ISC

1

Regulations, Standards, and Frameworks

Module

1	National Institute of Standards and Technology Frameworks	3
2	Privacy and Data Security Standards	15
3	Center for Internet Security Critical Security Controls: Part 1	21
4	Center for Internet Security Critical Security Controls: Part 2	33
5	COBIT 2019 Framework	43

© Becker Professional Education Corporation. All rights reserved.

MODULE 1

National Institute of Standards and Technology Frameworks

ISC 1

Overview

The application of information technology (IT) in an organization is the systematic implementation of hardware and software so that data can be transmitted, modified, accessed, and stored both securely and efficiently. As the field of information science advances, the speed at which IT devices can perform these tasks has rapidly increased, and organizations must reevaluate their technology on a regular basis.

Organizations adopt technology to enhance or support business operations, protect digital records and assets, and safeguard physical assets. This makes the selection and deployment of management information systems critical to the success of any organization.

1 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

1.1 NIST Background

The National Institute of Standards and Technology (NIST) was established in 1901 to remove barriers to industrial competitiveness and improve access to resources to promote U.S. research capabilities. In 1995, the NIST branched out into the cybersecurity field with the NIST Special Publication 800-12, *An Introduction to Information Security*. To date, three of the most prolific sets of standardized frameworks promulgated by NIST include the NIST Cybersecurity Framework (CSF), NIST Privacy Framework, and NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations.

1.2 Cybersecurity Framework

Introduction

The NIST Cybersecurity Framework is designed to help organizations of all sizes and sectors to manage and reduce their cybersecurity risks. It is a voluntary framework that includes three primary components to manage cybersecurity risk:

1. CSF Core
2. CSF Tiers
3. CSF Organizational Profiles

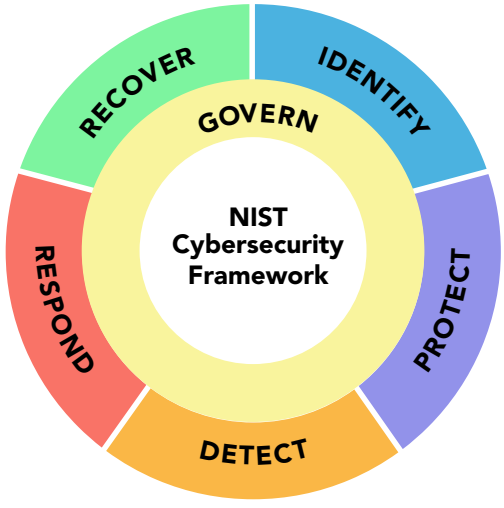
© Becker Professional Education Corporation. All rights reserved.

1.2.1 CSF Core

The NIST CSF Core describes cybersecurity outcomes that can be used by an organization of any size to reduce its cybersecurity risks. These outcomes create a taxonomy and structure to help organizations understand, assess, prioritize, and communicate critical cybersecurity risks.

The framework core consists of six functions, which represent different points in the security risk management life cycle that help enhance cybersecurity protection. These components are not ordered steps; they are functions that should be performed concurrently. The six functions are Govern, Identify, Protect, Detect, Respond, and Recover.

1. **Govern (GV):** This function establishes, communicates, and monitors the organization's cybersecurity risk management strategy, expectations, and policy. This function assists an organization in achieving and prioritizing outcomes of the other five functions in relation to the organization's mission and stakeholder expectations.
2. **Identify (ID):** This function focuses on understanding the assets and suppliers of an organization and the cybersecurity risks related to these assets and suppliers. This function also includes identifying improvement opportunities related to the organization's cybersecurity risk management policies, plans, processes, procedures and practices.
3. **Protect (PR):** This function focuses on an organization's ability to secure its assets to prevent or reduce the likelihood and impact of adverse cybersecurity events. Examples of the safeguards used to manage cybersecurity risks include identity management, authentication, and access control; awareness and training; data security; platform security; and infrastructure resiliency.
4. **Detect (DE):** This function focuses on the timely discovery of cybersecurity attacks and incidents by analyzing anomalies, indicators of compromise, and other potentially adverse events that may indicate that a cybersecurity attack or incident is occurring.
5. **Respond (RS):** This function focuses on a company's ability to contain the effects of cybersecurity incidents. Outcomes within this function cover incident management, analysis, mitigation, reporting, and communication.
6. **Recover (RC):** This function focuses on supporting the timely restoration of a company's normal operations to reduce the impact of cybersecurity incidents and communicate recovery efforts effectively and appropriately.



