In a digital world, do you know where your risks are?

Key considerations for your internal audit plan to help management navigate in the Transformative Age

The better the question. The better the answer. The better the world works.

Building a better working world

Table of contents

Introduction

Innovation continues to improve the world in which we live. One only needs to look around to see the benefits that we enjoy as a result of this innovation (e.g., global access to information through the internet, features within our cars and homes that strive to keep us safe and make our lives easier, and advances in medicine, energy production and distribution). However, the resulting volume and velocity of change have upended the business environment and rearranged the landscape. A study found that only 37.6% of the companies on the Fortune 500 list in 1995 were still on the list in 2016.[1] This does not necessarily mean that companies no longer on the list have failed — for example, mergers and acquisitions have changed the composition and some companies have simply been replaced by new organizations that have achieved a higher market capitalization. Regardless of the reason, competition among companies to survive and prosper is fierce and innovation is one of the key differentiators.

As we operate in the transformative age, companies are being forced to respond to a wide array of challenges and demands at an increasing pace — and there doesn't seem to be an end in sight. The potential for disruption can emerge from the introduction of new technology, new business models, a change in consumer preferences or the entry of new competitors — often from a different industry. Gone are the boundaries that once influenced how businesses defined their market and how they operated. For example, consider the effect of online shopping on brick-and-mortar retail establishments or the introduction of companies that offer vacation rentals and don't even own real estate.

In response, management is aggressively embracing new technologies to transform their business models, drive growth and improve efficiency. They are leveraging big data to drive competitive insights. And, they are entering into strategic transactions (e.g., mergers, acquisitions, divestitures, alliances and joint ventures) to enhance their competitive advantage. Management is also looking at their existing operating model to identify ways to become more agile and efficient so they can deliver results and still be able to respond quickly when a new challenge arises.

All of these pressures, whether from internal or external sources, create both an opportunity and a challenge for the Internal Audit (IA) function. IA must balance priorities and resources to help the organization address the risks it faces today, anticipate emerging risks and provide business insights that may help management gain a competitive advantage. The IA function must maintain a focus on basic and core activities, but it must also be ready to take on more of an advisory role. And it must be able to "look around the corner" to see tomorrow's risks today.

[1] Mark J. Perry, "Fortune 500 firms 1955 vs. 2016: only 12% remain, thanks to the creative destruction that fuels economic prosperity", 13 December 2016, accessed at http://www.aei.org/publication/fortune-500-firms-1955-v-2016-only-12-remain-thanks-to-the-creative-destruction-that-fuels-economic-prosperity/.

The new reality

An organization's processes and controls may be efficient and effective today yet be compromised tomorrow. For example, the introduction of robotics to execute transactions formerly performed by staff brings new risks. To avoid being placed at a disadvantage, organizations must adjust their processes and controls accordingly. IA can play a key role in helping management understand the impact of automation and changing team skills and dynamics.

IA must be more flexible than ever to help management understand the risks and their impact on the organization. A dynamic risk assessment and internal audit plan are no longer an option; they are required if IA wants to stay in the game. But organizations are increasingly calling for more. They are asking IA to take on a more advisory role in taking a proactive look at the design of controls in areas such as systems development, new product development and strategic transactions. And, they are asking for business insights that IA is in a unique position to provide given their broad mandate.

The risk assessment should be enterprise-wide and include all categories of risk — strategic, operational (including technology), financial and compliance. It should include management participation and a direct link to the organization's overall strategy and enterprise risk management program. It should also include both quantitative and qualitative considerations and should incorporate forward-looking perspectives, such as risks associated with corporate objectives, growth strategies, new products, and environmental and regulatory changes.
Additionally, in light of the fast pace of change in the market place, IA should embrace technology (e.g., advanced data analytics and predictive and behavioral modeling) to enable timely identification of changes to an organization's risk profile. While this is a journey, not something that can be done overnight, leading IA functions are implementing these tools today to prepare for tomorrow.

Conducting a risk assessment more frequently, ideally on a continuous basis, will go a long way to help IA and the business focus on the risks that matter. Through our work with our clients, we have identified a number of risks that are top of mind with the Board, management and IA including those that are emerging, have been ongoing focus areas or are core business processes. In the pages that follow, we have included a number of high-impact audits, including questions to consider that target these risks. We hope you find them helpful as you develop or refresh your risk management agenda.

Anti-corruption

In many places around the world, corrupt payments that personally benefit those in power are a cultural norm. However, as business has become more global and developing countries more prosperous, a movement has grown against the culture of corruption. The US, European nations and many other countries view corruption as perhaps the principal obstacle to free and fair trade, ultimately impeding economic growth, faith in government and the quality of life of societies around the world.

The US Government has made significant investments to combat bribery and aggressively enforce the Foreign Corrupt Practices Act (FCPA). We have seen companies pay tens and hundreds of millions of dollars in fines, as well as individuals found guilty and serving prison time. FCPA enforcement continues at increasing levels and global companies need to assess their risk and take action. This is not just because the bribery of foreign government officials is morally indefensible, illegal and a very serious violation of US law. It's because the FCPA is more than an anti-bribery statute.

Companies need to be proactive. The risks of doing nothing are just too great. Anti-corruption compliance begins with setting the proper tone at the top. Employees need to know in no uncertain terms where management stands when it comes to issues of integrity and following the law.

FCPA violations often result in significant fines and penalties paid to the Government. Criminal fines to companies can be up to $25m per violation or twice the gross gain associated with the violation. Civil fines and other remedies, including injunctions, cease-and-desist orders, accounting disgorgement and a ban against doing business with the US Government are also possibilities.

Anti-corruption audits act as a powerful motivator to promote compliance with anti-corruption program requirements, as well as detect and deter potential improper activity. Anti-corruption audits also assist in evaluating the effectiveness of the anti-corruption program, raise awareness, provide powerful feedback on how the program is working and often uncover new risks not previously identified or fully appreciated.

For many companies, anti-corruption audits are the primary method for anti-corruption monitoring. They should have two main focuses:

- Audit for compliance with the various requirements and controls within the anti-corruption compliance program
- Test high-risk transactions for substantive compliance with the FCPA requirements

Audits that have an impact	Key questions to consider
Risk assessment **Objective:** conduct an analysis to help the company assess the risk of FCPA violations in international business activities	▸ Does the organization assess the risk of FCPA violations in international business activities? ▸ Are interactions with foreign government officials evaluated in the context of customers (government contracts and buyers), regulators (statutory regulations such as licenses) and providers (receiving services from state-affiliated entities)? ▸ Are significant risks against anti-corruption program, policies and procedures identified?
Anti-corruption audits **Objective:** assess the effectiveness of anti-corruption program and compliance with program requirements	▸ Does the organization have an effective anti-corruption program that considers employee training and certifications, third-party due diligence procedures, escalation protocols surrounding high-risk transactions, financial controls over cash and other types of payments? ▸ Does the organization have a mechanism to conduct substantive testing of higher-risk activities to identify corruption red flags and detect potential violations?
Forensic data analytics **Objective:** evaluate the effectiveness of advanced data analytics and monitoring	▸ Does the organization use advanced data analytics techniques such as data visualization, text mining and transaction risk scoring in its anti-corruption audit program? ▸ Does the organization have monitoring capabilities in areas such as payments to agents, gift giving, travel, meals and entertainment expenses, petty cash and charitable donations?

The SEC and DOJ have provided guidance to companies defining the 10 elements of an effective program:

Hallmarks of an effective compliance program

1. Commitment from senior management and a clearly articulated policy against corruption
2. Code of conduct and compliance policies and procedures
3. Oversight autonomy and resources
4. Risk assessment
5. Training and continuing advice
6. Incentives and disciplinary actions
7. Confidential reporting and internal investigation
8. Third-party due diligence
9. Pre-acquisition due diligence and post-acquisition integration
10. Continuous improvement by period testing and review

Source: "A Resource Guide to the FCPA – US Foreign Corrupt Practices Act – By the Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission," accessed at https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf

Blockchain

Blockchain is a nascent technology that is revolutionary in its approach to data, process and systems management. It aims to transform traditionally siloed and business-controlled data, systems and processes to that controlled by a distributed ecosystem.

Blockchain could overturn entire business models in certain sectors by empowering the growth of "virtual organizations," also known as decentralized autonomous organizations (DAOs). DAOs operate through computer programs known as "smart contracts" that carry out the wishes of human shareholders by automatically and securely transmitting data. For example, transactions could include payment processing, online voting, executing contracts, digital signatures, creating verifiable audit trails and registering digital assets such as stocks, bonds and land titles. Its potential for application within the transaction-based financial services industry is particularly vast, but it is valuable in every sector.

Blockchain is a type of database known as a distributed ledger that does not have a central administrator and operates on a consensus basis. Whenever a user submits a new data block to the blockchain, the majority of other users must confirm that it is valid. Blockchain also enables decentralized groups to work together, from anywhere in the world, in a secure, trusted and verifiable way. Because blockchain-based systems enable secure, distributed work processes, they also enable tasks to be executed by distributed teams operating together in a much looser way — but with as much security as if they were working side-by-side. This could reduce office and staffing costs by taking the work to the people, rather than the people to the work.

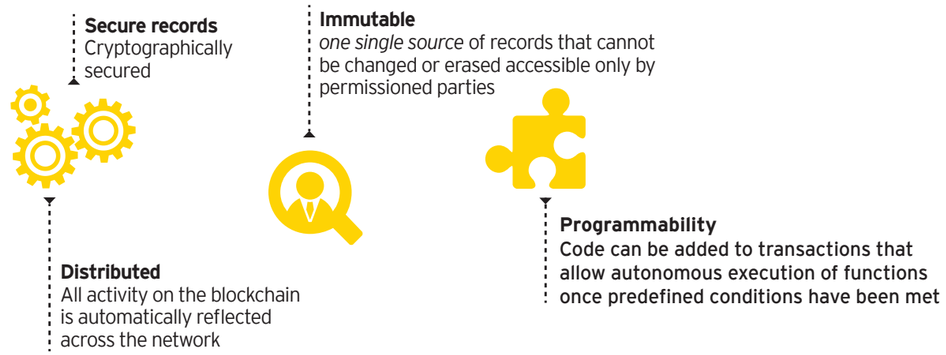
Because blockchain blurs the boundaries of organizations and requires data and processes to be shared outside the organization, companies must fully understand how the technology is implemented to establish appropriate risk management strategies. The internal audit function can help assess whether appropriate controls are in place that secure the organization.

One risk associated with blockchain is the use of a private digital key for identity verification. If the private digital key were compromised, outside agents could gain access to the blockchain. Companies should maintain a well-defined governance structure that manages the secure storage and use of their private keys.

Another blockchain risk exists with smart contracts, which contain a self-executing code that is designed to execute specific rules when defined conditions are met. As these smart contracts become more complex, they are more prone to errors that could provide external agents an opportunity to compromise the system. Companies should implement risk and control strategies to facilitate the integrity of these smart contracts.

Audits that have an impact	Key questions to consider
Blockchain implementation governance **Objective:** evaluate the organization's strategy for governing the implementation of blockchain usage	▸ Are the organization's structure, roles, responsibilities and controls pertaining to segregation of duties monitored? ▸ Are project management processes and controls developed? ▸ Is the steering committee or leadership involved in key project decisions? ▸ Is the proposed project delivery and project risk profile aligned?
Blockchain security and risk assessment **Objective:** evaluate the organization's controls and strategy in place to manage and mitigate risks surrounding blockchain	▸ Is the encryption strategy in place effective? ▸ Is the strategy of node distribution sufficient to limit the loss of data? ▸ Is the use of blockchain in alignment with industry regulatory bodies? ▸ Are effective controls in place to manage access to the distributed ledger? ▸ Is there a process for provisioning and de-provisioning access? ▸ Does the organization assess the controls of third parties surrounding the use of a blockchain-distributed ledger? ▸ How does the organization know the information being entered into the distributed ledger is complete and accurate?

A blockchain is a ledger shared among participants of a nework that is immutable, distributed, programmable and crytographically secure.



Cloud computing

Cloud computing is more than a buzz phrase: it enables organizations to shed their complex internal IT structure, allowing them to focus on strategy rather than operations and respond quickly to changing marketplace conditions.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is evolving rapidly, giving companies a variety of choices; however, like most technology changes, the cloud presents its share of risks and challenges that are often overlooked or not fully understood.

Some of the common cloud computing-related risks that management should address include:

Infrastructure and architectural risks	▸ These risks arise if providers do not achieve performance requirements that organizations and the providers have defined and agreed to at the outset of the contract.
Standards and interoperability risks	▸ It is vital that the organization's systems and those of the provider can communicate with one another.
Regulatory and compliance risks	▸ Organizations using cloud computing services, particularly software-as-a-service (SaaS), have lower transparency and ownership over security controls and processes that providers implement.
Cloud vendor management and governance risks	▸ Contractual risks stem primarily from the types of contracts that clients enter into with cloud service providers (CSPs).
Business continuity risks	▸ Cloud users are depending on their CSP's business continuity program and disaster recovery capabilities.
Strategy alignment and governance risks	▸ Organizations need a governance model including an enterprise-wide cloud risk management approach.

