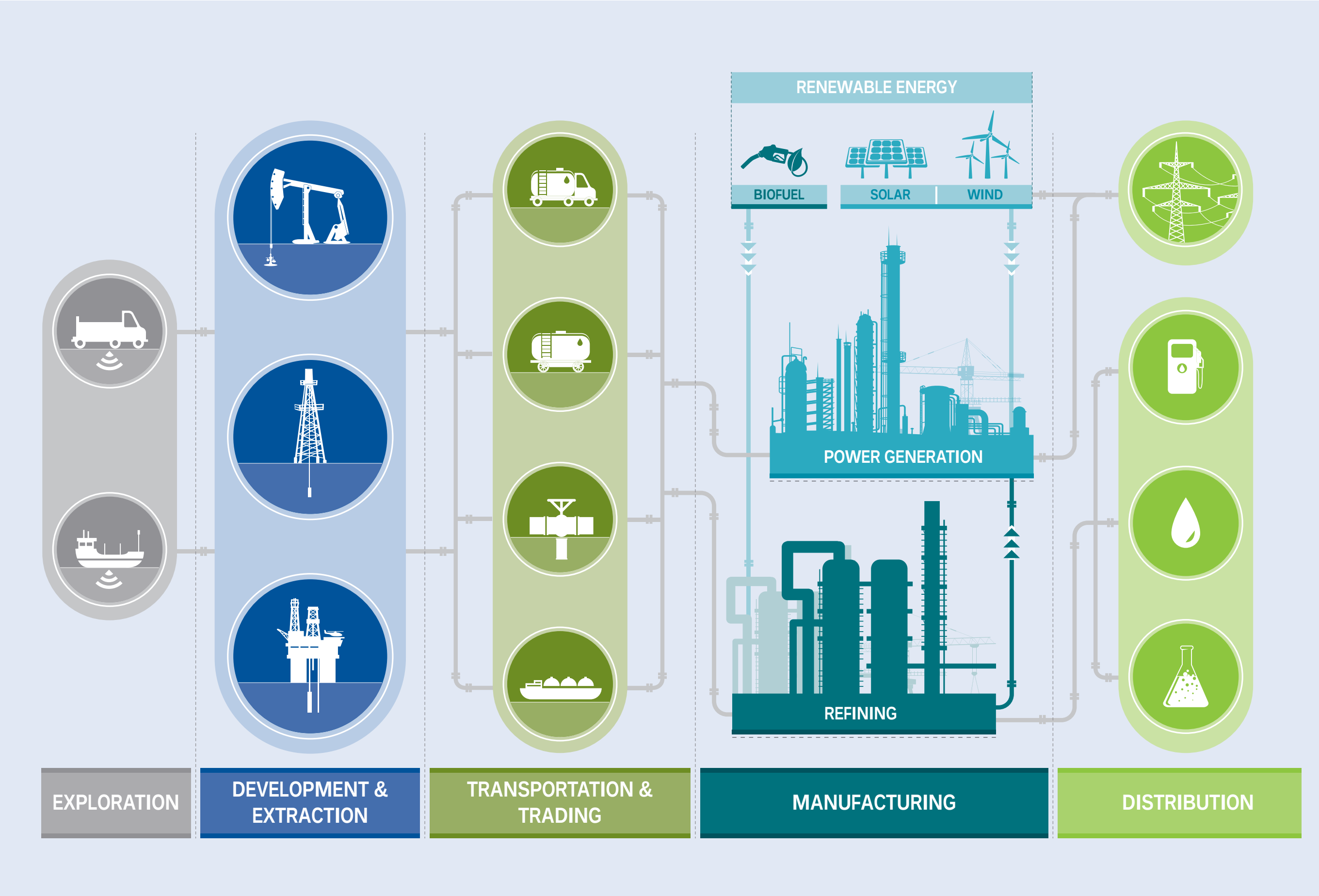
About the authors

Joshua Galvan is a principal based in Houston leading efforts in KPMG's Emerging Technology Risk practice. In his career focused on the entire energy value chain, he helps companies achieve better IT governance, performance, and business integration to derive more value from global IT risk management process frameworks, enabling automation solutions and organizational structures. His work has informed prevailing ITRM practices in the energy sector, while also working cross-industry to assist in developing ITRM better practices in the face of the evolving risk situation and technology advances.