Source: Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

© Becker Professional Education Corporation. All rights reserved.

These six functions define the high-level framework and are subdivided into categories and, subsequently, into subcategories.

Categories: Tie outcomes to specific activities and company needs.

Subcategories: Divide categories into management and technical activities that help achieve the category outcomes.

Function	Category	ID
GOVERN (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
IDENTIFY (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
PROTECT (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
DETECT (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
RESPOND (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
RECOVER (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Subcategory	Implementation Examples
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	**1st:** 1st Party Risk **Ex1:** Update near-term and long-term cybersecurity risk management objectives as part of annual strategic planning and when major changes occur **Ex2:** Establish measurable objectives for cybersecurity risk management (e.g., manage the quality of user training, ensure adequate risk protection for industrial control systems) **Ex3:** Senior leaders agree about cybersecurity objectives and use them for measuring and managing risk and performance

Source: Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

© Becker Professional Education Corporation. All rights reserved.

Illustration 1 Cybersecurity Framework Core: Detect, Respond, and Recover

Falcon CPAs and Associates is a large accounting and IT auditing firm that has several clients for whom it provides bookkeeping, tax work, and IT audit services. Falcon decided to run a scan using its new NIST-based security software for a client. The application scans various applications and devices, generating a report with findings.

The report came back with high-risk employee behavior and the use of high-risk devices as potential red flags. The employee behavior included access to records on the weekends and after business hours. The use of high-risk devices included excessive use of USB drives that were being plugged into the network to transfer data. Both were related to an individual who was later determined to be stealing employee banking information from the payroll department outside of normal working business hours.

Falcon's utilization of the application helped to detect high-risk areas and behaviors, including those determined to be from an individual committing theft of banking information. Falcon's response may include the analysis of impact, communication to those employees impacted by the stolen information, and mitigation strategies to reduce the risk of similar breaches. Falcon's recovery may include restoring any stolen data, improving protections to restrict unauthorized access, and taking necessary disciplinary or legal action against the individual committing the data theft.

Illustration 2 Detective Measures as Concurrent Protections

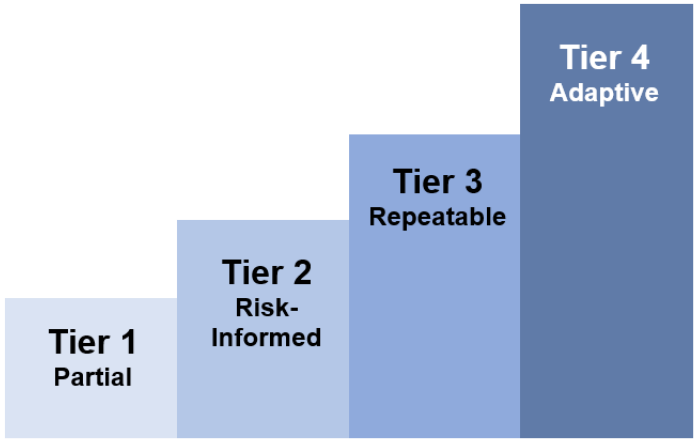
A locked door on an empty house is a preventive measure: if the criminal knows no one is home, the criminal is free to break the lock and steal from the house. If the same locked door has a webcam pointed at it to identify the thief and simultaneously alert the police, the presence of the camera may deter the thief from breaking into the house. The camera is not a preventive measure; it does nothing to stop a break-in, but because the thief can see the detective measure put in place, the camera may deter the crime.