Audits that have an impact	Key questions to consider
Cloud strategy and governance **Objective:** evaluate whether the organization's cloud strategy is aligned to overall business objectives	▸ Are cloud policies integrated with legal, procurement and IT policies? ▸ Are supporting policies including legal, governance and compliance in place? ▸ Are cloud services applications aligned to overall company objectives?
Cloud security and privacy **Objective:** assess the information security practices and procedures of the cloud provider	▸ Are procedures for periodic security assessments of the cloud provider(s) in place to evaluate internal security measures taken to protect company information and data? ▸ Does the organization apply secure authentication protocols for users working in the cloud? ▸ Are the cloud provider's Service Organization Control (SOC) 1, 2 or 3 reports provided to the organization? ▸ Does the organization utilize security service level agreements (SLAs) or conduct on-site vendor audits? ▸ Have security safeguards been established in the contracts with the provider covering their implementation, including Payment Card Industry-Data Security Standards (PCI DSS), data privacy and regulatory compliance?
Cloud provider services **Objective:** assess the ability of the cloud provider to meet or exceed the agreed-upon SLAs in the contract and the contingency plans in case of failure, liability agreements, extended support, and the inclusion of other terms and conditions as part of the service contracts, as well as availability, incident and capacity management, and scalability	▸ Are SLAs in place for uptime, issue management and overall service? ▸ Does the organization track and document compliance of the cloud provider with SLAs, deviations noted, root cause, and corrective and preventive actions taken by the cloud provider? ▸ Are the cloud provider's contingency plans and readiness in the event of major incidents in line with the contractual agreements? ▸ Is there an inventory of uses of external cloud service providers, sponsored both within IT and directly by the business units?

Commodities

Companies with commodity production, merchandising and marketing, trading or hedging operations routinely operate in financial and physical commodities markets to manage commodity risk and to drive financial performance. This is commonly achieved by using a variety of strategies that are fit-to-purpose for the individual company.

However, persistent risks associated with commodity market activities are embedded throughout the commodity transaction life cycle and may result in significant economic, financial, regulatory or reputational consequences if they are not properly controlled.

Internal audit functions are also increasingly focused on addressing a number of related high-profile risks.

Market price risk

Given the historic level of commodity price fluctuation, inadequate market risk management controls may lead to unacceptable market price risk.

Fraud and rogue-trader risk

The risk of fraud and rogue-trader activities is ever-present; inadequate controls across the commodity transaction life cycle may enable fraud and rogue-trader activities.

Credit and liquidity risk

The challenging economic environment in commodities markets has impacted the credit and liquidity standing of companies and their counterparties; inadequate controls may lead to unacceptable credit and liquidity risk.

Model risk

Complex spreadsheet models are widely used as operational tools within the system landscapes of commodities market participants; inadequate controls may lead to the use of incorrect data when transacting in markets and monitoring the related risks.

Business transformation risk

Business transformations driven by the dynamic economic environment can create process and control gaps and introduce risk in otherwise well-controlled organizations.

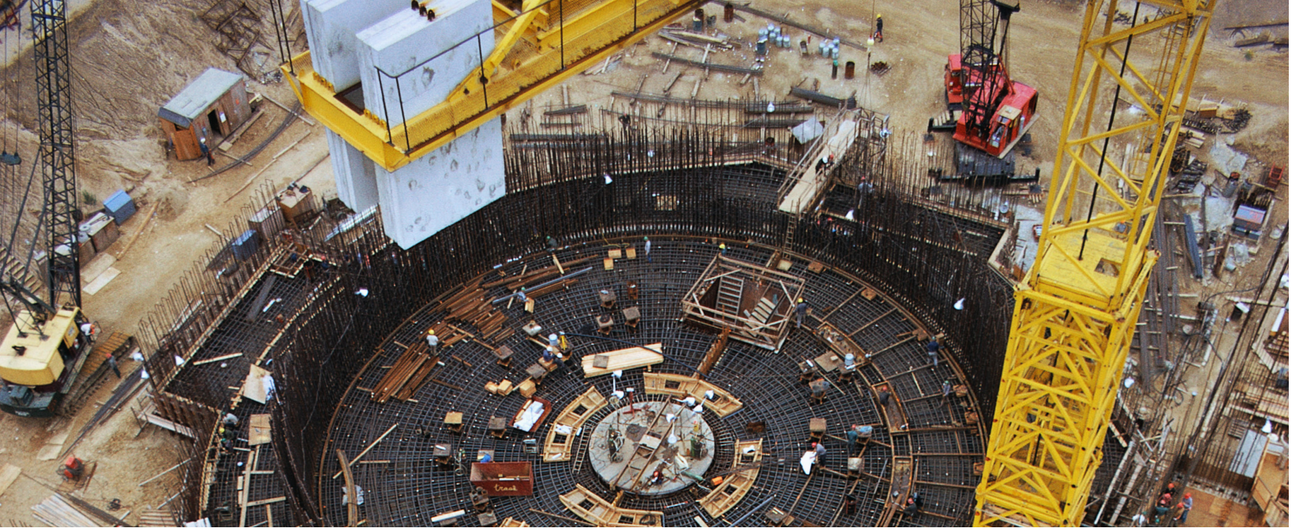
Commodity trading and risk management (CTRM) system implementation risk

The implementation of a CTRM system may introduce significant risks through the inadequate implementation of system-based or system-enabled controls.

Cybersecurity risk

Critical and proprietary financial and operational data is maintained in CTRM systems; inadequate cybersecurity controls may lead to financial and operational risks.

Audits that have an impact	Key questions to consider
Business transformation risk **Objective:** Assess current state and future state processes and controls	▸ How have policies and controls been adapted to manage the risks of new business activities – are more robust policies and controls required to keep up with more complex activities? ▸ How have organizational changes impacted the segregation of duties across key front, middle, and back-office processes?
Commodity trading and risk management (CTRM) system implementation risk **Objective:** Assess the risks in the future state of business processes and the use of a CTRM package's native functionality to support the design of future state controls	▸ Has the CTRM's full suite of native control functionality been assessed for applicability to the future state processes and controls? ▸ Have future state processes been reviewed, both system- and non-system-based, for risk and control implications?
Cybersecurity risk **Objective:** Assess the process and technology controls to protect data in the CTRM and related technology ecosystem	▸ Have the CTRM, key spreadsheets and other sensitive transaction data been secured from both internal and external threats? ▸ Have the risks of a cybersecurity incident been considered for both the ability to transact competitively in markets and the ability to operationally manage transactions across the transaction life cycle?
Full-scope front-to-back-office review **Objective:** Assess design or operational effectiveness of the processes and controls across the transaction life cycle	▸ Do the front, middle and back-office controls reflect industry practices? ▸ Are policies being complied with and are the related controls designed and functioning as management expects?



Construction and capital projects

Each year, organizations allocate significant dollars to build, update, expand or maintain facilities to support business imperatives and operational needs. These capital investments are critical components of an organization's strategic goals and objectives. More often than not, organizations lack the internal capacity and capability to adequately monitor and mitigate the risks impacting their capital program efficiency.

Many factors, both internal and external, can impact the success of a capital program or construction project:

- Macroeconomic risks: fluctuations in raw material prices or the availability of labor, material and equipment can have substantial impacts on schedule and budget performance.
- Capital program governance: limited transparency into capital program performance and integrity issues with data, metrics and reporting can impact the ability to proactively identify and mitigate variances.
- Dynamic programming requirements: competing stakeholder demands, aggressive project completion schedules, changes in the regulatory environment or market changes can impact the ability to effectively manage scope and quality.
- Fraud, waste and abuse: insufficient or ineffective oversight and controls can lead to misappropriation of program or project costs and resources, resulting in cost overruns and schedule slippage.
- Stand-alone systems, processes and controls: limited integration with organizational systems and a lack of real-time data sharing impacts the ability to effectively monitor and control key transactions and accurately report program or project progress.

Management of risks and oversight of capital investments and transactions are critical to achieve capital program objectives.

Potential benefits of performing capital program assessments can help clients address:

Optimized governance and controls
Enhanced transparency and reporting
Proactive risk management
Improved process and control efficiency
Robust compliance monitoring
Real-time auditing of project transactions
Detection and prevention of fraud, waste and abuse
Alignment of capital program and organizational objectives

Audits that have an impact	Key questions to consider
Governance and controls **Objective:** assess the policies, processes, controls, systems and reporting utilized in the management and control of a capital program or construction project	▸ Are the organization's structure, roles and responsibilities, and controls pertaining to segregation of duties monitored? ▸ Are project management processes and controls developed? ▸ Is the steering committee or leadership involved in key project decisions? ▸ Is the proposed project delivery and project risk profile aligned?
Procurement and contracting process **Objective:** assess the adequacy and integrity of the procurement and contracting process	▸ Is the organization in compliance with applicable policies and procedures? ▸ Is there a process to identify potential bidders, solicitation and selection? ▸ Is the contracting strategy in line with the owner's risk profile? ▸ Are controls evaluated during the initial project phase and updated at every phase of the project life cycle?
Contract compliance **Objective:** assess the costs incurred, as well as the processes, methodologies and reporting for a construction project in relation to the applicable contractual requirements	▸ Are compliance of construction costs incurred and invoiced with the contractual provision? ▸ Are change orders documented and approved? ▸ Are the contractor's obligations with regard to oversight, management and control monitored?
Project cost and schedule **Objective:** perform a detailed evaluation to determine whether the costs incurred are properly supported and allowable under the terms and conditions of the contract	▸ Are costs incurred properly supported and allowable under the terms and conditions of the contract? ▸ Are the project schedule, integrity testing including logic and duration, and assessment of critical path changes over time monitored? ▸ Are project delays supportable and justifiable?
Construction processes **Objective:** evaluate the execution of key processes for compliance with operating guidelines and alignment with leading industry practices	▸ Are key processes in compliance with operating guidelines and aligned with leading industry practices? ▸ Are construction payments reviewed and approved? ▸ Are change, quality, budget, schedule and risk management considered and monitored? ▸ Was construction project reporting and closeout complete and accurate?

Cybersecurity

Cybersecurity threats continue to evolve and grow with seemingly no rules or restrictions as to who can unpredictably be attacked. Users no longer need to gain physical access to a facility to cause harm to an organization. They can now gain access through malware or phishing attacks, connections with third parties, new technologies, and other new and evolving paths.

Organizations must focus on IT security and information security to avoid falling victim to cyber threats by developing a cyber audit program that addresses the following:

- The need to mature existing cybersecurity risk management processes
- New and quickly changing technologies
- Complex accounting and regulatory requirements
- Rapidly changing cyber environments requiring changes in policies and procedures
- Increased need for specialized skills and competencies to identify and mitigate risks
- Proactive assessment of new and emerging risks

The digital world offers many benefits and opportunities; however, the risks may have been underestimated.

Cybersecurity

Expanding dependence on technology by the entity
+
Concerns over the maturity of an entity's cyber risk management program
=
Numerous areas of heightened cyber-related risk

Audits that have an impact	Key questions to consider
Governance and risk assessment **Objective:** evaluate the processes and controls over the structure and oversight of the entity's cybersecurity risk management program, including the processes for identifying risks facing the entity	▸ Does the organization's risk management framework address cyber risks? ▸ Does the organization have the specialized skills necessary to identify and constantly evaluate cyber risks?
Security awareness **Objective:** evaluate the processes and controls over the training of users to heighten their awareness and sensitivity to attempts to gain unauthorized physical or logical access to the entity's information and systems	▸ Do training programs exist for employees to better identify unauthorized physical or logical access to the organization's information and systems? ▸ Are these training programs constantly updated for new risks and required to be taken by all employees?
Asset management **Objective:** evaluate the processes and controls over the retention of a comprehensive inventory of technology assets that have the ability to connect the entity's network	▸ Is a comprehensive listing of technology assets maintained? ▸ Do assets have the proper safeguards installed to protect information and identify unauthorized access? ▸ Are assets properly disposed when necessary?

Identity and access management
Objective: evaluate the processes and controls over the identification of authorized users and the addition, modification and deletion of user access to the entity's network
	▸ Are the following processes and controls in place?
	  ▸ Identification of authorized users
	  ▸ Addition, modification and deletion of user access to the entity's systems and applications

Threat management **Objective:** determine if processes and controls are in place to provide early identification of potential or evolving threats against the organization	▸ Are the appropriate processes and controls in place to provide early identification of potential or evolving threats?

Vulnerability management
Objective: determine if processes and controls are in place to address the entity's vulnerabilities
	▸ Do the following processes and controls exist?
	  ▸ Identification of vulnerabilities with the technology assets connected to the entity's network
	  ▸ Implementation of solutions to address the vulnerabilities

Vendor risk management **Objective:** evaluate the processes and controls over third-party service and supply chain vendors	▸ Can the organization provide a listing of all its vendors? ▸ Is the purpose of the relationship with each vendor understood? ▸ Are processes and controls in place to properly procure vendors? ▸ Is a risk assessment performed for each vendor to understand potential vulnerabilities the relationship may cause?
Data classification **Objective:** evaluate the processes and controls over the classification (e.g., public, internal, confidential) of information on the network	▸ Does the classification of information include public, internal and confidential information? ▸ Are the related protection requirements in place and effective?
Security monitoring **Objective:** evaluate the controls over the monitoring of network and application activity	▸ Are processes and controls in place sufficient to detect anomalies and other unusual behavior that may indicate an unauthorized user has gained or is gaining system access?
Incident response **Objective:** evaluate the processes and controls over the response procedures management employs when unusual activity is detected	▸ When unusual activity is detected, does the organization have processes developed to timely identify the incident and properly address the issues? ▸ Do processes exist to address the weakness that led to the incident?

