Assessment and Compliance with Federal Financial Institutions Examination Council (FFIEC) Requirements

DataGuardZ White Paper

What is the history behind FFIEC compliance?

Regulations from the Federal Financial Institution Examination Council (FFIEC) were put in place to protect against system disruptions-via natural disasters, cyber terrorism, or security breach-that threaten the security of both the institution and its customer information.

Compliance with FFIEC means comprehensive assessments of the control framework, continuous monitoring, control implementation and risk identification, mitigation and reporting.

FFIEC -- What is it?

The Federal Financial Institutions Examination Council (FFIEC) was established in 1979. It was given the authority to "prescribe uniform principles, standards, and report forms for the federal examination of financial institutions" under the authority of five agencies: the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

FFIEC -- IT Handbooks

The FFIEC issued booklets that address IT Risk Management that make up the FFIEC IT Examination Handbooks. The FFIEC publication of various examination handbooks includes the following:

- **The Audit Booklet** provides guidance on the risk-based IT audit practices of financial institutions and technology service providers. This booklet builds on the agencies' existing audit guidance and emphasizes the responsibilities of all levels of management and the board of directors for establishing a sound audit program. The booklet incorporates changes to the audit process brought about by the Gramm-Leach-Bliley Act of 1999 and the Sarbanes-Oxley Act of 2002.

- **The Information Security Booklet** provides guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices. The booklet addresses changes in technology, risk assessments, mitigation strategies, and regulatory guidance. The discussion of risk assessment reflects the maturation of that process related to information security. New or revised material is included regarding authentication, monitoring programs, and software trustworthiness. Many additional topics including malware, wireless, remote access, and trust services have also been incorporated or revised. The security of financial institutions' systems and information is essential to maintaining the privacy of customer information and safe and sound operations. The booklet describes how an institution should protect and secure the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers (TSPs) to maintain effective security programs tailored to the complexity of their operations.

- **The Business Continuity Planning Booklet** provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. The booklet includes enhancements to the business impact analysis and testing discussions and addresses emerging threats and lessons learned in recent years. The booklet also stresses the responsibilities of each institution's board and management to address business continuity planning with an enterprise-wide perspective by considering technology, business operations, communications, and testing strategies for the entire institution. Key elements of the FFIEC's December 2007 Interagency Statement on Pandemic Planning have been added to the booklet. A pandemic outbreak would present unique business continuity challenges. The methodologies detailed in the booklet provide a framework for financial institutions to develop or update their pandemic preparedness plans. All financial institutions should have plans that address how the institution will function during a pandemic event. The booklet also highlights the importance of business continuity planning for all financial institutions, regardless of whether their systems are provided in-house or through thirdparty service providers, as well as the lessons learned from financial institutions that suffered damage from hurricanes Katrina and Rita.

- **The E-Banking Booklet** provides guidance on risks and risk management practices applicable to a financial institution's e-banking activities. E-banking has created new opportunities for delivering traditional products and services to customers, as well as the potential to offer new products and services. With these opportunities come new challenges, including 24-hour, seven-day-a-week availability; Internet connectivity; increased access to systems and customer information; greater reliance on new service providers; and evolving regulations. These challenges increase threats to the institution's reputation, confidentiality of information, system and data integrity, system availability, and regulatory compliance. E-banking activities require careful planning, coordinated strategies between IT and business units, integrated subject matter expertise, strong controls, and ongoing monitoring and testing. This booklet includes guidance and examination procedures to evaluate the quality of risk management related to these threats and activities in financial institutions and technology service providers.

- **The Development and Acquisition Booklet** provides guidance on development, acquisition, and maintenance projects; project risks; and project management techniques. The booklet emphasizes the use of standardized policies, detailed plans, and well-structured project management techniques when directing project activities and controlling project risks. Effective development and acquisition should result in sound information systems that provide specific functionality, reliability, and strong security.

- **The Management Booklet** provides guidance on the risks and risk management practices applicable to financial institutions' information technology activities. Sound IT management is critical to the performance and success of a financial institution. An institution capable of aligning

its IT activities to support its business strategies adds value to its organization and positions itself for sustained success. The board of directors and executive management should understand and take responsibility for IT management as a critical component of their overall strategic planning and corporate governance efforts.

- **The Operations Booklet** provides guidance on the risks and risk management practices applicable to financial institutions' technology operations. Effective support and delivery from IT operations are vital to a financial institution's performance and success. The role that technology plays in supporting the business function has become increasingly complex. IT operations have become more dynamic and include distributed environments, integrated applications, telecommunication options, Internet connectivity, and an array of computer platforms. The booklet discusses tactical and strategic support and delivery risks, and the controls that should be in place to address those risks.

- **The Outsourcing Technology Services Booklet** provides guidance on the risks and risk management practices applicable to financial institutions' outsourcing IT activities, including service provider selection, contract issues, and ongoing monitoring of the relationship. The booklet also includes guidance on the risks and risk management issues unique to foreign service providers. Outsourcing an activity does not relieve management and the board of directors of their responsibility to ensure a secure processing environment and the maintenance of data integrity. Thus, ongoing monitoring of the relationship is crucial to ensure the service provider follows the terms of the service level agreements, safeguards the confidentiality of information, and maintains operational stability.

- **The Supervision of Technology Service Providers Booklet** covers the supervision and examination of services performed for financial institutions by technology service providers. It outlines the agencies' risk-based supervision approach and the examination ratings used for technology service providers. The guidance stresses that an institution's management and board of directors have the ultimate responsibility for ensuring outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.

