2020

FINANCIAL INSTITUTION COMPLIANCE CHECKLIST

Is your organization in compliance with FFIEC information security standards? Use this checklist to analyze your security posture.

RedTeam Security

THREAT PREVENTION EXPERTS

(612) 234-7848 | info@redteamsecure.com
www.redteamsecure.com

Table of Contents

About The FFIEC

The FFIEC, or Federal Financial Institutions Examinations Council, is an inter-agency governing body tasked with ensuring uniformity in the supervision of financial institutions.

The agency is comprised of representatives from the five major banking industry regulators: the Federal Reserve Board of Governors (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).

About This Checklist

The content herein was developed using cybersecurity assessment tools furnished by the FFIEC and supported by RedTeam's broad financial cybersecurity expertise. One of the FFIEC's functions is to help financial institutions gain an understanding of their cybersecurity risks and outline industry best practices for protecting the security of institutions, their vendors, their assets, and their customers.

The following checklist represents what the FFIEC and its collective members consider "baseline" cybersecurity requirements—that is, the expectations and compliance-driven objectives required by law.

For more information on the FFIEC's standards as well as additional resources for cultivating a robust financial security posture, visit ffiec.gov/cybersecurity.htm.

Part I: Cyber Risk Management and Oversight

- ☐ Are designated members of management held accountable by the board or an appropriate board committee for implementing and managing the institution's information security and business continuity programs?
- ☐ Are information security risks discussed in management meetings when prompted by highly visible cyber events or regulatory alerts?
- ☐ Does management provide a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually?
- ☐ Does the budgeting process include information security related expenses and tools?
- ☐ Does management consider the risks posed to the institution by other critical infrastructures (i.e. telecommunications, energy, etc.)?
- ☐ Does the institution have an information security strategy that integrates technology, policies, procedures, and training to mitigate risk?
- ☐ Does the institution have policies commensurate with its risk and complexity that address the following?
    - Information technology risk management?
    - Threat information sharing?
    - Information security?
    - External dependency or third-party management?
    - Incident response and resilience?
- ☐ Are all elements of the information security program coordinated enterprise-wide?
- ☐ Does the organization maintain an inventory of organizational assets (i.e. hardware, software, data, externally hosted systems, etc.)?
- ☐ Are organizational assets (i.e. hardware, systems, data, and applications) prioritized for protection based on the data classification and business value?
- ☐ Does management assign accountability for maintaining an inventory of organizational assets?
- ☐ Is a change management process in place to request and approve changes to systems configurations, hardware, software, applications, and security tools?

- ☐ Does an information security and business continuity risk management function exist within the institution?
- ☐ Does the organization use a risk assessment that is focused on safeguarding customer information to identify?
    - Reasonable and foreseeable internal and external threats?
    - The likelihood and potential damage of threats?
    - The sufficiency of policies, procedures, and customer information systems?
- ☐ Does the risk assessment identify internet-based systems and high-risk transactions that warrant additional authentication controls?
- ☐ Is the risk assessment updated to address new technologies, products, services, and connections before deployment?
- ☐ Has the institution clearly identified information security roles and responsibilities among personnel?
- ☐ Are processes in place to identify additional expertise needed to improve the organization's information security defenses?
- ☐ Does the institution provide annual information security training?
- ☐ If so, does the annual information security training include:
    - Incident response?
    - Current cyber threats (i.e. phishing, spear phishing, social engineering, mobile security, etc.)?
    - Emerging issues?
- ☐ Are situational awareness materials made available to employees when prompted by highly visible cyber events or regulatory alerts?
- ☐ Are awareness materials made readily available to customers?
- ☐ Does management hold employees accountable for complying with the organization's information security program?

NOTE: Cybersecurity should be regularly talked about, both at the board level and organization wide. It should not be a compartmentalized discussion, but one that is shared across departments and leadership levels. Especially if your organization surpasses the $10 billion mark in assets, you can expect to face strict scrutiny on these items from your respective regulatory authority.

Part II: Threat Intelligence and Collaboration

- ☐ Does the institution subscribe to a threat and vulnerability information sharing source that provides information on threats?
  - Does the organization use this threat information to monitor threats and vulnerabilities?
  - Does the organization use this threat information to enhance internal risk management and controls?
- ☐ Are audit log records and other security event logs reviewed and retained in a secure manner?
- ☐ Are computer event logs used for investigations once an event has occurred?
- ☐ Are information security threats gathered and shared with applicable internal employees?
- ☐ Is contact information for law enforcement and the regulator(s) maintained and updated regularly?
- ☐ Is information about threats shared with law enforcement and regulators when required or prompted?

NOTE: With FFIEC Security Standards, nothing is set in stone. Every regulator is different, and each will have his or her own unique interpretations of the guidelines. That's another reason communicating and sharing information with trusted sources in the industry is so important.

The Financial Services Information Sharing and Analysis Center and the U.S. Computer Emergency Readiness Team are two great threat resources for banks and credit unions.