Derivatives and hedging

In August 2017, the Financial Accounting Standards Board (FASB) finalized certain targeted improvements to the hedge accounting model in Accounting Standards Codification 815 (ASC 815), Derivatives and Hedging. The new targeted improvements make hedge accounting easier in some circumstances, allow for new hedging strategies and improve presentation transparency. Early adoption is permitted immediately and certain companies are considering adopting these improvements prior to the mandatory adoption date in 2019. In addition to making hedge accounting easier to apply and allowing for additional hedging strategies, these targeted improvements would change certain aspects of derivatives in hedge accounting relationships financial reporting, processes and controls around derivatives and hedging strategies.

Source: FASB Accounting Standards Update 2017-12, Derivatives and Hedging (Topic 815): Targeted improvements to accounting and hedging activities.

Companies of all sizes face exposure to the risks of fluctuating foreign exchange rates, interest rates and commodity prices. Many utilize derivative instruments to manage the volatility in cash flows and earnings caused by such risks. Derivative instruments and hedge accounting are powerful tools used by companies to mitigate risk, often quite effectively, but they require careful management since derivatives are recognized at fair value and are volatile. In addition, there is extensive and complex accounting literature around their usage, and the use of derivatives is one of the leading causes of material misstatement (in particular ones used in hedge accounting relationships).

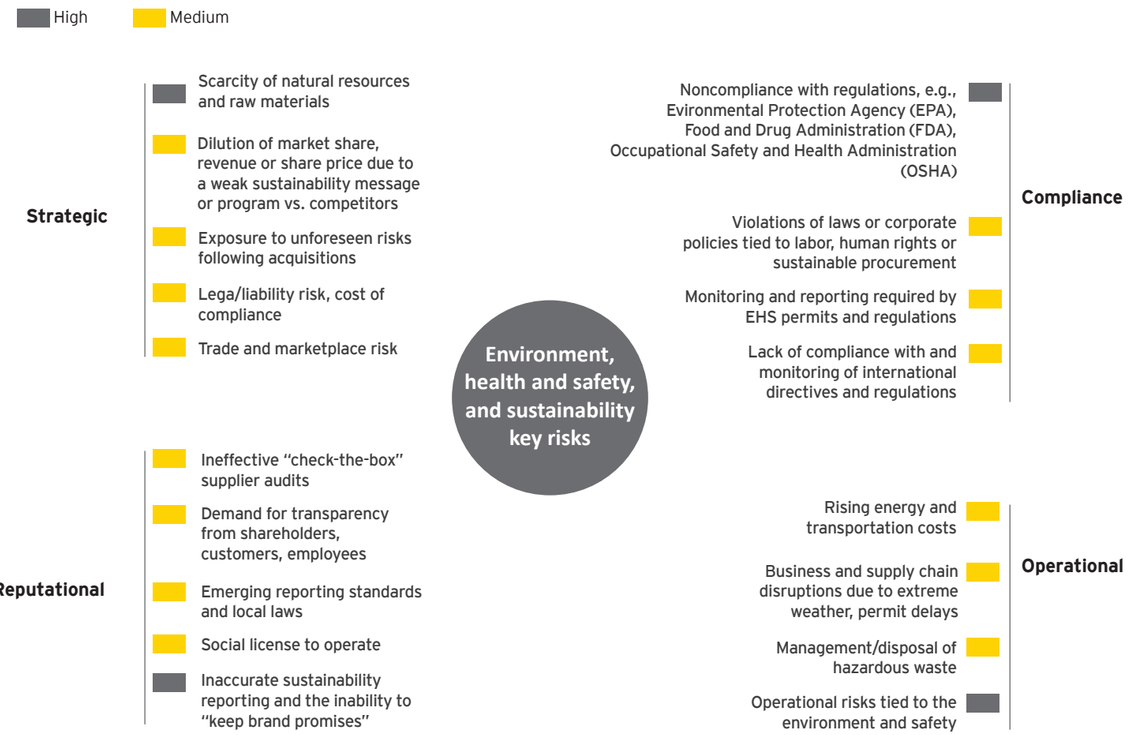
Weak internal control and process environments could place a company at risk in multiple ways. These risks include:

- Failure to comply with corporate policies when creating hedging strategies
- Inadequate risk assessment or inappropriate responses to identified risks
- Improper accounting treatment, including the implementation of FASB's targeted improvements to ASC 815, affecting valuation, reporting and disclosures
- Inadequate trade execution based on the company's policies and procedures
- Failure to manage and oversee relationships with counterparties in hedging transactions
- Lack of appropriate and secure technology to support treasury functions, including authorized access to technologies

Derivatives usage touches multiple functional areas within a company. Robust processes and controls across business functions are needed to manage the risk of material misstatement.

Audits that have an impact	Key questions to consider
Governance and strategy **Objective:** evaluate the organization's strategy for governing the use of derivatives and hedging practices	▸ Do existing policies and procedures have gaps or opportunities to implement leading hedging practices? ▸ Does the board of directors have oversight of derivatives usage policies and procedures? ▸ Do the controls around the cash flow and procurement forecasting processes identify potential gaps in exposure coverage or inconsistencies? ▸ What are the controls in place around the selection process of hedging instruments, including the understanding of roles of key personnel? ▸ Is there a process for how new counterparties are selected and whether the consideration of credit risk is appropriate?
Trade execution, accounting and reporting, technology and regulatory compliance **Objective:** assess the adequacy and effectiveness of processes and controls	▸ Are there processes and approvals in place for executing trades and appropriate limits? ▸ Does cash flow forecasting and exposure data gathering occur? ▸ Are segregation-of-duties controls in place, underlying communication protocols for hedge execution and the subsequent trade confirmation process? ▸ Are controls in place to confirm that derivatives intended to qualify for hedge accounting do so (designation, documentation and effectiveness testing), and have the impacts of FASB's targeted improvements to ASC 815 been assessed? ▸ Are controls over obtaining and challenging fair values of derivatives, including appropriate disclosure of hierarchy levels, implemented and effective? ▸ Is the technology utilized to support treasury functions (e.g., banking workstations, treasury software and Excel spreadsheets) and the interface with the company's accounting and reporting systems adequate? ▸ Are controls in place to bring about ongoing compliance with appropriate regulations?

Environment, health and safety, and sustainability



Environment, health and safety, and sustainability (EHS&S) matters are quickly making their way to the center of how companies strategically think about and address risk. According to The Global Risks Report 2017 of the World Economic Forum, environmental-related risks alone have been featured among the top global risks for the past seven years of the report.[2] The 2017 findings carried this trend forward, with environmental-related risks (e.g., water crises and the failure of climate change mitigation and adaptation) placing in the top five globally in terms of likelihood and impact. What's more, while recent extreme weather events have shone an even brighter light on environmental risks, the broader universe of EHS&S risks continues to expand into social, reputational, health and safety, and other matters. This poses challenges to companies with global footprints with operations that rely on natural resources or create significant environmental and social impacts. Factor in rising demand from stakeholders (e.g., customers, shareholders and others) for transparency regarding how companies are addressing EHS&S risks, and the mandate for thoughtful action becomes even more pressing.

IA plays a key role in helping the company identify and respond to EHS&S risks. In teaming with the EHS, sustainability, legal, compliance and finance functions, IA can play a central role in helping the organization to uncover the EHS&S risks it faces, understand their impacts on the business and operations, and determine steps to address these risks as part of an IA plan or broader enterprise risk management (ERM) program. In doing so, IA can help the company reduce the risk of: damage to the brand, market share, revenue and operations; and penalties from noncompliance.

Audits that have an impact	Key questions to consider
Program planning and execution **Objective:** assess EHS&S programs and processes	▸ Do EHS&S programs and processes address the following? ▸ Governance of EHS regulatory compliance ▸ Identification, compliance and monitoring of regulatory requirements ▸ Internal EHS&S processes and procedures
Regulatory compliance **Objective:** assess regulatory compliance issues or concerns	▸ Are specific regulatory compliance issues or concerns assessed to support the following? ▸ Deep dive into compliance with selected sustainability related regulatory requirements globally, e.g., Environmental Protection Agency (EPA), Occupational Safety and Health Administration (OSHA), Department of Transportation (DOT), the Food and Drug Administration (FDA), and other bodies and regulations
Information Technology **Objective:** assess IT enablement leveraged to support operations and compliance activities	▸ Are data collection processes consistent across business units and geographies? ▸ Are permitting and compliance reported in a timely, accurate and efficient manner? ▸ Are internal reporting and dashboards complete and accurate?
Sustainability reporting **Objective:** assess the controls over the public reporting of non-financial information	▸ Do the controls over the public reporting of non-financial information address the following? ▸ Governance, policies and procedures ▸ Data ▸ Materiality of key performance indicators ▸ Reporting procedures per recognized reporting standards ▸ Content including the report's affirmations and assertions

[2] World Economic Forum, *The Global Risks Report 2017*, 12th edition, 2017, http://www3.weforum.org/docs/GRR17_Report_web.pdf.

General data protection regulation

A little more than 20 years ago, the European Commission (EC) introduced the Data Protection Directive 95/46/EC (the Directive). The Directive defined the meaning of personal data and outlined parameters for collecting and managing personally identifiable information.

Technology advancements have fundamentally altered how organizations collect, use and manage data. In light of this, in 2012 the EC embarked on a process to both update, simplify and bolster privacy regulations, and allow EU residents to resume control over their personal data. The culmination of these efforts is the General Data Protection Regulation (GDPR). Released in 2016, with an effective date of 25 May 2018, the GDPR is an omnibus data protection law that builds upon and expands the Directive. The GDPR is a game changer for organizations. It introduces more stringent and prescriptive data protection compliance requirements, backed by fines of up to 4% of global annual revenue.

The GDPR requires an organization to be able to effectively demonstrate its compliance with the requirements. Adopting a control-based framework that spans an organization's three lines of defense will provide a disciplined and comprehensive approach to address privacy risk and compliance.

As part of the GDPR, there are many privacy risks that companies must navigate, and IA is a strong component of a company's defense against those risks. Organizations should leverage the valuable insights from IA's understanding of key business areas, processes or systems that pose the greatest privacy risk to the organization to conduct deeper, more focused GDPR privacy audits. IA can help a company achieve the principle of accountability that is deeply ingrained in the GDPR.

Source: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Audits that have an impact	Key questions to consider
GDPR program design review **Objective:** perform a review of an organization's GDPR remediation program design or remediation road map to evaluate alignment with the regulation, inputs considered and quality of analysis	▸ What are the key inputs to be considered (e.g., existing capabilities, control framework, business input)? ▸ What was the rationale for the selected focus areas and work streams and detailed remediation tasks? ▸ Are there change management and integration considerations? ▸ Are there details to support the operationalization (e.g., detailed implementation plan, timeline)?
GDPR rapid maturity assessment **Objective:** perform a rapid, high-level readiness assessment of an organization's privacy program	▸ Are there areas where policies, procedures and controls do not align to GDPR regulatory requirements? ▸ What is the organization's maturity rating based on industry-leading practices and recommendations that address people, process and technology enablers?
Focused or deep-dive GDPR gap assessment **Objective:** perform an assessment for a specific business function (e.g., human resources), process (e.g., product development) or systems (e.g., cloud storage), to assess the current controls in place to meet the relevant GDPR requirements	▸ How is personal information collected? ▸ Who within and external to the organization has access to personal data? ▸ How long is personal information retained once it is no longer needed? ▸ Do gaps and inefficiencies exist in the protection of personal data?

Global trade

Global trade consists of complex laws related to the movement of goods, software and technology across borders including customs, export controls, economic sanctions, free-trade agreements, preferential duty savings programs and anti-dumping. Some of these laws are harmonized at a global level, allowing for common processes and controls; others are unique to local jurisdictions.

Companies that are involved in moving goods across borders have inherent global trade risks, but certain factors trigger even greater risk. Global trade risks often arise through inadequate global processes and controls around import and export functions. The nature of a company's products and technology may increase the risk, including heavily regulated military, aerospace, chemical or technology products.

Companies that pay high customs duties or excise taxes or utilize free-trade agreements or other duty reduction techniques to reduce customs duties and taxes also have higher risks. Global trade risks often become more visible as the business changes, through acquisition or divestiture, reorganization, or entry into new markets.

The regulatory environment for global traders is very dynamic, requiring skill sets that cross multiple functions as well as across multiple countries. It can be difficult for internal teams to accurately assess their company's global trade footprint. However, with effective planning, use of subject-matter resources and use of data analytics it is possible for IA teams to more accurately assess their company's level of compliance.

