Third Party Regulatory Compliance: What IT Auditors and Risk Professionals Need to Know

Marta O'Shea

Global Regulatory Audit and Exam Readiness Program Executive

IBM

Governance, Risk & Compliance – G31



NOVEMBER 9-11, 2015

HOTEL NIKKO-SAN FRANCISCO

SF ISACA FALL CONFERENCE

AGENDA

- 1. Introduction
- 2. Overview of US Financial Services Regulatory Landscape
 - a. Regulatory Organizations
 - b. Key IT Guidelines
 - c. Third Party Relationship Management Guidelines
- 3. Deep Dive: Third Party Relationship Regulatory Guidelines
 - a. Five Phases of Relationship Lifecycle
 - b. Three Elements of Governance
- 4. Summary
 - a. IBM's Response to Third Party Regulatory Guidelines
 - b. Final Remarks
- 5. Questions

Disclaimer: IBM does not provide legal advice or represent or warrant its services or products will ensure that client is in compliance with any law or regulation.



1. Introduction



1. Introduction: My Background



- Began working with IBM in January 2015 and am a Certified Information Systems
 Auditor with 14 years of experience in IT audit. Prior to IBM, I worked with Visa for
 7 years, and prior to that with Charles Schwab for 7 years. I also worked for 10
 years in Operations roles in large-scale data centers, before switching to Audit.
- At Visa, I led the IT Audit team so am highly familiar with technology industry standards, guidelines and regulatory requirements for the financial services sector, including guidance issued by FFIEC agencies, NIST, the PCI Standards Council, ISACA and ISO.
- Throughout my career in Audit, I have routinely interacted with US FFIEC examiners to represent both Visa and Charles Schwab's IT audit programs, subsequently gaining deep insights into their expectations and preferences.
- I was hired specifically by IBM to establish a Global Third Party Regulatory Compliance Program focused on the Financial Sector. My technology control experience complements my new assignment at IBM, since technology considerations are specifically referenced in global regulatory guidance for third party risk management.



1. Introduction: Stories From Recent History

- Some incidents that may have influenced financial sector regulatory guidance around the management of third parties:
 - -Mortgage crisis in late 2000's
 - Heartland, Global Payments, Target data breaches



2. Overview of US Financial Services Regulatory Landscape



- 2. US Financial Services Regulatory Landscape: Regulatory Organizations
- FFIEC (Federal Financial Institutions Examination Council)
 - –Primary members are:
 - FDIC (Federal Deposit Insurance Corporation)
 - FRB (Federal Reserve Board)
 - OCC (Office of Comptroller of the Currency)



US Financial Services Regulatory Landscape: Key IT Guidelines

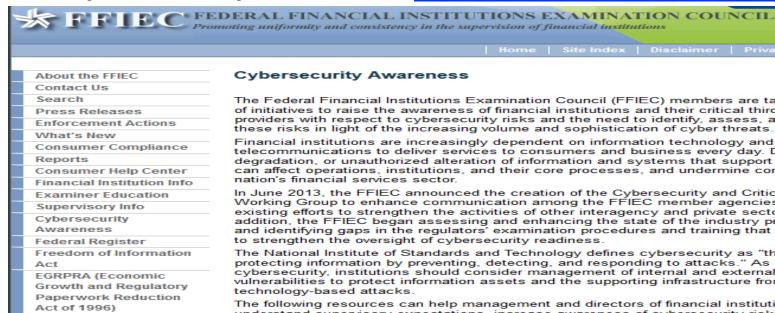
FFIEC IT Examination Handbooks: http://ithandbook.ffiec.gov/it-booklets.aspx





2. US Financial Services Regulatory Landscape: **Key IT Guidelines**

FFIEC Cybersecurity Awareness: http://www.ffiec.gov/cybersecurity.htm



Cybersecurity Awareness

The Federal Financial Institutions Examination Council (FFIEC) members are taking a number of initiatives to raise the awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

Financial institutions are increasingly dependent on information technology and telecommunications to deliver services to consumers and business every day. Disruption, degradation, or unauthorized alteration of information and systems that support these services can affect operations, institutions, and their core processes, and undermine confidence in the nation's financial services sector.