This concept applies to the NIST Framework Core. Detection processes may be included as part of the protection process as a way to protect information and data. Similar to the webcam in the empty house, if detection tools are in place to identify individuals who access information or data, such detection tools may serve as a deterrent and protect sensitive information.

© Becker Professional Education Corporation. All rights reserved.

1.2.2 CSF Tiers

The NIST CSF provides a measure of an organization's information security infrastructure sophistication in the form of four Tiers. These tiers do not serve to implement the six functions. Rather, the tiers categorize the degree to which information security practices are integrated throughout an organization. The tiers should complement an organization's existing cybersecurity risk management methodology and can be used as a benchmark to communicate its organization-wide approach to managing cybersecurity risks.



Source: Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

The CSF Organizational Profiles determine success or failure of information security implementation, whereas the CSF Tiers inform an organization as to the rigor of the governance and management practices associated with those profiles. Tiers are divided by level and then subdivided into cybersecurity risk governance and cybersecurity risk management.

© Becker Professional Education Corporation. All rights reserved.

CSF Tiers		
	Cybersecurity Risk Governance	**Cybersecurity Risk Management**
Tier 1 (Partial)	Risk management is ad hoc and reactive where prioritization of information security efforts is not formally based on organizational objectives or threat environment.	There is limited awareness of cybersecurity risks at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis and does not have processes that allow cybersecurity information to be shared within the organization for general awareness.
Tier 2 (Risk-Informed)	Cybersecurity prioritization is based on organizational risk, and management approves cybersecurity efforts; however, cybersecurity policies may be isolated and not be established as organizational-wide policies.	The organization is aware of the cybersecurity risks in general and specific risks associated with its suppliers, as well as the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.
Tier 3 Repeatable)	The organization utilizes cybersecurity in planning and has enshrined cybersecurity practices in formal, documented policies. These policies are frequently updated based on shifts in business requirements, threats, and technological landscape.	There is an organization-wide risk approach to cybersecurity where risks of assets, suppliers, and products and services are consistently and accurately monitored, as well as regularly communicated among senior leadership.
Tier 4 (Adaptive)	A risk-informed, organization-wide approach in managing cybersecurity risks. Senior executives monitor cybersecurity risks in the same context as financial and other organizational risks and cybersecurity risk management is part of the organizational culture.	Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely, effective manner to evolving, sophisticated threats.

1.2.3 CSF Organizational Profiles

CSF Organizational Profiles are the mechanisms by which NIST recommends companies measure cybersecurity risk and establish a road map to ensure the organization can minimize such risk. An Organizational Profile should include one or both of the following:

- A Current Profile that specifies the outcome that an organization is achieving (or is attempting to achieve) based on the current cybersecurity posture.
- A Target Profile that specifies the desired outcome that an organization has prioritized achieving, and that considers anticipated changes to the organization's cybersecurity posture.

In addition, there are also Community Profiles which are different than organizational profiles. Community Profiles are baseline outcomes developed among a number of organizations due to the shared interest and goals of a particular industry sector, topic, or use case. These profiles can be used by organizations to develop their own Target Profile.

Organizational Profiles should factor organizational mission objectives, stakeholder expectations, threat landscape, and risk management priorities.

© Becker Professional Education Corporation. All rights reserved.

NIST provides a repeatable five-step approach in using Organizational Profiles to help inform continuous improvement of an organization's cybersecurity posture:

- Scope the Organizational Profile.
- Gather the information needed to prepare the Organizational Profile.
- Create the Organization Profile.
- Analyze the gaps between the Current and Target Profiles and create an action plan.
- Implement the action plan, and update the Organizational Profile.

