Overview

IT Security & Cloud Guidance for Financial Institutions

Dan Pepper and Susan Linda Ross, Norton Rose Fulbright US LLP

Bloomberg Law

IT Security & Cloud Guidance for Financial Institutions

Contributed by Dan Pepper, and Susan Linda Ross, Norton Rose Fulbright US LLP

The following overview describes key federal regulatory guidance on IT security and cloud computing for financial institutions.

Interagency Guidelines Establishing Information Security Standards

In 2014, Board of Governors of the Federal Reserve System (Federal Reserve Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) issued guidelines on information security standards (Guidelines) that appear in 12 C.F.R. Part 364, Appendix B. The Guidelines set forth standards pursuant to sections 501 and 505(b), 15 U.S.C. §§ 6801 and 6805(b), of the Gramm-Leach-Bliley Act of 1999 (GLBA). The Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

The Guidelines require each financial institution to implement a written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. The program must be designed to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. Ensure the proper disposal of customer information and consumer information.

The Board of Directors (or appropriate committee) must approve and oversee the program.

The Guidelines also provide a list of requirements for each financial institution, which in summary reads:

1. Identify reasonably foreseeable internal and external threats.
2. Assess the likelihood and potential damage of these threats.
3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.
4. Design the information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the institution's activities:
    a. Access controls on customer information systems.
    b. Access restrictions at physical locations containing customer information;
    c. Encryption of electronic customer information, including while in transit or at rest;
    d. Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program;
    e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
    f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
    g. Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems; and

h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

5. Train staff to implement the institution's information security program.

6. Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the institution's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

7. Develop, implement, and maintain, as part of the institution's information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the Guidelines' requirements governing the development and implementation of information security programs.

8. Exercise appropriate due diligence in selecting the institution's service providers.

9. Require the institution's service providers by contract to implement appropriate measures designed to meet the objectives of the Guidelines.

10. Where indicated by the institution's risk assessment, monitor its service providers to confirm that they have satisfied their obligations.

11. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of the institution's customer information, internal or external threats to information, and the institution's own changing business arrangements.

12. Report to the institution's board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the institution's compliance with the Guidelines. The report, which will vary depending upon the complexity of each institution's program should discuss material matters related to its program, addressing issues such as: Risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.

Security in a Cloud Computing Environment

On April 30, 2020, the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee (collectively known as the FFIEC–Federal Financial Institutions Examination Council) issued guidance for risk management principles to financial institutions with operations in the cloud (*see* FFIEC Cloud Computing Statement). The FFIEC provided examples (not requirements) of relevant risk management practices for assessing risks related to and implementing controls. While not all examples the FFIEC will apply to all financial institutions, the considerations include the following:

Governance

Before moving to a third-party cloud service provider, the financial institution should consider "the appropriate level of governance, the types of systems and information assets considered for cloud computing environments, the impact on the financial institution's architecture and operations model, and management's comfort with its dependence on and its ability to monitor the cloud service provider."

Cloud Security Management

Due Diligence and Oversight. The FFIEC stated that "the process for risk identification and controls effectiveness may include testing or auditing, if possible, of security controls with the cloud." Nevertheless, the FFIEC recognized that some cloud service providers will not permit audits, and allowed management to accept independent audit reports such as SOC reports, as well as the tools and configuration management capabilities provided as part of the cloud services to monitor security provided by the cloud service provider.

Contract with Cloud Service Provider. The FFIEC indicated that the contract "should be drafted to clearly define which party has responsibilities for configuration and management of system access rights, configuration capabilities, and deployment of services and information assets to a cloud computing environment, among other things." Items to consider including in the contract include:

- management of encryption keys;
- security monitoring;
- vulnerability scanning;
- system updates;
- patch management;
- independent audit requirements;
- operational resilience capabilities;
- incident response obligations, including reporting, communication, and forensics;
- notification or approval requirements for the use of subcontractors (i.e., fourth parties);
- data ownership; and
- expectations for removal and return of data.

Security Configuration, Provisioning, Logging, and Monitoring. Misconfiguration of cloud resources is a "prevalent" vulnerability. The FFIEC allows financial institutions to use their own tools or those of the cloud service provider, but "a key consideration is the regular testing of the effectiveness of those controls to verify that they are operating as expected."

Resilience and Recovery

Business Continuity and Disaster Recovery. "Operations moved to cloud computing environments should have resilience and recovery capabilities commensurate with the risk of the service or operation for the financial institution."

Incident Response Capabilities. The FFIEC stated that the cloud "presents unique forensic issues related to jurisdiction, multi-tenancy, and reliance on the cloud service provider for a variety of forensic activities. Additionally, the service level agreement should identify specific activities for incident response and identify the cloud service provider's responsibilities in the event of an incident."

Audit and Controls Monitoring

Monitoring of Cloud Service Provider. The FFIEC listed several oversight and monitoring activities that financial institutions could take with respect to cloud service providers:

- requesting, receiving, and reviewing security and activity reports from the cloud service provider;
- reports of compliance with service level agreements;
- product validation reports; and
- reports of independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments) performed on the cloud computing services.

Unique Aspects of Cloud Environments. The FFIEC guidance provides several examples of the unique risk aspects of cloud computing, including management of virtual infrastructure through cloud security tools such as the use of "containers" in cloud computing environments, referred to as microservices. These examples of how cloud environments can be more difficult to manage than on-premises technology include oversight and monitoring activities include requesting, receiving, and reviewing security and activity reports from the cloud service provider; reports of compliance with service level agreements; product validation reports; and reports of independent assurance as well as reviews (e.g., audits, penetration tests, and vulnerability assessments) performed on the cloud computing services.

Outsourcing Technology Services

In 2004, the FFIEC issued the Outsourcing Technology Services – IT Examination Handbook (Handbook), which the FFIEC referenced in the 2020 cloud guidance above. *See* FFIEC Outsourcing Technology Services.

The 94-page Handbook is not a set of requirements for financial institutions, but rather is guidance for examinations performed on a financial institution's outsourced technology services.

The Handbook provides useful guidance for a range of different outsourcing types, including more than forty pages on Managed Security Service Providers (MSSPs). The FFIEC also listed additional risk factors in the event the service provide is based outside the United States:

- Country risk;
- Compliance risk;
- Export controls;
- Due diligence;
- Contracts;
- Security, confidentiality, and ownership of data;
- Regulatory authority;
- Choice of law;
- Monitoring and oversight; and
- Regulatory agency access to information. Per the Handbook, "[a]n organization's use of a foreign-based third-party service provider (and the location of critical data and processes outside of U.S. territory) must not compromise the ability of U.S. regulatory authorities to effectively examine the organization."

Supervision of Technology Services Providers

In 2012, the FFIEC issued another IT Examination Handbook, this time on the supervision of technology services providers. *See* FFIEC Supervision of Technology Service Providers. This handbook covers guidelines of the risks to be addressed by financial institutions and their service providers, including whether the financial institution is providing technology services to others.