protiviti®
Face the Future with Confidence

Agile Technology Controls for Startups — a Contradiction in Terms or a Real Opportunity?

Implementing Dynamic, Flexible and Continuously Optimized IT

Issue

It's not a secret that the last thing passionately discussed in the daily scrum at the typical Silicon Valley-type technology startup or latest cloud services provider is compliance. Cutting-edge tech companies prefer to stay focused on their immediate concern — meeting the evolving needs and expectations of their customers, which requires investing in engineering teams, keeping up with aggressive product development schedules and staying ahead of emerging technology trends. What's more, for many emerging startups, risk mitigation and internal controls can actually run counter to the company's "DNA" — its inherently irreverent culture and competitive mindset.

That is not necessarily true for the companies' chief financial officers (CFOs), executive teams and boards of directors. As these companies grow their customer base and begin to consider an initial public offering (IPO), the lack of a focus on IT controls can potentially hurt both their top line and their filing deadlines — and cause a few headaches for management and especially the CFO at audit time. CFOs should keep in mind the following important trends and drivers:

- Public companies are required to establish effective IT general control (ITGC) frameworks to comply with the Sarbanes-Oxley Act (SOX). This includes controls in the areas of change management, release deployments, access provisioning, data quality/governance and disaster recovery.
- Cloud and other service providers increasingly are being asked to provide Statement on Controls reports, commonly known as SOC reports (SOC1, SOC2 and SOC3 under SSAE No. 16[1]), for the ITGCs associated with their customer-facing systems environments. These reports have become "must-haves" if the provider is to support larger established companies with control and compliance requirements of their own.

[1] The American Institute of Certified Public Accountants (AICPA) Auditing Standard Board (ASB) Statement on Standards for Attestation Engagements (SSAE) No. 16 was published in April 2010 as a replacement for the Statement on Audit Standards No. 70 and the commonly referenced SAS 70 reports.

- The Public Company Accounting Oversight Board (PCAOB) and the updated COSO framework have introduced new requirements for financial controls assessment and increased scrutiny over ITGCs and IT risk management.[2] Organizations must now comply with more rigorous evidence retention standards to demonstrate key ITGC activities, such as formalized approvals, project documentation and system-generated reports.

Companies are often conflicted when trying to balance compliance requirements with the use of emerging technologies and non-traditional technology management processes. Does management sacrifice speed and innovation in favor of meeting auditor requirements, or does it allow the company to stay the course with its development priorities and risk non-compliance? Protiviti's experience working with numerous tech startups and other fast-growth enterprises indicates there is another way that satisfies control and compliance requirements without disrupting the company's culture of independence and innovation. We discuss this alternative in the sections that follow.

Challenges and Opportunities

There are a number of reasons technology startups face difficulties in instituting regulatory controls, especially for cloud-based business systems and systems development that leverages agile methods. These reasons include:

- Use of different methodologies for managing controls over corporate IT environments (i.e., for SOX compliance) and customer-facing environments (i.e., for SOC reports).
- Difficulty implementing and effectively managing controls across cloud-based business systems as a result of direct management of these systems by the functional teams (i.e., in a "shadow IT" capacity).
- Complexities of transferring financial data across multiple applications and platforms, resulting in errors and discrepancies.
- Deployment of software (code changes) as part of continuous integration and continuous deployment, with limited oversight and approvals.
- Developers retaining unrestricted access to production environments to validate and support newly deployed features/enhancements or troubleshoot issues resulting from deployments.
- The "single domain" cloud application model, which can result in inadequate customer data partitioning. In many instances, customer data can be accessed by internal users.[3]
- Password policies that do not accommodate the full set of authentication protocols in use across all environments, resulting in inconsistent enforcement (e.g., policies may differ between on-premise and cloud-based authentication systems).
- Confidential data being managed in personal box cloud storage, making it difficult to contain proliferation of corporate information.

Each of these practices can have a direct impact on the reliability of IT controls for the corporate, financial and customer-facing systems, and can ultimately affect a company's overall internal control environment. As a consequence, many startups and cloud-services providers find themselves scrambling to provide adequate evidence of approvals and other controls to audit teams — a time-consuming and disruptive process that can cause significant frustration within development teams and may still fail to satisfy external auditors and customers.