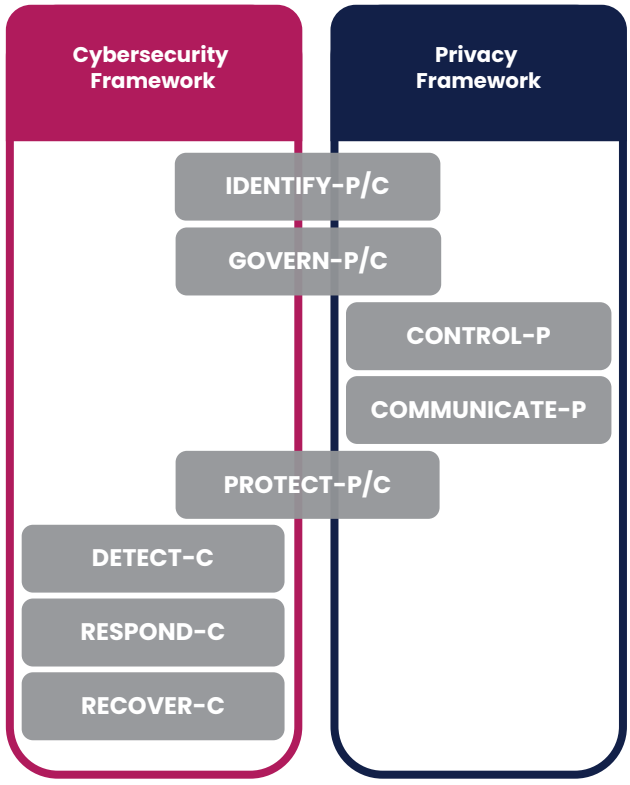
2 National Institute of Standards and Technology (NIST) Privacy Framework

2.1 Privacy Framework

The NIST Privacy Framework was published in early 2020 to protect individuals' data as used in data processing applications. The Privacy Framework provides a common language for understanding, managing, and communicating privacy risk with internal and external stakeholders. The framework can be adaptable to organizations in any industry and is a tool that is used to align policy, business, and technological approaches to managing and reducing privacy risk.

Leveraging a similar structure to NIST CSF, the Privacy Framework expresses control objectives in the form of a Framework Core, with sophistication measures in Framework Profiles, and finally mechanisms to drive organizational change and success through Framework Implementation Tiers.

In addition to the similar structure, there is a degree of overlap between the CSF and Privacy Frameworks. The following graphic shows concepts present in both, meaning they have similar risk management approaches, but they are applied to each subject matter differently. Additionally, the Privacy Framework can apply elements in practice that are only found in the Cybersecurity framework. For instance, the guidance in the NIST Privacy Framework suggests that the Cybersecurity Framework risks—Detect, Respond, and Recover—can be applied to the Privacy Framework risks to further support the management of cybersecurity-related privacy events.



© Becker Professional Education Corporation. All rights reserved.

Framework Core

The Privacy Framework Core is contained in Appendix A of the Privacy Framework and is divided into the following eight Framework Functions:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

© Becker Professional Education Corporation. All rights reserved.

These Functions help organizations answer the following questions:

- **Identify-P:** What are the company's privacy risks related to data processing activities?
- **Govern-P:** What is the best governance structure for privacy risks related to the company's data processing activities?
- **Control-P:** What is the best management structure for privacy risks related to data processing activities?
- **Communicate-P:** How should the organization drive dialogue around privacy risks related to data processing activities?
- **Protect-P:** What are the safeguards that should be in place around privacy risks related to data processing activities?
- **Detect:** How should the organization detect data privacy risks and events?
- **Respond:** How should the organization respond to data privacy events?
- **Recover:** How should the company continue business after data privacy events?

The Functions are subdivided into 29 categories to address privacy program considerations. Those categories, in turn, are divided into 100 subcategories. As with the NIST CSF, the subcategories in the NIST Privacy Framework are individual controls resulting in successfully addressing the 29 controls and the eight Framework Functions.

