VLCM's Cybersecurity Compliance Guide for Financial Institutions

Master the essentials of financial sector cybersecurity compliance with this comprehensive guide. Inside, you'll find concise overviews of key regulations, clear compliance checkpoints, and actionable insights to aid your compliance journey.

TABLE OF CONTENTS

About VLCM

Since 1983, VLCM, an accomplished IT solutions provider, has built its reputation on forging lifelong partnerships. Our strong relationships with clients and vendors underscore our commitment to delivering custom enterprise technology solutions that align with your unique business goals. We stay ahead of the curve through continuous learning, tackling complex business challenges, and offering innovative IT solutions. Our mission at VLCM transcends delivering solutions—it's about ensuring you consistently 'Get IT Right' and nurturing your business growth. Connect with us on LinkedIn, Facebook, Twitter, and Instagram at @vlcmtech, or visit www.vlcm.com. Let's collaborate to turn your IT complexities into strategic advantages for your business.

Introduction: Your Quick Reference for Cybersecurity Compliance

Cybersecurity compliance is a fundamental requirement for financial institutions. With a multitude of regulations and the ever-present cybersecurity threats, ensuring compliance is a constant endeavor. This guide is crafted to serve as your quick reference in this regard. It provides concise yet comprehensive information about key regulations, identifies the entities they affect, and presents the critical steps needed for compliance. Our objective is to simplify your path to compliance by offering a readily accessible, detailed, and informative resource. With this guide, mastering the essentials of cybersecurity compliance within the financial sector becomes a manageable task.

What is Financial Cybersecurity Compliance?

Financial cybersecurity compliance refers to the practice of adhering to legal, regulatory, and institutional standards that protect financial data from digital threats. Given the sensitive nature of financial data, it's crucial for institutions to meet these cybersecurity standards. Compliance ensures the integrity, confidentiality, and availability of this data, protecting not just the institutions but also their customers.

The Problem with Regulatory Compliance

While necessary, maintaining regulatory compliance can be challenging for financial institutions. The landscape of cybersecurity regulations is complex and ever-evolving, making it hard to keep track of all the requirements. In addition, implementing the required security measures can be costly and time-consuming. These challenges can result in compliance gaps, making institutions vulnerable to cybersecurity risks and penalties for non-compliance.

As we dive into this guide, we will explore these issues further and provide practical solutions for tackling the challenges of cybersecurity compliance in the financial sector.

How to Use This Guide

Our Cybersecurity Compliance Guide for Financial Institutions is a quick-reference resource aimed at assisting you in understanding and navigating key cybersecurity regulations. Here's a suggested approach to use this guide:

Refer to Specific Regulations: Each section of the guide is dedicated to a distinct regulation applicable within the financial sector. Familiarize yourself with the regulations that apply to your institution by referring to these individual sections.

Review Compliance Checkpoints: For each regulation, we have listed the key compliance checkpoints. These serve as a critical reference point for understanding what steps your institution needs to take to comply with each regulation.

By referring to this guide as a resource, you can enhance your understanding of your institution's regulatory obligations and take steps toward ensuring compliance.

The Top 8 Cybersecurity Regulations for Financial Institutions

1. GLBA

Gramm-Leach-Bliley Act

Summary

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. The Federal Trade Commission and other federal agencies enforce the GLBA, and noncompliance penalties include fines and criminal charges.

Who is Affected

Financial institutions, defined as entities of any size that are "significantly engaged" in providing financial products and services, including banks, insurance companies,
lenders, auto dealers that offer credit and leasing, payday lenders, professional tax preparers, real estate appraisers, and others.