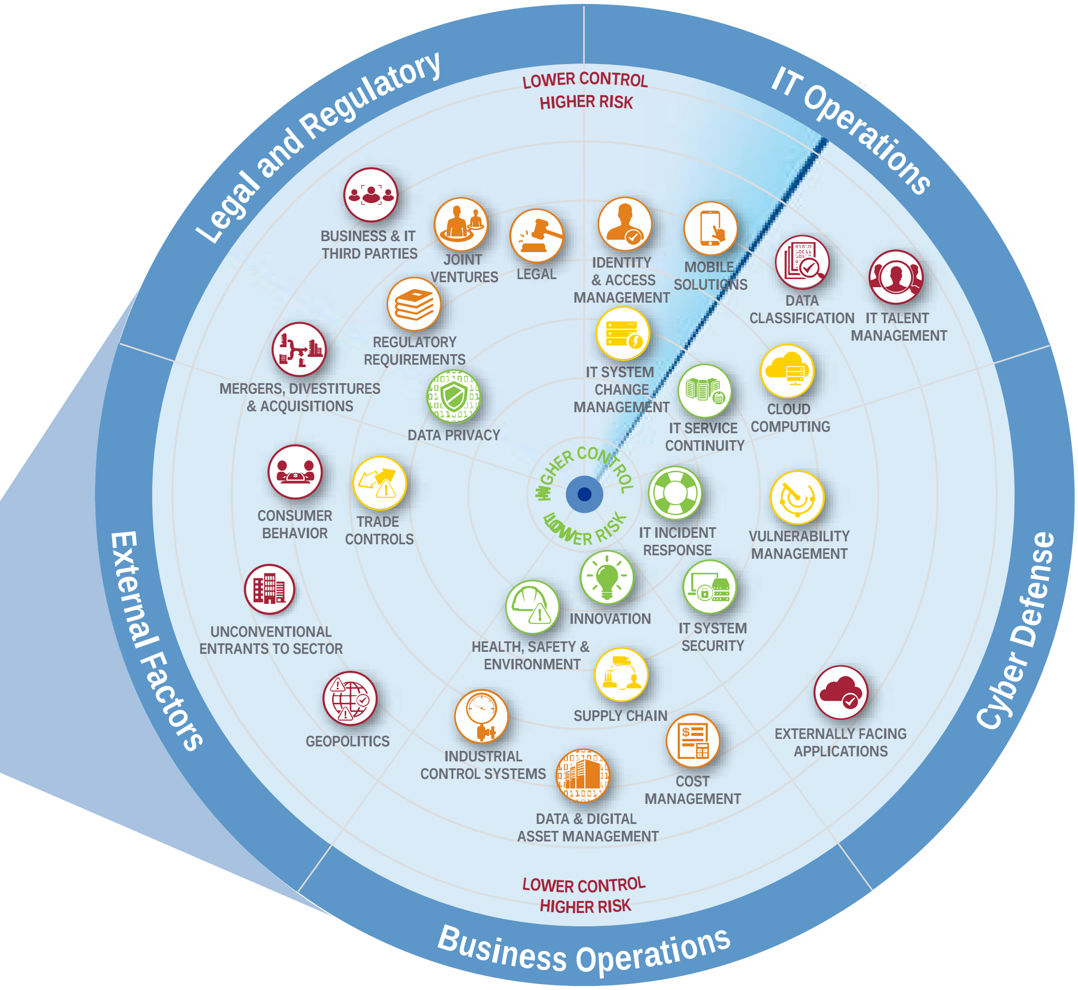
Chris McDonald is a director based in Houston and assists clients in establishing and improving their IT operational processes, IT internal controls, and IT governance structures. Chris leads teams in the evaluation of IT risk management capability and compliance performance across all IT asset classes and IT functional domains. From the corporate office to field operations, Chris helps energy companies define and align ITRM processes to company practice, industry standards, and regulatory requirements, with a keen eye on streamlining and cost-effective solutions.

Energy companies face increasing risks and regulatory challenges

As oil prices hover near multiyear lows, the energy industry will be challenged to spend smart and still achieve appropriate levels of ITRM, governance, and assurance. Security concerns from corporate espionage and state-led attacks on energy companies have increased. At the same time, the IT estate is becoming more complex, IT investment projects run afoul, IT third parties require more oversight, and pressure from regulators, investors, and auditors is increasing. These concerns serve as a wake-up call for the industry to make strategic investments in end-to-end ITRM operating models to help define a company's risk appetite and properly manage that risk.



Typical energy company IT risk inventories include what may be the cause, consequence, or part of a strategy to address the related risks on a prioritized scale.



● **Lower Control/Higher Risk** – Emerging or unknown risks, inhibiting energy companies to design suitable countermeasures

● ● **Medium Control/Medium Risk** – More predictable risks, allowing energy companies to design only approximate countermeasures

● **Higher Control/Lower Risk** – Stable and well-known risks, enabling energy companies to effectively design fit-for-purpose countermeasures

Energy companies have become increasingly skilled at leveraging advanced science, engineering, and computing technology to calculate and manage operations risk. However, the proliferation of new technologies and ever-expanding data volumes has increased the risk of a major IT incident.

For example, critical infrastructure environments are facing threats that are increasing in frequency, complexity, and persistence. This is driving both regulators and energy companies toward better system safeguards by establishing appropriate security controls and mechanisms that support critical infrastructure.

ITRM helps energy companies respond to both changing risks and business drivers

Historically, ITRM in the energy industry has been focused on security controls and compliance checks. While recent scares over data hacking and identity fraud make headlines, lapses in continuity, change execution, data integrity, or service delivery remain as great a threat.

ITRM must address a prioritized company IT risk profile and better integrate with IT operations to stay ahead of the evolving risk curve. A robust ITRM function manages and optimizes related processes and tools with the goals of improving risk awareness, operations effectiveness, and financial efficiency.