Audits that have an impact	Key questions to consider
Governance **Objective:** assess the organization's existing structure, procedures and policies to assess adequacy and effectiveness	▸ How is your global trade function organized? Centralized or decentralized? Globally, regionally or locally? ▸ Do you have roles specifically assigned to manage import and export processes? ▸ Is management aware of customs and export risks? ▸ Do you have documented policies and procedures on customs and export processes? ▸ Do you have metrics to assess effectiveness of the global trade operations? ▸ What are the defined objectives and strategy of the function?
Import processes **Objective:** assess effectiveness of customs processes and compliance with customs regulations	▸ In which countries do you act as importer of record or declarant for customs purposes? ▸ What are your import volumes by country? And what are your global customs duty costs by country? ▸ Do you realize duty reduction, elimination or deferral by utilizing special trade agreements or through the use of special trade programs (inward or outward processing, bonded warehouses, drawback)? What is the amount of duty avoided or deferred? ▸ Do you conduct and track results of post-entry audits? ▸ Have you been audited or do you have an ongoing dispute with customs authorities in any jurisdiction? ▸ Do you import products from related entities? If yes, do you have intercompany agreements (e.g., a royalty or procurement service agreement) or payment arrangements with these entities? ▸ Do you make any additions to (i.e., assists, commissions, royalties) or deductions (i.e., freight charges, installation charges) from your import value?
Export processes **Objective:** assess effectiveness of export processes and compliance with export control and sanctions regulations	▸ In which countries do you act as the exporter of product or provision of services outside the country? ▸ Do you have transactions with embargoed or sanctioned countries? ▸ Do you sell through distributors or direct to customer, or both? ▸ Do you have a process for screening internal and external partners against various denied party lists? ▸ Do you have an export classification and licensing process? ▸ Does the company have any export-controlled technical data or technology? ▸ Do you export products that are dual-use items controlled for national security?

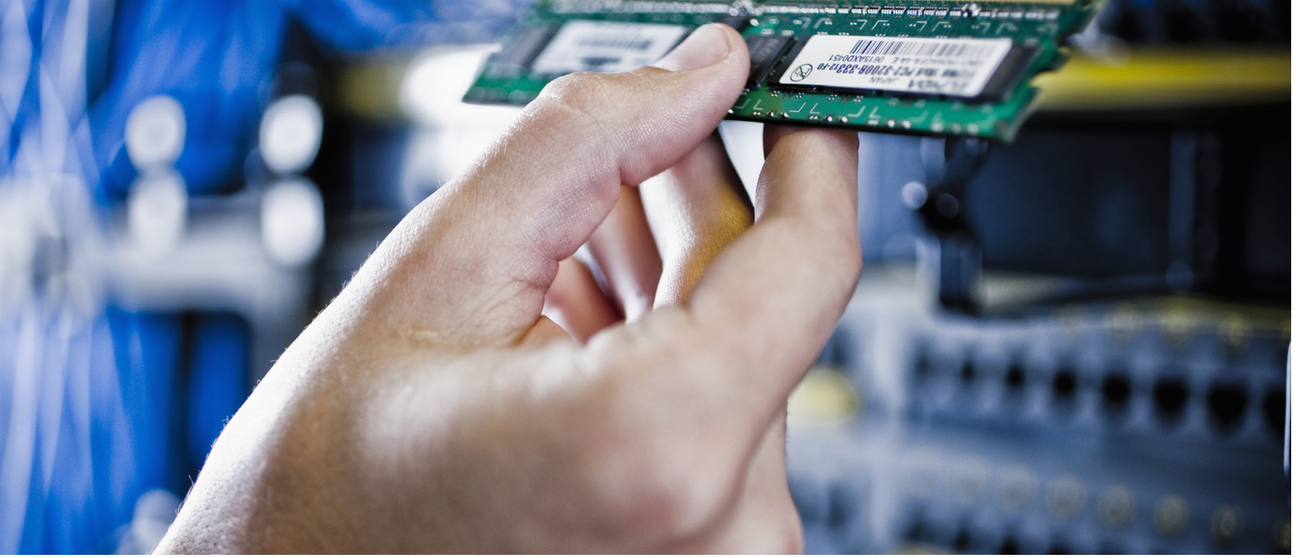
Indirect tax: value-added tax and goods and services tax

While greatly accelerating the pace of all their tax legislation, the world's governments have relied most heavily on indirect taxes for extra revenue. As a result, there is increased risk that taxpayers will be caught unprepared. Some 165 countries operated a value added tax (VAT) at the time of the completion of the International VAT and goods and services tax (GST) Guidelines in 2016, more than twice as many as 25 years before[3]. The failure to comply with a country's indirect tax legislation may result in fines or penalties being imposed by the government. The following tax topics are receiving attention across the enterprise and should be considered during the risk assessment and potentially in the audit plan:

1. **Failure to integrate indirect tax in large global initiatives** – large initiatives such as moves to a shared service environment, implementation of enterprise resource planning (ERP), supply chain or operating model transformation are all examples of initiatives that are critical for indirect tax to be considered up front. Where indirect tax is not considered, tax compliance issues, process inefficiencies or a lack of available data for tax purposes all emerge as concerns for the organization.
2. **Lack of availability of data** – tax is one of the largest consumers of data within any organization. A lack of accurate and accessible transactional data for tax purposes is a top root cause of tax compliance issues, not to mention a driver of inefficiencies and excess cost for the organization.
3. **VAT and other indirect taxes** – transactional taxes continue to create risk due to the fact that, as they are being levied on a transaction-by-transaction basis, they can give rise to non-US indirect tax obligations when there is nexus in a VAT jurisdiction, even where there is no physical presence in the jurisdiction (e.g., US-based software companies with overseas customers or US-based clients selling, purchasing or moving goods outside the US). Moreover, heavy reliance is placed on the accuracy of information in the business to comply. While the tax department can provide direction and guidance related to indirect taxes, the transactions being executed by the business drive compliance, and organizations often do not have the right processes and controls in place to connect the dots between transactions occurring in the business and their indirect tax impact for which the tax department should take responsibility. Indirect tax compliance does not just entail the timely submission of VAT returns and remittance of VAT. It requires a thorough understanding of transactions, business processes and their indirect tax implications and how all that culminates in a VAT or GST return and other reporting obligations. Identifying the right structure in the business to manage VAT and other indirect taxes is a complex issue companies continue to assess.

Audits that have an impact	Key questions to consider
Tax data **Objective:** evaluate the nature, availability and completeness of data and related resources	▸ What data and related resources are the most critical to efficient and effective tax compliance within the organization? ▸ Where does lack of data availability, completeness or accuracy create inefficiencies (from a cost or time standpoint) for the organization? ▸ What is the impact of those inefficiencies, and why do they exist? ▸ How can the gaps be addressed, and what would be the benefits of addressing them?
VAT and GST (indirect taxes) **Objective:** assess the processes in place for effectiveness and efficiency	▸ Is the data needed for indirect tax purposes captured accurately and completely? ▸ Are controls in place to determine if VAT is calculated accurately? ▸ Who is responsible for VAT processes, and do they have the necessary skills to perform compliance activities? ▸ Are there opportunities for cost savings related to VAT?
Tax compliance **Objective:** evaluate the processes and controls related to compliance for design adequacy and operating effectiveness	▸ How efficient is the process to complete data for the tax provision? ▸ Is there global visibility into the process? ▸ Are controls related to compliance designed and operating effectively? ▸ Are there opportunities to increase the efficiency of controls?

[3] OECD (2017); International VAT/GST Guidelines, OECD Publishing, Paris



Insurance risk management

Insurance is constantly changing, causing companies to face uncertainty when answering the following questions:

- Where are the company's insurance dollars going?
- Is the company's insurance program complete?
- Are all risks assumed covered by insurance?
- Are vendors related to insurance risk management providing the right service at the right costs?
- Are there adequate controls in place to confirm that the function is being managed appropriately?

The chief financial officer (CFO) or his or her department typically covers insurance risk management duties, but often there is no dedicated staff. The insurance risk management department exercises good faith when using information provided to them by the insurance community and tends not to perform sufficient due diligence on the material. The insurance risk management function often operates independently within a company and is not formally reviewed or understood.

Companies need to confirm that their assets, liabilities and people are protected and hedged appropriately through insurance. They can do this by:

1. Identifying and validating risk
2. Evaluating risk retention and transfer strategy
3. Assessing claims and management losses
4. Reviewing vendor management
5. Assessing risk management department staffing
6. Reviewing compliance

Insurance risk management key risks — High — Medium

Risk identification and valuation	Not identifying all the essential risks of the business Understanding business operations' contingent risk exposures Over- or undervaluing a risk or the magnitude of the risk frequency
Risk retention or transfer strategy	Over- or undervaluing the retention/limits, leading to inefficient use of insurance dollars Choosing the appropriate risk transfer products or vehicles
Claims management	Lack of data or data integrity may lead to incorrect or delayed claims decisions The decisions (or indecisions) of claims administrators may have a negative financial impact Key controls around data to confirm accuracy and adherence to established claims management processes
Vendor management	Confirm accurate insurance provisions within contracts/agreements Vendor relationships are not monitored, and there is lack of transparency
Risk management department staffing	Roles and responsibilities not clearly defined, documented or sufficient to facilitate accountability Inefficient use of resources and capital to service risk management function
Compliance	The risk of loss resulting from inadequate or failed internal processes, people, systems or external events Failure to comply with regulatory compliance A third party's inability to perform as per contract

Audits that have an impact	Key questions to consider
Insurance program assessment **Objective:** identify gaps in an insurance program structure and department and provide recommendations based on benchmarking of an organization's insurance program	▸ Are limits, retentions and premiums benchmarked with those of peer companies? ▸ Has an insurance coverage adequacy and gap analysis been completed? ▸ Is the insurance risk department operating in accordance with formalized process and controls?
Vendor management **Objective:** review vendor management process, conduct gap analysis and recommend areas for improvement	▸ Are insurance provisions within contracts and agreements accurate? ▸ Do vendor contracts adhere to contract provisions? ▸ Are there opportunities for cost reduction and process efficiency?
Claims management **Objective:** review claims management processes, conduct gap analysis and recommend areas to reduce leakage	▸ Is there a claims cost review completed to identify claims cost savings? ▸ Are losses being managed effectively? ▸ How does the organization determine the reasonableness and appropriateness of outstanding liabilities?
Captive insurance company **Objective:** there are two options as it pertains to captive insurance studies: 1. Conduct a captive feasibility analysis where there is no captive insurance vehicle in place 2. Conduct a captive utilization analysis where a captive insurance vehicle is in place	▸ Are premium transfer pricing and capital structure and loss reserve adequate? ▸ Are there gaps in captive and investment management services? ▸ Are captive taxation and taxation benefit, if applicable, in line with current state and IRS guidelines?

Intellectual property

More than ever before, companies are experiencing first-hand the unprecedented rate of change when it comes to the adoption of new and disruptive technologies. Nearly every company is on the forefront, pioneering in our rapidly changing world. From the C-suite through engineering and beyond, innovation has become the driving force. As companies rapidly move forward they need to ask themselves if they have taken the appropriate steps to identify the intellectual property (IP) they have created and if the appropriate controls are in place to protect and mitigate the potential risks associated with their IP.

There are significant risks associated with IP that are embedded throughout the life cycle and may result in significant economic, financial, competitive and reputational consequences for organizations if they are not properly controlled and managed. Companies must concern themselves with the protection of IP and confirm that the assets are protected and employees have the appropriate knowledge and awareness of their responsibilities and obligation to their employer regarding:

- Confidential Information
- Proprietary Information
- Trade secrets
- Third-party IP
- Innovations
- Trademark
- Copyright
- Software

Intellectual property (IP) risks

High Medium

Sensitivity of information	High	Employees invloved in the generation of IP may inadvertently leak sensitive company information creating a statutory bar date(s) resulting in the loss of IPR
	High	Disclosure of trade secrets leading to exposure of sensitive information resulting in loss of competitive advantage
Employee IP knowledge and awareness	Medium	Lack of employee IP knowledge and awareness leading to the ineffective execution of policies and procedures and the inability to identify, capture and properly protect company IP
Reputational harm	High	Damage to brand or company reputation from the mismanagement and/or lack of protection and exposure of company or third-party IP
Software-open source	Medium	Use of software and code obtained from open source communities with unfavourable terms and conditions can result in the loss of IP and company developed code
Intellectual property	Medium	Inappropriate or unapproved use of third-party IP such as trade secrets and patented technologies (infringement)
	High	Loss of intellectual property rights (IPR) through inappropriate management and protection
Governance and strategy	Medium	IP strategy not aligned to business requirements
	High	Lack of a structured and well-thought-out strategy as an organization develops and leverages IP

Audits that have an impact	Key questions to consider
Governance and risk assessment **Objective:** evaluate the processes and controls over the structure and oversight of the entity's IP management and strategy program	▸ Do the organization's policies and procedures properly address IP risks? ▸ Does the organization have the specialized skills necessary to identify and constantly evaluate IP risks?
Knowledge and awareness **Objective:** evaluate the processes and controls over the training of users to heighten their awareness and sensitivity to attempts to gain unauthorized physical or logical access to the entity's information and systems	▸ Do training programs exist to increase employee knowledge and awareness to better identify IP and understand their obligations and the associated risks? ▸ Are training programs updated to address new risks and legal changes?
Asset and access management **Objective:** evaluate the processes and controls over the identification and inventory of IP owned or used by the organization	▸ Are processes and controls in place to identify newly created or obtained assets? ▸ Is an inventory of assets (e.g., trade secrets) maintained? ▸ Do systems have the proper safeguards to protect against unauthorized access and do they track and record who has accessed them and when?
Third-party risk management **Objective:** evaluate the processes and controls over the use and protection of third-party IP	▸ Can the organization provide a listing of all third-party assets it uses or possesses and the source of the assets? ▸ Does the organization understand the obligation it has to protect third-party IP? ▸ Are processes and controls in place to make certain contractual obligations regarding IP are properly met?
Security monitoring **Objective:** evaluate the processes and controls over the monitoring of network and application activity	▸ Are processes and controls in place sufficient to detect anomalies and other unusual behavior to indicate an unauthorized user has gained or is gaining system access to IP?
Incident response **Objective:** evaluate the processes and controls over the response procedures that management employs when unusual activity is detected	▸ If an incident is identified would an employee know the appropriate person to whom the incident should be reported? ▸ Would an employee know the appropriate method to report the incident to mitigate additional risk?