Part III: Cybersecurity Controls

- ☐ Are network perimeter defense tools like border routers and firewalls used?
- ☐ Are systems that are accessed from the Internet or by external parties protected by firewalls or other similar devices?
- ☐ Are all ports monitored?
- ☐ Do systems configurations (for servers, desktops, routers, etc.) follow industry standards? Are these standards enforced?
- ☐ Are ports, functions, protocols, and services prohibited if no longer needed for business purposes?
- ☐ Is access to make changes to systems configurations controlled and monitored?
- ☐ Are programs that can override system, object, network, virtual machine, and application controls restricted?
- ☐ Are system sessions locked after a pre-defined period of inactivity or terminated after pre-defined conditions are me?
- ☐ Do wireless network environments require security settings with strong encryption for authentication and transmission?
- ☐ Is employee access granted to systems and confidential data based on job responsibilities and the principles of least privilege?

NOTE: The **principle of least privilege** is a computer security concept that promotes minimal user profile privileges based on users' job necessities. It can also be applied to processes on the computer; each system component or process should have the least authority necessary to perform its duties.

- ☐ Does employee access to systems and confidential data provide for separation of duties?
- ☐ Are administrator privileges limited and tightly controlled (i.e. assigned to individuals, not shared, and require stronger password controls)?
- ☐ Are user access reviews performed periodically for all systems and applications based on the risk to the application or system?
- ☐ Are changes to physical and logical user access, including those that result from voluntary and involuntary terminations, submitted to, and approved by appropriate personnel?

- ☐ Are identification and authentication required and managed for access to systems, applications, and hardware?
- ☐ Do access controls include password complexity and limits to password attempts and reuse?
- ☐ Are all default passwords and unnecessary default accounts changed before system implementation?
- ☐ Does customer access to Internet-based products or services require authentication controls (i.e. layered controls, multifactor) that are commensurate with the risk?
- ☐ Are production and non-production environments segregated to prevent unauthorized access or changes to information assets?
- ☐ Are physical security controls used to prevent unauthorized access to information systems and telecommunication systems?
- ☐ Are all passwords encrypted in storage and in transit?
- ☐ Is confidential data encrypted when transmitted across public or untrusted networks?
- ☐ Are mobile devices (laptops, tablets, smartphones, removable media) encrypted if used to store confidential data?
- ☐ Does remote access to critical systems by employees, contractors, and third parties use encrypted connections and multifactor authentication?
- ☐ Are administrative, physical, or technical controls in place to prevent users without administrative responsibilities from installing unauthorized software?
- ☐ Does customer service utilize formal procedures to authenticate customers commensurate with the risk of the transaction or request?
- ☐ Is data disposed of or destroyed according to documented requirements and within expected time frames?
- ☐ Are controls in place to restrict the use of removable media to authorized personnel?
- ☐ Do developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards?
- ☐ Is independent testing (including penetration testing and vulnerability scanning) conducted according to the risk assessment for external-facing systems and the internal network?
- ☐ Are the security controls of internally developed software periodically reviewed and tested?

- ☐ Are the security controls in internally developed software code independently reviewed before migrating the code to production?
- ☐ Are intellectual property and production code held in escrow?
- ☐ Are antivirus and anti-malware tools used to detect attacks?
- ☐ Are firewall rules audited or verified at least quarterly?
- ☐ Are e-mail protection mechanisms used to filter for common cyber threats (i.e. attached malware or malicious links)?
- ☐ Is the institution able to detect anomalous activities through monitoring across the environment?
- ☐ Are customer transactions generating anomalous activity alerts monitored and reviewed?
- ☐ Are logs of physical and/or logical access reviewed following events?

NOTE: Learn more about best practices for controlling your access policies and procedures here.

- ☐ Is access to critical systems by third parties monitored for unauthorized or unusual activity?
- ☐ Are elevated privileges (i.e. admin rights) monitored?
- ☐ Is a normal network activity baseline established?
- ☐ Are mechanisms (antivirus alerts, log event alerts, etc.) in place to alert management to potential attacks?
- ☐ Are processes in place to monitor for the presence of unauthorized users, devices, connections, and software?
- ☐ Have responsibilities for monitoring and reporting suspicious systems activity been assigned?
- ☐ Is the physical environment monitored to detect potential unauthorized access?
- ☐ Is a patch management program implemented? Does it ensure that software and firmware patches are applied in a timely manner?
- ☐ Are patches tested before being applied to systems and/or software?
- ☐ Are patch management reports reviewed? Do they reflect missing security patches?
- ☐ Are issues identified in assessments prioritized and resolved based on criticality and within the time frames established?

NOTE: Maintaining tight controls on passwords, access rights and patches is not fun, and in practice it admittedly can slow down everyday operations. Yet, it is one of the most basic and critical steps an organization can take to maintain a strong security posture. Insiders are responsible (either knowingly or by accident) for almost half of all breach incidents and taking these steps can dramatically reduce those statistics.

