ARCTIC WOLF

END CYBER RISK

Cybersecurity Compliance Guide

Understanding information security and data protection requirements

Table of Contents

3 | Introduction

4 | Consumer Transactions

5 | **PCI DSS** – Payment Card Industry Data Security Standards

6 | Education

7 | **FERPA** – Family Educational Rights and Privacy Act

8 | **State Laws**

9 | Energy

10 | **NERC CIP** – North American Electric Reliability Corporation Critical Infrastructure Protection

11 | Financial Services

12 | **SOX** – Sarbanes-Oxley Act

13 | **GLBA** – Gramm-Leach Blilely Act

14 | **FFIEC** – Federal Financial Institutions Examination Council

15 | **NCUA** – National Credit Union Administration

16 | **BCBS** – Basel III IT Operations Controls

17 | Government

18 | **NIST 800-171** – The National Institute for Standards and Technology Special Publication 800-171

19 | **NIST 800-172** – Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

20 | **NIST 800-53** – Security and Privacy Controls for Information Systems and Organizations

21 | **FISMA** – Federal Information Security Management Act

22 | **CJIS** – Criminal Justice Information Services

23 | **FAR 52.204-21** – Federal Acquisition Regulation: Basic Safeguarding of Covered Contractor Information Systems

24 | **IRS Pub 1075** – Internal Revenue Service Publication 1075

25 | **ITAR** – International Traffic in Arms Regulations

26 | Healthcare

27 | **HIPAA** – Healthcare Insurance Portability and Accountability Act

28 | **HITRUST** – Healthcare Information Trust Alliance Common Security Framework

29 | Manufacturing

30 | **DFARS** – Federal Acquisition Regulation: Defense Federal Acquisition Regulation Supplement

31 | **CMMC 2.0** – Cybersecurity Maturity Model Certification 2.0

32 | Location Specific

33 | **CCPA** – California Consumer Privacy Act

34 | **GDPR** – General Data Protection Rule

35 | **SHIELD** – New York SHIELD Act

36 | **NYDFS / 23 NYCRR 500** – New York State Department of Financial Services Cybersecurity Regulation

37 | Supplementary

38 | **CIS** – Center for Internet Security Critical Security Controls

39 | **NIST CSF** – National Institute of Standards and Technology Cybersecurity Framework

40 | **SOC 2 Type II** – Service Organization Control 2 Type II

41 | Next Steps

Cybersecurity Compliance:

What You Need to Know

Compliance is an important part of a cybersecurity program. Heavily regulated industries are often a bigger target for cybercriminals because of their highly valuable data, e.g., patient data in healthcare, financial data in banking, identity data in government.

The purpose of cybersecurity laws and regulations are to ensure that organizations take the right steps to protect this data. And regardless of what industry you're in, you need to comply with state privacy laws, GDPR, and other regulations that apply to all sectors.

While meeting compliance requirements doesn't guarantee that your organization is secure, it provides you with a solid foundation for security practices. Not to mention that noncompliance may lead to fines and other penalties.

Use this guide as an overview of compliance requirements for your industry and location. We've provided a summary of each rule and key requirements, along with resources for more information.

Consumer Transactions

Protecting customer data is important for maintaining your brand reputation and customer trust. Regardless of your industry, if you accept debit and credit cards, you are subject to Payment Card Industry Data Security Standards (PCI DSS). This set of standards is developed, maintained, and enforced by the payment card industry, and noncompliance can result in fines.

PCI DSS

Payment Card Industry Data Security Standards

Summary

Payment Card Industry Data Security Standards (PCI DSS) are not government regulations but rather a set of industry rules that payment card issuers and financial institutions enforce for merchants and service providers who accept payment cards. The PCI Security Standards Council develops and maintains the standards, which also apply to anyone who stores, processes, or transmits cardholder data. Additionally, there are requirements for software developers and hardware manufacturers of applications and devices used in payment transactions.

Merchants must assess their compliance, remediate vulnerabilities, and report compliance to the respective financial institution or payment card brand.

Key requirements

PCI-DSS has a set of six core objectives, each with specific requirements:

- Build and maintain a secure network—using a firewall and strong password practices
- Protect stored cardholder data—including encryption of cardholder data when it's transmitted over open, public networks
- Maintain a vulnerability management program—using and regularly updating anti-virus and secure apps
- Implement strong access control measures—including restricted access to data based on roles and unique IDs for those with access
- Regularly monitor and test networks—tracking and monitoring access to networks and data, and regularly testing security
- Maintain an information security policy—covering both employees and contractors

Who's affected

Entities anywhere in the world that transmit, store, or process cardholder data.

Resources

- PCI Security Standards Council: Payment Card Industry Data Security Standard: Requirements and Testing Procedures Version 4.0
- Arctic Wolf: Simplify PCI-DSS Compliance Requirements
- Arctic Wolf: PCI DSS Security Compliance Checklist

Education

K-12 schools and institutions of higher education need to protect the privacy of their student records. All schools funded by the U.S. Department of Education programs must comply with the federal Family Educational Rights and Privacy Act, whose aim is to ensure the protection of education records and personally identifiable information (PII). Additionally, most states have their own laws that apply to the education sector.

FERPA

Family Educational Rights and Privacy Act

Summary

The Family Educational Rights and Privacy Act (FERPA) is a federal privacy law that protects students' education records and personally identifiable information from unauthorized disclosure. All schools that receive certain types of U.S. Department of Education funds must comply, and noncompliance can result in loss of the federal funding. Enacted in 1974, FERPA prohibits the disclosure of student records without written consent, with some specific exceptions.