Compliance Checkpoints

The GLBA has two core components:

1. The Safeguards Rule requires financial institutions to protect the consumer information they collect. Requirements include:
    a. Designating an individual or group to coordinate an information security program
    b. Identifying and assessing risks to customer data and evaluating the effectiveness of the existing controls
    c. Implementing, monitoring, and testing a safeguards program
    d. Evaluating the program when changes take place in business operations and other circumstances
    e. Ensuring service providers can maintain the appropriate safeguards
2. The Privacy of Consumer Information Rule (or Privacy Rule) requires regulated entities to inform consumers about their information-collection practices and to explain their rights to opt out. The rule includes requirements for the contents of the notices, delivery methods, and frequency.

Non-Compliance Penalties

- Financial institutions found in violation face fines of $100,000 for each violation.
- Individuals in charge found in violation face fines of $10,000 for each violation.
- Individuals found in violation can be put in prison for up to 5 years.

Resources

- FTC: How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act
- FTC: Updating you on FTC privacy and data security initiatives
- FTC: FTC Safeguards Rule: What Your Business Needs to Know

2. PCI-DSS

Payment Card Industry Data Security Standard

Summary

PCI-DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It was introduced by the major credit card companies to help prevent credit card fraud and protect cardholder data across three primary stages of the cardholder data lifecycle: Processing, Storage, and Transfer.

Who is Affected

Any organization that handles cardholder data from major credit cards, such as Visa, MasterCard, American Express, Discover, and JCB, needs to comply with PCI-DSS. This includes businesses of all sizes and sectors that process card payments, as well as third-party service providers that store, process, or transmit cardholder data on behalf of other businesses.

Compliance Checkpoints

The PCI-DSS is built around 12 requirements, divided into six control objectives:

1. **Build and Maintain a Secure Network and Systems:** This includes installing and maintaining a firewall configuration to protect cardholder data and not using vendor-supplied defaults for system passwords and other security parameters.
2. **Protect Cardholder Data:** Includes requirements to protect stored cardholder data and to encrypt the transmission of cardholder data across open, public networks.
3. **Maintain a Vulnerability Management Program:** Requires the use of and regular updates of anti-virus software and the development and maintenance of secure systems and applications.
4. **Implement Strong Access Control Measures:** Businesses need to restrict access to cardholder data by business need to know, assign a unique ID to each person with computer access, and restrict physical access to cardholder data.
5. **Regularly Monitor and Test Networks:** Track and monitor all access to network resources and cardholder data and regularly test security systems and processes.
6. **Maintain an Information Security Policy:** Maintain a policy that addresses information security for all personnel.

Non-Compliance Penalties

Non-compliance with PCI-DSS can result in penalties from the payment card brands, ranging from $5,000 to $100,000 per month. The exact amount depends on the size of the organization, its volume of transactions, the duration of non-compliance, and the severity of the non-compliance. Businesses may also be liable for the costs of any fraud or breaches that occur, as well as the associated costs of remediation, which can include forensic investigations, reissuing cards, and fines or lawsuits from affected customers.

In addition, non-compliant businesses may also suffer reputational damage, loss of customer trust, and could potentially lose the ability to accept card payments altogether if they are deemed to be a persistent offender.

Resources

- PCI: PCI DSS Quick Reference Guide
- PCI DSS Guide: What are the PCI Compliance Fines and Penalties?

3. FFIEC

The Federal Financial Institutions Examination Council Cybersecurity Resource Guidelines

Summary

The Federal Financial Institutions Examination Council (FFIEC) is a U.S. government interagency body that sets standards for the examination of financial institutions. The FFIEC provides guidelines to evaluate the safety and soundness of financial institutions, their compliance with consumer protection laws, and their adherence to community reinvestment standards. The IT-related guidelines issued by FFIEC are a crucial part of this evaluation process.

The FFIEC is governed by the following five financial regulators:

- The Board of Governors of the Federal Reserve (FRB) - Regulates Domestic Banks
- The Federal Deposit Insurance Corporation (FDIC) - Regulates Federal Banks
- The Office of the Comptroller of the Currency (OCC) - Regulates Federal Banks
- The National Credit Union Administration (NCUA) - Regulates credit unions.
- Consumer Financial Protection Bureau (CFPB) - Regulates banks, thrifts, and credit unions.