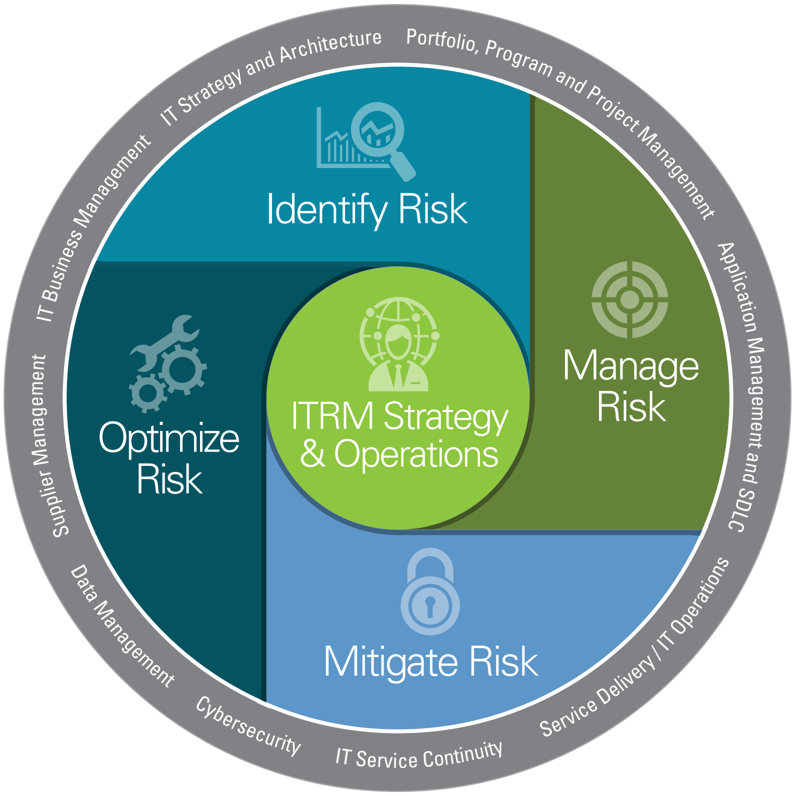
ITRM in energy companies should be an ally of the CIO as well as of the business segment and corporate leaders. It must take business priorities into account and play a key role in the relationship "networks" that keep a company's risk universe and risk appetite current. ITRM should have visibility into the IT solution and service pipeline and provide IT with a risk perspective while responding to shifts in business performance as well as external marketplace factors.

Changing business landscape		**Key objectives of ITRM**
Changing market and client need	Critical national infrastructure, high-profile IT failures, predictive analytics	Resilient technology infrastructure Ability to track the right metrics *before* an IT failure
External factors	Organized crime, nation states, cyber espionage, hacktivism, insider threats, public expectations on security	Staying ahead of the constantly evloving cyber threat landscape Security of intellectual property and customer data
Change in the way business is conducted	Technology for all things, The Chief Digital Officer, and the post-digital age	Ability of IT infrastructure to meet increasing business demand Reduced IT complexity and operational costs
Regulatory compliance	Letters on IT from the regulators, privacy, regulatory "horizon scanning", records management	Understanding of current and upcoming regulatory expectations
Rapid technology change	Cloud computing, big data, social media, BYOD, mobile strategies	Translating risk from emerging technology into competitive advantage

Energy companies are accustomed to placing bets on risks related to large capital projects, whether in extractive, refined product, or power-related industries. They are further challenged to apply related concepts and practices to both field and corporate operations. In response, energy companies must improve capabilities for measuring and optimizing operations around favorable unexpected outcomes (upside risk), in addition to unfavorable unexpected outcomes (downside risk).

An ITRM framework tailored to energy company risk appetite

There are a number of influences that impact the amount of IT risk an organization can manage. Energy companies should establish their overall risk appetite, evaluate the risk inventory on a continual basis, and accordingly tune related strategies to throttle the amount of risk that will or will not be taken. KPMG sees four phases around a centralized framework to help businesses identify, manage, mitigate, and optimize the IT risks impacting their organization.

