Smart IT compliance
Continuous testing and monitoring of IT controls
Gaining a new vantage point for IT controls and compliance

At a glance

Diligent, continuous monitoring and testing form the backbone of an effective IT compliance and controls program that supports IT strategy, while proactively identifying areas and processes needing improvement. The intelligence this type of program produces can be returned to management’s risk and controls assessment process to provide deeper insight into the level of management preparedness – that is smart IT compliance. Such insight helps unlock the potential of a sustainable IT compliance program because successful compliance activities are not always ones that produce a positive result but ones that identify weaknesses in process design and operations. This feedback loop helps evolve the compliance program, as it gets smarter with time.

Making the right practice investments and establishing effective risk coverage and streamlined reporting are crucial to simplifying your organization’s IT compliance processes and enhancing the value of IT compliance. Smart IT compliance is centered on not only identification of risks but proactively examining and creating analytics around leading vs. lagging indicators.

We discuss the need for, trends in and next steps in enabling smart IT compliance in this paper.
Today’s business climate is one of continual innovation and change propelled by enhanced technologies, evolving customer needs and interactions, mergers and acquisitions, globalization, shifting business models, and regulatory pressures—all of which present continual and emerging IT demands. The IT organization sits at the epicenter of the company’s ability to both seize its evolving opportunities and manage the risks and compliance obligations inherent in business growth and change.

With such a vast scope to manage, many CIOs cite a variety of challenges when looking to improve IT compliance programs, including:

- Focusing on the broader risk management landscape of the business in addition to the technology-related risks. Identifying and responding to business threats and potential breaches is an important part of any integrated risk management program.
- Facing increased threats and vulnerability to sensitive data and corporate assets.
- Responding to headline hitting and brand defining IT breaches, which drive the push for more comprehensive compliance processes.
- Navigating IT regulations and industry mandates which demand additional resources to meet IT compliance standards.
- Supporting decentralized business with numerous platforms and no common control structure.
- Coping with IT risk management talent shortages – IT compliance is not a core IT competence within most IT organizations.
- Remediating material weaknesses and significant deficiencies in environments that are continually changing.

With IT as a critical hub in a company’s overall success, IT organizations need new models and ways of working that will help them succeed. A smart IT compliance program built on continuous controls testing and monitoring can help companies cost-effectively gain a new vantage point for IT controls and compliance and free-up more resources to focus on the strategic priorities of the business.

**Spotlight on IT Compliance**

Imagine this scenario – The Chief Information Officer of a large consumer products company returns to his office from a strategy workshop where he learned that two exciting new products have received executive management support and Board approval. The product lifecycle points to a Q2 launch and in each of the top five priorities discussed during the workshop, IT is the common denominator. That leaves less than 100 days to provide necessary support and resources for on-time product launches—all while supporting the business units to meet Q1 revenue targets and addressing the 23 IT compliance remediation activities recently identified by Internal Audit.

On top of that, the CIO receives an email from the PMO of an on-going implementation citing lack of alignment between functional business requirements and the IT architecture plan his team drafted last week. _How can this team manage multiple, equally high priorities without compromising timelines, quality and/or morale?_

The unprecedented focus and rigor on IT risks compounds the CIO’s challenge. Gone are the days when IT risks are addressed once and refreshed annually by applying some resources for a few weeks. With IT at the center of all business processes, and end users demanding enhanced services with quicker turnaround times, IT risks need to be managed every day. This is a constant challenge that grows and evolves as the organization grows.

Due to the reliance on technology throughout the value chain (starting with the customer experience), combined with the speed of change in most technology environments, companies’ controls around IT security, privacy, change management, access, business continuity and other areas are more complex than ever. This elevates the importance of making sure that IT processes are built with the right controls so that customer and other end user demands across the globe are met every day, that the business is supported in achieving its objectives and the company is effectively managing risk.

In order to best address these challenges, forward looking organizations and their IT executives are going through a point of inflexion. Some common threads across IT organizations include:

**Staying current with new threats.** With fast paced growth and disruptive business models taking on a mainstream role, the ability to spot emerging threats before they become reality has become a top priority. So the question really is – What are our capabilities in assessing both existing and emerging IT vulnerabilities? Are we investing in the right time and talent and do we have a proactive focus?