Who is Affected

The FFIEC guidelines affect all U.S. financial institutions, such as banks, credit unions, and savings and loan associations.

Compliance Checkpoints

1. **The FFIEC Cybersecurity Assessment Tool:**
   The FFIEC Cybersecurity Assessment Tool is designed to help financial institutions understand their inherent cybersecurity risks and readiness. It comprises two parts:

   Inherent Risk Profile: The tool identifies the institution's inherent risk across five categories: technologies and connection types, delivery channels, online and mobile products and technology services, organizational characteristics, and external threats. This assessment helps institutions understand the type and level of risk they inherently face before implementing any cybersecurity controls.

   Cybersecurity Maturity: The tool then determines the organization's maturity level across five domains: cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience. This helps institutions gauge their risk management practices and controls and identify areas for improvement.

2. **The FFIEC IT Examination Handbook Series:**
   The Handbook Series consists of eleven comprehensive guides that each focus on a specific area of IT for financial institutions:
   - **Information Security Handbook**: Offers guidance for establishing and maintaining an effective information security program.
   - **Management Handbook:** Discusses IT governance and risk management strategies.
   - **Business Continuity Management Handbook:** Provides direction on business continuity and disaster recovery plans.

- **Retail Payment Systems Handbook:** Details IT examination procedures for various retail payment systems.
- **Wholesale Payment Systems Handbook:** Focuses on wholesale payment systems' IT examination procedures.
- **Outsourcing Technology Services Handbook:** Guides on risk management for institutions outsourcing technology services.
- **Development and Acquisition Handbook:** Outlines the processes for managing risks in system development, acquisition, and maintenance.
- **Operations Handbook:** Discusses managing the operational controls and maintenance of an institution's IT operations.
- **Supervision of Technology Service Providers Handbook:** Offers guidance on managing relationships with third-party technology service providers.
- **Audit Handbook:** Provides guidelines for maintaining an effective IT audit function within the institution.
- **Mobile Financial Services Handbook:** Discusses risk management strategies for mobile financial services.

Each handbook provides a framework for identifying and managing risks associated with each specific area of IT in a financial institution. Using these handbooks, institutions can ensure a comprehensive approach to their IT risk management.

Non-Compliance Penalties

Non-compliance with FFIEC guidelines can lead to a range of penalties, depending on the severity and impact of the non-compliance. These can include formal and informal enforcement actions, which might involve corrective measures, fines, and penalties. Serious or repeated non-compliance can lead to the institution being deemed "unsafe or unsound," which can significantly affect its reputation and operations. Severe cases can lead to criminal charges and fines. Additionally, non-compliance can lead to higher costs due to potential data breaches, system failures, and service disruptions.

Resources

- FFIEC Cybersecurity Assessment Tool
- FFIEC IT Booklets (11)
- FFIEC Cybersecurity Resource Guide for Financial Institutions

4. SOX

Sarbanes-Oxley Act

Summary

The Sarbanes-Oxley Act (SOX) is a US federal law enacted to protect investors from fraudulent financial reporting by corporations. While its primary focus is corporate governance and financial disclosure, it has significant implications for IT as it mandates the establishment of internal controls and reporting methods to ensure the accuracy and integrity of financial data.

Who is Affected

SOX applies to all publicly traded companies in the United States, including wholly-owned subsidiaries and foreign companies that are publicly traded and do business in the US. Additionally, it impacts external auditors, consultants, and any other party that plays a role in the corporation's financial reporting and disclosure.

Compliance Checkpoints

SOX compliance for IT primarily revolves around three sections of the Act:

Section 302: Corporate Responsibility for Financial Reports: This section requires the company's principal officers to certify the accuracy and completeness of all financial reports. This includes ensuring that these reports do not contain any untrue statements or material omissions that would make them misleading. In terms of IT, this means ensuring that the systems and software used to generate these reports are reliable, accurate, and secure from tampering or unauthorized access.