IT governance

As the business world continues to digitize around the globe and technology platforms become more complex, expectations of IT organizations continue to rise. The role of business executives is evolving too, as they must understand and manage technology and associated risks as part of their core business strategy. The risk of a failed initiative, rising IT costs and concerns about the significant incidents related to IT risk, such as data loss or security breaches, that have been reported in the news are just some of the questions being raised by executives and the board of directors. As a result, business leaders ask that IT professionals provide strategic differentiation through innovative systems, infrastructure technologies and applications with the appropriate level of risk management oversight and a strong control framework.

Complex systems represent complex risk profiles and IT professionals are expected to develop and implement systems and applications under tremendous time pressure. Often times, the risk profiles associated with such complex systems may not be fully understood, or may be underestimated or under-reported. Additionally, the overall IT risk and its impact on the company's operations and potentially the corporate brand may not be fully understood at the C-suite level. Companies should consider adjusting their mindset and approach toward IT risk to address a new normal as the IT risk profile and threat landscape rapidly changes and risks increase. More than ever, there is a need for the board, audit committee, executive management, general counsel and chief risk officer to work alongside IT leaders, including the information security and privacy officers, to fully understand and address the organization's risk exposure, approach and preparedness. Companies should implement a robust IT risk management program that proactively and effectively manages IT, including cyber risks.

It is important that IT functions are able to effectively address the following questions:

- Can management articulate their strategy to identify, mitigate and monitor IT risks to the audit committee?
- How and when is management convinced that it has identified all key IT risks that would prevent the company from achieving its strategic objectives and initiatives?
- How does management monitor the continued effectiveness, longevity and relevance of the IT risk assessment framework, in light of rapidly evolving technologies?

IT internal auditors should stay abreast of technology developments and associated risks and should be proactively involved in implementation projects early on. Only then will internal audit organizations be positioned to bring the required subject-matter knowledge and business insights to provide an objective assessment of how well current IT governance structures and processes are providing direction and monitoring.

Focused reviews and audits of IT systems and risks at the implementation level are effective and impactful ways of helping management mitigate risk.

Audits that have an impact	Key questions to consider
IT risk management strategy **Objective:** assess the robustness of the IT organization's risk management strategy and determine if the risk assessment framework is capable of covering new and complex technologies	▸ How well does IT identify risks? ▸ What actions are taken once a risk is identified? ▸ Are IT risk management processes followed? ▸ Does the IT risk program cover all of IT, including shadow organizations? ▸ Is responsibility for risk coverage clearly defined? ▸ How are IT risks identified, remediated or accepted?
IT governance **Objective:** evaluate the governance framework and structures for the organization to mitigate key IT governance risks	▸ Does the organization have an IT risk assessment framework and does it align with established governance frameworks, e.g., control objectives for information and related technologies (COBIT) and information technology infrastructure library (ITIL) ? ▸ Do formalized processes for governing IT exist? ▸ What can be done to increase business confidence in IT governance? ▸ Are IT governance processes and requirements applicable across all of IT? ▸ Are there formal charters, mandates and responsibilities documented and followed by key steering committees?
IT risk assessment **Objective:** evaluate IT's risk assessment, remediation plans and progress against those plans to address issues noted	▸ Is there a comprehensive risk assessment performed to identify all IT risks? ▸ Is the IT risk assessment process effective? ▸ How can the process be enhanced? ▸ Do remediation plans include enough detail and is progress monitored by management? ▸ Is there a road map to initiate improvements?
Technology enablement **Objective:** assess the need for or use of a governance, risk and compliance software package for effectiveness and reliability	▸ Is a governance, risk and compliance (GRC) software package used within the organization? If so, how effectively is it being used, (e.g., maturity level, use of functionality and risk reporting?)

Lease accounting

In 2016, the Financial Accounting Standards Board (FASB) issued an Accounting Standards Update (ASU) intended to improve financial reporting about leasing transactions. The ASU will take effect for public companies for fiscal years, and interim periods within those fiscal years, beginning after 15 December, 2018. For all other organizations, the ASU becomes effective for fiscal years after 15 December, 2019, and for interim periods within fiscal years beginning after 15 December, 2020.

The new lease accounting standard will require entities to do more than simply reflect lease assets and liabilities for what today are lessee's operating leases. For both lessees and lessors, the new standard will require changes to the policies, processes, controls and IT systems that support lease accounting, marketing and lease procurement, lease administration and tax. Companies may also want to consider the implications for financial statements and metrics as they negotiate contracts that are, or may contain, leases. These activities will require involvement from a variety of departments throughout the organization. The new standard also requires certain judgments and estimates that will necessitate additional or expanded management review controls.

Following are some of the significant changes:

Accounting and finance: Accounting policy updates will be required along with timely dissemination of these updates throughout the organization. Management will need to make more estimates and judgments than under current guidance. To evaluate the effects of these changes, management must identify areas for which key judgments and estimates will be required.

Business processes: Management will need to reassess the entity's current processes and controls for tracking new, existing and modified contracts that are or contain a lease. In addition, key judgments, processes and controls are necessary to identify when certain reassessments are required (e.g., a lessee's reassessment of lease payments, lease term, change in the amount that the lessee is probable of paying under a residual value guarantee).

Tax: A lessee's recognition of "right-of-use" assets and lease liabilities on its balance sheet may affect its deferred tax calculations. Companies may need to revise their processes and data collection tools to capture new deferred tax assets and liabilities, including their assessment of the recoverability of deferred tax assets.

IT: Applications may need to be modified. As a result of implementing the new standard (including its disclosure requirements), entities may need new data points that are not currently captured in any IT system. For example, an entity may need to enhance its systems and processes to allocate contract consideration if lease and non-lease components are identified.

Legal: Enhanced communication between the legal and accounting departments may be required. At a minimum, the legal department will need to understand the accounting implications of key lease terms in the standard (e.g., the definition of a lease, the identification of lease and non-lease components and variable lease payments).

Human resources: If the standard's effect on the entity's arrangements is significant, the entity may need to allocate additional resources to the implementation effort. The entity will also need to assess whether existing personnel are sufficiently trained and supervised to implement the standard.

Source: FASB Accounting Standard Update- No 2016-02, February 2016

Considerations for evaluating the organizational effect of the lease guidance

Audits that have an impact	Key questions to consider
Lease contract data administration **Objective:** Assess current state for the lease contract data administration, IT systems, policies and business controls	▸ How does management collect information about leases and what IT systems or processes are in place? ▸ What is the anticipated effect of the new standard on the company's businesses, processes and financial reporting? ▸ What are the company's plans for communicating with stakeholders for changes in entity's accounting and reporting policies, IT systems and business processes to meet the new requirements? ▸ If the entity operates in a decentralized environment and has leases that are subject to different processes at different locations, how does management plan to analyze them and determine whether any new processes, internal controls or systems are necessary?

Controls assessment
Objective: Identify and assess risks of material misstatement in a contract that is or contains a lease
	▸ What are the controls implemented by management for areas of misstatements such as:
	  ▸ completeness of the population of contracts that is a lease or contains a lease
	  ▸ separation of lease and non-lease components and allocation of contract consideration
	  ▸ determination of the lease term, including the commencement date of the lease
	  ▸ lease classification, modifications and appropriate disclosures
	▸ What is the source of the information (e.g., contract) used to account for the lease?
	▸ How do you make sure that the source information is (1) correctly entered into the IT application and (2) completely and correctly downloaded (e.g., from an IT application) or manually input into an end-user computing tool (e.g., Excel)?
	▸ How do you make sure that any changes to, or manipulation of, the data in Excel are complete, accurate and appropriate?

Mobile computing

Advanced mobile devices have had a deep and transformational role in the way organizations support all aspects of their business operations and provide customers real-time information on the go. Over the past 15 years, there has been a massive influx of mobile devices into organizations through employees using their own devices at work and accessing corporate data or organizations replacing old mobile fleets and giving employees the latest devices. Clearly, consumerization has had an irreversible impact on enterprise mobility.

Notably, mobile devices were designed and marketed as means of voice and, data communications for individuals and consumers, not necessarily for business use. Advanced ease of use and convenient features, not security or data safeguarding, were the underlying reasons for the rapid adoption and popularity of such devices by individuals. The modern mobile device sits at the crossroads of personal use and highly sensitive business information. As the old saying goes, the chain is only as strong as its weakest link and business data residing on mobile devices is no exception.

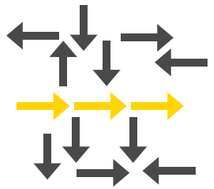
This technology allows employees to access and distribute organizational information anytime, anywhere, increasing the efficiency and productivity of employees. However, this same access and distribution capability also introduces significant risks. For example, increased usage of public Wi-Fi networks by business users exposes sensitive information to complete strangers, if not properly encrypted. As with any technological advancement, an organization must first identify and address the risks and then monitor the environment to better understand the impact mobility has on the corporate risk profile.

Mobile computing risks to be considered include:

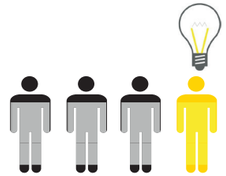
- Potential loss or leakage of important and sensitive business information
- Security challenges given the range of devices, operating systems, and firmware limitations and vulnerabilities
- Theft of mobile device, given the considerable magnitude of data they store
- Compliance with state, federal and international privacy regulations that vary from one jurisdiction to another as employees travel with mobile devices
- Navigation of the gray line on privacy and monitoring between personal and company use of the device

Organizations must learn to harness the power of mobile computing while minimizing and mitigating their risks and IA will play a vital role in the discussion.

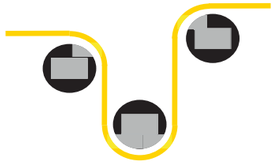
What are the benefits of mobile computing?



Improving productivity: improving employee productivity by extending reach of existing apps, e.g., mobile time sheets



Enabling employees: enabling employees via new or more efficient business processes. processes, e.g., mobile field support, mobile CRM



Enabling new business: targeting new markets or offering clients new products or services, e.g., mobile commerce apps

Audits that have an impact	Key questions to consider
Device configuration **Objective:** identify risks in mobile device settings and vulnerabilities	▸ Does the organization have policies, standards and device management strategies? Are they centralized or regional? ▸ Are security and configuration settings established and implemented for the mobile devices and are they enforced through approved policies? ▸ Are data management processes for lost or stolen devices established and implemented and are communications, forensic and legal defense strategies in place? ▸ Do end-user devices use any unauthorized or unapproved applications by jail-breaking? ▸ Does the network architecture support end-user device activation and usage? ▸ Do security policies and segregation of work and private data spaces exist pertaining to third parties?
Mobile application black box **Objective:** use front-end and black box testing techniques in an attempt to exploit the vulnerabilities identified in mobile applications	▸ Do vulnerabilities, business logic and authorization flaws exist? ▸ Does the organization use non-intrusive analysis and usage of tools (e.g., cross-site scripting, cross-site request forgery and directory structure)? ▸ Are application configurations, mapping of application functionality and permissions in place? ▸ Does the organization utilize device-based mobile application vulnerability exploitation? ▸ Are encryption mechanisms in place?

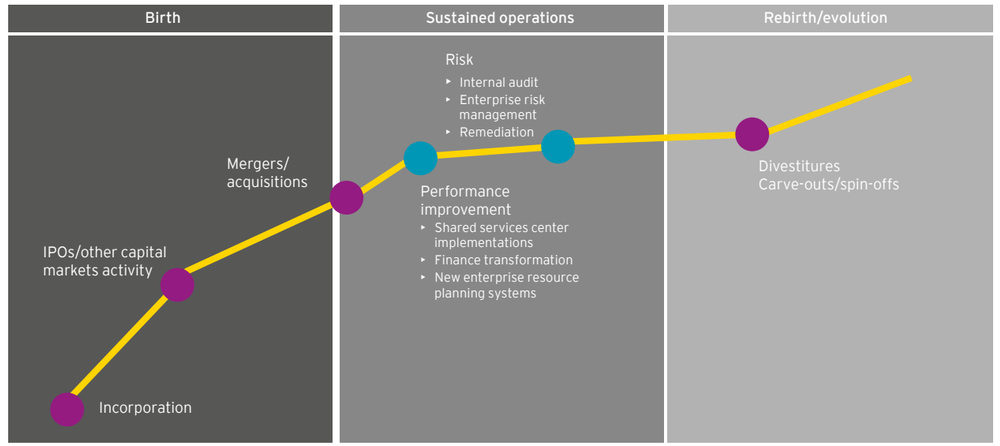
Mobile application gray box
Objective: prioritize high-risk areas of the code, maximize code coverage and identify root cause of identified vulnerabilities
	▸ Does the organization undertake reconnaissance and application mapping, including:
	  ▸ Administrative interfaces
	  ▸ Multi-part forms
	  ▸ Transmission of sensitive information
	  ▸ Use of mobile protocols
	  ▸ Visual modeling of the application and definition of trust boundaries
	▸ Does the organization utilize code analysis and scan, including permission analysis, control flow analysis and data flow analysis?