Part IV: External Dependency Management

- ☐ Have critical business processes that are dependent on external connectivity been identified?
- ☐ Does the institution ensure that third-party connections are authorized?
- ☐ Is a network diagram in place to identify all external connections?
- ☐ Are data flow diagrams in place to document information flow to external parties?
- ☐ Is risk-based due diligence performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls?
- ☐ Is a list of third-party service providers maintained?
- ☐ Is a risk assessment conducted to identify criticality of service providers?
- ☐ Are formal contracts in place that address relevant security and privacy requirements for all third parties that process, store, or transmit confidential data or provide critical services?
    - Do the contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits?
    - Do the contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party?
    - Do the contracts identify the recourse available to the institution should the third party fail to meet defined security requirements?
    - Do the contracts establish responsibilities for responding to security incidents?
    - Do the contracts specify the security requirements for the return or destruction of data upon contract termination?
- ☐ Is the third-party risk assessment updated regularly?
- ☐ Are audits, assessments, and operational performance reports obtained and reviewed regularly to validate security controls for critical third parties?

- ☐ Do ongoing monitoring practices include reviewing critical third-parties' resilience plans?

NOTE: Some of the most prolific data breaches in recent memory, including the 2017 Equifax breach, have been attributed to third-party vendors. For financial institutions, it is even more critical to be attentive not only to your own organization's security health, but that of anyone you do business with.

Part V: Cyber Incident Management and Resilience

- ☐ Has the institution documented how it will react and respond to cyber incidents?
- ☐ Do communication channels exist to provide employees a means for reporting information security events in a timely manner?
- ☐ Are roles and responsibilities for incident response team members defined?

NOTE: My company was hacked. Now what? Learn the next steps to take here.

- ☐ Does the response team include individuals with a wide range of backgrounds and expertise, from many different areas within the institution (i.e. management, legal, public relations, as well as information technology)?
- ☐ Does a formal backup and recovery plan exist for all critical business lines?
- ☐ Does the institution plan to use business continuity, disaster recovery, and data backup programs to recover operations following an incident?
- ☐ Are scenarios used to improve incident detection and response?
- ☐ Does business continuity testing involve collaboration with critical third parties?
- ☐ Are systems, applications, and data recovery tested at least annually?
- ☐ Are alert parameters set for detecting information security incidents that prompt mitigating actions?
- ☐ Do system performance reports contain information that can be used as a risk indicator to detect information security incidents?
- ☐ Are tools and processes in place to detect, alert, and trigger the incident response program?

- ☐ Are appropriate steps taken to contain and control incidents to prevent further unauthorized access to or use of customer information?
- ☐ Does a process exist to contact personnel who are responsible for analyzing and responding to an incident?
- ☐ Do procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information?
- ☐ Does the institution prepare an annual report of security incidents or violations for the board or an appropriate board committee?
- ☐ Are incidents classified, logged, and tracked?

NOTE: The best incident response plan is just that—a plan—not a mandate. Your incident response plan should allow leeway for the responding parties to adapt to the specific circumstances of the incident and make the best tactical decisions possible for moving forward.

About RedTeam Security

RedTeam Security has been a premiere provider of offensive information security services since 2008. In today's marketplace, companies are overwhelmed by security threats from hackers originating from all over the world. Studies show that the number of attacks against companies are increasing and at the same time becoming more complex. As a result of these attacks, the number of data breaches have cost companies' tens of millions of dollars as well as grave reputational damage.

The information security experts RedTeam Security have years of experience helping organizations of all sizes identify and mitigate security vulnerabilities. Our team of highly trained analysts hold the following indsutry certifications;

- Certified Networking Associate (CCNA)
- Cisco Certified Networking Associate Security (CCNA Security)
- Cisco Certified Networking Associate Cyber Ops (CCNA Cyber Ops)
- Comptia Security+
- OSCP (Offensive Security Certified Professional)
- GWAPT (GIAC Web Application Penetration Tester)
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Python Coder (GPYC)
- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Web Application Defender (GWEB)

At RedTeam Security we are committed to securing your organization. Whether you are ready to begin a project today or are looking for guidance on where to start, our team of security experts are here to help you navigate the complexities around information security. Schedule a free consultation with our team today, or answer a few questions to help us get started on a customized proposal for you immediately. We look forward to working with you.

Jon Anderson

President, RedTeam Security

Portfolio of Services

- Network Penetration Testing
- Web App Penetration Testing
- Physical Penetration Testing
- Cryptocurrency Penetration Testing
- Social Engineering
- Red Teaming
- Cyber Security Awareness Training
- Compliance (PCI, NERC, HIPAA, FDIC)

> **LEARN MORE**

Take the Next Step

Ready to improve your security posture with the help of RedTeam Security?

LOOKING FOR SOME GUIDANCE

Not sure where to start? Discuss your unique security needs and get your questions answered during a one-on-one consultation with one of our security professionals.

GO

READY FOR A PROPOSAL

Ready for us to prepare a proposal? Fill out our scoping questionnaire and give us a bit of background information on your project and we will send you a customized proposal.

GO

2020

Find. Fix. Fortify.

RedTeam Security

THREAT PREVENTION EXPERTS

(612) 234-7848 | info@redteamsecure.com
www.redteamsecure.com