IT Compliance for Banking and Finance

UpGuard

Table of Contents

I. Introduction

Banking and financial services organizations face daunting challenges as the industry continues to transition into the Information Age. Moving at the pace of today's markets, firms must navigate through treacherous waters: the omnipresent threat of cyber attacks, rising competition from increasingly agile competitors, and evolving challenges of global finance set the stage against a convoluted regulatory backdrop. While it may seem like business as usual in this heavily regulated sector, current and future technological advances-- though instrumental in spurring growth-- pose complex challenges of increasing scale and magnitude.

Innovations like mobile banking, cloud-based trading platforms, and online payment systems have created new business opportunities and mechanisms for deeper customer engagement. The flip side to these benefits are the risks, concerns, and resulting regulations that mandate adherence. For instance, the cloud enables banks and financial services to efficiently and cost effectively scale their services for a rapidly growing online customer base. However, implementing security and control mechanisms in these environments is more complicated, and underlying systems can be harder to troubleshoot than their traditional, on premise counterparts. Laws governing use and management of technology therefore tend to be vague in implementation detail, but exist nonetheless to reduce any negative impacts technical innovation may have on customers.

Many firms choose to adopt technologies without fully assessing the impact this may have on their environments, and are subsequently at a loss when related infrastructure problems occur. Others are saddled with legacy IT systems, processes, and methodologies-- and are stuck with integrating and supporting software/hardware inherited through various M&A activities over time. Compliance measures and resulting IT controls also ensure that firms have the proper controls and security mechanisms in place to keep older systems safely updated and operational.

IT Under the Gun

The topic of compliance has seen much press lately due to the many incidents of accounting fraud and security breaches that continue to plague the industry. High-profile corporate scandals may steal the limelight, but the fact is that most corporate non-compliance transgressions are IT-related and deal with internal control failures. White collar crime may have been the initial catalyst for broad-sweeping regulatory action, but the resulting legislation has also snared countless IT-related failures in its wide net by design.

As the life support system of any information-driven organization, the IT department-- especially in banking and finance firms-- is under enormous pressure to deliver consistently optimal service levels to both customers and company employees. They are responsible for building, managing, and maintaining the systems that power activities like reporting financial data, storing/retrieving customer information, and processing transactions such as deposits and trades, among others. Those without the necessary control mechanisms in place will find themselves in the crosshairs of cyber attackers, competitors, and last but not least, compliance auditors.

II. Control Frameworks

The most commonly cited difficulty with compliance is that legislation and measures often lack the necessary critical details regarding specific requirements, even as the consequences of non-compliance are clear. Control frameworks have therefore been employed to distill the high-level language of compliance regulations and measures into tangible objectives and supporting activities. Depending on the nature of the firm's business activities, different laws and measures-- and therefore control frameworks-- may apply. By using common, auditor-sanctioned control frameworks that include the critical missing detail level and language, firms can gain a quick footing on the path towards compliance. Some popular control frameworks include:

- ITIL (Information Technology Infrastructure Library)
- ISO/IEC 27001
- ISO/IEC 27002
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
- COBIT 5 (Control Objectives for Information and Related Technology)

COBIT is the most popular control framework for IT governance and compliance purposes, and is especially effective when applied to SOX compliance, as it provides the most comprehensive and clearly defined requirements to benchmark against. Currently on version 5, the framework was developed by ISACA (Information Systems Audit and Control Association) and is based in-part on COSO. Whereas the latter deals mainly with controls for financial processes, COBIT focuses on IT controls. COBIT serves as the de-facto standard for various compliance auditors when measuring the effectiveness of a firm's documented internal controls and has gained general acceptance among third parties and regulators. Firms using COBIT 5 as a guideline for their IT compliance efforts are more likely to achieve successful audit results.

Defining Material Weakness

The concept of material weakness is central to compliance and related auditing criteria and activities. Material weaknesses are defined as deficiencies in the system's internal controls that could lead to reporting errors. In the context of Sarbanes-Oxley (SOX), for instance, an internal control failure can lead to material misstatement in a company's financial statements, and if found is noted by auditors as a material weakness. Each deficient item can be thought of as a negative mark on a firm's compliance report card.

A recent study by the Clute Institute found that IT-related material weaknesses accounted for the majority of material weaknesses in SOX 404 compliance failures.

