CIO Journal.
THE WALL STREET JOURNAL.

January 8, 2015, 10:39 AM ET

Software's Jarring Effect on Financial Services: DevOps and Audits

Financial services (FinServ) has embraced software innovation as much as, if not more than, any other. Everything about software's pervasiveness in the FinServ industry is mission-critical – driving the heart and soul of transactions – anytime, anywhere and any place.

This evolution is happening because of the rising demands of Web, mobile applications, and business services. Therefore, implementing fully-automated, integrated systems is a must in order to keep pace with the increasing volume of software delivery requirements. FinServ organizations are moving beyond static deployment models and are embracing a Continuous Delivery/DevOps style approach. But DevOps and the automation of build, test and deployment processes also shine a light on another ever-present and evolving business factor – security and compliance.

Banks and FinServ providers know what the regulatory environment is like and how costly mishaps can be. With the rise of software as a business function, FinServ CIOs have even more on their plates, especially since the SEC has begun counting all of the computing and software applications as part of their overall business assets. New software audit and compliance regulations, coupled with cutting-edge software development practices, bring the industry a new challenge: what control environment(s) does a FinServ organization have in place to prevent bad things from happening and how does it provide demonstrative evidence that it exists?

First of all, the auditing process is not easy, but in a world where threats are abundant, it must be embraced. Assurance plays a large role when businesses need to find trust between each other. Third party reporting provides that confidence. In addition, audits provide a critical feedback loop to the DevOp practices to ensure continuous improvement and management of regulatory and security risks. Just like Agile and DevOps practices, auditors require a collaborative approach with clear communication and transparency to help the business achieve its goals. If software development and IT operations teams (often geographically dispersed for large enterprises) are proactive participants in the process, it will only strengthen the foundation of the organization's control environment.

The truth is DevOps and software audits are actually complimentary to one another and can provide business value collectively. Consider ISO 27002 Audit Standard "12.1.4 Separation of development, testing and operational environments." This states a control objective that, “Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.” This makes perfect sense from a risk mitigation and compliance perspective, but is counterintuitive from a DevOps perspective. However, the most important thing that organizations can do from the onset of an audit is to help show the linkage between what the control objectives are, and what internal procedures are in place to support this control. By eliminating the interdependence of software development and IT operations through DevOps practices, it can be easier to show the linkage of said processes and procedures to demonstrate how these activities tie into the overall business model.

How a business quantifies risk also becomes very important within the context of an audit scenario. Business risk assessments help design the security program and the compliance program together. Unlike Continuous Delivery where it’s all about how fast we can deploy and getting excited about its cost-effectiveness, efficiency, etc. across a time window of days to weeks, audit programs are built top down with a quarterly viewpoint. Therefore, early gathering of the established control objectives is recommended to have an understanding of what risks are critical to the business and how the DevOps work streams can support the management of them within the organization. What is equally important to remember is that the business itself decides what the control objectives are for the procedures in place. Enabling a company’s disparate organizations to become part of that process means the procedures being asked for software development and IT operations to execute against are already in-line with those of the business. Remember, the control objectives and evidence being audited is based upon the business’ view of risk – not the auditor’s view.

Being able to apply Agile methodologies to an audit process also has plenty of benefits. For example, ascertaining the consolidated scope and bound of what the business cares about is critical so that the deployment environment fits that overall structure. By identifying how to represent its control environment, an organization should then draw up how it is going to reflect those representations and have management sign off on them beforehand. This procedure creates visibility across the organization so when it is time for an audit, this step already has addressed that variance. Furthermore, the communications born out of a DevOps culture can help auditors understand the concept of automated testing when deploying into production systems as a “magic middle man” that is also handling the negotiation of risk. This is inherent intelligence that an organization has built, and that it can take credit for.

If organizations can start thinking of DevOps methodologies and auditing systems as equal parts of a continuous improvement program, this sets a framework for corporate sustainability. Development teams would be encouraged to input a feedback loop with IT operations personnel (and vice versa), and the auditors themselves to help improve the process year over year. At a recent FinServ event, Steve Brodie, CEO of Electric Cloud, shared a statistic that demonstrates the value of integrating audit and DevOps systems within an enterprise. According to Brodie, continuous improvement programs such as this can create a 10x reduction in time spent, thereby increasing the potential for productivity while also addressing business risk and compliance necessities.

Overall, successful audit and compliance performance require skills beyond balancing the needs and output of disparate teams; it requires the talent of connecting the development and operations activities to the governance of the business at the highest control level. The ability to serve the customer is only half of the job description. The other half consists of considering internal business stakeholders (internal auditing, marketing, information security, and compliance procedures). FinServ organizations have the opportunity to achieve a greater balance across controls to audit safeguards beyond those of traditional brick-and-mortar development shops. Adopting DevOps and proactive risk mitigation techniques, and viewing these two process-driven opportunities as value-added concepts to the business, will continue to push the bounds of this once sluggish and traditional industry further into the hotbed of innovation.

James J. DeLuccia IV is a Senior Manager in the Advisory Services practice of Ernst & Young LLP. Mr. James, a published author with John Wiley & Sons, specializes in multi-national enterprise governance, privacy, and security initiatives involving holistic technology and controls reengineering. He oversees the firm’s ISO advisory and certification services in the Americas, and coordinates globally the Payment Card Industry practice.