To address these challenges effectively and institute proper controls, companies need to understand and proactively address the situations that raise red flags for auditors. At the same time, these companies need to define and enact controls in a measured manner that is aligned with their technology and operations. This requires shifting focus away from traditional control checklists and templates to a lighter, more optimized ITGC framework and implementation methodology that is compatible with innovative, leading software development practices like development operations (DevOps) and agile project management. By taking this approach, technology companies and cloud services providers can strengthen their controls and achieve compliance objectives (e.g., for SOX and SOCs) without compromising the flexibility, speed, drive and ingenuity so critical for their success in the competitive emerging technology landscape.

[2] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and provides frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

[3] For more on data security in the cloud, see www.protiviti.com/US-en/insights/cloud-security-keeping-data-safe-boundaryless-world-cloud-computing.

Our Point of View

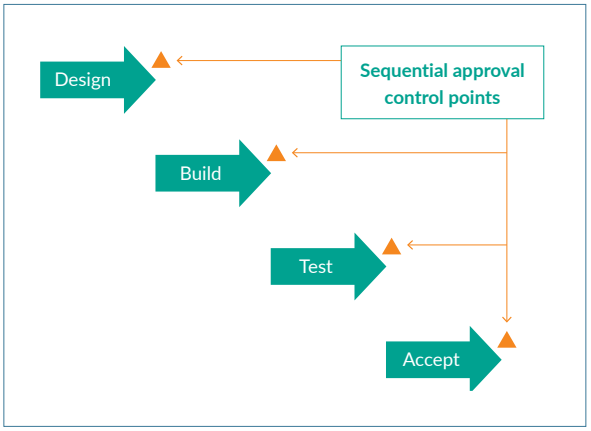
ITGC design at emerging technology companies must be dynamic, flexible and continuously optimized to reflect the companies' emerging and evolving business models. The ITGC framework must not only be effective but also palatable from a workload and cost perspective. Designing this new ITGC framework involves the following activities:

- Rationalizing common processes and control activities across business systems and software platforms.
- Designing preventive and detective control activities that are effective in the new environment, both from a risk management and operational scalability perspective.
- Designing security models that are specific to each company's environment and are effective and easy to implement.
- Centralizing ownership of ITGCs to lower cost.
- Establishing approaches to continuous monitoring and rebalancing of ITGCs to maximize agility and minimize restrictions on innovation.

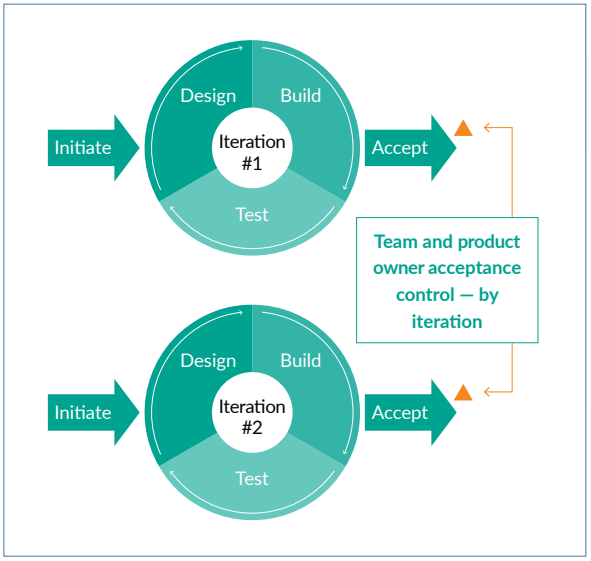
Using the methodology broadly outlined above, technology startups and cloud-based providers can establish effective controls over systems and development processes and meet their regulatory requirements without a significant impact to the way they do business. Two key areas of opportunity in this effort are process rationalization and agile activity alignment.

Process Rationalization. Process rationalization starts with determining how the key technology processes are structured. In many companies, different teams are tasked with supporting disparate applications using similar, yet unconnected, processes — particularly in the areas of IT change management, software development and access management. Identifying these groups and instituting common, baseline process elements that work for a maximum number of stakeholders can help a company apply common control activities across a process, rather than redundant ITGCs requiring separate validation effort within each individual group. To achieve this, processes should be aggregated under common owners wherever possible, and duplicating activities should be rationalized to avoid redundancy. For example, production environment access management controls can often be improved by providing user access based on role/title rather than individual requests sent to various administration teams, which must then perform similar actions.