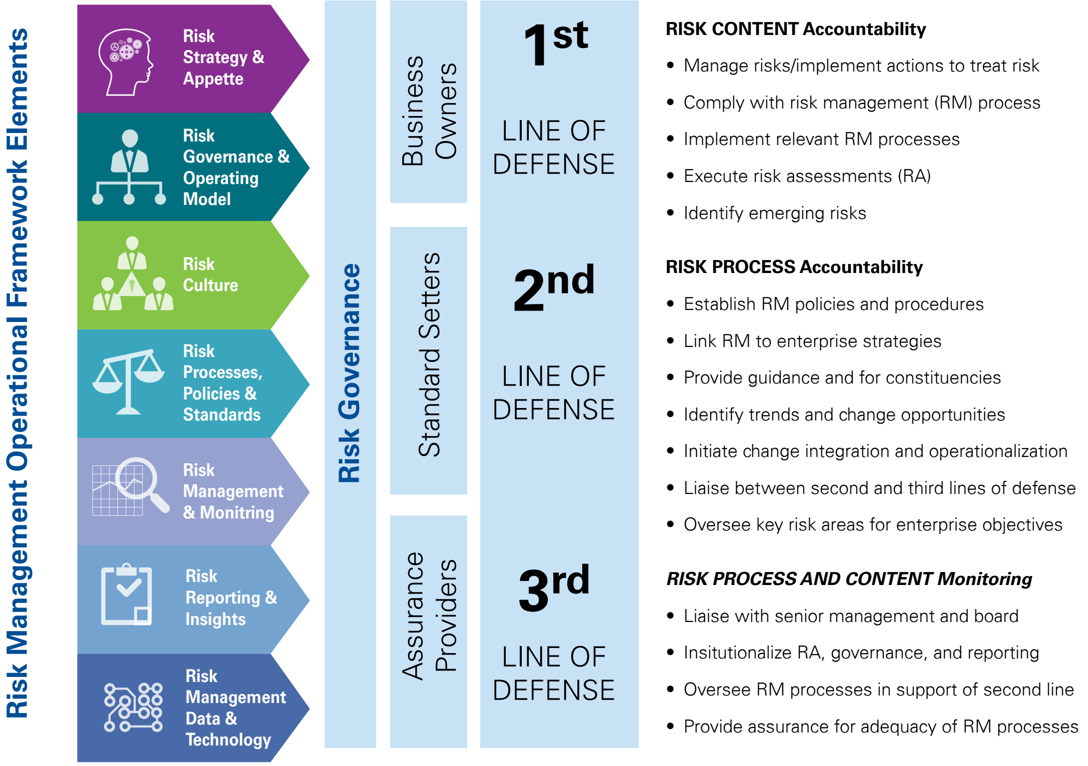

IT Strategy and Architecture
Portfolio, Program and Project Management
Application Management and SDLC
Service Delivery / IT Operations
IT Service Continuity
Cybersecurity
Data Management
Supplier Management
IT Business Management
Identify Risk
Manage Risk
Mitigate Risk
Optimize Risk
ITRM Strategy & Operations

ITRM Strategy & Operations	Identify Risk	Manage Risk	Mitigate Risk	Optimize Risk
• Capability Maturity Assessment • Target Operating Model • IT Risk Appetite • ITRM Training and Awareness	• Emerging Technology Risk Analysis • Application Risk Assessment • Real-time Implementation Review • Vendor Risk Assessment	• Emerging Technology Risk Governance and Controls • Risk and Controls Library • Key Risk Indicators and Dashboard Reporting • Service Risk Management	• Control Design and Implementation • Process, Risk and Control Transformation • Issue Resolution Planning and Oversight • Root Cause Analysis and Remediation	• Controls Optimization and Rationalization • GRC Tooling and Automation • ITRM Staff Augmentation and Co-sourcing

A recent KPMG survey found that only about 20 percent of energy companies have established their risk appetite. Most have only done so informally or implicitly and generally only for managing unfavorable outcomes, or downside risk, with no mention of optimizing favorable outcomes, or upside risk.

ITRM in the context of the "three lines of defense"

The governance of risk management involves the business owners, the standard setters, and the assurance providers. These three lines of defense coordinate to reveal and manage risk in a way that optimizes funding and assurance objectives. Energy companies should involve business and IT leadership to define a lines of defense model that integrates the risk functions to adjust the risk appetite over time, maintain the control blanket, and share risk information for timely responses and operating model enhancements that stick. The ITRM operating model, in this context, largely represents the first line of defense for IT.



Risk Management Operational Framework Elements

Risk Strategy & Appetite

Risk Governance & Operating Model

Risk Culture

Risk Processes, Policies & Standards

Risk Management & Monitring

Risk Reporting & Insights

Risk Management Data & Technology

Risk Governance

Business Owners — 1st LINE OF DEFENSE

RISK CONTENT Accountability

- Manage risks/implement actions to treat risk
- Comply with risk management (RM) process
- Implement relevant RM processes
- Execute risk assessments (RA)
- Identify emerging risks

Standard Setters — 2nd LINE OF DEFENSE

RISK PROCESS Accountability

- Establish RM policies and procedures
- Link RM to enterprise strategies
- Provide guidance and for constituencies
- Identify trends and change opportunities
- Initiate change integration and operationalization
- Liaise between second and third lines of defense
- Oversee key risk areas for enterprise objectives

Assurance Providers — 3rd LINE OF DEFENSE

RISK PROCESS AND CONTENT Monitoring

- Liaise with senior management and board
- Insitutionalize RA, governance, and reporting
- Oversee RM processes in support of second line
- Provide assurance for adequacy of RM processes

Companies are also building a so-called line of defense "1.5" to challenge, enable, and innovate for the first line of defense. This function also provides meaningful engagement and integration with the second line of defense around risk and control standards, as well as the third line of defense for audit and regulatory compliance.

Aligning ITRM within the enterprise improves overall risk management results

Energy companies face increasing demands to not only streamline the cost and operations of their ITRM capability but also to deal with unknown or unquantifiable IT risks. In reacting to a host of forces that the first line of defense faces externally (e.g., regulatory, geopolitical, or market-driven forces and attackers) and internally (e.g., new IT products and services, solution acquisitions, or implementations, as well as attacks from within employee ranks), there is pressure to deal not only with what is happening today, but also with what is right around the corner.

Through better alignment with other company risk oversight functions (e.g., internal audit, enterprise risk management, compliance, legal, and regulatory), ITRM can improve effectiveness in anticipating, managing, and optimizing IT risks. In doing so, energy companies can improve managing upside and downside risk in IT that affect operations, market share, reputation, and future prospects. The examples provided in the following pages demonstrate the need for better alignment of risk functions in which ITRM is critical.

A variety of industry situations demonstrate the need for energy companies to coordinate and embed ITRM practices throughout the enterprise

Export compliance penalties

The U.S. Justice Department has investigated energy companies for violations of U.S. export control laws and sanctions programs and has levied nine-figure fines. IT-enabled risk systems can better monitor transactions involving controlled information and the exchange of goods and services.

EPA tightens toxic air standards for oil refineries and petrochemical plants

The EPA has tightened toxic air standards and issued guidelines to correct the chronic underestimation of toxic air pollutants emitted from oil refineries and petrochemical plants. Facilities must evaluate whether they require a new permit or updates to their existing permits. Pollutant tracking and reporting demands reliability, transparency, and timeliness in IT systems, data capture, and review.