Key requirements

FERPA gives parents of students under 18 specific rights with regards to student records, and those rights transfer to the students when they reach age 18. These rights include the ability to:

- Inspect the student records maintained by the institution
- Request the correction of records that they believe are inaccurate
- Provide written permission for the records to be disclosed

Certain conditions are exempt from the written permission requirement, including organizations conducting studies on behalf of the school, law-enforcement and court entities, and officials conducting audits. Additionally, FERPA allows disclosure without consent of directory information, such as student name, address, and date of birth, but requires institutions to provide parents or eligible students the opportunity to opt out.

Who's affected

In general, educational agencies and institutions that receive funds administered by the U.S. Secretary of Education and provide services or instruction to students, or are authorized to direct and control public educational institutions (with some exceptions).

Resources

- U.S. Department of Education: FERPA
- EdTech: Understanding FERPA, CIPA and Other K–12 Student Data Privacy Laws

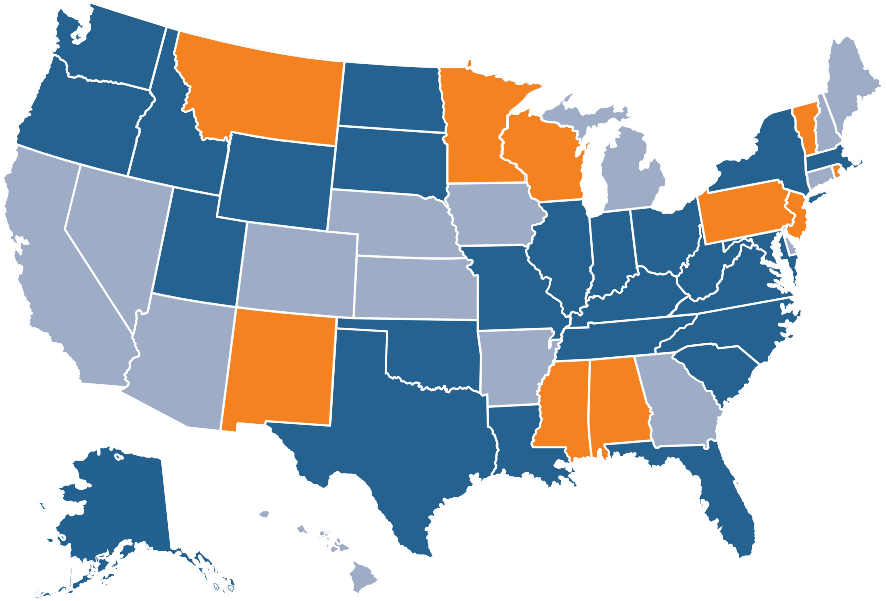
State Laws

Summary

At least 40 states have enacted their own legislation to protect the privacy of student data.

More than 20 of them have modeled their laws after California's 2014 Student Online Personal Information Protection Act (SOPIPA), while others have used frameworks such as the Student Data Privacy, Accessibility, and Transparency Act, originally developed by the Foundation for Excellence in Education.

SOPIPA, which came into effect in January 2016, applies to entities that operate websites, online services, and online and mobile apps that are designed and marketed primarily for K-12 educational purposes. It requires these operators to implement reasonable security practices to protect the student data, and prohibits them from sharing the data or using it for advertising for noneducational purposes.



States that have enacted their own legislation to protect the privacy of student data

States that modeled their laws after the Student Online Personal Information Protection Act (SOPIPA)

States that introduced legislation to protect the privacy of student data, but did not become law

Energy

The standards outlined in the Critical Infrastructure Protection (CIP) program use a results-based approach focusing on performance, risk management, and entity capabilities to protect organizations against ever-evolving threats. NERC updates its CIP standards frequently in order to stay on top of the rapidly changing technology and cyber threat landscape, so it's important to review the standards regularly to ensure that your organization remains compliant.

NERC CIP

North American Electric Reliability Corporation Critical Infrastructure Protection

Summary

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan is a set of standards aimed at regulating, enforcing, monitoring, and managing the security of the Bulk Electric System (BES) in North America. These standards apply specifically to the cybersecurity aspects of BES. The NERC CIP standards provide a cybersecurity framework to identify and secure critical assets that can impact the efficient and reliable supply of electricity of North America's BES.

Key requirements

NERC CIP standards include the following categories:

- BES Cyber System Categorization
- Security Management Controls
- Personnel and Training
- BES Cyber System Logical Isolation
- Physical Security of BES Cyber Systems
- System Security Management
- Incident Reporting and Response Planning
- Recovery Plans for BES Cyber Systems
- Configuration Change Management and Vulnerability Assessments
- Information Protection
- Supply Chain Risk Management

Who's affected

The NERC CIP standards are mandatory security standards that apply to entities that own or manage facilities that are part of the U.S. and Canadian electric power grid.

Resources

- NERC: CIP V5 Implementation Information
- NIST: Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards

Financial Services

The financial sector is heavily targeted by cybercriminals, who typically go where the money is. In response, several government agencies aim to protect consumer information. The Gramm-Leach-Bliley Act enforces the safeguarding of sensitive data for organizations that offer financial products, with penalties including not only fines but also criminal action against individuals. The Federal Financial Institutions Council provides a Cybersecurity Assessment Tool to help mitigate security risks. Additionally, the Sarbanes-Oxley Act requires controls that ensure financial reports are complete and accurate, and the international Basel Committee on Banking Supervision has IT requirements related to data integrity.

SOX

Sarbanes-Oxley Act

Summary

The Sarbanes-Oxley Act of 2002 (SOX) regulates financial practices and corporate governance, and applies to all publicly traded companies as well as accounting firms and other entities that provide financial services to those companies. Its main objective is to protect investors from fraudulent accounting activities. SOX requires the regulated entities to implement internal accounting controls and report the adequacy of those controls to the Securities and Exchange Commission (SEC). Noncompliance can result in fines and other penalties, including criminal liability.