Section 404: Management Assessment of Internal Controls: Perhaps the most well-known part of SOX, this section requires both management and an external auditor to report on the adequacy of the company's internal control over financial reporting. For IT, this involves developing and maintaining effective control structures and procedures for financial systems. This includes ensuring that all systems involved in financial reporting are secure, functioning correctly, and protected against unauthorized access or manipulation.

Section 802: Criminal Penalties for Altering Documents: This section outlines the penalties for tampering with or destroying documents in relation to a federal investigation or bankruptcy. From an IT perspective, it mandates the creation and preservation of detailed audit logs and other evidence that can verify the integrity of financial data and demonstrate compliance. This means that organizations must have robust data retention and management policies in place, which include the storage of electronic records and evidence of authorized and unauthorized access or alterations.

Non-Compliance Penalties

Non-compliance with SOX can lead to a range of penalties, including fines and imprisonment. Corporate officers who certify false reports can face fines of up to $5 million and imprisonment for up to 20 years. In addition to these legal penalties, non-compliance can also result in damage to a company's reputation and loss of investor confidence.

Resources

- SANS Institute: An Overview of Sarbanes-Oxley for the Information Security Professional
- TechTarget: 4 steps to remain compliant with SOX data retention policies

5. BSA

Bank Secrecy Act

Summary

The Bank Secrecy Act (BSA), also known as the Currency and Foreign Transactions Reporting Act, is a U.S. law designed to prevent financial institutions from being used as tools by criminals to hide or launder money. The BSA requires banks and other financial institutions to maintain records and file reports on certain types of transactions and activities that could be associated with money laundering or other financial crimes.

Who is Affected

The BSA affects all financial institutions in the United States, including banks, credit unions, broker-dealers, money services businesses (MSBs), and casinos.

Compliance Checkpoints

- **Currency Transaction Reporting (CTR):** Financial institutions must file a CTR for each transaction in currency (deposit, withdrawal, exchange, or other payment or transfer) of more than $10,000 by, through, or to the financial institution.
- **Suspicious Activity Reporting (SAR):** Financial institutions are required to report suspicious transactions that could signify money laundering, tax evasion, or other criminal activities. This includes any transaction involving $5,000 or more if the financial institution knows, suspects, or has reason to suspect that the transaction involves funds from illegal activities or is intended to hide such funds.
- **Record Keeping:** Financial institutions are required to keep certain records that have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings. This includes records for all wire transfers of $3,000 or more and the sale of monetary instruments totaling $3,000 to $10,000.
- **Customer Identification Program (CIP):** Financial institutions must implement a CIP adequate to verify the identities of their customers.
- **AML Program Requirements:** Under BSA, financial institutions are required to establish an anti-money laundering (AML) program that includes, at a minimum, internal controls, independent testing, designated individuals responsible for day-to-day operations, and training for appropriate personnel.

Non-Compliance Penalties

Non-compliance with the BSA can result in severe penalties, including substantial fines, criminal charges, and reputational damage. Civil penalties can be as high as $25,000 per day for each day the violation continues, and criminal penalties can include fines of up to $500,000 and imprisonment for up to ten years. In recent years, regulators have increasingly enforced BSA/AML violations with multi-million-dollar penalties.

Resources

- FFIEC: BSA/AML Manual
- OCC: Bank Secrecy Act (BSA)
- FDIC: Bank Secrecy Act / Anti-Money Laundering (BSA/AML)

6. GDPR

The European Union's General Data Protection Regulation

Summary

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside these regions. The GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international businesses.

Who is Affected

GDPR applies to all companies operating in the EU and EEA, as well as companies outside these regions if they offer goods or services to, or monitor the behavior of, EU/EEA residents.

