Confidence in the Connected World

Center for Internet Security®

A Cyber Defense Guide for the Financial Sector

Compliance and Risk Controls for Banks, Credit Agencies, Lenders, and other Financial Institutions

The Threats Are Real

The financial industry faces dangerous cyber-attacks every day. From data breaches to monetary theft to protecting tax information, banks, credit unions, and other financial institutions must be on guard. In 2018 alone, there were over 500 security incidents affecting financial and insurance organizations – and almost 25% with confirmed data disclosure (Verizon Data Breach Investigations Report, 2018). Institutions don't just owe it to their customers to be secure. They are also required to meet regulatory and industry compliance standards such as:

- PCI DSS: Regulates organizations that store, process, or transmit cardholder information
- GDPR: Governs personal data protection for EU data subjects
- GLBA: Sets requirements for the collection, safekeeping, and use of private financial data

The bottom line is simple. If you work somewhere that manages personal information or financial records, it's imperative to protect the systems holding and managing that data. Thankfully, there are many resources available to help you get started.

Implementing Security Controls: A Risk-Based Approach

There are multiple regulations and the need for security is clear, but where should you begin? No matter which cybersecurity frameworks or compliance standards you implement, many of the cyber defense principles will be the same. The CIS Controls™ provide an on-ramp to help organizations implement security controls in a prioritized way. It starts with basic cybersecurity best practices and moves on to more sophisticated defense techniques. The CIS Controls are:

- Consensus-developed by a global community of cyber experts
- Mapped to popular frameworks such as National Institute of Standards and Technology (NIST)
- Free for organizations to download and implement

Download CIS Controls

Organizations should use a risk-informed method to weigh potential security controls. Measure the impact of updating firewall settings and network configuration options against the risk of *not* implementing such solutions. As you progress and complete the impact analysis, CIS Risk Assessment Method (CIS RAM) helps businesses organize the CIS Controls and Sub-Controls based on a customized assessment of risk. This free download provides instructions, examples, templates and exercises for conducting a cyber risk assessment.

Download CIS RAM

A risk-based assessment will help you identify security gaps and flaws in existing programs. Once you've completed this assessment, it's time to start implementing the security controls you'll need the most.

Getting Technical: Configuration and Patching

Two of the largest vectors for cyber-attacks are misconfigured or unpatched systems. These are common ways for cybercriminals to gain unauthorized access to systems or data. With misconfigured

systems, attackers can manipulate the environment through the settings. These settings can include default password requirements, "root" or administrative privilege access, or open ports. Unpatched systems, on the other hand, are simply out-of-date, allowing cybercriminals to take advantage of known flaws in operating systems and software applications. Exploit kits are easy for any aspiring hacker to find online and start searching for flaws. Thankfully, organizations can secure against both configuration gaps and unpatched systems. Let's begin with configuration:

Start secure.

Before deploying a technology in your environment, you'll want to implement a trusted configuration standard. The CIS Benchmarks™ are consensus-developed configuration best practices for operating systems, servers, cloud environments and more. They're trusted by organizations around the world to help protect systems and data from cyber-attacks. The CIS Benchmarks are referenced by PCI DSS Requirement 2 for security. Combined with the CIS Controls, the CIS Benchmarks can help with multiple aspects of PCI compliance, including:

- Firewall and Router Configurations
- 6.1 Patch Management
- 7.1 Access Control
- 6.4 Change Control

PCI DSS Requirement 2

This requirement covers security parameters for organizations that process payment card information. PCI DSS 2.2 specifically points to the CIS Benchmarks as "industry accepted hardening standards" for system configuration.

Download CIS Benchmarks™

Deploy. Patch. Repeat.

Once you have a secure configuration in place, systems must be continuously updated (or "patched") against emerging threats and new exploits. Patches should always be applied to a test environment to ensure they won't disrupt businesses processes. CIS Benchmarks are patched regularly to ensure the latest security updates are in place; best of all, they are free to download in PDF.

Data Privacy & GDPR

2018 was "the year of data privacy," when GDPR became enforceable at the end of May. Whether applicable to your organization or not, this regulation provides us with an opportunity to improve our data handling processes. First, you'll need to understand how data flows through the organization. There are areas around data handling which every organization will need to review and fine-tune. Some questions to start your investigation:

- What data do we have?
- How do we use it?
- Where is it stored and processed?

The answers to these questions will form a reference point for your organization to gain a controlled foothold over its data and information management processes.

Implementing GDPR

The requirements under the GDPR have provided a new compliance path for many organizations around the globe. This path has multiple steps in order to conform to the regulatory requirement. Let's take a look at how organizations can take the first few steps towards GDPR compliance.