Key requirements

From a cybersecurity perspective, three sections of SOX are particularly relevant:

- **Section 303** requires the chief executive officer and chief financial officer to personally certify that their company's financial reports are accurate and complete, and places responsibility on them for assessing and reporting the effectiveness of the internal controls related to financial reporting.
- **Section 404** requires the entity to assess the effectiveness of internal controls and report it annually to the SEC. An outside auditing firm must review this assessment, which includes a comprehensive review of the internal controls. However, SOX doesn't provide guidance around specific controls that must be assessed.
- **Section 802** contains three rules that affect recordkeeping. The first deals with destruction and falsification of records. The second strictly defines the retention period for storing records. The third rule outlines the specific business records that companies need to store, which includes electronic communications.

Who's affected

All publicly traded companies regardless of size and industry; some provisions also apply to private and nonprofit entities.

Resources

- SANS: An Overview of Sarbanes-Oxley for the Information Security Professional
- TechTarget: SOX Compliance Checklist

GLBA

Gramm-Leach-Bliley Act

Summary

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions and other entities that provide financial products—including loans, insurance, and investment advice—to safeguard sensitive data and to explain their information-sharing practices to their customers. The Federal Trade Commission and other federal agencies enforce the GLBA, and noncompliance penalties include fines and criminal charges.

Key requirements

The GLBA has two core components:

1. The Safeguards Rule requires financial institutions protect the consumer information they collect. Requirements include:
   - Designating an individual or group to coordinate an information security program
   - Identifying and assessing risks to customer data and evaluating the effectiveness of the existing controls
   - Implementing, monitoring, and testing a safeguards program
   - Evaluating the program when changes take place in business operations and other circumstances
   - 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.

Who's 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.

Resources

- FTC: How to Comply with the Privacy of Consumer Information Rule of the Gramm-Leach-Bliley Act
- FTC: Updating you on FTC privacy and data security initiatives

FFIEC

The Federal Financial Institutions Council Cybersecurity Assessment

Summary

The Federal Financial Institutions Council (FFIEC) has released the Cybersecurity Assessment Tool to help banks and credit unions assess and mitigate their cybersecurity risks. The assessment, which is voluntary, maps to the Nation Institute of Standards and Technology (NIST) Framework, which is widely used by all industries as a tool to strengthen cybersecurity posture.

Key requirements

FFIEC guidance applies to federally supervised financial institutions. The FFIEC Cybersecurity Assessment Tool has a twofold objective:

- To identify the institution's inherent risk profile—including activities, products, and services in five categories: technologies and connection types, delivery channels, online and mobile products and technology services, organizational characteristics, and external threats
- To determine the organization's maturity level—focused on five domains: cyber risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyber incident management and resilience

Who's affected

FFIEC guidance applies to federally supervised financial institutions.

Resources

- FFIEC: Cybersecurity Assessment Tool website
- Arctic Wolf: Simplify Compliance for FFIEC-NCUA
- Arctic Wolf: 5 Steps to Ace the FFIEC Assessment

NCUA 12 CFR 748

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

Summary

The National Credit Union Administration (NCUA) uses a risk-based approach to examining and supervising credit unions.

All federally insured credit unions receive an NCUA examination on a periodic basis. To ensure both compliance with applicable laws and regulations, as well as safety and soundness, a review of the credit union's information security program is performed at each examination. The Code of Federal Regulations (CFR) Title 12, Part 748 (12 CFR Part 748) includes guidance for the development and implementation of an information security program.

Key requirements

Although the NCUA uses a variety of resources and frameworks for their risk-based examination and provides high-level information security requirements through 12 CFR Part 748, credit unions supervised by the NCUA should follow the Federal Financial Institutions Examination Council (FFIEC) compliance standards. You can find FFEIC information on the previous page (page 14).

Who's affected

NCUA guidance applies to federally insured credit unions.

Resources

- NCUA: NCUA's Regulations and Guidance
- Arctic Wolf: Enhancing Detection Improves Credit Union Cybersecurity and Compliance

BCBS

Basel III IT Operational Controls

Summary

The Basel Committee on Banking Supervision (BCBS) is an international supervisory authority that maintains several standards and voluntary frameworks for financial institutions. Basel III (and Standard 239), in particular, affects IT infrastructure and operations, as it includes principles related to data architecture and IT infrastructure, as well as accuracy and integrity of risk data.

Key requirements

To comply with the BCBS effective risk data aggregation and risk reporting principles, financial institutions must have a robust and resilient IT infrastructure that supports risk aggregation capabilities and risk reporting practices both in normal times and in times of stress or crisis.

Who's affected

Basel III applies to internationally active banks.

Resources

- Basel Committee on Banking Supervision: Principles for Operational Resilience
- Deloitte: Basel III Final Rule Summary

Government

To protect the security and privacy of its information and systems, some government agencies have cybersecurity requirements for their contractors, including commercial entities and nonfederal agencies. The National Institute for Standards and Technology develops and maintains the requirements, which include NIST 800-171, required by the Department of Defense and others. Contractors may also be subject to the Federal Information Security Management Act.

NIST 800-171

The National Institute for Standards and Technology Special Publication 800-171

Summary

The National Institute for Standards and Technology (NIST) Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, provides recommendations for cybersecurity standards and data protection for nonfederal entities that serve as federal contractors, including commercial and state or local government organizations. Several federal agencies, such as the Department of Defense and the General Services Administration, mandate compliance with these standards.