The struggles of U.S. energy suppliers to Ukraine and Russia

The U.S. Department of Commerce's Bureau of Industry and Security issued a rule denying export, re-export, or foreign transfer of certain items for use in Russia's energy sector that may be used for exploration or production from deepwater, Arctic offshore, or shale projects that have the potential to produce oil. Companies must commit to securing and sustaining the use of IT systems that provide reliable item tracking and transfer of custody records in order to avoid related penalties and fines.

Hackers are increasingly targeting energy companies

In 2013, 40 percent of all cyber attacks uncovered by the Department of Homeland Security targeted the energy sector, elevating concerns about the security of the country's electricity supply as one of the biggest challenges facing U.S. power companies. As an evolving response, the Critical Infrastructure Protection requirements for power companies exist as a series of requirements focused on improving the North American power system's security through standards and provisions that affect operations, physical security, and IT systems.

> *IT Risk Management must "… be an integrated part of the company's overall management systems … systematically recognizing and preparing for factors that cause uncertainty and threats to company objectives and operations" within management-defined acceptable risk levels that shift with the evolving situation in a continuous cycle.*

(from https://www.itforbusiness.org/content/uploads/2015/07/it-standard-for-business-2015-07-03.pdf)

> *…The other challenge is to prepare for what the CEO of one major corporation called the "bad new world" of cyber vulnerability. The infrastructure that produces and delivers our energy is at the top of the list of "critical infrastructures," and the risks only grow as the world continues to digitise and the Internet becomes ever more pervasive.*

"New Challenges to Energy Security," Daniel Yergin, The Journal of the International Energy Agency, Issue 3 – Autumn 2012

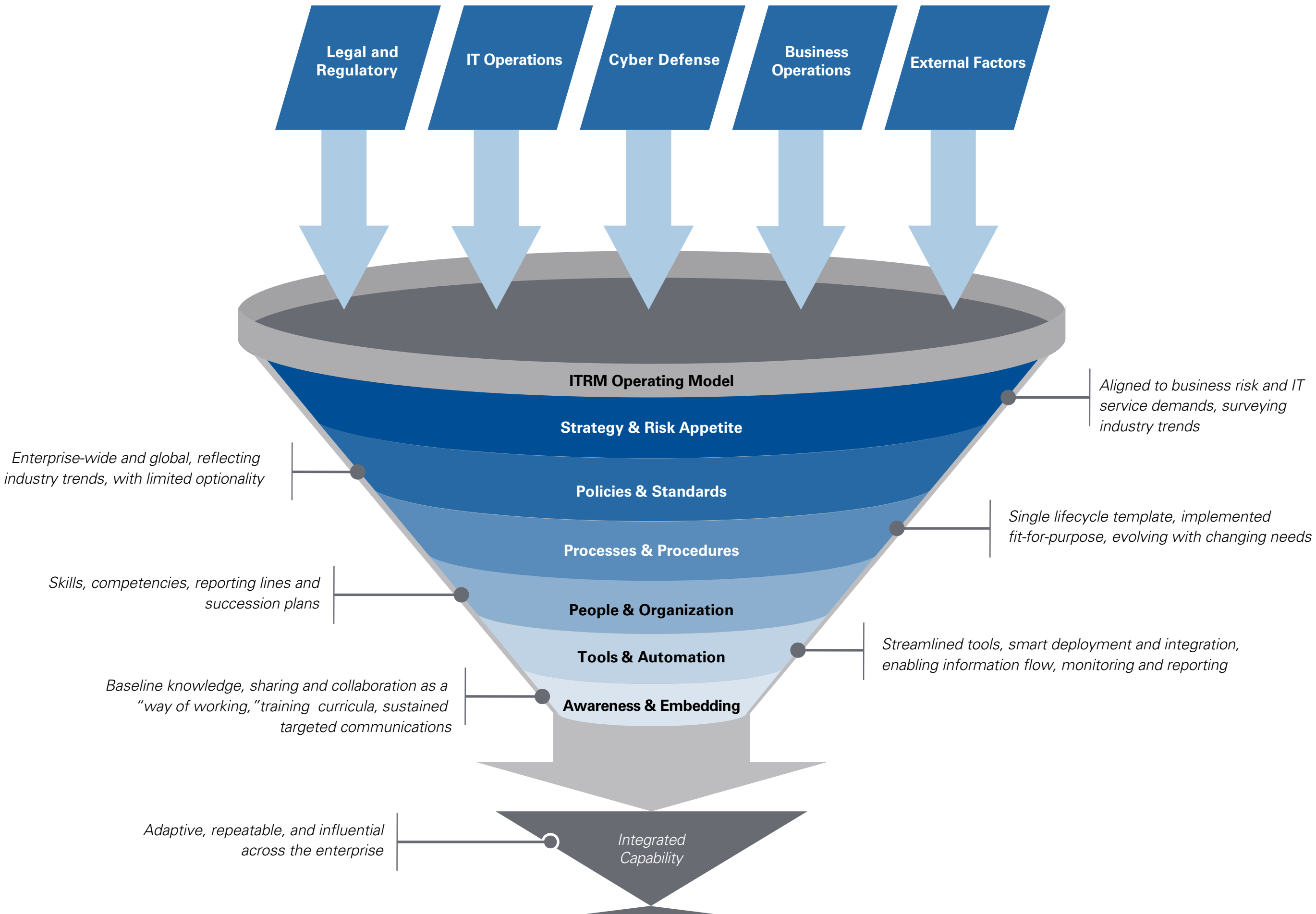
> *… attack against CIP [Critical Infrastructure Program] systems has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to be reduced. … More comprehensive work is needed, however, to realize the vision of a secure CIP system … and allow operators to 'fly with fewer controls.'*