- **Framework Profiles**

  NIST Privacy Framework Profiles operate identically to NIST CSF Framework Profiles. NIST identified a successful model in the NIST CSF and replicated that same platform for other control sets.

  The NIST Privacy Framework recommends creating a Current and Target Profile and using those to gauge maturity and sophistication while developing a gap analysis and road map for improvement. As with the NIST CSF, the Privacy Framework Current Profile refers to current state privacy practices, while Target Profile refers to future privacy practices.

- **Framework Implementation Tiers**

  The Privacy Framework Tiers mirror those found in NIST CSF. There are four Tiers: Partial, Risk- Informed, Repeatable, and Adaptive. Also, similar to the NIST CSF is the utility of those Tiers, which is gauging performance and communicating internally about how to allocate resources based on current and target Tiers.

  As with the CSF, the subdivisions in the Privacy Framework are divided into four Tiers. For the risk management process, risk management program integration, and ecosystem relationships, the implementation statements are materially identical and reframed for privacy.

  One key difference is the addition of workforce as a Tier subdivision. As part of the measurement of Tier maturity, NIST added the measurement of workforce dedicated to an organization's privacy function. At the Partial end of the spectrum, no one is assigned to privacy, and training is ad hoc. At the Adaptive end of the spectrum, there are dedicated privacy personnel throughout the organization and regular broad-based training.

  Another difference between the NIST CSF and Privacy Framework Tiers is the expression of progression through the Tiers. In the Privacy Framework, progression is recommended based on accomplishing goals in prior Tiers. In the Privacy Framework, Tiers are used more as a gauge of privacy maturity.

© Becker Professional Education Corporation. All rights reserved.

3 NIST Security and Privacy Controls

3.1 NIST SP 800-53

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations has evolved into a set of security and privacy controls applicable to all information systems and has become the standard for federal information security systems.

NIST SP 800-53 is a stricter standard compared to the NIST CSF or Privacy Frameworks. While the CSF and Privacy Frameworks are designed for cost-effectiveness and best-practice implementation, the controls in NIST SP 800-53 are designed for protecting information systems against sophisticated threats. Even though there is a cost-based approach to NIST SP 800-53 implementation, organizations must carefully evaluate adopting the framework because it can become burdensome given that there are nearly 1,200 detailed controls.

- **Purpose and Applicability**

  NIST SP 800-53 establishes controls for systems and organizations that can be implemented within organizations or systems that process, store, or transmit information. These standards are designed to help organizations identify the security and privacy controls needed to manage risk and satisfy the following security and privacy requirements:

  - **Office of Management and Budget (OMB) Circular A-130:** Requires the controls for federal information systems.
  - **The Federal Information Security Modernization Act (FISMA):** Requires the implementation of minimum controls to protect federal information and information systems.

- **Target Audience**

  The following audience is intended for the NIST SP 800-53:

  - Individuals with system, information security, privacy, or risk management and oversight responsibilities, including authorizing officials, chief information officers, senior agency information security officers, and senior agency officials for privacy
  - Individuals with system development responsibilities, including mission owners, program managers, system engineers, system security engineers, privacy engineers, hardware and software developers, system integrators, and acquisition or procurement officials
  - Individuals with logistical or disposition-related responsibilities, including program managers, procurement officials, system integrators, and property managers
  - Individuals with security and privacy implementation and operations responsibilities, including mission or business owners, system owners, information owners or stewards, system administrators, continuity planners, and system security or privacy officers
  - Individuals with security and privacy assessment and monitoring responsibilities, including auditors, inspectors general, system evaluators, control assessors, independent verifiers and validators, and analysts
  - Commercial entities, including industry partners, producing component products and systems, creating security and privacy technologies, or providing services or capabilities that support information security or privacy

© Becker Professional Education Corporation. All rights reserved.