Policy and governance

Policies and procedures are core to an organization's control environment. When they are clear, consistent and current, they strengthen not only the control function but also the relationships among management, employees and investors. They act as the glue that binds and aligns cross-functional and geographically dispersed operations. However, they often fall short of these goals, reducing an organization's efficiency and effectiveness and increasing its risks. Moreover, finance and governance professionals consistently rank accounting practices and policies as one of their top concerns. To manage these risks, management must be proactive.

A number of triggers can turn a lingering worry about the state of your policies and governance processes into a critical need for immediate diagnosis and repair. The most common triggers are company-specific, typically involving changes to an organization's operating model. They can also stem from transformational events — everything from initial public offerings (IPOs) and restructurings to divestitures, mergers and acquisitions. A lack of standardized policies may cause global companies to experience weak controls and missed reporting deadlines. Another set of triggers is industry-specific, encompassing business as usual, regulatory changes and shifts in the business environment that will affect your policies and practices, either immediately or over time. A further trigger is staff frustration with inconsistent policies that frequently occurs with large, geographically dispersed and decentralized organizations.

When to focus: all across the corporate life cycle



Major transactions: Driven by changes in capital structure, new regulatory oversight and other major organizational changes

Remediation or improvement projects: Driven by a need to remedy risk events or improve efficiency in organizations: these occur in any phase of the corporate life cycle

Businrftess as usual: Driven by changes in accounting standards, regulations and business processes throughout the corporate life cycle

Audits that have an impact	Key questions to consider
Policy governance **Objective:** assess the organization's existing processes to create, revise and decommission policies	▸ Does management have issues related to the organization's current state policy governance process? ▸ Does organizational management have key documents, data and information related to the existing policy governance process? ▸ Are the organization's current policy governance processes sufficient at the enterprise or corporate functional level? ▸ Does the organization prioritize the steps needed to revise the accounting policy framework and any impacted policies?
Policy library completeness **Objective:** identify areas of improvement within an organization's existing policy library	▸ Are accounting, finance, treasury, human resources, tax and risk policies up to date? ▸ Are all organization business processes and reporting requirements captured in the policy library? ▸ Does the organization utilize leading practices for their policies from a format and layout perspective? ▸ Are organizational policies user-friendly (i.e., use plain English and relevant examples)? ▸ Do findings from policy review highlight gaps and opportunities for improvement?
Deployment readiness **Objective:** assess the organization's ability to effectively deploy policy and procedure changes to personnel	▸ Do existing platforms deploy policies and procedures to the organization to identify improvement opportunities? ▸ Do policy training deployment methods and frequency align with similarly situated companies? ▸ Are findings summarized from the review, highlighting gaps and opportunities for improvement?

Program risk management

Program complexity is growing at a rate faster than companies can adapt, and investment portfolios are being expanded to keep up with emerging trends. As companies continue to look for ways to increase efficiency and reduce costs, they are undertaking significant initiatives to redesign and standardize business processes, reduce costs and improve productivity. These large initiatives frequently end up being technology-related projects.

Risks associated with program management are embedded throughout the life cycle and may result in significant economic, financial, regulatory and reputational consequences for organizations if they are not properly controlled and managed. The margin for error is small, and the environment in which transformation needs to happen continues to increase in complexity. However, many companies have not demonstrated the ability to adapt their approach, processes, governance, controls and tools to address the complexity of these programs.

Programmatic risks are increased due to the complexity in business processes and the emerging technology landscape such as cloud, robotics, mobile and new digital technologies. Internal audit can provide forward-looking insights by proactively assessing the enterprise portfolio, program and project risks to determine the key threat risks to mitigate and opportunity risks to pursue and leverage. These capabilities are essential in being more competitive in the marketplace by improving the speed to business value realization considering the programmatic and operating risk landscape.

Drivers of disappointing results:

Complexity:
- Relentless speed of change
- Industry convergence and regulatory change
- Highly complex projects that are the drivers of benefits, but carry the highest risk profile

Constraints:
- Limited capital to achieve strategic objectives
- Fixed or fewer resources to deliver value
- Lack of forward-looking view on risk

Results:
- Increased project cost and time
- Decreased benefits realization
- Lengthened time and unplanned cost allocations to achieve benefits
- Misaligned internal control environment

Audits that have an impact	Key questions to consider
Project management methodology **Objective:** assess the program management methodology	▸ Has the program methodology and governance framework been established including planning and execution approach, the right team composition, monitoring and communication protocols? ▸ Have controls been included in the methodology to deliver the project on time and on budget? ▸ Is there a process to measure whether intended benefits were achieved?
Project and program execution **Objective:** assess the execution of the program and project management	▸ Is there adherence to the project management methodology? ▸ Is the project management office monitoring the project against the timeline? ▸ Is there adequate communication among the project team members?
Portfolio risk review **Objective:** assess the governance framework	▸ Has a robust portfolio management process, including demand planning, project prioritization, funding and decision-making process been developed and implemented? ▸ Is the risk assessment approach comprehensive? And does it include a process to mitigate risks? ▸ Is there a process in place to respond to changing corporate objectives?
Process redesign review **Objective:** assess processes and controls to mitigate risks associated with process redesign	▸ Have project team member roles been defined and communicated? ▸ Is there an internal control work stream focused on identifying and mitigating risks? ▸ Is the project team using automation and system controls to their full advantage?
Shared service center review **Objective:** assess processes and controls around transition to a shared service center	▸ Have processes been developed and implemented to make the transition to a shared service center? ▸ Has the project team validated the control framework and technology utilized to facilitate the transition?

Revenue recognition

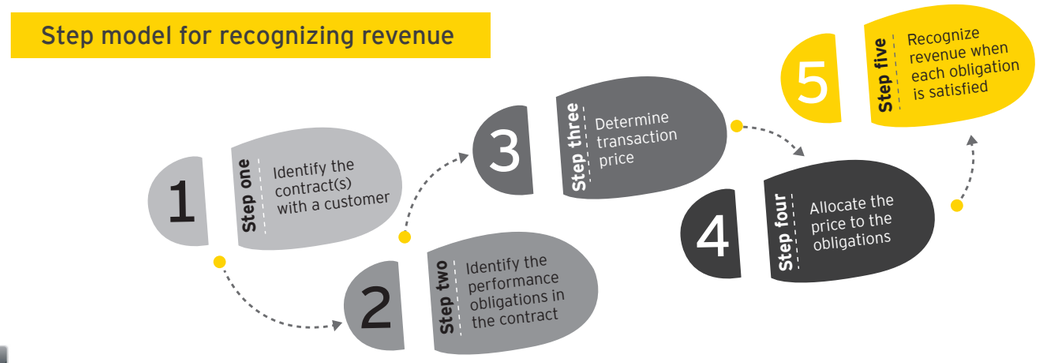
Companies have been hearing about the new revenue recognition standard for years, and as the effective date approaches, they are evaluating the state of their implementation efforts. Many companies were relieved when the effective date was deferred to 2018 for calendar-year public entities, but now they are ensuring they have the ability to get things under control in a limited amount of time.

Many organizations are finding that implementing the new revenue recognition standard issued by the Financial Accounting Standards Board (FASB) requires more effort than they anticipated. With just a few months until the standard's effective date, public companies likely need to accelerate their work to complete their implementation.

A great deal is on the line, since the new standard could affect investor perceptions of company performance. Now is the time to focus sharply on continuing to prepare for the new revenue recognition standard. The truth is that the difference between complying on time and falling behind is going to be razor thin for some organizations.

But the good news is that amidst all this change, there may be opportunities. In the case of revenue recognition, a thoughtful implementation may produce new efficiencies, enhanced systems, processes and controls, and more robust order to cash automation. The benefits could improve a company's business and not just transform its accounting.

The core principle of the new standard is to recognize revenue to depict the transfer of promised goods or services to customers in an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services. Companies will need to exercise judgment when considering the terms of the contract(s) and all of the facts and circumstances, including implied contract terms. They will also have to apply the requirements of the standard consistently to contracts with similar characteristics and in similar circumstances.



Audits that have an impact	Key questions to consider
Revenue recognition readiness assessment **Objective:** assess current state for the new standard implementation efforts and evaluate readiness relative to people (organizational), processes, systems and control considerations using agreed criteria	▸ What is the anticipated effect on the company's businesses, processes and financial reporting? ▸ What is the process to monitor and consider organization readiness relative to people, process and technology? ▸ Have company personnel been trained? ▸ What are the company's plans for communicating with stakeholders?
Revenue accounting process review **Objective:** identify areas of improvement in current revenue accounting process for complying with the requirements of the new standard	▸ What are some important challenges and opportunities with the current state revenue accounting processes that could represent areas for potential improvement in implementing the new standard (e.g., manual workarounds, spreadsheet tracking separate from transaction processing systems)? ▸ What is the cycle time for the current state process from the time of deal closure through the setup of the appropriate revenue accounting approaches required for the financial reporting process (sometimes referred to as the "revenue allocation" process)? ▸ Are common processes executed for operations (e.g., sales, fulfillment and invoicing) and revenue recognition? Are these operations centralized in a shared service center, center of excellence (COE) or distributed? ▸ Are data objects (e.g., products, materials and customers) managed via a master data management solution or manual processes?

Controls assessment
Objective: identify and assess risks of material misstatement related to adoption
	▸ What are the controls implemented by management for the period of adoption related to:
	  ▸ Revenue stream identification and scoping?
	  ▸ Contract analysis?
	  ▸ Accounting policies (for all revenue streams even if no transition effect)?
	  ▸ Amounts disclosed in the financial statements?
	▸ How are significant changes communicated and reported for Sarbanes Oxley (SOX) Section 302 disclosures for material modifications or omissions?

Risk culture

Risk culture is the behavior in an organization that influences the management of risk. Risk culture connects the broader culture of an organization with its risk-taking and risk control activities. Regulators globally have highlighted that culture has risen higher on their agenda as part of addressing what they perceive to be major conduct and control failures that could have a systemic impact if not addressed properly. This creates practical challenges in implementation, and mandated time scales may require short-term, tactical solutions.

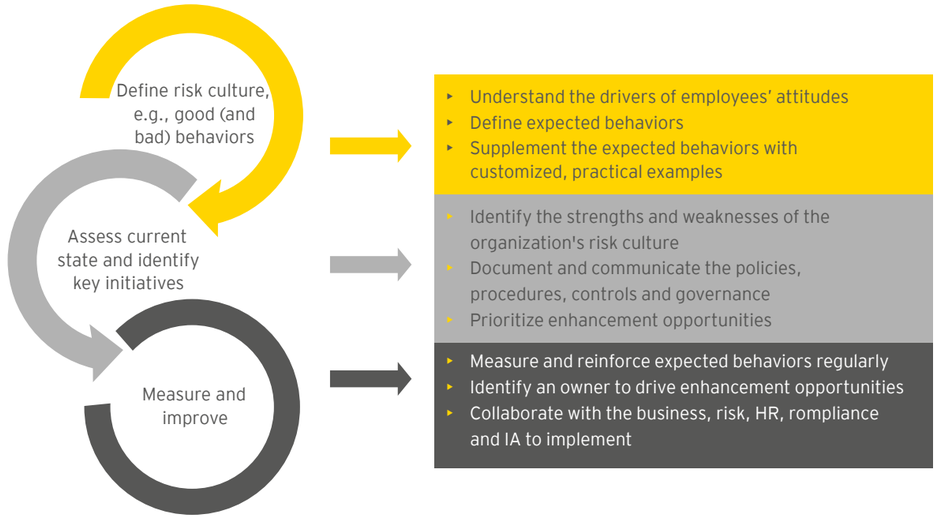
Enhancing the behaviors of an organization requires careful consideration of other aspects of the risk governance model. To achieve a sound risk culture, organizations need to express guiding risk culture principles and articulate the desired behaviors individuals are expected to emulate. Risk culture is not something that can be designed and executed; it must be proactive, and everyone — board, management and individuals — must understand that they have a responsibility for their own risk behavior and that they should proactively report the unacceptable behavior of others.

A shift from a tone at the top corporate culture to tone in the middle and at the bottom is needed to present a clear view of desired risk behaviors. Organizations should focus on having forward-looking metrics in place to measure both financial and nonfinancial risks. Risk appetite should be consistent with the firm's business strategy and embedded into decision-making.

