Bolster Application Security and Internal Controls Compliance with Design-In Processes and Automation

At a Glance

Security and control compliance can safeguard an entity's digital assets during enterprise transformation. To achieve success, companies should:

- Use a process-oriented approach that is end-to-end
- Engage with business leaders and applying change management strategies
- Align security with business goals
- Have the right resources in place
- Collaborate with business leaders and essential stakeholders
- Approach security holistically

Business process controls and application security are not just valuable for organizations looking to transform to a modernized state — they are critical. As technology becomes increasingly pervasive, the complexity of the information technology (IT) and digital landscape is growing exponentially. Regulatory requirements and the constant news regarding the latest security and data breach of a high-profile company are increasing the pressure on IT resources to provide evidence of security measures taken during large transformation initiatives. And, as a result, many executives are now adopting, more than ever before, a design-in approach to application security and internal controls.

Today's technologies for application security and internal controls optimization allow for deeper automation of testing processes while being fully integrated across the technology environment. Manual controls may no longer be effective or sustainable. Automating security brings return on investment (ROI) by protecting digital assets while increasing efficiency and reducing the burden on IT departments. Effective CIOs heighten ROI by defining the parameters for success while considering and mitigating risk to avoid penalties and prevent fraud or other repercussions. They apply a forward-thinking approach to avert unnecessary costs and complications, and they partner with business leaders to accomplish their goals rather than using a siloed implementation approach.

Experienced CIOs incorporate controls and security *along* the transformation and modernization journey rather than tacking it on the back end of the program. Why? Because a *design-in* approach improves ROI. It addresses all necessary controls by focusing on automation and incorporating continuous controls monitoring and assessments. Incorporating a design-in approach to technology modernization projects lowers remediation costs after systems are live. It brings peace of mind to external auditors and facilitates the company's ability to maintain and sustain secure systems. While design-in costs may be higher in the short term, the costs of remediating poor security and compliance concerns far outweigh the near-term investment of a design-in approach.

Use a process-oriented approach

Process-oriented approaches offer end-to-end attention while bringing automation, efficiency and more comprehensive security. Leveraging tools that elevate access monitoring (such as segregation of duties and sensitive access) as well as IT process automation (including user provisioning and annual recertifications) facilitates the efficiency organizations need. Technology transformation is more successful when tools are used to address compliance and IT process automation. Artificial intelligence (AI) and machine learning (ML) technologies allow companies to create and implement complex use cases that can make it possible to detect fraud scenarios. And intelligent process automation (IPA) solutions allow companies to automate legacy technologies with relatively low effort. Far from being one-use-case assets, these tools transform inefficient activities across core IT processes through continuous monitoring and automation.

Adopt engagement and change management strategies

Experienced CIOs recognize that transformation projects are not purely technical. They know that engaging with business leaders early and throughout deployment leads to effective implementation and user adoption. Key players such as audit, risk and compliance groups who have a seat at the IT think-tank table are particularly important to the adoption of security and controls compliance.

Change management and enablement can compound adoption success. IT can enable change management initiatives by working across the organization to help address risk ownership, training, behavior and culture.

Bolster security with vested stakeholders

CIOs must go beyond involving business leaders in the transformation. They must collaborate with other essential stakeholders regardless of level. Collaboration builds buy-in and facilitates engagement in the preparation and execution of testing and signoffs. Vested stakeholders validate that data is complete and accurate from a business perspective. Engaging stakeholders is paramount regardless of the transformation strategy.

Dedicate resources — it is a must, not a luxury

Having a dedicated workstream is core to the ownership of security and compliance efforts. Where it was previously an afterthought, it is now a necessity. Rather than addressing issues after the fact and after damage has been done, forward-thinking CIOs are preemptively and formally dedicating resources to security and controls workstreams.

Collaborative understanding brings results

When addressing security and controls compliance integration, successful CIOs:

- Have an effective steering committee
- Apply a clear understanding of the audit committee's priorities
- Outline KPIs as part of the governance process
- Evaluate business leader requirements for success
- Apply reporting and analytics as tools to achieve goals

Approach security and controls holistically

Addressing security *holistically* is fundamental. CIOs must consider the complete portfolio of security and controls when tackling enterprise transformations. In fact, a holistic approach to security might have mitigated the damage suffered by companies who fell victim to more than 281,000 data breaches since the GDPR legislation went into effect in mid-2018.

However, enterprise transformation cannot be successful using a one-size-fits-all approach — rather, it involves thoughtful consideration of security issues beyond common topics. It needs more than siloed consideration of identity access management and cyber breaches. It requires comprehensive consideration of the complete portfolio of security and controls. A holistic approach may include questions such as:

- What broader security measures must be taken across all layers of the digital landscape (e.g., databases, servers and operating systems, networks and storage, backups and disaster recovery operations, etc.)?
- What is the impact to data security and privacy during transformation deployment?
- Where does personal information reside in the future state?
- How are regulatory requirements being handled to prevent breach-related fines?
- What are the automation opportunities related to controls compliance and business process optimization?

Impact on the C-suite

CIOs have the opportunity to serve as digital enablers and thought leaders. They understand how security and controls can support business goals to build value. The right involvement of key C-suite leaders and global process owners is essential to achieving technology alignment with organizational goals. Certain unique issues relevant to the C-suite as they pertain to security and internal controls compliance include:

- **Chief financial officer (CFO) and business leaders** — Alignment with business priorities is paramount, therefore collaboration with C-suite leaders for input on IT efforts is essential. Business leaders must consider the entirety of what the modernization will require, including shared services and centralized master data functions.
- **Chief audit executive (CAE), chief compliance officer (CCO) and chief risk officer (CRO)** — Involvement and consultation with the compliance, controls and security workstream is essential to ensuring that industry and regulatory requirements are being addressed. Additionally, the CRO and CAE are instrumental in offering guidance for a design-in approach that aligns with risk objectives.
- **Chief data officer (CDO) and chief marketing officer (CMO)** — Security, controls and compliance have an impact on data governance objectives. Collaboration with the CDO and CMO on prevention and mitigation of data breaches is fundamental.

Across the C-suite, executives must have full understanding and insight into how their business processes truly intersect, along with deviations from standard and manual work arounds. A technology like process mining enables quantitative analysis on improvement areas and bottlenecks, which enables executives to implement real-time predictive analysis on a single process, providing more effective services to the customer.

Where do companies go from here?

As organizations undertake technology transformation initiatives, high-stakes considerations include:

- Applying a design-in approach for process and compliance automation and efficiency

- Using an agile approach to meeting objectives in a dynamic digital environment
- Determining the parameters for success, including KPIs, change management initiatives and strategic business goals
- Integrating security programs into the organization's culture
- Ensuring user adoption through two-way communication plans that incorporate feedback
- Having a dedicated security and controls workstream with consultation from the audit function

Ensuring sound security and controls compliance practices is essential to maintaining and supporting the value of technology transformation. The ultimate outcome is increased efficiency and improved quality of security and business processes, along with reduced costs and fewer error-prone manual controls, enabling transformation to continuous monitoring.

AUTHORS

TONI LASTELLA, Managing Director, Enterprise Application Solutions, New York
JOHN LIVINGOOD, Managing Director, Enterprise Application Solutions, San Francisco
MARCO GEISENBERGER, Director, Technology Consulting, Munich

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, please contact us at TechnologyConsulting@protiviti.com.