- **Organizational Responsibilities**

  When managing security and privacy risks, the following are required by the organization:

  - Well-defined security and privacy requirements for systems and organizations
  - The use of trustworthy information system components based on state-of-the-practice hardware, firmware, and software development and acquisition processes
  - Rigorous security and privacy planning and system development life cycle management
  - The application of system security and privacy engineering principles and practices to securely develop and integrate system components into information systems
  - The employment of security and privacy practices that are properly documented and integrated into, and supportive of, the institutional and operational processes of organizations
  - Continuous monitoring of information systems and organizations to determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of security and privacy organization-wide

NIST SP 800-53 is subdivided into 20 different control families that cover organizational risk. Those families are listed below with the organizational questions they seek to answer.

- **AC–Access Control:** How does the organization manage application and resource access?
- **AT–Awareness and Training:** How should the company deliver training on information security risk?
- **AU–Audit and Accountability:** How does the company evaluate information security controls?
- **CA–Assessment, Authorization, and Monitoring:** How does the organization collect information security telemetry and use it to hunt for threats?
- **CM–Configuration Management:** How are assets and software configured securely?
- **CP–Contingency Planning:** How is the company prepared for downtime and outages?
- **IA–Identity and Authentication:** How is identification and authentication managed?
- **IR–Incident Response:** How is the organization prepared for information security and events?
- **MA–Maintenance:** How does the company ensure secure maintenance of infrastructure?
- **MP–Media Protection:** How is information on physical media managed?
- **PE–Physical and Environmental Protection:** How are facilities secured from intrusion or harm?
- **PL–Planning:** How does the organization manage information security planning?
- **PM–Program Management:** How does the organization securely manage its information security program?
- **PS–Personnel Security:** How are employees evaluated for potential compromise?
- **PT–PII Processing and Transparency:** How is personally identifiable information (PII) managed?
- **RA–Risk Assessment:** How is environmental risk evaluated?
- **SA–System and Services Acquisition:** How are systems securely evaluated and acquired?
- **SC– System and Communications Protection:** How is data securely transmitted digitally?

© Becker Professional Education Corporation. All rights reserved.

- **SI–System and Information Integrity:** How is the integrity of data in company systems maintained and evaluated?
- **SR–Supply Chain Risk Management:** How does the company secure its supply chain (new to NIST 800-53 Rev. 5)?

The control families are subdivided into controls and control enhancements. Controls are the objectives to be implemented for family conformance. Control enhancements are best practices, some of which are recommended, while others are necessary for conformance to a baseline.

Controls and control objectives are written as statements for implementation. Some of those statements for implementation include bracketed and italicized language, which is an organization-defined parameter. Organizations are required to enter values or compliance statements in lieu of the placeholder.

One key difference between NIST SP 800-53 Rev. 4 and NIST SP 800-53 Rev. 5 is that the latest revision dropped priority and baseline allocation. In prior iterations, NIST categorized the NIST SP 800-53 standards into low, moderate, and high control baselines. Those baselines informed the sensitivity of federal systems to which the controls applied. As those are inapplicable and potentially confusing in the private sector, the control baselines were dropped in favor of comprehensive conformance.

With respect to implementation models, NIST SP 800-53 outlines three control implementation approaches that are to be implemented on a per-control basis:

1. **Common (Inheritable):** Implement controls at the organizational level, which are adopted by information systems.
2. **System-Specific:** Implement controls at the information system level.
3. **Hybrid:** Implement controls at the organization level where appropriate and the remainder at the information system level.

© Becker Professional Education Corporation. All rights reserved.

Privacy and Data Security Standards

1 Data Privacy

1.1 Privacy Laws

Privacy laws exist to protect an individual's private life and keep personal details out of the public domain. These laws also create trust between consumers and enterprises so that when a consumer's personal information is shared, such as with a credit card company or a health care provider, sensitive information will be safeguarded according to rules outlined in applicable privacy regulations.