Key requirements

Controlled unclassified information (CUI) refers to information that is not classified but is considered sensitive. SP 800-171 includes basic and derived requirements in 14 domains:

- Access controls (such as limiting access to authorized users)
- Awareness and training
- Audit and accountability (such as maintaining system audit logs)
- Configuration management (for hardware, software, and firmware)
- Identification and authentication (includes users, processes, and devices)
- Incident response
- Maintenance of systems
- Media protection (both physical and logical controls)
- Personnel security
- Physical protection
- Risk assessment
- Security assessment
- System and communications protection (including data transmission)
- System and information integrity

Who's affected

Commercial businesses and state or local government agencies that serve as federal contractors for certain federal agencies (including the Department of Defense).

Resources

- NIST: Special Publication 800-171
- Arctic Wolf: Achieving NIST 800-171 Compliance

NIST 800-172

Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

Summary

Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 (NIST 800-172) – formerly referred to in draft form as 800-171B – details enhanced security requirements for controlled unclassified information (CUI) for non-federal systems and organizations. The 35 requirements introduced in NIST 800-172 are designed to protect the high-value assets and critical programs of DoD contractors from modern attack tactics and techniques related to advanced persistent threats (APTs).

While still in the process of developing the requirements, the DoD has announced it will require the implementation of NIST SP 800-172 for CMMC 2.0 Level 3.

Key requirements

NIST 800-172 controls provide the foundation of an enhanced protection strategy with the 35 requirements of NIST 800-172 falling into three protection strategy categories:

- **Penetration-resistant architecture:** Use of technology and procedures to limit the opportunities for an adversary to compromise the system
- **Damage-limiting operations:** Focus on detecting compromises and limiting the effect of both detected and undetected system compromise
- **Cyber resiliency and survivability:** Ability to anticipate, withstand, and recover from an attack

Who's affected

The enhanced security requirements are only applicable for a non-federal system or organization when mandated by a federal agency in a contract, grant, or other agreement.

Resources

- NIST: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171
- ISACA: Novel Ideas From NIST for Fighting APTs

NIST 800-53

Security and Privacy Controls for Information Systems and Organizations

Summary

The controls established by NIST 800-53 have three primary objectives:

1. Provide a comprehensive and flexible catalog of controls for evolving technology and threats.
2. Build a foundation for assessing the effectiveness of controls.
3. Improve communication across organizations by providing a common language for risk management concepts. Although designed specifically for U.S. federal government agencies, NIST 800-53 is a highly regarded standard and is cross-referenced by many other industry-accepted security standards.

Key requirements

NIST 800-53 Rev. 5 includes 20 families of controls that provide operational, technical, and managerial safeguards to ensure the privacy, integrity, and security of information systems.

- Access control
- Awareness and training
- Audit and accountability
- Assessment, authorization, and monitoring
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance of systems
- Media protection
- Physical and environmental protection
- Planning
- Program management
- Personnel security
- PII processing and transparency
- Risk assessment
- System and services acquisition
- System and communications protection
- System and information integrity
- Supply chain risk management

Who's affected

NIST 800-53 applies to all federal agencies, state agencies administering federal programs, and private sector organizations supporting federal contracts.

Resources

- NIST: SP 800-53A Rev. 5
- Schellman: What is NIST Special Publication (SP) 800-53?

FISMA

Federal Information Security Act

Summary

The Federal Information Security Act of 2002 (FISMA) requires federal agencies to develop, document, and implement an information security program for the data and systems that support the agencies' operations and assets. The requirement also applies to information and systems provided or managed by other sources, such as contractors and nonfederal agencies. Entities funded by certain federal grants, such as educational institutions, may also be required to comply with FISMA.

Key requirements

NIST develops the standards and guidelines for FISMA compliance using a risk-based approach. It uses a framework that includes seven core steps, some of which map to specific NIST Special Publications (SPs):

- **Prepare:** Conducting the essential activities to help prepare for risk management under the framework
- **Categorize:** Classifying the information and systems that must be protected
- **Select:** Establishing the baseline controls for protecting the categorized systems and data
- **Implement:** Deploying the appropriate controls and documenting them
- **Assess:** Determining if controls are working correctly and leading to desired outcomes
- **Authorize:** Authorizing the operation of the system based on the risk determination
- **Monitor:** Continuously monitoring and assessing the security controls for effectiveness

Who's affected

Federal agencies, state agencies that administer federal programs, entities funded by certain federal grants, and government contractors who exchange data directly with federal government systems.

Resources

- TechTarget: Federal Information Security Act
- NIST: FISMA Implementation Project

CJIS

Criminal Justice Information Services

Summary

The Criminal Justice Information Services (CJIS) Security Policy provides minimum security requirements for access to Federal Bureau of Investigation (FBI) CJIS division systems and information. The CJIS Security Policy ensures continuity of information protection and provides the appropriate controls to protect criminal justice information (CJI) from creation to dissemination, whether at rest or in transit. Improper access, use, or dissemination of CJI files may result in denial of access to any FBI database or CJIS system, and is subject to fines, and state and federal criminal penalties.

Key requirements

The CJIS Security Policy provides requirements and standards for the following 13 policy areas:

- Information exchange agreements
- Security awareness training
- Incident response
- Auditing and accountability
- Access control
- Identification and authentication
- Configuration management
- Media protection
- Physical protection
- Systems and communications protection and information integrity
- Formal audits
- Personnel security
- Mobile devices

Who's affected

Every individual contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity with access to, or who operate in support of, criminal justice services and information.

Resources

- FBI: Criminal Justice Information Services Security Policy
- FBI: Requirements Companion Document to the FBI CJIS Security Policy

FAR

Federal Acquisition Regulation

Summary

The Federal Acquisition Regulation (FAR) is a set of regulations that establishes the rules that the government has to follow to acquire goods and services with procurement contracts.

Notably, FAR 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems" is a clause within FAR that defines specific cybersecurity regulations applying to federal contractors. It lays out a set of 15 cybersecurity controls for safeguarding contractor information systems that store, process, or transmit federal contract information.