In June 2013, the FFIEC announced the creation of the Cybersecurity and Critical Infrastructure Working Group to enhance communication among the FFIEC member agencies and build on existing efforts to strengthen the activities of other interagency and private sector groups. In addition, the FFIEC began assessing and enhancing the state of the industry preparedness and identifying gaps in the regulators' examination procedures and training that can be closed to strengthen the oversight of cybersecurity readiness.

The National Institute of Standards and Technology defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks.

The following resources can help management and directors of financial institutions to understand supervisory expectations, increase awareness of cybersecurity risks, and assess and mitigate the risks facing their institutions.

Cybersecurity Assessment Tool

FFIFC Resources

- FFIEC Cybersecurity Assessment Tool Presentation
- FFIEC Statement on Destructive Malware (PDF)
- FFIEC Statement on Compromising Credentials (PDF)
- FFIEC IT Examination HandBook InfoBase
- Introduction to the FFIEC's Cybersecurity Assessment
- May 7, 2014 Webinar: Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See.



2015 Fall Conference - "CyberSizeIT" November 9 - 11, 2015

- 2. US Financial Services Regulatory Landscape: Third Party Relationship Management Guidelines
- FDIC Financial Institution Letter 44-2008 Guidance for Managing Third Party Risk
 - https://www.fdic.gov/news/news/financial/2008/ fil08044a.html
- FRB Supervision & Regulation Letter 13-19 Guidance on Managing Outsourcing Risk
 - http://www.federalreserve.gov/bankinforeg/srletters/ sr1319a1.pdf
- OCC Bulletin 2013-29 Third Party Relationships Risk Management Guidance
 - http://occ.gov/news-issuances/bulletins/2013/ bulletin-2013-29.html



3. Deep Dive: Third Party Relationship Regulatory Guidelines



- 3. Five Phases of Third Party Relationship Lifecycle
- 1. Planning & Risk Assessment
- Due Diligence & Third Party Selection
- 3. Contract Negotiations
- 4. On-going Monitoring
- 5. Termination



3. Three Elements of Governance During Third Party Relationship Lifecycle

- Oversight & Accountability
- Documentation & Reporting
- Independent Reviews



Five Phases of the Third Party Relationship Lifecycle



- 3. Five Phases of Third Party Relationship Lifecycle: **Planning & Risk Assessment**
- Developing a plan to manage the relationship is often the first step in the third-party risk management process. This step is necessary when a bank is considering contracts with third parties that involve critical activities.



- 3. Five Phases of Third Party Relationship Lifecycle: **Due Diligence & 3**rd **Party Se**lection
- Conducting a review of a potential third party before signing a contract helps ensure that the bank selects an appropriate third party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite.



3. Five Phases of Third Party Relationship Lifecycle: **Due Diligence & 3**rd **Party Selection**

16 areas of focus:

Strategies & Goals	Management of Information Systems
Legal & Regulatory Compliance	Resilience
Financial Condition	Incident Reporting & Management Programs
Business Experience & Reputation	Physical Security
Fee Structure & Incentives	Human Resource Management
Qualifications, Backgrounds & Reputations of Company Principals	Reliance on Subcontractors
Risk Management	Insurance Coverage
Information Security	Conflicting Contractual Arrangements with Other Parties



- 3. Five Phases of Third Party Relationship Lifecycle: **Contract Negotiations**
- Developing a contract that clearly defines expectations and responsibilities of the third party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance.



3. Five Phases of Third Party Relationship Lifecycle: **Contract Negotiations**

18 areas of focus:

Nature and Scope of Arrangement	Cost and Compensation	Insurance
Performance Measures or Benchmarks	Ownership and License	Dispute Resolution
Responsibilities for Providing, Receiving, and Retaining Information	Confidentiality and Integrity	Limits on Liability
The Right to Audit and Require Remediation	Business Resumption and Contingency Plans	Default and Termination
Responsibility for Compliance With Applicable Laws and Regulations	Indemnification	Customer Complaints
Subcontracting	Foreign-Based Third Parties	OCC Supervision



- 3. Five Phases of Third Party Relationship Lifecycle: **On-going Monitoring**
- Performing ongoing monitoring of the third-party relationship once the contract is in place is essential to the bank's ability to manage risk of the third-party relationship.