See chart on next page

Material Weaknesses In Internal Control
Panel A: Number of Material Weaknesses Per Company

	Mean	Maximum
IT-Related Material Weaknesses	2.33	7
All Material Weaknesses	4.75	18

Material Weaknesses In Internal Control
Panel A: Number of Material Weaknesses Per Company

	N
Access Controls	72
Change Management	32
Documentation	18
Spreadsheet Controls	16
Disaster Recovery Plan	15
Segregation of Duties	15
Application Controls	7
Other	79
Total	254

Data courtesy of The Clute Institute.

The study also revealed that most common IT-related material weaknesses had to do with access controls, change management, and documentation. Implementing a specific control framework to address these areas can provide actionable plan for bringing IT systems into compliance. For example, here's one COBIT 5 requirement concerning change management:

COBIT DS9.1-- Configuration Repository and Baseline Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.

Clearly, the detail level of COBIT's instructions will suffice in creating a precise action plan. In this case, configuration management (CM) tools like GuardRail can be implemented by IT as a system of record for configuration items, thereby satisfying COBIT DS9.1.

The Importance of Baselining

To determine if a measure is within the boundaries of control, a point of reference needs to exist for comparison. This is commonly referred to as the baseline, or starting point from which future states of deviations and changes can be measured. For example, to determine if systems have drifted out of compliance, a comparison is made between the current state and the baseline-- the previous "known good" state that was in line with regulatory requirements prior to the drift/changes.

Baselines are a key component of change management as they make powerful comparative analyses possible. Since control frameworks like COBIT 5 focus heavily on the firm's control over the change management process, baselining should also be a critical component of IT's compliance efforts. Powerful CM platforms like UpGuard were designed for this, capturing "golden" system configurations and infrastructure/environment states for control purposes and future remediation activities. Solutions like Puppet or Chef can double as automation tools as well as repositories for executable code that can serve as evidence of material control.

"In system administration, the same best practices documents that are used in auditing would help in configuring a system baseline."

- SANS Institute's "Quick and Effective Windows System Baselining and Comparative Analysis for Troubleshooting and Incident Response"

Overarching Benefits of Control Frameworks

The reality is that compliance laws and measures are implemented to maintain a safe environment for banks/financial services firms and customers to transact. Even as the threat of stiff penalties and criminal sanctions for non-compliance casts an ominous shadow over all concerns, the pursuit of compliance invariably leads to better control measures and processes being put in place. Control frameworks like COBIT 5 are indispensable and should be implemented, if even just for improving the firm's information technology governance and management practices. Tighter security and control mechanisms serve to protect customer data, corporate assets, as well as appease the relevant oversight bodies and auditors. Banks and financial services firms may face a myriad of challenges to attain compliance, but ultimately realize superior gains and opportunities from the resultant changes.

III. Main Compliance Laws and Standards

Various types of compliance measures and standards exist, and may apply depending on what type of banking or financial services a firm provides. Some are federally mandated laws, while others provide assurances to customers and governing bodies who require certain levels of security and control. The following is a list of items likely to affect firms engaged in banking and finance, followed by tips and advice for attaining compliance status.

Sarbanes-Oxley (SOX) Act of 2002

Purpose	To protect investors and shareholders of a publicly-traded company from corporate accounting fraud and deception. Strict reforms were mandated by the legislation to improve transparency in corporate financial disclosures.
Type	US Federal Law
Applies To	U.S. public company boards, management and public accounting firms.
Requirements	For publicly held companies, internal controls and procedures for financial reporting must be implemented to reduce the possibility of corporate fraud. SOX Sections 302, 409, and 404 in particular mandates internal controls and procedures for financial reporting be established, documented, tested, and maintained for quality and accuracy.
Non-Compliance Penalty	Civil and/or criminal sanctions, including imprisonment.
Tools for Compliance	COBIT 5 framework, software tools for security, CM, and automation.
Material Evidence of Control	Assets and artifacts per COBIT, logs and reports generated from tools/software used for control and internal auditing purposes.
For More Information	http://www.sec.gov/about/laws/soa2002.pdf

Graham Leach Bliley Act (GLBA)

Purpose	To control the ways that financial institutions deal with the private information of individuals.
Type	US Federal Law
Applies To	All financial institutions
Requirements	Requires that firms ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.
Non-Compliance Penalty	Civil and/or criminal sanctions, including imprisonment.
Tools for Compliance	Specific guidelines provided by the Federal Financial Institutions Examination Council (FFIEC), software tools for monitoring, security, CM, and automation.
Material Evidence of Control	Assets and artifacts per COBIT, logs and reports generated from tools/software used for control and internal auditing purposes.
For More Information	https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