**Assessing capability.** When evaluating one’s ability to spot, prevent and detect risks and vulnerabilities, having an honest assessment of one’s capability is imperative – not only core IT credentials but also experience and technical IT risk management skills.

**Finding innovative alternatives.** The need to find cost-effective ways to keep pace with emerging threats is driving IT organizations to seek innovative alternatives to a traditional approach of managing IT compliance. This is leading to the emergence of third-party solutions that help organizations use technology-enabled and cost-leveraged methods to proactively manage IT compliance with substantial (but achievable) levels of coverage.
The case for smart IT compliance

As companies strive for effective and efficient IT risk and compliance monitoring, IT leaders are asking themselves:

1. **Is it complete?** Do I know the key IT risk and compliance obligations that matter most to the company?
2. **Is it standardized?** Is there a common understanding of the IT risk and compliance requirements, including the design and implementation of standardized risk, processes, and controls?
3. **Is there effective testing and monitoring?** Are key IT risk and compliance controls effectively tested and monitored, and are the results effectively communicated to Management?
4. **Is it relevant and current?** What worked a year ago may not be relevant and does it learn from the results of continuous monitoring? Does it factor in recent changes in IT and business landscape?

Recent cases of IT breaches and control failures have drawn considerable attention to the effectiveness of the organization’s risk and compliance programs. Many of these situations occurred despite diligent efforts and ‘green’ compliance scores with various IT regulatory requirements and standards. This demonstrates that standards alone can only take a company so far to protect the organization from surprise failures. Most control breakdowns are not a failure of the technology or standards themselves but rather a failure to achieve effective compliance across large and changing organizations. The best laid plans can be ineffective unless an on-going testing and monitoring program is well established.

A point in time approach is no longer enough to address on-going IT compliance. There are simply too many evolving regulatory expectations and risks to manage and monitor without a centralized, risk-based approach (see Figure 1). Five immediate drivers for taking a new approach to IT compliance include:

- **Rapidly shifting business complexities.** In order to execute their mandate and fulfill their role to build trust in society, regulators are stepping up expectations with changing business complexities and rapidly evolving IT landscape. For example, for financial institutions regulated by the SEC, the OCIE recently announced it will continue to focus on the implementation of cybersecurity and controls as part of its Examination Priorities. Examiners will also focus on areas including governance, risk assessment, access rights and controls, data loss prevention, vendor management, employee training and incident response. And that implies increased rigor as well. Examples of monitoring activities that must be present and functioning for an effective system of internal control, include:
  - Monitoring of user activities, exceptions, and information security events to support investigations and access control monitoring;
  - Assessing change requests for evidence of documentation, testing and approvals prior to implementation (even in an Agile environment);
  - Reviewing and assessing controls performed by service organizations to determine their impact on the company;
  - Monitoring of third party provider compliance against company security requirements;
  - Monitoring of user provisioning and de-provisioning procedures for granting and revoking access to all information systems and services.

- **Intensifying pressure on IT control structures and deficiencies.** With the constant changes and proliferation of new technologies and associated application and IT general controls, IT control testing exceptions are increasing. Also, the expansion of new IT processes, such as Agile development, is challenging long-standing control paradigms. Given organizations’ significantly higher reliance on technology-enabled processes, companies are experiencing much greater time sensitivity in addressing these concerns. Moreover, leading companies are looking to implement and test common control structures across all critical platforms to ensure high quality and reliability of IT processes.

- **More stringent oversight of third parties.** To further complicate matters, concerns over inadequate oversight of third parties has resulted in the need for more stringent monitoring. As a general rule, where certain functions can be outsourced, accountability cannot. Because of that, increased pressure has been placed on companies to proactively manage the risks associated with their use of third parties. While most third party risk management programs include the performance of due diligence in key areas such as financial, information security, and reputational risk, they sometimes fall short in other key areas known to carry significant risk—particularly in technology, privacy, and compliance.