This clause also corresponds to Cybersecurity Maturity Model Certification (CMMC) Level 1.

Key requirements

1. Limit information system access to authorized users.
2. Limit information systems to the types of transactions and functions that authorized users are permitted to execute.
3. Verify and control/limit connections to and use of external information systems.
4. Control information posted or processed on publicly accessible information systems.
5. Identify information system users, processes acting on behalf of users, or devices.
6. Verify the identities of those users, processes, or devices as a prerequisite to allowing access to organization information systems.
7. Sanitize or destroy information system media containing federal contract information before disposal or release for reuse.
8. Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
9. Escort visitors and monitor visitor activity; maintain audit logs of physical access; control and manage physical access devices.
10. Monitor, control, and protect organizational communications.
11. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
12. Identify, report, and correct information and information system flaws in a timely manner.
13. Provide protection from malicious code at appropriate locations within organizational information systems.
14. Update malicious code protection mechanisms when new releases become available.
15. Perform periodic scans of the information system and real-time scans of files from external sources.

Who's affected

Federal Acquisition Regulation (FAR) applies to all federal contracts, not just those with the Department of Defense.

Resources

- Federal Register: Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems
- Acquisition.gov: Basic Safeguarding of Covered Contractor Information Systems

IRS 1075

Internal Revenue Service Publication 1075

Summary

Internal Revenue Service Publication 1075 (IRS 1075) provides guidance for U.S. government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practices, and controls to protect its confidentiality. IRS 1075 aims to minimize the risk of loss, breach, or misuse of FTI held by external government agencies.

Key requirements

To protect FTI, IRS 1075 prescribes security and privacy controls for application, platform, and data center services.

Some of the controls needed are as follows. These include both electronic and physical:

- **Record Keeping Requirements:** Maintain a persistent system of all FTI records and anything related to it, including access rights
- **Secure Storage:** Details about the physical and electronic security of place where FTI data is kept, including restricted areas, authorized access, locks and keys, safes/vaults, transportation security, security of computers and storage media
- **Restricting Access:** Details related to access of FTI data
- **Reporting Requirements:** Periodic reports like SAR (Safeguard Activity Report) and SPR (Safeguard Procedures Report) need to be sent to IRS
- **Training and Inspections:** Awareness about security and annual certification of employees and annual inspections to validate proper implementation
- **Disposal:** Proper standards related to FTI data disposal for physical and electronic media
- **Computer System Security:** Probably the most complex and detailed section of this regulation related to everything from access control, cryptography, emails, networking to wireless technologies, and any emerging technologies

Who's affected

U.S. government agencies and their agents that access federal tax information (FTI)

Resources

- IRS: Tax Information Security Guidelines For Federal, State and Local Agencies
- IRS: Safeguards Program

ITAR

International Traffic in Arms Regulations

Summary

The United States' International Traffic in Arms Regulations (ITAR) control the manufacture, sale, and distribution of defense and space-related articles and services.

Key requirements

Typically, ITAR compliance is met by ensuring all data centers are managed solely by U.S. citizens within the U.S. and its territories and data is not shared outside of the U.S.

However, in March 2020, the State Department issued a ruling that companies can share unclassified technical data with their supply chain or outside the U.S. In this instance, the data must be secured with end-to-end encryption.

Follow these basic principles to secure your ITAR data:

- Discover and classify sensitive data
- Map data and permissions
- Manage access control
- Monitor data, file activity, and user behavior

Who's affected

ITAR applies to companies that manufacture, export, and distribute defense products and services, including hardware and software, and companies and third parties that act within the defense sector.

Resources

- U.S. Department of State: The International Traffic in Arms Regulations (ITAR)
- AWS: US International Traffic in Arms Regulations: (ITAR)

Healthcare

The healthcare sector is one of the most regulated of all industries in terms of data protection. Healthcare providers and their business associates must comply with the Healthcare Insurance Portability and Accountability Act (HIPAA), which protects the privacy of patient data. Noncompliance can result in fines totaling millions of dollars.

HIPAA

Healthcare Insurance Portability and Accountability Act

Summary

The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to healthcare providers, has requirements for protected health information (PHI) that is created, collected, maintained, and transmitted. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 extended the HIPAA requirements to business associates. The Office of Civil Rights within the U.S. Department of Health and Human services enforces HIPAA compliance and levies steep fines against providers as well as business associates for violating HIPAA provisions.

Key requirements

To protect electronic PHI (ePHI), HIPAA's Security Rule requires covered entities to maintain reasonable administrative, technical, and physical safeguards. The regulation doesn't prescribe specific practices, and each organization must determine what is considered "reasonable" based on its unique circumstances.

The rule has four core requirements:

- Ensuring the confidentiality, integrity, and availability of all ePHI that organizations create, receive, maintain, or transmit
- Identifying and protecting against "reasonably anticipated" threats to the security or integrity of the information
- Protecting against unauthorized use and disclosure
- Ensuring workforce compliance with the requirements

Who's affected

Covered entities include healthcare providers that transmit electronic data, as well as health plans and health clearinghouses. Additionally, business associates that carry out activities and functions on behalf of covered entities must comply with the same requirements.

Resources

- HHS: Summary of the HIPAA Privacy Rule
- Arctic Wolf: Arctic Wolf Platform for the HIPAA Security Rule
- Arctic Wolf: A HIPAA Compliance Cheat Sheet

HITRUST

Healthcare Information Trust Alliance Common Security Framework

Summary

The Healthcare Information Trust Alliance (HITRUST) developed the Common Security Framework (CSF) based on a variety of federal and state regulations, frameworks, and standards. The CSF provides regulated healthcare organizations with a common set of standards they can adopt as well as use for evaluating their vendors.