Privacy laws regulate how those entrusted with private information must collect, process, maintain, and disclose it. Generally, those entrusted with the information must be clear about what data they collect, keep it confidential, and limit access to only those who need it.

Today's modern privacy laws in the United States focus on particular types of data or entities, such as health care data, financial data, or data held by federal agencies. There is no single federal law that applies generally and regulates all personal data. Unlike the United States, the European Union enacted one comprehensive data privacy law, the General Data Protection Regulation (GDPR), that applies generally and governs how all entrusted with personal data should handle such information. A few U.S. states, such as California, have enacted similar privacy laws of general applicability that apply to those doing business in the state or the data of the people in the state.

1.2 Data Breaches

With society's use of the internet and the cloud, data exchange is more prevalent than ever. The rise in available data has led to a surge in data breaches. A data breach is the exposure of confidential information to unauthorized persons. There are two categories of data breaches:

- **Unintentional:** A breach resulting from negligence or error.
- **Intentional:** A breach resulting from bad actors illegally gaining access to data.

Data breaches can create significant consequences for companies and consumers. For companies, a data breach can cause business disruption, reputational harm, financial loss, data loss, and potential legal and regulatory implications. The IBM Cost of Data Breach Report for 2022 shows that the average cost of a data breach is over $4 million. This cost includes four categories of expenditures:

- **Detection and Escalation:** The cost to detect a breach, such as forensics and investigative efforts.
- **Notification:** The cost to notify necessary parties, such as consumers and regulators.
- **Post-breach Response:** The cost to rectify the effects of the breach, such as paying regulatory fines, implementing credit-monitoring services for consumers, and providing ongoing communications to consumers.

© Becker Professional Education Corporation. All rights reserved.

- **Loss of Business and Revenue:** Revenue is temporarily lost during downtime caused by data breaches, and this can ultimately lead to loss of customers, which creates a more permanent loss of revenue.

For consumers, the impact is different and more personal. A data breach can mean exposure of personal information, such as name, home address, Social Security number, and payment or banking information. This exposure puts consumers at risk of identity theft and monetary theft.

2 Modern Privacy Regulations

2.1 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the Department of Health and Human Services to adopt national standards promoting health care privacy and security. In response, the department adopted the Privacy Rule and the Security Rule. HIPAA and the rules that resulted regulate how the health care industry maintains and discloses health information.

The HIPAA Privacy Rule governs the privacy of protected health information (PHI). This rule applies to specific health care-related entities and businesses, called covered entities, which include any of the following:

- Health care providers that transmit health information electronically
- Health plans
- Health care clearing houses
- Business associates who are service providers who need access to PHI to perform services for covered entities

The Privacy Rule permits a covered entity to use and disclose PHI, with no further authorization required:

- To the individual.
- For treatment, payment, and health care operations.
- Incident to an otherwise permitted use and disclosure.
- With valid authorization.
- After giving the individual the opportunity to agree or object.
- As a limited (redacted) data set for research, public health, or health care operations.
- For public interest and benefit activities provided by the law.

The HIPAA Security Rule specifically governs electronic PHI. Under the Security Rule, all covered entities must:

- Ensure the confidentiality, integrity, and availability of all electronic PHI;
- Protect against reasonably anticipated threats to the security of the information;
- Protect against reasonably anticipated impermissible uses or disclosures; and
- Ensure compliance by the covered entity's workforce.

© Becker Professional Education Corporation. All rights reserved.

HIPAA requires different safeguards for covered entities or business associates, including the following:

- **Administrative Safeguards:** Standards include security management processes, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plans, and evaluation.
- **Physical Safeguards:** Standards include facility access controls, workstation use, workstation security, and device and media controls.
- **Technical Safeguards:** Standards include access control, audit controls, data integrity controls, person or entity authentication, and transmission security.