- **Scarcity of skills.** Increased demands and expectations are forcing many IT organizations to “control their own
destiny” by building and operating an IT governance structure under which security, compliance and regulatory issues fall. In this regard, the skill set conversation has advanced from a “rent-versus-hire” discussion to the need for scalable, highly specialized resources and relevant company insights, on-demand. Not only has this created a race to acquire diversified skill sets and experiences, it has significantly increased the attrition rates in most IT shops.

Optimizing value and costs. The acute shortage of qualified IT risk-intelligent resources coupled with unprecedented attrition rates are putting significant pressure on IT budgets. To add to that mix, business expectations are elevating IT’s role as a strategic business ally – forcing IT to deliver exceptional value while optimizing tight budgets.

As all of these demands converge, tried and tested techniques of managing IT risk and compliance are no longer sufficient. IT organizations need new and innovative ways to cost-effectively monitor and test IT controls on an ongoing basis.

The key to effective IT compliance is to not only establish an effective, on-going monitoring program but a model that evolves and learns from the results of compliance monitoring, changing complexities of the business landscape and gets more agile as the program matures. Enter ‘smart IT compliance’.

**Figure 1: IT risk landscape**
Establishing smart IT compliance

An IT controls testing and monitoring program establishes a risk-based rigor to identify the key IT controls governing access, change management, segregation of duties, security, privacy, disaster recovery and other key IT risk and compliance processes. As regulatory requirements and business needs evolve, the controls monitoring program adjusts itself to align with the new requirements by way of a continuous feedback loop to the business. These programs provide companies with important information for monitoring risk exposure and then adjusting as necessary to meet changing business and regulatory needs.

These smart compliance monitoring programs are particularly enticing for IT executives because they are ‘plug and play’, regardless of the organization’s current maturity of IT risk management and compliance practices. They also offer an attractive delivery mechanism; a managed services solution supported by a distributed delivery model strategically leverages lower cost resources. Factors that enable IT risk-intelligent, centralized (often off-shore) resources to be the core support for such programs include:

- Centralized governance model
- Workflow technology
- KPIs and metrics to monitor and report on performance
- Feedback loop to continuously enhance the model in line with business needs

The following steps can help establish a sustainable controls testing and monitoring model to help achieve smart IT compliance in your organization (see Figure 2):

**Step 1: Perform risk assessment. Scan. Scope. Repeat.** A top-down risk-based approach evaluates the IT controls associated with high-risk business processes and transactions to assess and prioritize IT compliance monitoring priorities. A structured risk assessment thoroughly scans and analyzes all known and relevant risk factors, including both current and emerging ones. It should also be quantitative. Examining real data and risks from transactional volumes and using and analytics is an important part of proving out the risk assessment. Remember, risk assessment is not an annual, point-in-time activity – it is a continuous process and key results should be factored in the overall IT compliance program on a real time basis.

**Step 2: Establish a common controls framework.** IT controls are identified in alignment with IT risks and are continually refreshed as the business changes. The controls identification process extends well beyond ICFR, as it is not uncommon for global organizations to be operating thousands of critical (and disparate) technology applications, only a fraction of which are in-scope for ICFR. Additionally, a standardized intake process is established for new applications (and related controls) as processes and technology change.

Mapping controls to specific business and compliance requirements, including regulatory requirements, SOC 1/SOC 2 and internal policies, helps establish a framework where all risks and requirements are mapped across control activities. A common controls framework aligns to strategic priorities and may leverage existing frameworks such as COSO, COBIT and NIST. Such a common framework helps significantly minimize (eliminate in many cases) duplication and redundancies that often creep in any risk management process in large organizations. It also helps to keep the various controls frameworks used by the organization in sync. These frameworks and processes are best enabled by a technology platform that enables monitoring activities in an integrated way versus stand-alone, point-in-time solutions.

**Step 3: Rationalize controls.** Successful, centralized (and cost-efficient) controls monitoring programs embed automation and analytics as a strong foundation. The continual development of analytical tools is an asset to any controls monitoring program. For example, analytical tools can be used in many systems for automated testing of segregation of duties controls. While automation and analytics may evolve as the controls monitoring program matures, starting off with a foundation of data driven controls monitoring techniques helps organizations maximize their ROI.