Key requirements

The HITRUST CSF uses a risk-based approach that includes:

- Organizational factors such as geographic scope and business volume
- Regulatory factors that are based on compliance requirements specific to the organization's circumstances, including sector and geography
- System factors that impact data management risks, such as data storage and transmission, internet access, third-party access, number of users, and number of daily transactions

The framework also has allowances for alternate management, technical, or operational controls that can be applied under specific conditions.

Resources

- RSI Security: HITRUST Compliance: What You Need to Know
- HITRUST Alliance: Understanding and Leveraging the CSF

Manufacturing

Given the ramifications of a successful attack, manufacturers must prioritize building a security posture that is strong enough to prevent attacks and keep production flowing. They must eliminate security risks so they can satisfy partners and customers who depend on a consistent production schedule. In addition, manufacturers have an increasing number of regulations they must meet to maintain compliance.

DFARS

Federal Acquisition Regulation: Defense Federal Acquisition Regulation Supplement

Summary

A supplement to the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS) has been a requirement since Dec. 31, 2017, requiring all Department of Defense (DoD) contractors and subcontractors that store or process controlled unclassified information (CUI) to comply with the minimum security standards outlined in the DFARS. Failure to adhere to DFARS requirements may result in termination of existing DoD contracts.

Key requirements

There are 110 granular requirements contained within the 14 main sections, and DoD contractors must comply with all of them. We've narrowed the broader sections down to seven of the most infosec-oriented categories.

1. **Section 3.1** - Access Control: Granting or denying permissions to access and/or use information.
2. **Section 3.3** - Audit and Accountability: Tracking, reviewing, and examining adherence to system requirements.
3. **Section 3.5** - Identification and Authentication: Managing user identities and adequately authenticating those identities for use with information/processes.
4. **Section 3.6** - Incident Response: Establishing well-tested incident-handling processes (e.g., threat detection, analysis, response, recovery) for organization information systems.
5. **Section 3.11** - Risk Assessment: Periodically assessing risks to information systems and data to effectively track and manage organizational risk.
6. **Section 3.13** - System and Communication Protection: Monitoring, controlling, and protecting all organizational communications.
7. **Section 3.14** - System and Information Integrity: Monitoring all information and communication systems for indicators of threatening traffic and/or activity.

Who's affected

All Department of Defense (DoD) contractors and subcontractors that store or process Controlled Unclassified Information (CUI).

Resources

- Acquisition.gov: Defense Federal Acquisition Regulation Supplement
- Acquisition.gov: Safeguarding Covered Defense Information and Cyber Incident Reporting

CMMC 2.0

Cybersecurity Maturity Model Certification 2.0

Summary

The Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) has replaced its predecessor CMMC 1.0 as a unified standard for implementing cybersecurity across the Department of Defense (DoD), as well as any contractor that works with it. It verifies that suitable levels of cybersecurity systems and processes are established to ensure the security of controlled unclassified information (CUI) stored on networks of DoD contractors.

Key requirements

The CMMC model includes 3 levels, each with a corresponding set of practices and processes. The DoD may require contractors to meet both the associated practices and the given processes to achieve each specific CMMC level.

CMMC 2.0 Level 1: Level 1 parallels the FAR 52.204-21 requirements, which all federal contractors must meet. If you're already doing business with the DoD, you should already be compliant. The 17 controls outlined in Level 1 are all basic cyber hygiene practices and outline the bare minimum any contractor should already have established.

CMMC 2.0 Level 2: Level 2 parallels CMMC 1.0 Level 3, marking a major jump in requirements under this new security framework. Level 2 requires you to establish, maintain, and resource a plan that demonstrates the management of activities for practice implementation. Level 2 focuses on CUI and includes all security requirements specified in NIST SP 800-171, plus some additional methods to mitigate threats.

CMMC 2.0 Level 3: Level 3 is currently undefined but is likely to resemble CMMC 1.0 Level 5. Level 3 requires you standardize and optimize process implementation across the organization. At the same time, its practices center on protecting CUI from advanced persistent threats (APTs). The DoD has announced it will require the implementation of NIST SP 800-172 for CMMC 2.0 Level 3.

Who's affected

There are nearly 300,000 companies in the Defense Industrial Base (DIB), including contractors and subcontractors. The DoD estimates that 80,000 DIB organizations will require CMMC 2.0 Level 2 certification.

Resources

- Federal Register: Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward
- Arctic Wolf Platform for CMMC (1.0)
- Arctic Wolf: CMMC 2.0: What You Need to Know

Location Specific

States have enacted their own laws protecting the security and privacy of consumer data. If you do business in those states, you'll need to comply. Some laws are specific to industries, such as financial, while others apply across the board. Additionally, if you serve customers in the European Union, you need to comply with the General Data Protection Rule, regardless of where you're headquartered.

CCPA

California Consumer Privacy Act

Summary

The California Consumer Privacy Act (CCPA), effective Jan. 1, 2020, is the first consumer privacy legislation of its kind in the United States. It gives consumers the ability to request, free of charge, information about what businesses collect about them. This includes what sources are collecting information, and for what purpose. They can also request to opt out from having their data sold, and/or request that their data be deleted. The California Attorney General enforces the law, which includes provisions for civil litigation and penalties.

Key requirements

The CCPA applies to any business that sells products and services to Californians—and even displaying a website could count as advertising in the state. The law, however, exempts entities that have $25 million or less in revenues, collect data on fewer than 50,000 consumers, and derive less than half of their revenues from selling consumer data. The list of what personal data must be disclosed or deleted upon request is comprehensive and includes web browsing history, biometrics, and geolocation.