Data Controllers and Processors

Think about the data your organization manages and how it is processed. Is data management an internal function or outsourced? Do you make decisions about how you collect data and how it is processed within your organization? If yes, you are a data controller. The data controller has a specific role in GDPR. However, if you process requests for such actions (data processing or management) from a customer or data provider then it is more likely you are in the data processor role.

What data is now considered "personal"?

Personally identifiable information (PII) consists of typical data elements plus some other items that you may not have considered:

Personal data

- Basic identity information such as name, address, and ID numbers
- Web data 'online identifiers' such as location, IP address, cookie data, and RFID

Special Personal Data

- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

No matter which roles apply to your organization, if your company handles EU data subjects' personal data, GDPR compliance is still required.

Assessment & monitoring

Regular cybersecurity assessments are key to understanding where your organization's security posture stands and where you want to go. Using a configuration assessment tool, you can determine where there are security gaps in your current environment. CIS-CAT Lite, our free tool, and CIS-CAT Pro, available through CIS SecureSuite® Membership, both allow users to measure their compliance to the CIS Benchmark recommendations.

CIS-CAT Pro Assessor has been awarded NIST Security Content Automation Protocol (SCAP 1.2) Validation as an "Authenticated Configuration Scanner" with the "Common Vulnerabilities and Exposures (CVE) Option" for specific platforms. This means that in addition to scanning against CIS Benchmark conformance, you can also use the tool to check for known vulnerabilities.

Once you've conducted an assessment, use the findings to plug configuration gaps and improve your security posture. Next, you'll want to implement continuous monitoring and change management processes to defend against future attacks.

Continuous monitoring

Once you've confirmed compliance to a baseline, consider regular cadence monitoring. This involves rechecking the systems to confirm their deployed compliant status is still in effect. How often this monitoring takes place could be based on criticality of the system, the size of data centers, or other factors. For example, critical systems may require weekly or monthly reviews while a large data operation may only require annual monitoring.

Change management

This comes into play when a configuration is needed (such as the installation of particular applications or software) that is not aligned to the secure baseline. In these cases, the required change should be documented as part of a change management process. Be sure to document the impact of any configuration change on your system by running another compliance scan after the change has been implemented.

Security is a Journey

The systems and data that help run commerce are under daily attack. CISOs, technical managers, and IT professionals have to work together to develop resiliency against cyber threats. Organizations that maintain a process including security controls, compliance, and monitoring will be better defended against cyber-attacks. Using a risk-based approach, secure baselines, and regular assessments improves your overall cybersecurity posture.

Through CIS SecureSuite Membership, resources like CIS-CAT Pro help more than 1,800 organizations worldwide along the path to security and compliance. Membership also provides remediation kits for rapidly implementing CIS Benchmark guidance, unlimited technical support, and custom configuration policy development through our online collaboration platform. Each part of this process will increase overall cyber hygiene and provide the impetus for maturing an information security program.

Learn more about CIS SecureSuite Membership

Summary: Resources to help improve your cybersecurity defenses

CIS Controls: Prioritized cybersecurity best practices to help organizations defend against threats and attacks. https://learn.cisecurity.org/cis-controls-download

CIS RAM: Free assessment method for developing a risk-informed cybersecurity program. https://learn.cisecurity.org/cis-ram

CIS Benchmarks: Secure configurations for operating systems, cloud environments, servers, network devices, and more. https://learn.cisecurity.org/benchmarks

CIS-CAT Pro: Configuration assessment tool with remote assessment functionality that quickly compares a target machine's settings to the secure CIS Benchmark guidelines. Available to CIS SecureSuite Members. https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/

CIS SecureSuite Membership: Cost-effective suite of cybersecurity resources; Members can create custom configuration policy, assess endpoints with CIS-CAT Pro, implement secure configurations quickly via remediation kits, and more. https://www.cisecurity.org/cis-securesuite/

Addendum

The regulations described in this document are not an exhaustive list. Additional regulations and resources for financial compliance include, but are not limited to:

Bank Secrecy Act / Office of Foreign Assets Control (BSA/OFAC)
USA Patriot Act
Financial Crimes Enforcement Network (FinCEN)
Federal Financial Institutions Examination Council (FFIEC)

About CIS

CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

The CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals.

Our CIS Hardened Images™ are virtual machine emulations preconfigured to provide secure, on-demand, and scalable computing environments in the cloud.

CIS is home to both the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC™), which supports the cybersecurity needs of U.S. State, Local and Territorial elections offices.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
learn@cisecurity.org