3. Five Phases of Third Party Relationship Lifecycle: **On-going Monitoring**

15 areas of focus:

Business Strategy & Reputation	Management of Information Systems
Legal & Regulatory Compliance	Resilience
Financial Condition	Incident Reporting & Management Programs
Insurance Coverage	Physical Security
Key Personnel & Retention of Essential Knowledge	Customer Relationship Management
Pro-active Risk Management	Reliance on Subcontractors
Timely Control Enhancement That Considers External Landscape	Conflicting Contractual Arrangements with Other Parties
Information Security	



- 3. Five Phases of Third Party Relationship Lifecycle: **Termination**
- Developing a contingency plan to ensure that the bank can transition the activities to another third party, bring the activities in-house, or discontinue the activities, if appropriate.



Three Elements of Governance During the Third Party Relationship Lifecycle



- 3. Three Elements of Governance During Third Party Relationship Lifecycle: **Oversight & Accountability**
- Assigning clear roles and responsibilities for managing thirdparty relationships and integrating the bank's third-party risk management process with its ERM framework enables continuous oversight and accountability.



- Three Elements of Governance During Third Party Relationship Lifecycle: **Documentation &** Reporting
- Proper documentation and reporting facilitates oversight, accountability, monitoring, and risk management associated with third-party relationships.



- 3. Three Elements of Governance During Third Party Relationship Lifecycle: **Independent Review**
- Conducting periodic independent reviews of the risk management process enables management to assess whether the process aligns with the bank's strategy and effectively manages risk posed by third-party relationships.



4. Summary



4. IBM's Response to Third Party Regulatory Guidelines

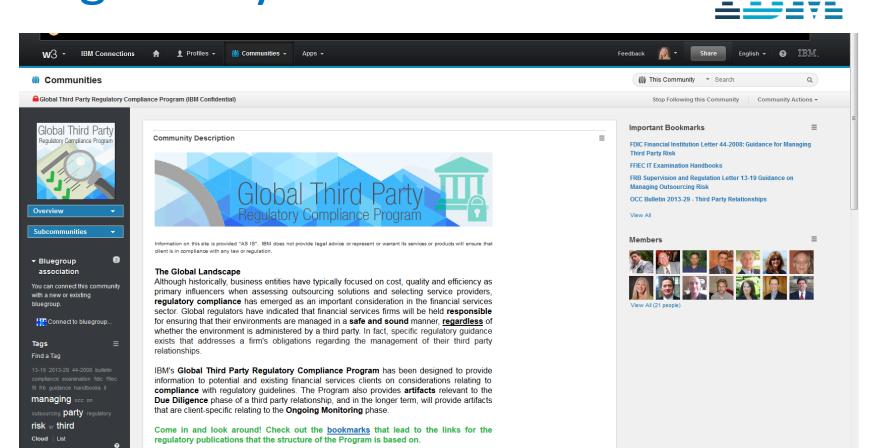
Global Financial Sector Third Party Regulatory Compliance Program

Key Program Characteristics

- Provision of a web-enabled tool that provides guidance to clients and relevant IBM personnel (i.e. deal and delivery teams) on regulatory requirements for managing risk associated with the use of third parties, throughout the life-cycle of the relationship
- Guidance is structured based on considerations articulated in Third Party Risk Management publications from the US FDIC, FRB and OCC
- Provision of key artifacts that clients can download, to demonstrate their intent to evidence a well-managed third party relationship, throughout the life-cycle of that relationship:
 - **Due Diligence Phase**: 16 elements referenced, with guidance on compliance considerations for each, and sample base-level artifacts available for download that substantiate IBM's profile
 - On-Going Monitoring Phase: To preserve client security, each client is assigned their own separate web-enabled "container". 15 elements for On-Going Monitoring referenced, with client-specific and generic IBM artifacts provided for download



4. IBM's Response to Third Party Regulatory Guidelines



Click on the Relationship Lifecycle button below to understand more about the typical third party relationship lifecycle phases and governance actions that regulators have described in their publications, including quidance on what types of and how much work should be done to

demonstrate an intent to comply and how IBM can help

San Francisco Chapter

4. Final Remarks

 Financial regulatory guidance could be leveraged across any industry "It represents good business practice"

 Degree of application of the guidance should depend on the scale, risk and nature of the activities being outsourced



4. Final Remarks

Outsourcing critical activities can result in a reduction in an organization's overall risk profile, if the third party has strong controls and governance



5. Questions



THANK-YOU!