Compliance Checkpoints

- **Data Subject Rights:** The GDPR introduces a suite of rights for data subjects, including the right to access, rectification, erasure ("right to be forgotten"), restriction of processing, data portability, objection to processing, and rights related to automated decision-making and profiling. Organizations must ensure they can accommodate these rights if they process the personal data of EU/EEA residents.
- **Lawful Basis for Processing:** GDPR requires organizations to have a lawful basis for processing personal data. There are six lawful bases: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public interest, and legitimate interests.
- **Data Protection Impact Assessments (DPIAs):** Organizations must conduct DPIAs for processing activities that result in high risk to data subjects.
- **Data Breach Notification:** GDPR mandates that data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the appropriate supervisory authority within 72 hours of the organization becoming aware of it.
- **Data Protection Officer (DPO):** Organizations that engage in large-scale systematic monitoring or processing of sensitive personal data must appoint a DPO.
- **Data Protection by Design and Default:** GDPR requires organizations to incorporate data protection into the design of systems and processes (data protection by design) and to make privacy-friendly settings the default (data protection by default).

Non-Compliance Penalties

GDPR non-compliance can lead to hefty fines of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever is higher. Additionally, non-compliance can lead to reputational damage, loss of customer trust, and a decrease in shareholder value.

Resources

- GDPR - Everything you need to know about GDPR compliance

7. NCUA 12 CFR 748

National Credit Union Administration Code of Federal Regulations Title 12, Part 748

Summary

The National Credit Union Administration's (NCUA) 12 CFR Part 748 is a regulation that outlines the minimum security procedures that federally insured credit unions must adopt to protect against unauthorized access to member information. It includes guidelines for developing an effective information security program and requirements for reporting on the status of such programs.

Who is Affected

Federally insured credit unions in the United States are affected by NCUA 12 CFR Part 748.

Compliance Checkpoints

- **Development of an Information Security Program:** Credit unions must develop an information security program tailored to the size and complexity of their operations. This program must be designed to manage and control risks associated with unauthorized access to or use of member information.
- **Board of Directors Role:** The credit union's board of directors is required to approve the institution's information security program and oversee its implementation and maintenance.
- **Risk Assessment:** Credit unions must conduct a comprehensive risk assessment to identify potential threats to member information.
- **Risk Management and Control:** Based on the risk assessment, credit unions must manage and control the identified risks by designing and implementing information security measures.
- **Service Provider Oversight:** If the credit union outsources any of its information processing or storage functions, it must ensure that its service provider maintains appropriate security measures to protect member information.
- **Response Program:** Credit unions must develop a response program for incidents of unauthorized access to member information.
- **Program Updates:** The information security program must be evaluated and adjusted as necessary in light of changes to the credit union's operations, technology, threats, testing results, or other relevant factors.

Non-Compliance Penalties

Non-compliance with NCUA 12 CFR Part 748 can result in penalties for the credit union. These may include fines, sanctions, orders to cease and desist, orders of prohibition, and removal and prohibition orders. Further, the NCUA may initiate civil litigation or refer matters for criminal prosecution. The penalties vary depending on the severity and duration of the violation.

Resources

- NCUA's Regulations and Guidance

8. BCBS

Basel Committee on Banking Supervision

Summary

The Basel Committee on Banking Supervision (BCBS) is an international committee formed by central bank governors from the world's leading economies, known as the Group of Ten (G-10). The BCBS provides recommendations on banking laws and regulations, including the Basel Accords, which provide an international standard for banking regulations with a focus on risk management.

Who is Affected

BCBS regulations and recommendations are primarily applicable to banks and financial institutions that operate internationally. While the BCBS doesn't have formal authority over the laws of individual countries, its guidelines are widely accepted and implemented by countries worldwide.