**Step 4: Conduct centralized testing.** Leveraging a common workflow technology with automated reporting of results, a centralized testing team is able to connect the dots, significantly increase the efficiency in compliance testing activities and identify systemic process and system breakdowns. These centralized Centers of Excellence (COEs) are able to effectively leverage advanced skill sets ranging from IT security to data privacy, IT general controls, business resiliency and sector-specific regulatory requirements. Organizations are also creating models including co-sourcing to access leading practices and accelerate the journey.
Consider this example of IT controls evolution...

Many organizations are adopting agile systems development techniques that require different processes and more nimble change management control structures than traditional development. As these systems development methods change and mature, control structures need to be re-designed to match...and the related controls need active oversight to ensure they are meeting objectives.

Many IT organizations are outsourcing or co-sourcing with third party specialist providers to establish a smart IT compliance testing and monitoring program that enables organizations to respond to operational performance imperatives and regulatory changes quickly, effectively and in a scalable manner. Additionally, by leveraging external risk management and compliance providers, companies can in many cases decrease the overall cost of compliance and focus core in-house IT resources on partnering with the business stakeholders to drive business performance.

Figure 2: Controls testing and monitoring model

- **A. Perform risk assessment**
  - Identify high processes and transactions for ongoing testing

- **B. Establish common controls framework**
  - Establish a common controls framework and identify key controls critical for strategic and operational business objectives

- **C. Rationalize controls**
  - Streamline and automate controls

- **D. Centralized testing**
  - Ongoing scalable monitoring and testing through automation and low cost global delivery centers where possible

- **Active analytics**

- **Enabling technology**
  - Continuous feedback

- **IT processes**
Active Analytics Reporting anytime, anywhere. Stakeholders need to have on-demand access to key metrics and controls performance should be on the list. An effective IT continuous testing and monitoring program uses technology to make real-time, streamlined, and consolidated reporting a reality—on day one! The primary objective behind this demand is the need to make real time business decisions that require real time reporting – the opportunity cost for cyclical, period based reporting is too high.

Smart IT compliance is about helping business and compliance leaders obtain complete and accurate data sets, in the right context, so that they can align the right level of risk coverage and innovation in their IT compliance program and adopt an IT control and compliance structure in a manner that keeps up with the changing needs of the business. The versatility of such a smart IT compliance program enables organizations with diverse scope, size, complexity and maturity to realize immediate benefit. Once the program is adequately calibrated to the growth trajectory and maturity of an IT organization, the compliance program evolves with the changing regulatory landscape and the organization’s business realities. Furthermore, a dedicated COE supporting the compliance testing and monitoring activities has an excellent opportunity to identify systemic process and control weaknesses. They can also connect the dots to identify ways to streamline and strengthen the underlying business processes and systems. With limited investment to set up such a program, and significant upside of expected value, no wonder many IT executives see outsourcing or co-sourcing the continuous testing and monitoring of IT controls as a smart thing to do.
Your IT backbone has a friend.

An established, smart IT compliance program helps strengthen an organization’s second line of defense and has a direct impact on the overall control environment. Some key distinctions include:

- Helps ensure that IT-driven processes are meeting customer, regulator and internal requirements
- Helps the company grow and move fast with minimal disruption
- Streamlines and simplifies the burden of IT risk and compliance
- Increases the overall ROI on IT risk management and compliance spend
- Increases internal focus on key strategic and operational business priorities
- Helps provide just in time resources with specialized skill sets and organizational insights
- Helps identify and correct systemic process and system weaknesses

Contact information

Want to know more? If there was ever a time to talk about simplifying your organization’s IT compliance processes and enhancing the value of IT compliance, this is IT. For a follow-up conversation on how PwC’s proprietary diagnostic and technology tools can help establish a cost-leveraged compliance-monitoring model, contact:

**Princy Jain**  
Internal Audit, Compliance & Risk Management Solutions Partner  
princy.jain@pwc.com  
408 817 3870

**Dhiraj Malhotra**  
Internal Audit, Compliance & Risk Management Solutions Partner  
dhiraj.malhotra@pwc.com  
415 498 8461

**Seth Rosensweig**  
Advanced Risk & Compliance Analytics Principal  
seth.rosensweig@pwc.com  
646 471 6762