(from https://www.onepetro.org/conference-paper/SPE-168320-MS?sort=&s2_parent_title=&peer_reviewed=&published_between=&rows=10&start=0&q=cybersecurity&dc_issued_year=2014&dc_publisher_facet=&from_year=&fromSearchResults=true&dc_type=&to_year=#)

Energy companies need an end-to-end ITRM operating model

Gone are the days of operating ITRM processes designed exclusively in response to regulatory requirements. Energy companies are now called to redouble their efforts towards dedicated cost-effective and end-to-end ITRM capabilities. While the past trends in ITRM have often resulted in fragmented knowledge, inadequate skills, or cumbersome solutions, their greatest impacts may be a lack of company and industry context; reduced emphasis on risk insights and intelligence; limited to no partnering with the business across risk functions; and reduced readiness for enabling (not stalling) IT solution innovation.

Now is the time for energy companies to design and operate end-to-end, sustainable ITRM operations that enhance business prospects and are scaled to a company's risk appetite.



Aligned to business risk and IT service demands, surveying industry trends

Enterprise-wide and global, reflecting industry trends, with limited optionality

Single lifecycle template, implemented fit-for-purpose, evolving with changing needs

Skills, competencies, reporting lines and succession plans

Streamlined tools, smart deployment and integration, enabling information flow, monitoring and reporting

Baseline knowledge, sharing and collaboration as a "way of working," training curricula, sustained targeted communications

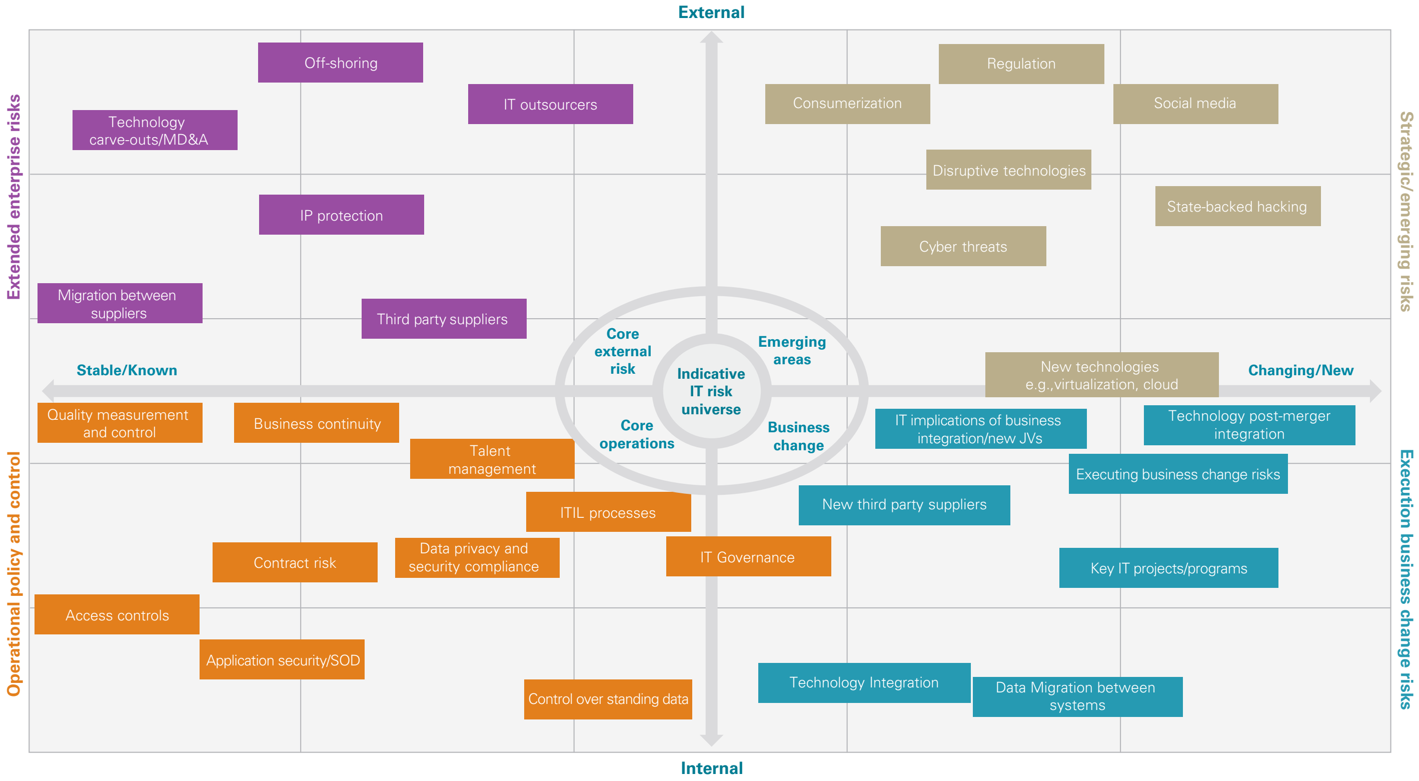
Adaptive, repeatable, and influential across the enterprise

Prevailing Benefits of ITRM Operating Models

- Proactive risk identification and evaluation
- Visibility and management of third-party relationships
- Business-aligned risk appetite
- Effective reporting and decision making
- ITRM automation and integration
- Enterprise incident/disaster response capability
- Defense-in-depth security model
- Common user identity solutions
- Scalable application and infrastructure environment (i.e., cloud services)
- Improved protection of sensitive data

Paving the road to sustainable ITRM maturity

Energy companies can focus on the improvement of their ITRM program maturity through a series of quick wins that build momentum for a true transformational change. An illustration of energy company risks confirms the complex situation the industry faces. By building and sustaining an IT risk universe (example illustration below), then cross-sectioning as forces evolve, energy companies can prioritize their ITRM baseload activity as well as improvement initiatives and investments.