Who's affected

All for-profit businesses, regardless of their physical location, that fall under at least one of these three categories:

- Sell to California consumers and earn more than $25 million in annual gross revenues
- Collect (buy, receive, access) data on more than 50,000 consumers
- Earn more than half of their revenues from selling personal data of consumers

Resources

- Security Magazine: Cybersecurity Response to the California Consumer Privacy Act
- Arctic Wolf: How the California Consumer Privacy Act Increases Your Cybersecurity Responsibilities

GDPR

General Data Protection Rule

Summary

The General Data Protection Rule (GDPR), established by the European Commission, regulates data protection for entities that store or process personal data of EU citizens. In addition to protecting personal data, the rule gives consumers broad rights regarding their information, and imposes steep penalties for noncompliance. You don't need to have a business presence in the European Union to be subject to GDPR.

Key requirements

Some of the most important GDPR requirements include:

- Appointing a data protection officer
- Using a "privacy by design" approach
- Implementing data security measures
- Notifying regulators of data breaches within 72 hours

GDPR also gives consumers the right to access their data, be informed about data that's being collected, restrict processing of their data, and more.

Who's affected

All entities, regardless of their physical location, that collect and process data of European Union subjects and have more than 250 employees. Organizations with 250 or fewer employees also must comply if they process data systematically, which could include anything from sending out newsletters or using Google Analytics to analyze website traffic, to storing employment data.

Resources

- General Data Protection Regulation (GDPR) – Official Legal Text
- CSO Online: GDPR: What You Need to Know to Stay Compliant

SHIELD

New York Stop Hacks and Improve Electronic Data Security Act

Summary

New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, effective March 21, 2020, implements cybersecurity requirements for businesses that collect private data on state residents. The statute expands existing legislation, including the definition of private data. The law is not limited to consumer information, so employers and others also need to comply—or risk penalties.

Key requirements

The SHIELD Act has three main elements:

- Administrative safeguards, such as assessment of internal and external risks, while providing employee training
- Technical safeguards, such as assessment of security risks to networks, software design, and information processing
- Physical safeguards, such as protecting against unauthorized physical access and use during or after the collection, transportation, and disposal of data

Who's affected

Any entity or individual, regardless of physical location, who owns or licenses private digital data of New York state residents.

Resources

- Arctic Wolf: New York State's Upcoming SHIELD Law: Is Your Business Ready?
- PWC: NY SHIELD Act: More protection for NY consumers, higher bar for companies that serve them
- The National Law Review: New York Enacts the SHIELD Act

NYDFS / 23 NYCRR 500

New York State Department of Financial Services Cybersecurity Regulation

Summary

The New York State Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) applies to financial institutions—including banks, mortgage and other lenders, and insurance companies—that are licensed, registered, or chartered under NYDFS. It imposes strict cybersecurity requirements that align with the NIST Cybersecurity Framework.

Key requirements

The regulation establishes minimum standards for protecting customer information and IT systems. Requirements include:

- Maintaining a cybersecurity program based on risk assessment for both internal and external risks, including the performance of annual penetration testing and bi-annual vulnerability assessments
- Implementing policies and procedures for identifying and responding to cybersecurity incidents
- Maintaining a program for assessing and mitigating IT systems' vulnerabilities
- Limiting user access privileges to sensitive data
- Developing a cybersecurity policy and incident response plan, as well as security policies for third-party service providers

Who's affected

A covered entity is defined as a person who operates under, or is required to operate under, a license, charter, registration, certificate, permit, accreditation, or other form of authorization under the State of New York Banking Law, Insurance Law, or Financial Services Law.

Resources

- Arctic Wolf: Simplify Compliance for NY DFS Cybersecurity Requirements
- National Law Review: New York Cracks Down on Cybersecurity Compliance

Supplemental

How can your organization be better prepared to stop cybersecurity threats? This is a question that's on every security professional's mind. For CISOs and IT managers, keeping up with the rapidly evolving threat landscape can feel like an impossible task. Whether you're just starting to research ways to strengthen your cybersecurity perimeter or seeking to build onto your existing security program, it's important to always implement industry best practices.

CIS

Center for Internet Security Critical Security Controls

Summary

The Center for Internet Security (CIS) Critical Security Controls supplement almost every other security framework—including NIST, ISO 27001, PCI, and HIPAA—and are a useful baseline to develop or assess a security program. They were created in 2008 to help organizations implement a set of best practices to stay safe from cyber attacks.

Key requirements

CIS Controls v8 contains the following 18 controls:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

Who's affected

Anyone looking to improve cybersecurity within their organization.

Resources

- Center for Internet Security: Critical Security Controls v8
- Arctic Wolf: Address the CIS Critical Security Controls

NIST CSF

National Institute of Standards and Technology Cybersecurity Framework

Summary

The NIST Cybersecurity Framework (NIST CSF) leverages and integrates industry-leading cybersecurity practices that have been developed by organizations like NIST and ISO. The NIST CSF comprises a risk-based compilation of guidelines that can help organizations identify, implement, and improve cybersecurity practices, and creates a common language for internal and external communication of cybersecurity issues.

Key requirements

- **Identify:** Develop an organizational understanding to managing cybersecurity risk
- **Protect:** Support the ability to limit or contain the impact of a potential cybersecurity event
- **Detect:** Define the appropriate activities to identify the occurrence of a cybersecurity event
- **Respond:** Enable timely discovery of cybersecurity events
- **Recover:** Support the ability to contain the impact of a potential cybersecurity incident

Who's affected

According to Gartner, the ISO 27001 and the NIST CSF will remain the predominant enterprise security frameworks complemented by localized and industry-specific standards and regulations through 2024. The NIST CSF is often used as a tool to report security to executive leadership, since the five high-level categories it uses makes it easier to report complex topics under this perspective.