- **The Retail Payment Systems Booklet** provides guidance on the risks and risk management practices applicable to financial institutions' retail payment systems activities. The revised booklet, which updates the March 2004 Retail Payment Systems Booklet, addresses changes in technology and provides guidance on the Check Clearing for the 21st Century Act of 2004. This booklet also provides expanded guidance on merchant card processing and ACH activities. It provides a more in-depth discussion of the increased risks posed by these activities and some of the risk management tools that financial institutions can use to mitigate them. In addition, there is an increased emphasis on risk management practices related to third parties in the payments arena, such as Third-party-senders in ACH, or merchant processors in credit card networks. There is also

a brief discussion on emerging technologies in retail payment systems. The booklet includes information on remotely created checks and electronically created payment orders, both of which are being used more frequently as payment devices. Lastly, the booklet addresses remote deposit capture and provides examination procedures for use in conjunction with the FFIEC guidance, Risk Management of Remote Deposit Capture (January 14, 2009).

- **The Wholesale Payment Systems Booklet** provides guidance on the risks and risk management practices applicable to financial institutions' wholesale payment systems activities, including interbank and intrabank payments, messaging, and securities settlement systems. Financial institutions play an important role in wholesale payments systems. However, they face increasing challenges to meet demands for resiliency and reliability, while continuing to develop and deploy innovative payment solutions to meet expanding global payment processing demands. Because of these challenges, institutions must exercise greater diligence to ensure that confidentiality of information, system and data integrity, system availability, and regulatory compliance are maintained. Wholesale payment system activities require careful planning and coordination between IT and business units, and their operation must include strong internal controls and ongoing monitoring. The Wholesale Payment Systems Booklet includes examination procedures to evaluate the quality of risk management related to these activities in financial institutions and technology service providers.

IT Examination Handbooks are used by federal examiners when auditing the IT management, operations and security of financial institutions for due diligence and compliance with their obligations.

FFIEC: Who must comply?

Financial institutions that are regulated by the Federal Reserve System, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency and the Office of Thrift Supervision are subject to the examination standards of the FFIEC.

What is at stake if you don't follow the rules?

FFIEC compliance is mandatory and non-compliance may result in fines and penalties. For example, a first-tier penalty of up to $5,000 per day may be assessed on a financial services company for any violation. A third-tier fine of up to $1,000,000 per day may be assessed for any knowing or reckless violation.

If your organization suffers a breach that may have been prevented by following the FFIEC guidelines, your organization will not only by liable to penalties imposed by regulators, but it may also suffer the following:

Loss of client confidence - The loss of business due to an unforeseen confidential data loss or a security breach can be permanent. Data that is destroyed is seen within any industry, particularly financial, as a poor business process and the loss of consumer confidence are evident as well.

Data Breach Notification Laws - Now consider that while you may have the same devastating business loss as you suffered above, with a data breach, your organization may now have additional and expensive responsibilities. If the data that was lost is considered confidential and consumer related, it is considered a Security Data Breach that may require your organization to conform to any number of Data Breach Notification Laws or risk federal or state penalties. The notification process is very expensive; current estimates are over $200.00 per account lost, and penalties and fines are starting to increase to unrecoverable amounts.

So what are you required to do to comply with FFIEC mandates?

The Federal Financial Institutions Examination Council (FFIEC) has created the IT Handbooks and an exhaustive set of comprehensive control tests to assess its compliance, specifically related to controls over the confidentiality, integrity and availability of its systems as well as its third party service providers. Regulators are particularly interested in an effective enterprise wide methodology that identifies control weaknesses and that such weaknesses are being addressed in a timely manner.

Must periodic audits be performed to ensure FFIEC compliance?

YES! Consumer and institutional financial data must, at a minimum, ensure that its control framework is in accordance to the FFIEC IT Handbooks with the intent to ensure that confidential data remains protected. According to the FFIEC Information Security Handbook (page 68):

"Management is responsible for considering the following key factors in developing and implementing independent tests:

Personnel. Technical testing is frequently only as good as the personnel performing and supervising the test. Management is responsible for reviewing the qualifications of the testing personnel to satisfy itself that the capabilities of the testing personnel are adequate to support the test objectives.

Scope. The tests and methods utilized should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling security risks.

Data Integrity, Confidentiality, and Availability. Management is responsible for carefully controlling information security tests to limit the risks to data integrity, confidentiality, and system availability. Because testing may uncover nonpublic customer information, appropriate safeguards to protect the information must be in place.

Frequency. The frequency of testing should be determined by the institution's risk assessment. High-risk systems should be subject to an independent test at least once a year. Additionally, firewall

policies and other policies addressing access control between the financial institution's network and other networks should be audited and verified at least quarterly.

Why partner with DataGuardZ to ensure FFIEC compliance?

DataGuardZ provides services which help companies comply with FFIEC requirements by performing audits to determine the existence and/or effectiveness of controls required by the regulators. Our competent staff will provide a report focusing on the non-compliance with the guidelines, we then suggest a cost effective action plan which would mitigate risks while also satisfying the regulators by demonstrating management's goodwill and due diligence in managing IT risk. Furthermore, since we are independent of the company, our services may allow the regulatory agency and external auditors to rely on the results of our procedures to reduce the amount and extent of their evaluation procedures.

The extensive experience of our partners and personnel with internal control related services uniquely positions our firm to provide effective and detailed FFIEC Audit Preparation services. This experience allows us to provide logical solutions to issues encountered and as a result, may reduce the overall compliance effort for our clients.