Compliance Checkpoints

- **Credit Risk Management:** The BCBS guidelines mandate that banks must maintain a certain level of capital to offset credit risks. Banks must also implement robust risk management systems to identify, track, and minimize credit risk.
- **Operational Risk Management (Basel III):** Basel III guidelines require banks to maintain a certain level of capital to mitigate operational risks, which include system failures, cyberattacks, and data breaches. Banks need to ensure they have robust IT systems and security measures in place.
- **Market Risk Management:** The BCBS guidelines require banks to manage their market risks effectively. Banks must have in place reliable IT systems capable of accurately tracking and reporting market positions and risk exposures.
- **Liquidity Risk Management (Basel III):** Basel III introduced two minimum standards for funding liquidity. Banks need reliable IT systems to accurately monitor and report liquidity metrics.

Non-Compliance Penalties

The BCBS doesn't impose penalties itself. However, regulatory authorities in individual countries that have adopted BCBS guidelines can impose penalties for non-compliance, including fines, sanctions, and restrictions on business activities. These penalties vary depending on the specific regulations of each country.

Resources

- Basel Committee on Banking Supervision: Principles for Operational Resilience
- Deloitte: Basel III final rule summary

How to Reach Cybersecurity Compliance

Achieving cybersecurity compliance as a financial institution requires a strategic approach. With numerous regulations to adhere to and an ever-evolving cyber threat landscape, financial institutions must be proactive and systematic. Here are key steps to take:

1. Understand the Regulations: With a multitude of cybersecurity regulations affecting the financial sector, understanding the details of each one is critical. The first step is to understand the requirements of each regulation your institution must comply with. This may include regulations such as GDPR, BSA, SOX, FFIEC, NCUA, and more.
2. Conduct a Risk Assessment: Identify potential risks by conducting a comprehensive risk assessment of your current IT infrastructure. This includes identifying potential vulnerabilities in your networks and systems, evaluating the impact of potential breaches, and identifying any existing gaps in your current cybersecurity measures.
3. Develop a Compliance Strategy: Based on your understanding of the regulations and the results of your risk assessment, develop a comprehensive compliance strategy. This should include policies and procedures to ensure compliance, a plan for regular audits and reviews, and a strategy for handling potential breaches.
4. Implement Robust Security Measures: Depending on the requirements of the regulations and your risk assessment, you'll need to implement robust security measures. This may include firewalls, intrusion detection systems, encryption technologies, two-factor authentication, and other advanced cybersecurity tools.
5. Regularly Review and Update Your Compliance Measures: Compliance isn't a one-time task. It's important to regularly review and update your compliance measures to address changes in regulations and to cope with new threats and vulnerabilities. This involves regular auditing, monitoring, and testing of your cybersecurity defenses.
6. Train Your Staff: Your employees play a crucial role in maintaining cybersecurity. Ensure they understand the importance of compliance and are aware of the security measures in place. Regular training will help them stay updated on the latest threats and learn how to avoid potential breaches.
7. Partner with Experts: Partnering with a trusted IT solutions provider like VLCM can provide you with the necessary expertise and resources to navigate the complex cybersecurity landscape. We can help you develop and implement a compliance strategy that meets all necessary regulatory requirements while also strengthening your overall cybersecurity posture.

By following these steps, you can achieve cybersecurity compliance in the financial sector and ensure your institution is well-protected against potential cyber threats.

VLCM: Your Trusted Partner in Cybersecurity Compliance

Complying with cybersecurity regulations in the financial sector is challenging and resource-intensive. If your institution is struggling with time or resource constraints, VLCM is ready to assist. We provide comprehensive, customized solutions designed to meet your specific regulatory requirements while also enhancing your overall cybersecurity posture. Don't let the complexity of compliance impede your institution's success - reach out to VLCM today and let us handle your cybersecurity needs, so you can focus on what you do best: serving your customers and growing your business.

Visit www.vlcm.com/cybersecurity to learn more.

VLCM
Enterprise Technology +
Cybersecurity Solutions Provider

852 E. Arrowhead Lane
Salt Lake City, UT 84017

www.vlcm.com

sales@vlcm.com

801-817-1504