Resources

- NIST: Five Functions
- TechTarget: NIST Cybersecurity Framework

SOC 2 Type II

Service Organization Control 2 Type II

Summary

SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA). The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.

A SOC 2 report is not standardized, but rather tailored to an organization. A SOC 2 Type II report attests that the non-financial reporting controls used by an organization to safeguard customer data are suitably designed and implemented, and attests to the operating effectiveness of those controls.

Key requirements

A SOC 2 Type II audit includes five TSCs that can be included in the report:

- **Security:** Information is protected from vulnerabilities and unauthorized access
- **Availability:** Information and systems are available for operation and use to meet the organization's objectives
- **Processing integrity:** System processing is complete, valid, accurate, timely, and operates as intended
- **Confidentiality:** Information designated as confidential is protected by limiting its access, storage, and use
- **Privacy:** Sensitive personal information is safeguarded against unauthorized users

Who's affected

SOC 2 Type II audits are most applicable to service organizations that store, process, or otherwise interact with consumer data.

Resources

- Law Technology Today: What SOC 2 Type II Certification Means
- AICPA: SOC 2® - SOC for Service Organizations: Trust Services Criteria
- SANS: SOC 2: Five Trust Service Categories (TSCs) and how to select which to include in reports

Next Steps

Compliance is no longer a matter limited to highly regulated businesses.

Regardless of your industry, company size, or location, you need to comply with a variety of cybersecurity and privacy laws. Otherwise, you're putting yourself at risk for legal troubles, as well as potentially damaging your bottom line.

Do you have the tools you need to meet your industry, state, and federal regulation requirements?

The experts at Arctic Wolf®, the leader in security operations, can help.

Gain protection and start experiencing industry-leading security operations as a concierge service. Contact us to find out how to better manage your risks and stay compliant in an evolving landscape.

REQUEST A DEMO

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

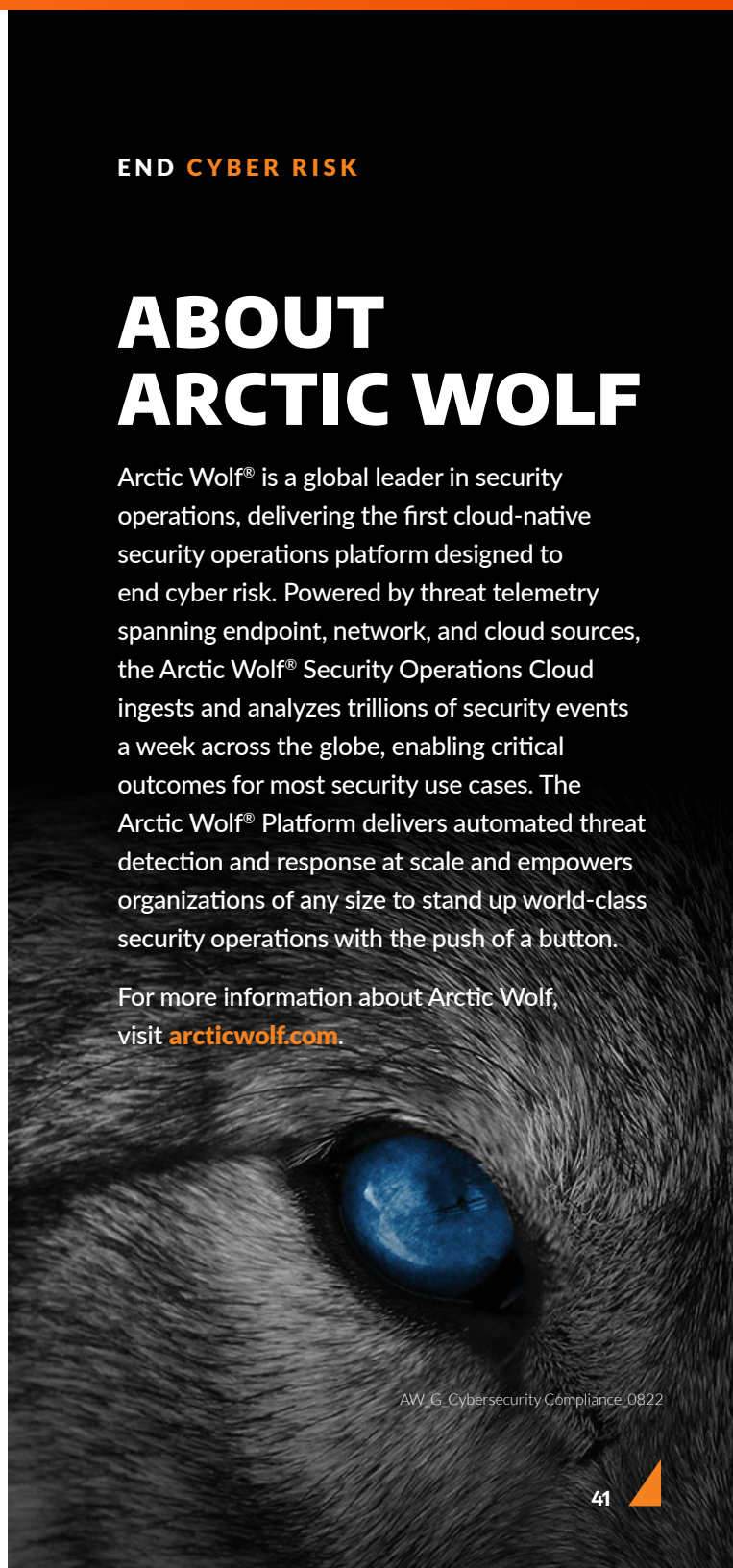
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

END CYBER RISK

ABOUT ARCTIC WOLF

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events a week across the globe, enabling critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit arcticwolf.com.



AW_G_Cybersecurity Compliance_0822