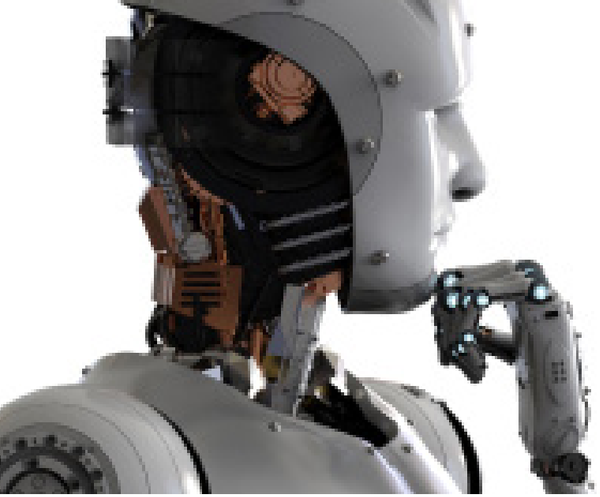
Organizations should also consider a shift from a strong focus on financial incentives only, to include nonfinancial incentives. Talent management, including recruiting, onboarding and exiting, should be designed so that employees share the firm's values and desired risk culture.

The alignment of an organization's board, leadership team and business units, globally, around a common understanding of risk culture is crucial to changing, monitoring and managing behavior. Risk management, the board, senior management and IA all have a role to play in developing and maintaining the desired risk culture.

How can an organization improve its risk culture?



Audits that have an impact	Key questions to consider
Risk culture framework **Objective:** assess if the organization has the policies, processes and incentives in place to support its mission, vision and strategic objectives	▸ Are the organization's mission, vision and values clearly aligned and communicated throughout the organization? ▸ Do corporate values consider desired behaviors (good and bad), are they communicated across the organization, and are they well-understood at the top, middle and bottom of the organization?
Risk culture assessment **Objective:** assess the organization's overall risk culture including leadership actions and incentives; identify and evaluate gaps between desired and actual behaviors, determine root cause and provide recommendations	▸ Is the message consistent, well-understood and accepted throughout the organization? Is it reinforced periodically? ▸ Is the board periodically apprised of the results of management's assessment of the risk culture framework? ▸ Are metrics and incentives designed to drive the expected behavior? ▸ Does management periodically assess the organization's acceptance of and alignment to the mission, vision and values? ▸ Is assessing culture driven by compliance with regulatory expectations or a genuine desire to understand "how we do what we do"? ▸ Is broad risk training carried out across the organization? ▸ Is risk appetite appropriately factored into the organization's risk culture? ▸ How are compensation and risk-taking behaviors linked? ▸ Does the culture support risk transparency and enable concerns to be voiced? ▸ How are whistle-blowers treated? ▸ What regulatory requirements are currently imposed? What is likely to influence regulators or boards in setting desired risk culture?



Robotic process automation

While robotics helps companies automate manual labor within warehouse operations, software robotics, or robotic process automation (RPA) promises to transform the cost, efficiency and quality of executing many of the back-office and customer-facing processes that businesses rely on people to perform. However, this automation does not come without its own set of risks. IA should be involved from the beginning and must be able to identify and advise management on how to mitigate risks quickly as technology continues to rapidly change.

More than one of the issues outlined below is often present or linked, creating a significant multiplier effect. It takes sufficient forethought or outside help to mitigate these issues. Unfortunately, if more than one of these issues occurs – which is common – there's a significant multiplier effect that can lead to loss of belief in RPA or cause the project to stop.Whether an organization is embarking on its RPA journey or is already well on its way, it is likely that RPA will become an integral part of key business processes. It is vital for an organization to establish an RPA strategy that includes comprehensive governance, risk and control practices, and IA can bring business, risk and internal control insights to that strategy.

Organizations may bring in IA after implementation to assess how well the process and controls are operating but what they fail to understand is the value IA can provide before, during and after RPA implementation. IA can help management navigate each stage of RPA implementation by providing an independent evaluation and strategic advice. The financial and reputational implications of waiting to act and getting it wrong are steep. IA can help chart a course for success.

The below risks and controls should be considered by an organization's internal audit department when developing an RPA risk analysis and audit program:

1. A lack of robotics governance can lead to ineffective and inefficient process automation and an inability to support and meet business requirements.
2. Robotics access management is ineffectively managed leading to the compromise of systems, applications and their associated data.
3. Process automation requirements are not accurately identified and documented leading to robotics developments that do not meet business needs or support the business/IT strategy, resulting in a negative impact on business processes and financials.
4. Robotics implementations are not appropriately designed and tested, leading to requirements not being met or a negative impact on production systems, resulting in a negative impact on the business and financial losses.
5. Automation problems are not identified in a timely manner and managed, leading to a delay in their resolution and resulting in a negative impact to business processes.
6. Risks are not effectively mitigated for robotics vendor relationship and outsourced services, leading to financial and reputation exposure.

Audits that have an impact	Key questions to consider

Governance
Objective: assess whether a robotics governance framework has been designed to address key organization risks and if it provides a definition of the oversight required to determine if support is aligned to business objectives
	▸ Is a governance framework around the use of robotics defined and maintained?
	▸ Does the governance framework include the following?
	  ▸ Leadership
	  ▸ Roles and responsibilities
	  ▸ Information requirements
	  ▸ Processes
	▸ Are relevant components of change management including organizational, process and technical aspects included in the governance framework?
	▸ Do processes exist to manage the implementation, testing and support requirements for robotics across the organization?
	▸ Are robotics change and development needs properly documented and mapped to business needs?
	▸ Are automation problems and errors continually evaluated and corrected?

Investments **Objective:** assess whether the organization has defined key performance indicators with the ability to deploy suitable monitoring related to robotics process governance	▸ Are robotics investment decisions properly evaluated, approved and prioritized? ▸ Has the company defined approved robotics vendors? ▸ Do the organization's measurements include regulatory and legal objectives, return-on-investment (ROI) and robotics performance?
User access **Objective:** evaluate the organization's strategy to determine if it defines 1) how access is provisioned to robotics capabilities, 2) how the organization protects its robotics assets, and 3) the method the organization uses to determine its security risks related to the use of robotics	▸ Does the organization have a comprehensive strategy to protect its robotic assets? ▸ Are controls in place to prevent unauthorized users from accessing the robots? ▸ Has the organization developed an access provisioning or deprovisioning strategy that allows robots to interact with IT production systems in a controlled manner?

Social media

Social media creates a powerful marketing tool for organizations to build greater awareness of their brands, create customer loyalty and increase efficiencies and connectivity between corporate employees and their respective customer base. The speed, spontaneity and deep penetration of social media into routine and daily business operations have transformed the relationship between companies and their customers, employees, suppliers and regulators.

Companies have taken advantage of social media to:

- Strengthen their brand
- Build customer loyalty
- Grow market share
- Increase efficiencies in their supply chains

Lack of a robust and comprehensive social media strategy gives rise to potentially significant and unforeseen business risk. Companies should consider various organizational and cultural aspects of their social media usage along with technology platforms and infrastructure as they seek to mitigate their risks.

Without a social media strategy in place the following risks may arise:

- Inadvertent leakage of confidential information by company employees
- Intentional transmission and distribution of confidential information by an external party
- Brand and reputational damage
- Greater risk of hacking or fake executive accounts across social media platforms
- Greater risk of viruses, malware and phishing
- Employee improper use or misuse of social media platforms
- Employee payments to external parties via social media platforms

A robust social media strategy should:

- Align social media use to organizational strategies and corporate values
- Develop, execute and communicate social media compliance directives to employees
- Rapidly identify, mitigate and monitor current and emerging risks due to the constantly changing IT and social media environment
- Protect company and customer data and reputation
- Quickly respond to social media incidents
- Monitor information disclosed by employees through social media

Internal audits of social media are effective and impactful ways of helping management mitigate risk.

Audits that have an impact	Key questions to consider
Risk assessment **Objective:** evaluate the risk assessment methodology and framework pertaining to social media; review the social media activities that create the highest levels of risk exposure	▸ Has the organization developed a comprehensive social media strategy? ▸ Has the organization established a methodology and framework pertaining to social media? ▸ Are the organization's risk management and regulatory compliance expectations effectively communicated by management and well-understood by employees?

Governance
Objective: evaluate social media policies and procedures, including a review against leading practices; identify gaps or weaknesses in the policies and procedures
	▸ Has the organization established social media policies and procedures that address:
	  ▸ Strategy alignment to operations and values
	  ▸ Governance structure and controls
	  ▸ Employee and vendor compliance
	  ▸ The appropriate level of security
	  ▸ Key performance indicators
	  ▸ Licensing

Operations **Objective:** assess robustness of business integration and identify gaps in alignment between business operations and social media	▸ Has the organization effectively integrated business and social media? ▸ Are employee activities evaluated and monitored against social media policies and procedures? ▸ Are appropriate tools and infrastructure in place to monitor employee activity on social media? ▸ Is the policy effectively communicated to employees? ▸ Does the organization provide training and assess employee awareness of social media policies and procedures?

Supply chain

Supply chain is the organizational strategy to create competitive advantage by reducing operating costs, improving customer service levels, reducing inventory, better managing risks and increasing agility. The functions that reside within an organization's supply chain operations are research and design (R&D) and engineering, sales and operations planning, sourcing and procurement, manufacturing operations, logistics, and after-sales service. Many organizations are searching for ways to sustain growth by improving margins in developed markets, and may also be seeking growth opportunities in emerging markets. This increases the demands placed on an organization's supply chain.

By placing these pressures on supply chain functions in an unpredictable economy, organizations often turn their focus to improving sales and operations planning processes, sourcing and supplier management, manufacturing and logistics. Within this setting, the following risks can arise:

- A lack of integration among sales demand, supply and production, causing a disconnect between what is produced and customer demand
- Conflicts of interest, anti-corruption, fraud, undiversified supply base, lack of supplier capabilities, poor contract management with suppliers, regulatory compliance issues and failure to identify low-cost suppliers within procurement processes
- A lack of consideration of import and export regulations and tariffs
- Operational inefficiencies and productivity losses
- Environmental Health and Safety (EH&S) risks caused by evolving requirements

Audits that have an impact	Key questions to consider
Supplier risk management **Objective:** evaluate the organization's policies and application of policies to manage supplier relations and reduce supplier risk	▸ Does the organization have established policies, processes and internal controls in place to evaluate the risk of global suppliers? ▸ How are suppliers selected and onboarded? ▸ Is there consistency in the application of the supplier risk management processes across the organization? ▸ Is there a standard supplier scorecard for direct materials suppliers? ▸ Do processes and controls exist to evaluate suppliers for direct and indirect purchases?
Transportation and logistics **Objective:** evaluate the organization's strategies and policies to mitigate transportation risk and identify cost savings opportunities	▸ Are there monitoring and management processes in place for transportation and logistics expenses? ▸ Are there opportunities to reduce transportation and logistics costs? ▸ Do service level agreements (SLA) exist with vendors and are they monitored on a regular basis? ▸ Does the organization properly understand and monitor regulations?
Sales and operations planning **Objective:** evaluate the organization's strategy and sustainability for aligning supply chain, operations and sales	▸ Are formal policies and procedures to integrate sales, supply chain and operations documented and communicated? ▸ Are sales, supply chain and operations processes integrated across the organization to meet customer demand forecasts? ▸ How are demand and supply planning executed? ▸ Are there high levels of shortages for some materials
Contract management **Objective:** evaluate the organization's strategy, ability to set up contracts with suppliers and customers, and monitor contract compliance	▸ Does the organization have processes in place to monitor compliance with contracts both internally and externally? ▸ Are pricing and discounts on purchase orders accurate and in line with the contract? ▸ Are strong controls in place to make sure contracts initially receive appropriate approvals and any changes are approved timely? ▸ Is compliance with contract terms and conditions monitored and enforced?
Waste **Objective:** evaluate the organization's strategy and ability to monitor, dispose of and reduce waste	▸ Does the organization properly monitor waste across its facilities? ▸ Is waste data being received from facilities complete and accurate? ▸ Are waste reduction procedures in place? ▸ Does the organization have defined waste metrics it monitors on a regular basis?

Supply chain *(continued)*

Audits that have an impact	Key questions to consider
New product launch **Objective:** assess the new product development (NPD) process and procedures for effectiveness	▸ Are failure modes and effects analyses (FMEA) performed during the NPD process? Is there a feedback loop in place so that FMEAs are updated? ▸ Is the current spend on research and development, and NPD activities understood? ▸ At what stage of the NPD process do sourcing and procurement, manufacturing, and quality become involved? ▸ Have there been recent product recalls, and how were those managed? ▸ To what extent have enterprise software solutions been deployed to support NPD?
Asset reliability and total productive maintenance **Objective:** evaluate strategy and practices regarding asset reliability and maintenance	▸ Is an enterprise level asset reliability strategy documented? ▸ Is the workforce involved in autonomous maintenance? ▸ What predictive maintenance techniques are used? ▸ Is a computerized maintenance management system (CMMS) in place to support maintenance? Is the enterprise software used to its fullest extent? ▸ Is the consumption rate of spares for equipment used to plan preventive maintenance work? ▸ Do standard equipment commissioning and decommissioning processes exist?
Spare parts and service management **Objective:** assess the approach to spare parts and service management	▸ Are spare parts and service management managed by a third party or the original equipment manufacturer (OEM)? ▸ Is service customer segmentation performed? ▸ Are spare parts planned and procured via their own process or together with regular production parts? ▸ What key performance indicators (KPIs) are used to measure service management, and how are those used to improve service and spare parts performance?