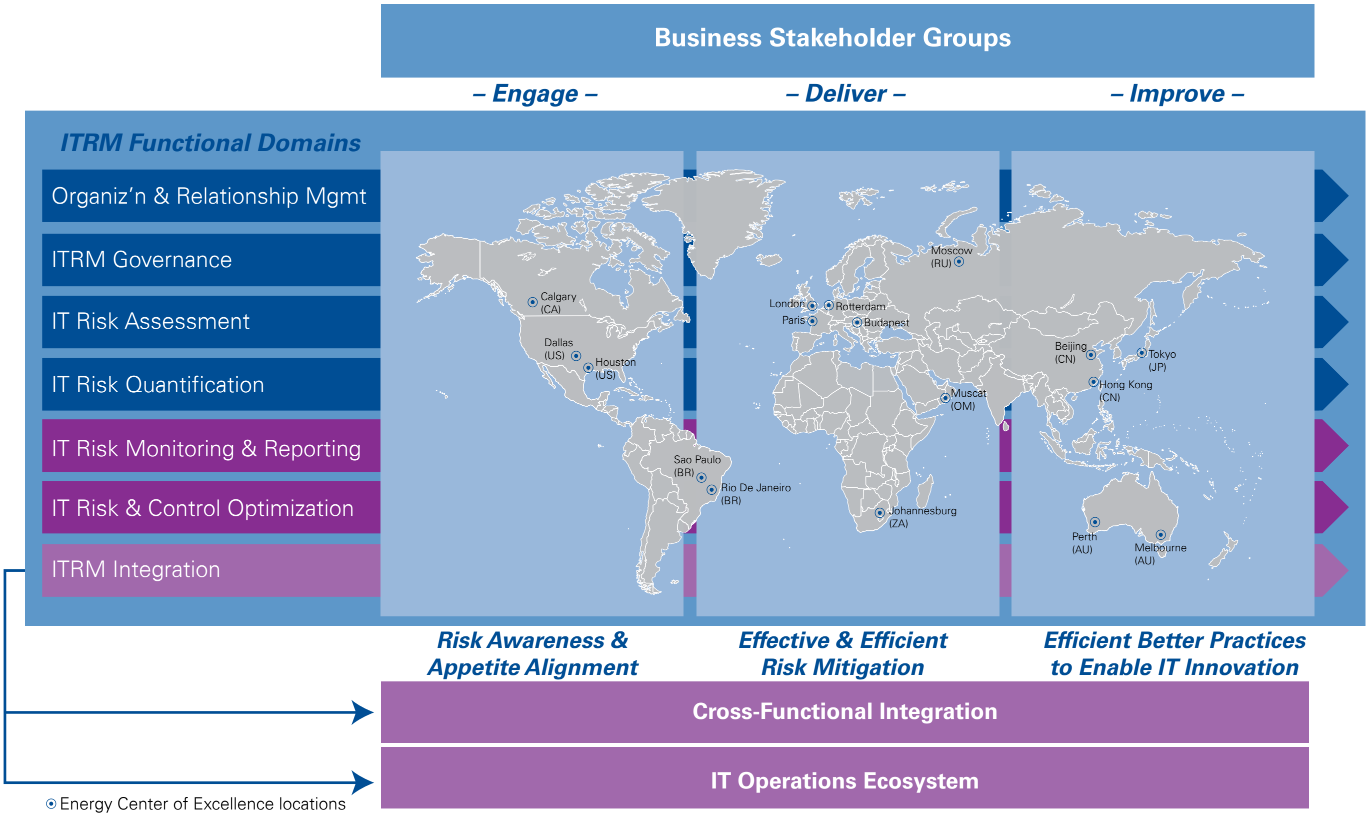

External
Internal
Stable/Known
Changing/New
Extended enterprise risks
Operational policy and control
Strategic/emerging risks
Execution business change risks
Indicative IT risk universe
Core external risk
Emerging areas
Core operations
Business change
Off-shoring
IT outsourcers
Technology carve-outs/MD&A
IP protection
Migration between suppliers
Third party suppliers
Regulation
Consumerization
Social media
Disruptive technologies
State-backed hacking
Cyber threats
New technologies e.g.,virtualization, cloud
Quality measurement and control
Business continuity
Talent management
ITIL processes
Contract risk
Data privacy and security compliance
IT Governance
Access controls
Application security/SOD
Control over standing data
IT implications of business integration/new JVs
Technology post-merger integration
Executing business change risks
New third party suppliers
Key IT projects/programs
Technology Integration
Data Migration between systems

To meet the challenges posed by emerging risk factors, energy companies must commit to clearly articulating their risk appetite to properly influence associated IT risk and control design. They in turn sustain ITRM over time with investment in sound methods of practice for the baseload activity set and innovation, as well as content management, automation platforms (data analysis, dashboarding, and decision support), and talent management (workforce capacity, skills maintenance, and collaboration networks). Energy companies can advance ITRM maturity from a focus on mere awareness, compliance, and passing audits, to achieving more predictive IT risk identification, and value enhancement.