PCI DSS

Purpose	To enforce the implementation and management of proper security and control measures for protecting cardholder data.
Type	Proprietary standard created by the Payment Card Industry Security Standards Council
Applies To	All merchants who accept electronic payments online.
Requirements	12 requirements broken into multiple sub-requirements for payment card security policies, procedures and guidelines.
Non-Compliance Penalty	Penalties from individual payment brands, loss of customer/partner trust, potential lawsuits
Tools for Compliance	Specific guidelines provided by the PCI Security Council (https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0), software tools for monitoring, security, CM, and automation.
Material Evidence of Control	Logs and reports generated from tools/software used for control and internal auditing purposes.
For More Information	https://www.pcisecuritystandards.org/

Statement on Standards for Attestation Engagements (SSAE 16/SAS 70)

Purpose	To verify the design of controls and their operating effectiveness.
Type	Standard created by the the Auditing Standards Board (ASB) of the AICPA (American Institute of Certified Public Accountants.)
Applies To	All service organizations.
Requirements	Calls for service organizations to give a description of controls and a description of its system.
Non-Compliance Penalty	Loss of customer/partner trust, potential lawsuits
Tools for Compliance	Software tools for monitoring, security, CM, and automation.
Material Evidence of Control	Assets and artifacts per COBIT 5, logs and reports generated from tools/software used for control and internal auditing purposes.
For More Information	http://ssae16.com/SSAE16_overview.html

Basel II

Purpose	Regulates finance and banking internationally to minimize the financial/operational risks faced by banking institutions.
Type	Regulation put forth by the Basel Committee on Bank Supervision
Applies To	Large investment banks active in international capital markets.
Requirements	Requires firms to properly identifying credit risk, market risk, and operational risk and verify they have enough capital to cover any potential losses due to said risks.
Non-Compliance Penalty	Loss of customer/partner trust, loss of favorable capital treatment, disfavor among international banking community.
Tools for Compliance	Software tools for monitoring, security, CM, and automation.
Material Evidence of Control	Assets and artifacts per COBIT 5, logs and reports generated from tools/software used for control and internal auditing purposes.
For More Information	http://www.bis.org/bcbs/index.htm

IV. Summary

A pragmatic approach to attaining compliance starts with determining which laws, measures, and certifications apply to your organization. This will shed light on which control framework can be used to map out objectives to actionable tasks, which in turn can carried out with the appropriate technologies and software tools. Frameworks like COBIT 5 are auditor-sanctioned and comprehensive enough to satisfy several compliance laws and/or measures at once.

Baselining is critical activity to change management and related compliance requirements, as it documents the configurations of a system's known good state for use in troubleshooting, remediation, and auditing. Solutions capable of creating baselines for control efforts (e.g., CM platforms like GuardRail or automation tools like Puppet or Chef) are essential to compliance efforts. These tools also create the necessary artifacts that can serve as material evidence of control to auditors.

In short, the markets of tomorrow are full of opportunities but also rife with numerous pitfalls. Though compliance laws and measures may have been originally created to protect the interests of consumers and the general public, in reality the lion's share of benefits go to firms that have reached or are undergoing compliance efforts, as substantial operational improvements are almost guaranteed. Compliance may indeed be a necessary evil, but it need not be looked down upon as such. Beyond the avoidance of fines, penalties, and sanctions are the important intrinsic values of compliance: better security, controls, and business as a whole. ■

V. Appendix

References

http://www.financialexecutives.org/KenticoCMS/Financial-Executive-Magazine/2012_07/Sarbanes-Oxley--A-Decade-Later.aspx#ixzz3W09KeZes

http://blogs.wsj.com/moneybeat/2013/09/19/sarbanes-oxley-harpoons-the-whale/

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

http://www.hunton.com/files/Publication/cfe049cf-6aec-4319-a6cc-30343048e8da/Presentation/PublicationAttachment/484fc409-20fd-4f86-8eec-5c6c78435eae/Hladjk_IT_compliance-security.pdf

http://www.ffiec.gov/pdf/authentication_guidance.pdf)
http://www.sans.org/reading-room/whitepapers/incident/quick-effective-windows-system-baselining-comparative-analysis-troubleshooting-inci-33884

http://www.coresecurity.com/ffiec-information-security-guidelines

http://www.tripwire.com/regulatory-compliance/basel-ii/

http://www.coresecurity.com/system/files/attachments/2014/06/Core-Security-PCI-DSS-matrix-6-14.pdf

http://www.metricstream.com/insights/IT_sys_val.htm

http://searchcompliance.techtarget.com/definition/control-framework

http://www.sox-online.com/coso_cobit.html

http://www.investopedia.com/terms/b/baselii.asp