FFIEC Guidance

Meets SANS Top 20 Compliance

HOW DIGITAL DEFENSE ADDRESSES YOUR NEEDS

DIGITAL DEFENSE®
INCORPORATED

Inventory of Authorized & Unauthorized Devices

FFIEC Guidance: CSC 1.1 & 1.4

Historically there hasn't been a way for institutions to compare and contrast FFIEC guidance with accepted industry standards like the SANS Top 20, but that is no longer the case. FFIEC and SANS information security controls offer various standard that provide benchmarks that both financial institutions and their regulators can draw upon for the development of industry expectations and security practices.

- Establish an inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. (FFIEC Information Security Booklet, page 9)
- Automated tools enable tracking, updating, asset prioritizing, and custom reporting of the asset inventory.
- Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s).
- Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device.

As a solution, **Frontline Vulnerability Manager (Frontline VM)** makes it simple. Digital Defense's Frontline VM puts security innovation at your fingertips. Leverage the power of a next generation security assessment system and patented scanning technology, coupled with certified and knowledgeable security analysts and industry leading support staff, to ensure your organization never has to navigate the security and compliance maze alone.

Vulnerability Scanning

FFIEC Guidance: CSC 4.1 & 4.3

In order to determine whether or not an institution is in compliance with FFIEC guidelines, comprehensive assessments of the internal environment must be conducted to identify potential security weaknesses and threats. Then goals must be set, solutions implemented and periodic risk assessments performed in order to maintain an adequate level of security.

- Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external facing systems and the internal network. (FFIEC Information Security Booklet, page 61)
- Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.
- Weekly vulnerability scanning is rotated among environments to scan all environments throughout the year.
- Vulnerability scanning is performed on a weekly basis across all environments.
- Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk.

FFIEC Guidance: CSC 4.4, 4.7 & 4.8

- Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.
- Ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.
- Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.
- Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization.
- Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops).

DDI's flagship offering, **Vulnerability Management-Professional (VM-Pro)** is a fully managed service that provides Industry leading scanning technology and expert insight to engineer, configure and operationalize vulnerability management processes. VM-Pro is recognized for exceeding client expectations and providing exceptional value. DDI clients praise our managed service, from the personalized guidance to the efficiencies gained through a streamlined management workflow system, allowing them to focus on their core business objectives.

"Employees & **negligence** are the leading causes of **security incidents** but remain the least reported issue."

Experian 2015 Second Annual Data Breach Industry Forecast

Malware Defenses

FFIEC warns organizations of the potential for destructive malware attacks, As the potential for destructive malware attacks increases, follow these guidelines to help keep your systems and data secure.

FFIEC Guidance: CSC 8.2

- Antivirus and anti-malware tools are used to detect attacks. (FFIEC Information Security Booklet, page 55)
- Antivirus and anti-malware tools are updated automatically.
- Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature based detection to identify and filter out malicious content before it arrives at the endpoint.

"Breaches have cost the healthcare system an estimated $50 billion."

-19 Latest Healthcare Data Breaches: Health & CIO Review

Application Software Security

FFIEC Guidance: CSC 20.1,20.5 & 20.6

- The security of applications, including web-based applications connected to the internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.
- Independent penetration testing of network boundary and critical web facing applications is performed routinely to identify security control gaps. (page 81 FFIEC)
- Independent penetration testing is performed on internet-facing applications or systems before they are launched or undergo significant change.
- Test in-house-developed web and other application software for coding errors and potential vulnerabilities prior to deployment, using automated static code analysis software, as well as manual testing and inspection.

It can be difficult for organizations to tell which of these web-based offerings are secure. DDI provides **Web Application Penetration Testing (WAPT)** to ensure your internally or third-party developed web-based applications do not introduce unforeseen vulnerabilities that can ultimately lead to hacks and breaches and jeopardize corporate or customer data.

Wireless Access Control

FFIEC Guidance: CSC 15.1 – 15.6

- Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s).
- Wireless networks use strong encryption with encryption keys that are changed frequently.
- The broadcast range of the wireless network(s) is confined to institution controlled boundaries. (page 41 FFIEC)
- Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. (page 33 FFIEC)
- Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

Information Security Training

FFIEC Guidance: CSC 17.1 – 17.4

- Annual information security training is provided. (FFIEC Information Security Booklet, page 66)
- Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues. (FFIEC Information Security Booklet, page 66)
- Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
- Deliver training to fill the skills gap.
- Implement an online security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion.
- Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.

The most sophisticated technology in the world can be quickly and easily breached by a weak or compromised password, as well as other lax security behavior. Effective security awareness training for your employees and clients can improve your overall security posture, and could be the most important investment you make this year.

Our **Security Awareness Education** helps you provide relevant, easy-to-understand, web-based security training for key audiences: your employees, contractors and patrons. This frees up your staff to focus on their core competencies and support your strategic initiatives.

Port Scanning

FFIEC Guidance: CSC 3.6, 9.3 & 11.3

- Scanning for technical vulnerabilities. (page 80 FFIEC).
- Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

Penetration Testing

FFIEC Guidance: CSC 20.1, 20.4, 20.5 & 20.6

- The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.) (FFIEC Information Security Booklet, page 59)
- The security of applications, including web-based applications connected to the internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.
- Independent penetration testing of network boundary and critical web facing applications is performed routinely to identify security control gaps.
- Independent penetration testing is performed on internet-facing applications or systems before they are launched or undergo significant change.
- Penetration tests include cyber attack simulations and/or real-world tactics and techniques such as red team testing to detect control gaps in employee behavior, security defenses, policies, and resources.
- Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
- Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.
- Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset.
- Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.

Penetration testing services are performed around the clock and around the world. With our ability to test remotely, we are able to service you quickly and cost effectively. DDI allows you to focus on your core business, removing the burden of performing penetration testing with complicated tools.

CONCLUSION

First issued in 2005, the Federal Financial Institutions Examination Council's (FFIEC) guidance for financial institutions took a strong stance in support of the deployment of stronger authentication methods, as well as fraud detection techniques, to protect customer identities and information during online banking transactions.

New network vulnerabilities are being discovered every day. No matter the size of your organization, vulnerability scanning is the cornerstone element in defending against the ever-increasing threat of data breaches. Comprehensive security awareness education ensures that you and your staff can detect threats and protect your organization and its critical information assets. Combined, these two efforts provide actionable security intelligence and give a holistic view of the threats your organization is facing on a day-to-day basis.

Digital Defense, Inc. (DDI) is a premier provider of managed security risk assessment solutions protecting billions in assets for small businesses to Fortune companies in over 65 countries. DDI's dedicated team of experts helps organizations establish a culture of security through regular information security assessments, awareness education and decisive security intelligence, helping our clients become better prepared to reduce risk and keep their information, intellectual property and reputations secure.


45%
of financial institutions
have suffered from
economic
crime
in the past year
-PricewaterhouseCoopers

9000 Tesoro Drive, Suite 100 San Antonio, TX 78217 | 888.273.1412 | www.digitaldefense.com