Audits that have an impact	Key questions to consider

Quality
Objective: evaluate the effectiveness and efficiency of the organization's approach to quality
	▸ How well-understood and documented are product and process specifications?
	▸ Have there been recent product recalls and how were those managed?
	▸ What are some of the root-cause identification techniques in place?
	▸ Are quality KPIs standard across the enterprise?
	▸ Do enterprise systems gather non-conformance data?
	▸ What is the portion of overall quality costs incurred in each of the following?
	  ▸ Process failure
	  ▸ Appraisal and inspection
	  ▸ Prevention

Inventory management **Objective:** assess inventory management practices	▸ What are levels of slow moving, obsolete, damaged or lost inventory? ▸ How is inventory planned? ▸ How frequently are physical counts performed? ▸ How do the inventory turns compare with those of peers in the sector? ▸ How are inventory transactions recorded in the enterprise resource planning (ERP) software?
Production and manufacturing **Objective:** evaluate the efficiency and effectiveness of the policies, procedures and practices	▸ Are procedures and processes clearly mapped and up to date? ▸ Are work instructions clear and in electronic format? How are they updated? ▸ Do the facilities use visual management boards or monitors? ▸ Are the conditions safe for operators? ▸ Do material shortages delay production's actual start times? ▸ Do defective or nonconforming raw materials impact production?

Third-party risk management

Companies across a diverse range of industries are relying on third parties more heavily than ever before to achieve business objectives. This growing dependence on outside providers introduces significant new levels of risk to organizations.

While functions and services can be outsourced, the associated risks are still the responsibility of the company.

Companies without a well-defined third-party risk management (TPRM) program in place can find themselves facing a diverse set of risks. The leading organizations of the future must be able to transform uncertainty into confidence by developing trust with third parties.

Risks posed by a third party can have a significant impact on your organization's business operations, may expose your company to legal liability or may impact its reputation and increase costs unnecessarily through regulatory fines, loss of customer, etc. You can bring control expertise and business insights and advice to your company's third-party risk assessments, its program development and its implementation and monitoring processes. Internal audit should play a key role in helping your company respond to the diverse set of third-party risks.

Risk associated with third parties

Audits that have an impact	Key questions to consider

Third party risk management program
Objective: assess the foundational components of third-party risk management program
	▸ Does the organization have a comprehensive risk management program for third parties?
	▸ Does the organization have the governance framework, processes and controls in place to address the following?
	  ▸ Contract compliance (suppliers, vendors, alliances, joint ventures, collaborations, royalty and licensing, and software intellectual property)
	  ▸ Distributors and resellers
	  ▸ Marketing and advertising contracts
	  ▸ Does the organization utilize continuous monitoring?
	  ▸ Is there an overall oversight program for third parties?
	  ▸ Are changes in regulations impacting certain changes in third-party contracts monitored?
	  ▸ Is a process in place to monitor service level KPIs?
	▸ Has the organization conducted a global risk assessment across the third-party universe?

Contract risk management
Objective: provide assurance over contract delivery
	▸ Does the organization perform contract benchmarking?
	▸ Does the organization perform contract analytics (spend analytics, accounts payable analytics, travel and entertainment analytics, invoice validation, and purchase price validation) to identify potential issues?
	▸ Do contracts with third parties include the following?
	  ▸ Contract review – legal and business risk factors
	  ▸ Third-party contract risk profiling
	  ▸ Comparison of controls and processes to leading practices
	  ▸ Compliance verification procedures
	  ▸ Compliance and monetary findings
	  ▸ Process and control improvement recommendations

Treasury

The role of treasury within organizations has expanded profoundly and so have the inherent risks associated with its activities. More than ever, treasury has a full suite of responsibilities – the management of cash, working capital, liquidity and credit; the need to add value to earnings, cash flow, market share and competitive advantage; and the need to understand and incorporate new and revised regulations and accounting guidance, among many others.

The function now has a key seat at the decision-making table and is relied upon to strategically grow the global business. Treasury is no longer the company's bill payer or cash flow manager, but a key partner that is fully integrated into the organization.

With this added complexity the related risks have increased and expanded notably, making internal audits an important item on the board's agenda. For companies it is essential to nurture the expertise and subject matter knowledge required to perform internal audits of the treasury function. This expertise includes knowledge of the specifics, technical complexities and associated risks of a modern treasury function. Following are high-level treasury risks that all companies should be evaluating regularly.

Policy and governance:

- Insufficient oversight of treasury activities (e.g., no treasury committee, insufficient reporting)
- Exposure to fraudulent transactions due to a lack of fraud controls
- Outdated or incomplete treasury policies
- Treasury roles and responsibilities not clearly defined, raising risk of segregation of duties violation

Cash liquidity management:

- Treasury does not have complete visibility and control of all cash in the global organization
- Insufficient monitoring of liquidity risks

Funding and capital market:

- Insufficient monitoring of potential financial covenant breaches and lack of disclosure (commitments and contingencies)
- Unauthorized trading due to control weaknesses or inadequate platform

Financial risk management:

- Unhedged exposures (related to FX, interest rate or commodity positions) leading to earnings "surprises"
- Insufficient monitoring of credit risk, e.g., relating to derivatives or collateral

Accounting and valuation:

- Incorrect valuation methods (models) or input parameters
- Incorrect or incomplete treasury reporting, leading to incorrect decision-making
- Insufficient or no hedging documentation
- Hedge effectiveness not tested properly

Treasury technology:

- Outdated legacy treasury systems leading to financial reporting risks (including MS Excel)
- Inadequate treasury application controls

Audits that have an impact	Key questions to consider
Regulation and compliance review **Objective:** assess the processes and controls in place to comply with governmental regulations and internal policies	▸ Are the processes and controls adequately designed to comply with government regulations and internal policies (e.g., European Market Infrastructure Regulation (EMIR), Report of Foreign Bank and Financial Accounts (FBAR), cash management, external borrowing, policies and procedures)
Treasury governance framework review **Objective:** review existing treasury governance structure	▸ Is the governance framework effectively designed? ▸ Are treasury policies up to date and adequate to address the current market and operating risks? ▸ Are roles and responsibilities clearly and effectively defined?
Control framework and SOX compliance audit **Objective:** assess the existing control framework and execution of SOX testing	▸ Are processes and controls in place to properly manage bank account management, financial risk management, cash management and intercompany loans? ▸ Is there a defined universe of treasury risks? ▸ Does the SOX control framework appropriately mitigate the risks identified?
Treasury system review **Objective:** review treasury system setup and perform treasury technology diagnostic to identify opportunities to enhance overall system use and efficiency	▸ Are the appropriate treasury functional areas managed in the treasury system? ▸ Is the treasury system security configuration in place and properly controlled? ▸ Is a treasury system consistently utilized across the organization to effectively manage and control treasury processes across all regions?

Treasury fraud and investigation
Objective: review the effectiveness of key operational processes and controls to determine the likelihood of fraud and to assess remediation strategies and level of relevant trainings
	▸ Are key operational processes and controls in place and operating effectively to determine the likelihood of fraud in the organization in the following areas?
	  ▸ Cash management
	  ▸ Bank account management
	  ▸ Treasury technology and governance framework
	▸ Have remediation strategies been developed and are they being followed?
	▸ Has the organization provided the necessary fraud training and is it effective?

Treasury management assessment and maturity model
Objective: assess treasury management activities against industry standards and comparable organizations
	▸ Are treasury management activities consistent with industry standards or comparable organizations?
	▸ How effective are the treasury activities in the following areas?
	  ▸ Bank account management
	  ▸ Financial risk management
	  ▸ Cash management
	  ▸ Intercompany transactions
	  ▸ Interest rate risk management
	  ▸ Technology

eXtensible business reporting language

Preparing eXtensible Business Reporting Language (XBRL) exhibits to comply with the Securities and Exchange Commission (SEC) mandate can be challenging. Many companies rely on external production vendors to handle the XBRL process, without first appreciating the complexity and breadth of the SEC rules. It is critical for management to understand those requirements to make informed decisions during the creation and review of XBRL-tagged financials.

The SEC staff continues to identify serious recurring errors in XBRL exhibits, is starting to contact companies about issues and has issued "Dear CFO" letters on the requirement to include calculation relationships in XBRL exhibits. As a result, dozens of companies have amended their SEC filings to resubmit XBRL exhibits and correct mistakes.

Common XBRL issues of noncompliance include:

- Improperly selecting broadly defined tags or extending tags (rather than using standard tags)
- Not tagging all required levels and amounts, e.g., parenthetical amounts and amounts in the notes and schedules
- Using incorrect signs, i.e., positive and negative
- Having problems with reporting dates, decimals, units and missing calculations
- Improperly excluding XBRL exhibits with non-initial public offering registration statements
- Not establishing robust controls

To produce high-quality, compliant documents, companies need to understand all of the technical requirements, exercise diligence in the selection of appropriate tags and verify that all details in the existing filings are accurately captured in the XBRL submissions.

Companies should consider the following concerns related to XBRL:

- The SEC continues to make modifications and observations, typically updating the XBRL requirements quarterly.
- The volume of SEC guidance (e.g., EDGAR Filer Manual, FAQs, SEC staff observations) is significant; moreover, the guidance is often complexly worded.
- Many registrants do not fully understand the complexities involved in detail tagging.
- The SEC has reiterated that controls over the preparation of XBRL exhibits should be a component of the issuer's disclosure controls and procedures.

Internal audit can bring the required subject-matter knowledge and business insights to provide an objective assessment of the current state and offer guidance on developing an efficient and effective internal process over XBRL reporting.

Audits that have an impact	Key questions to consider
Regulation and compliance **Objective:** review XBRL exhibits for compliance with the SEC's rules	▸ **Documentation:** has documentation been evaluated or created around the tag selection for the financial statements, including the face of the statements, notes and schedules to verify that it narrowly and accurately reflects what is being disclosed and clearly describes to the user and the SEC what the tags represent? ▸ **Document completeness**: have amounts and concepts in the financial statements, notes to the statements and Regulation S-X schedules been evaluated for completeness? Have items that may not be included at all required levels been identified? Do items that are not tagged (if any) include a documented reasoning for not tagging? ▸ **Tag selection**: has there been assessment of selection of tags and identification of potential alternative elements and dimensions that have definitions similar to the elements and dimensions chosen and the financial concepts for properties not conforming to XBRL guidance? ▸ **Structural and consistency compliance of the instance document**: has the XBRL exhibit been assessed around structural or consistency errors, focusing on the EDGAR manual requirements that the SEC has identified as more frequent violations in initial XBRL submissions, including compliance around the correct signage (negative vs. positive values), decimal attributes, unit types, certain contexts and calculation relationships?
Governance, policy and internal control processes **Objective:** assess the quality and efficiency of the governance, policies and related controls over the company's creation of its SEC XBRL exhibits (including compliance with the SEC XBRL rules)	▸ Is there a formalized XBRL implementation and review process? ▸ Has there been a comparison of the current state of key implementation, review process and procedure areas with leading practices? ▸ Are there sufficient XBRL implementation processes, governance, policies and internal controls processes and applicable documentation to sufficiently comply with the SEC XBRL rules and disclosure controls and procedures requirements?

Why should registrants care about their XBRL exhibit?

Complexities and observations

- Separate SEC XBRL requirements included in the SEC EDGAR Filer Manual
- Filed errors identified by XBRL-US's consistency suite
- SEC issued written comments and data quality reminders
- Information excluded by hundreds of companies, according to XBRL-US
- Amended Forms 10-K and 10-Q due to issues and errors in the original XBRL exhibits
- Standard operating procedures, principles and criteria issued by the American Institute of Certified Public Accountants (AICPA) to address complexities
- XBRL data used in SEC's Accounting Duality Model to flag companies that require closer inspection

Risks

- Financial reporting goodwill and reputation risk
- The same liability as the traditional formatted filing (e.g., Forms 10-Q, 10-K) and potential civil liability
- Resubmission, prospective changes or other SEC actions
- Within the scope of "disclosure controls and procedures" in complying with Exchange Act Rules 13a-15 and 15d-15 and Item 307
- Lack of acceptance by the SEC (i e., won't upload through EDGAR) if it fails validation tests
- "Dear CFO" letters from the SEC and calls to companies about errors that resulted in dozens of amended filings
- Aspects of XBRL exhibits leveraged by the SEC in comments included in the Division of Corporation Finance (DCF) comment letter process

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2018 Ernst & Young LLP.
All Rights Reserved.

SCORE No. 00185-181US
CSG No. 1710-2433395

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or go to ey.com/advisory to ey.com/advisory.

Global and Americas Advisory Risk Leader		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
Americas Advisory Internal Audit Leader		
Lisa Hartkopf	+1 312 879 2226	lisa.hartkopf@ey.com
Americas Advisory Region Risk Leaders		
Central		
Kevin Janes	+1 312 879 5400	kevin.janes@ey.com
Northeast		
Marcelo Bartholo	+1 215 448 2638	marcelo.bartholo@ey.com
Southeast		
AJ Desai	+1 704 331 1983	aj.desai@ey.com
Southwest		
Geoff Beatty	+1 713 750 1467	geoffrey.beatty@ey.com
West		
Scott Coolidge	+1 213 977 4206	scott.coolidge@ey.com