How KPMG helps energy companies achieve ITRM maturity

KPMG has helped companies across the energy value chain develop cost-effective global ITRM operating models by properly applying the company's appetite for IT risk, while not unduly affecting business and technology innovation. Our experience ranges from global integrated oil and gas companies to independent producers, from power generators to diversified utilities, and the variety of energy services firms.

KPMG assists energy companies in implementing integrated ITRM strategies and frameworks that deliver improved risk intelligence, timeliness, awareness, and automation. These capabilities have not only provided transparency in the evolving risk landscape, but they are also scalable for fostering a sustainable and repeatable ITRM practice both within company corporate walls and also into their important field and joint venture operations.



Business Stakeholder Groups

– Engage – – Deliver – – Improve –

ITRM Functional Domains

- Organiz'n & Relationship Mgmt
- ITRM Governance
- IT Risk Assessment
- IT Risk Quantification
- IT Risk Monitoring & Reporting
- IT Risk & Control Optimization
- ITRM Integration

Risk Awareness & Appetite Alignment

Effective & Efficient Risk Mitigation

Efficient Better Practices to Enable IT Innovation

Cross-Functional Integration

IT Operations Ecosystem

⦿ Energy Center of Excellence locations

KPMG's Global Energy Institute

The KPMG Global Energy Institute (GEI) launched in 2007, the GEI is a worldwide knowledge-sharing forum on current and emerging industry issues. This vehicle for accessing thought leadership, events, webcasts and podcasts about key industry topics and trends provides a way for you to share your perspectives on the challenges and opportunities facing the energy industry – arming you with new tools to better navigate the changes in this dynamic area. Learn more at: http://www.kpmgglobalenergyinstitute.com

Our assistance to energy company ITRM programs

Operationalizing a full life cycle of ITRM activities

KPMG assisted a global integrated oil and gas company with a variety of ITRM embedding challenges, including establishment of a project management office, design of governance operations, stakeholder communications, capability assessments, comparator studies, and improvement plans for operations enhancement, and issue remediation management. KPMG's assistance has helped align business and IT stakeholders on risk profiles and appetite, and continues to operationalize and improve ITRM services for this globally complex organization.

Unifying ITRM activities across business segments

A large midstream company experienced inefficiency and redundancy in its ITRM framework. The activity set was often performed informally or common elements were conducted in multiple work streams when a single thread would suffice. Business and operating units operated different processes, captured different data, and adhered to different time lines and reporting protocols. In an effort to bring cost-effectiveness and transparency to the risk management life cycle, KPMG assisted management in integrating processes on a common platform, thus enabling more timely and enterprise-wide IT risk analysis and decisioning.

Focusing resources on most critical IT assets

KPMG assisted with the identification, categorization, and prioritization framework of critical IT assets for a global energy company. In reference to existing company ITRM operations, KPMG executed a comprehensive end-to-end assessment of governance, process mechanics, automation tools, and information flow for effective communications and hand-offs. KPMG codeveloped a multidimensional road map for improving company awareness and operations for sustainably managing critical IT assets on a prioritized basis, within the context of the wider ITRM operating model.

Uncovering the IT risks of oil and gas field operations

Recognizing the volume of IT that permeates field operations, energy companies are bringing related risks into focus. KPMG assisted a large oil and gas company in defining and deploying a prototype for repeatable IT risk assessment processes and tools for all business segments, joint ventures, and assets. Encompassing operational IT and traditional IT, the company, its partners and suppliers are collaborating to improve IT risk visibility, control assurance, and the related operational "health" impacts of field operations.

Roadmapping an enterprise ITRM improvement program

An engineering and services firm launched a global ITRM improvement program in response to the slow degradation of established company-wide IT control and compliance standards. KPMG provided industry insights that sharpen the program goals, scope, timeline, and solution alternatives. In a little over a year's time, the integrated road map delivered harmonized global processes, more automated controls in core systems and infrastructure, redefined global accountabilities, and a rationalized central governance and communications model.

Transforming ITRM in support of power industry regulatory change

Due to emerging regulatory requirements, power generation, transmission, and distribution companies have been tasked with rethinking traditional regulatory compliance and taking advantage of the benefits of a modern ITRM capability. KPMG has assisted power companies in anticipating standards, assessing impact and implementing effective operations to not only comply but also derive new insights and develop skills for improving business resiliency and ITRM effectiveness. In helping power companies understand their needed maturity levels, KPMG teams have also designed more effective ITRM team structures, aligned IT risk, compliance and incident management, and transformed the purpose and value of IT in regulatory compliance.

Contact us

Phil Lageschulte
KPMG Partner and National Leader for Emerging Technology Risk
T: 312-665-5380
E: pjlageschulte@kpmg.com

Regina Mayor
KPMG Principal and National Sector Leader, Energy & Natural Resources
T: 713-319-3137
E: rmayor@kpmg.com

Joshua Galvan
KPMG Principal, Energy & Natural Resources
T: 713-319-2082
E: jgalvan@kpmg.com

Chris McDonald
KPMG Advisory Director
T: 713-319-2586
E: crmcdonald@kpmg.com

kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.