Traditional Software Development Life Cycle (SDLC) Controls



Agile SDLC Controls



DevOps and Agile Activity Alignment. Product quality control is an inherent component of effectively implemented DevOps and agile processes; however, traditional controls approaches often fail to recognize and leverage these activities, leading to implementation of unnecessary, unaligned, and, ultimately, ineffective control activities. Instead, existing DevOps and agile process activities should serve as the basis for identification and definition of key ITGCs (e.g., test case

coverage, automation of regression testing, automated linking of testing and requirements, systematic capture of deployment approval, etc.). While additional control activities can be added, these additions should be applied only where necessary to close specific control gaps (e.g., additional financial reconciliation, production deployment monitoring, etc.). Approvals in agile software development processes can also be leveraged, but they require a shift from waterfall, or sequential, approvals (e.g., signoff at each process stage) to signoff at the completion of each development iteration. For organizations with effectively operating agile processes, this helps avoid unnecessary administrative effort that is not additive to the production of quality software.

To be effective, ITGCs should be customized and aligned to each company's unique IT and software development processes and organizational structures. Companies should do and ask the following to determine the right solution:

- Analyze the systems environment:
  - What systems and processes are in scope for the purpose of our compliance audits (SOX or SOC)?
  - Who owns each key process?
  - What applications and process areas can be excluded from the scope of compliance activities?
  - What is the best way to create boundaries between compliance areas (e.g., financial versus non-financial, customer versus internal, etc.)?
- Look at systems that are key corporate data activities — how are they supported?
  - What areas are in need of additional controls?
  - What existing activities can be used to mitigate key risks?
  - What are alternative approaches to mitigating key risks?
- Define a future-state vision (not so much a redesign plan, but a roadmap):
  - How do processes fit together?
  - What is the "backlog" of improvement opportunities and initiatives?
  - Can automated activities be leveraged for ITGCs to increase efficiency, instead of adding new manual activities?

How We Help Companies Succeed

Protiviti's experienced Technology Consulting professionals clearly understand the challenges technology companies face. We work with our clients to define IT processes and controls that satisfy regulatory requirements while remaining in alignment with each company's culture and existing technology delivery expectations. We recognize the essential value that non-traditional processes and organizational structures provide to innovative companies, and we partner closely with the IT, engineering, and business organizations to define realistic solutions based upon existing practices. We utilize agile project management techniques to enable timely implementation of solutions and provide real-time measurement of progress, while also allowing for rapid realignment of priorities in response to changing business needs.

Example

Protiviti was engaged by an online financial services provider to formalize the IT controls and risk management approach related to the company's cloud-based production systems. While the software engineering processes adequately supported business operations, the company needed to identify controls to satisfy external auditor requirements and align the processes with internal risk management needs. However, the executives were adamant that risk management activities should not disrupt or diminish the agility, innovation or continuous delivery capabilities of the engineering SDLC.

Our integrated team of IT and risk management professionals worked with the technology team managers to address these needs. Through a series of working sessions, we helped the engineering team develop a comprehensive picture of the production systems environments, including key functionality, critical transactions, process and control owners, and alignment to key business risk factors. Together, we mapped the end-to-end production system support and maintenance processes, identifying existing activities that satisfied control objectives and pinpointing control gaps. We then designed process enhancements to mitigate the gaps, utilizing agile implementation methods to enable real-time benefits measurement and course correction.

Specific deliverables to the client included:

- Engineering team system and process flows and supporting documentation
- Updated policies, procedures and control matrices
- Engineering improvement backlog (continuously maintained)
- Agile-based status reporting (e.g., "burn-down" charts)

Our approach enabled the company to meet its goal of establishing formalized IT controls while minimizing adverse impacts to engineering process agility and delivery. Additionally, the application of agile techniques for the control implementation enabled continuous feedback and course correction and provided benefits visibility to management throughout the process/control improvement implementation efforts.

Contacts

Ronan O'Shea
+1.415.402.3639
ronan.oshea@protiviti.com

Steve Hobbs
+1.415.402.6913
steve.hobbs@protiviti.com

Jason Brucker
+1.415.402.6937
jason.brucker@protiviti.com