FFIEC Handbook Guide and Emerging Areas of Focus

Brian Bettle CISSP, CISA
Federal Reserve Bank of Atlanta
Brian.Bettle@atl.frb.org

FIBA

Organized by:

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Agenda:

- FFIEC Handbook Overview
- Emerging Areas of Focus:
  - SR 11-9 *Interagency Supplement to Authentication in an Internet Banking Environment*
  - *FFIEC reference document on External Cloud Computing*
  - *Future Regulatory Direction*

FFIEC Handbook Overview

•The Federal Financial Institution Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS). Visit the Council's website for press releases and information on the mission and work of the Council at:

http://www.ffiec.gov/

http://ithandbook.ffiec.gov/

FFIEC Handbook Overview

- Audit
- Business Continuity Planning
- Development and Acquisition
- E-Banking
- Information Security
- Management
- Operations
- Outsourcing Technology Services
- Retail Payment Systems
- Supervision of Technology Service Providers
- Wholesale Payment Systems


FFIEC
IT Examination HandBook InfoBase
IT Booklets
Resources
Reference Materials
Presentations
Glossary
Help
Search
What's New
Audit
Business Continuity Planning
Development and Acquisition
E-Banking
Information Security
Management
Operations
Outsourcing Technology Services
Introduction
Board and Management Responsibilities
Risk Management
Related Topics
Appendix A: Examination Procedures
Appendix B: Laws, Regulations, and Guidance
Appendix C: Foreign-Based Third-Party Service Providers
Appendix D: Managed Security Service Providers
Retail Payment Systems
Supervision of Technology Service Providers
Wholesale Payment Systems
Welcome » IT Booklets » Outsourcing Technology Services
Outsourcing Technology Services
The "Outsourcing Technology Booklet" is one of several that comprise the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook).
Downloads
Printable Version of Outsourcing Technology Services IT Booklet
Workprogram - Generic word-processing version
Workprogram - Microsoft Word 2007 version
MSSP Workprogram - Microsoft Word 2007 version
Chapters
Introduction
Board and Management Responsibilities
Risk Management
Related Topics
Appendix A: Examination Procedures
Appendix B: Laws, Regulations, and Guidance
Appendix C: Foreign-Based Third-Party Service Providers
Appendix D: Managed Security Service Providers
Sitemap | Disclaimer | Privacy Policy

SR 11-9 ***Interagency Supplement to Authentication in an Internet Banking Environment***

- ***Supplement to SR 05-19***
- ***The evolving security threats required enhancements to security controls***

Supplement: Key Points

- Annual, or as needed, risk assessment updates
- Recognize the differing risk between retail and commercial accounts
- Layered security for all “high risk” accounts/transactions
- **Minimum layered security for all accounts**
  - **Suspicious activity detection and response**
  - **Additional control over admin functions for business**
- Simple device ID and challenge questions are no longer effective as primary control
- Customer awareness

Suspicious Activity Detection

- Method to identify suspicious behavior
  - At user login/authentication
  - Upon funds transfer to another party
- Detection can be automated or manual; includes “learned” baselines or user set baselines
- Response can be preventive (halt behavior) or detective (verify/notify of behavior)
- Based on a risk assessment
  - The risk assessment determines where in the process to place anomaly detection

Outsourced Cloud Computing

- FFIEC issued guidance "for information purposes only" July 10, 2012
- There is no clear definition: generally cloud computing is the migration from owned resources to shared resources in which client users receive IT services on demand, from a third-party
- Firms that contemplate or use a cloud model that is outsourced should consider the FFIEC IT Handbooks, particularly: *Outsourcing Technology Services Booklet*

Cloud Computing Risks

- Operations and Outages
- Monitoring
- SLA's
- Staffing
- Confidentiality
- Outside Providers
  - Does your vendor outsource your key operations to another cloud vendor?
- Breaches

Business Impact Analysis

- How will we be harmed if the asset became widely public and distributed?
- How will we be harmed if an employee of our cloud provider accessed the asset?
- How would we be harmed if the process or function were manipulated by an outsider?
- How would we be harmed if the process of function failed to provide expected results?
- How would we be harmed if the information/date were unexpectedly changed?
- How would we be harmed if the asset were unavailable for a period of time?

Protecting Yourself

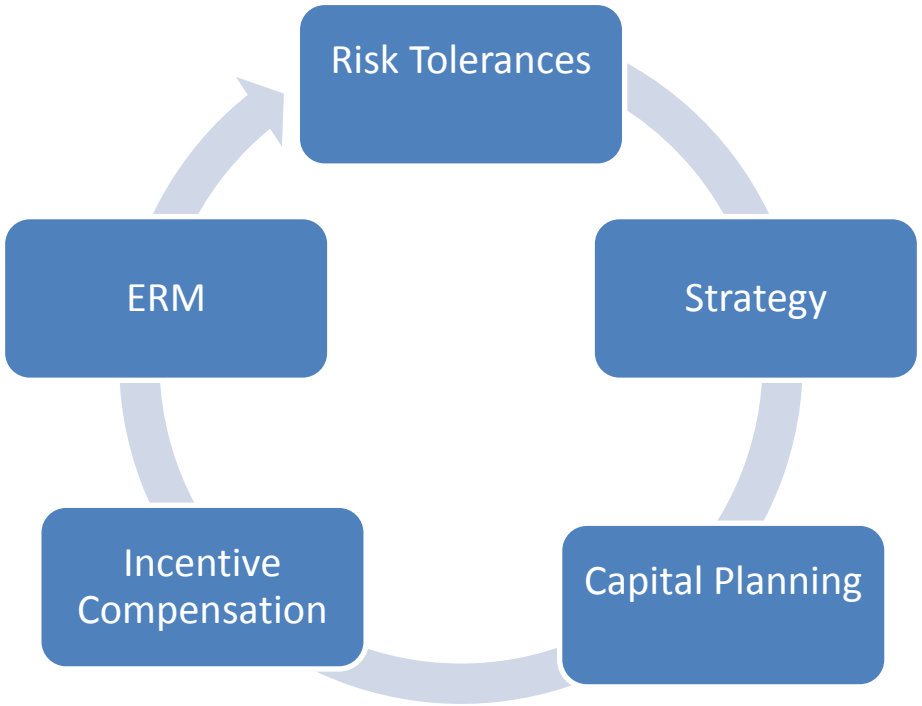
- Establish expectations in the contract
- Define SLA's
- **Insist on the Right to Audit (including downstream vendors)**
- Agree on Notification Requirements
- Document Minimum Certification Requirements
- Articulate any Specific Control Requirements

Additional Information

- ITIL Service Delivery Library
- ISO 20000 Series- Standard for Service Management
- Center for Internet Security
- NIST 800 Series
- A6 / CloudAudit.org
- Cloud Security Alliance

Future Regulatory Direction

- Vendor management focus
- Risk Management Convergence



Questions?