2.1.1 Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

HIPAA was amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH was enacted in 2009 to promote health information technology and the transition from paper to electronic records. HITECH amended HIPAA in a few ways. Namely, it increased penalties for HIPAA violations, required that patients receive the option to obtain records in electronic form, and added "business associates" as a covered entity. The U.S. Department of Health and Human Services defines covered entities as individuals, organizations, and agencies who must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

The most significant change resulting from HITECH, however, is the addition of breach notification rules. HITECH requires that covered entities provide notice of a breach to impacted individuals within 60 days after discovery of the breach.

2.2 General Data Protection Regulation (GDPR)

Effective May 2018, GDPR became the European Union's general applicability law regulating the privacy of data. GDPR provides circumstances when it is lawful to process personal data, such as with proper consent or when complying with a legal obligation. This law is one of the strictest privacy laws in the world, as it imposes steep penalties for violators, with fines reaching millions of dollars. Although enacted by the EU, the law's scope extends beyond the EU. GDPR applies to any of the following:

- Data processors based in the EU, even if the actual processing takes place outside of the EU
- Data processors not based in the EU if the processor is offering goods or services to those in the EU or is monitoring the behavior of those in the EU
- Data processors not based in the EU but where EU law applies via public international law (e.g., EU embassies)

GDPR provides the following principles that must be followed when processing data:

- **Lawfulness, Fairness, Transparency:** Data must be processed lawfully, fairly, and in a transparent manner. Organizations have a responsibility to inform individuals (also known as data subjects) about their right to data portability (transparency) and process requests without delays (fairness). Technical or procedural barriers cannot be used to obstruct portability requests.
- **Purpose Limitation:** Data must be processed for specified, explicit, and legitimate purposes. Data subjects can also limit how their personal data is used, also known as the right to restriction of processing. Further processing beyond the purpose is permitted for public interest archiving, scientific or historical research, or statistical purposes.

© Becker Professional Education Corporation. All rights reserved.

- **Data Minimization:** Data processing must be adequate, relevant, and limited to what is necessary for the purpose.
- **Accuracy:** Data must be accurate and kept updated. Data subjects have the right to have inaccurate personal data corrected and to have incomplete personal data completed, also known as the right of rectification.
- **Storage Limitation:** Data must be stored only for as long as is necessary. This includes the right to be forgotten, also known as erasure, allowing data subjects to request the deletion of their personal data. Storing it for longer periods is permitted for public interest archiving, scientific or historical research, or statistical purposes.
- **Integrity and Confidentiality:** Data must be processed securely and protected against unauthorized or unlawful processing, accidental loss, destruction, or damage.

All processors or controllers of data shall be responsible for, and able to demonstrate, compliance with these principles (accountability).

2.2.1 Privacy Shield

To support transatlantic commerce, the European Union (EU) and the United States implemented the Safe Harbor Framework, allowing companies to transfer data between the EU and the United States legally. Ultimately, the EU's court declared the Framework invalid in 2015. As a result, the EU and the United States negotiated the Privacy Shield in 2016 to replace the invalidated Safe Harbor Framework agreement. Then, in July 2020, the EU court declared the Privacy Shield invalid as well.

Until the EU and the United States reach a new agreement, companies that transfer data across the Atlantic live in uncertainty. The U.S. Federal Trade Commission, responsible for enforcing the Privacy Shield in the United States, expects U.S. companies to continue complying with their obligations under the Privacy Shield until further notice.

3 Data Security Standards

3.1 Payment Card Industry Data Security Standard (PCI DSS)

With the rise of cashless transactions, financial institutions in the payment card industry created the PCI (Payment Card Industry) Security Standards Council to enhance payment security. The council created the PCI Data Security Standard (DSS), an applicable framework for entities to promote data security when processing payments. Data subject to PCI DSS includes both cardholder data (e.g., primary account number or PAN, cardholder name, expiration date, and service code) and sensitive authentication data (e.g., full track data, card verification code, PIN). Cardholder data and sensitive authentication data are collectively referred to as account data.

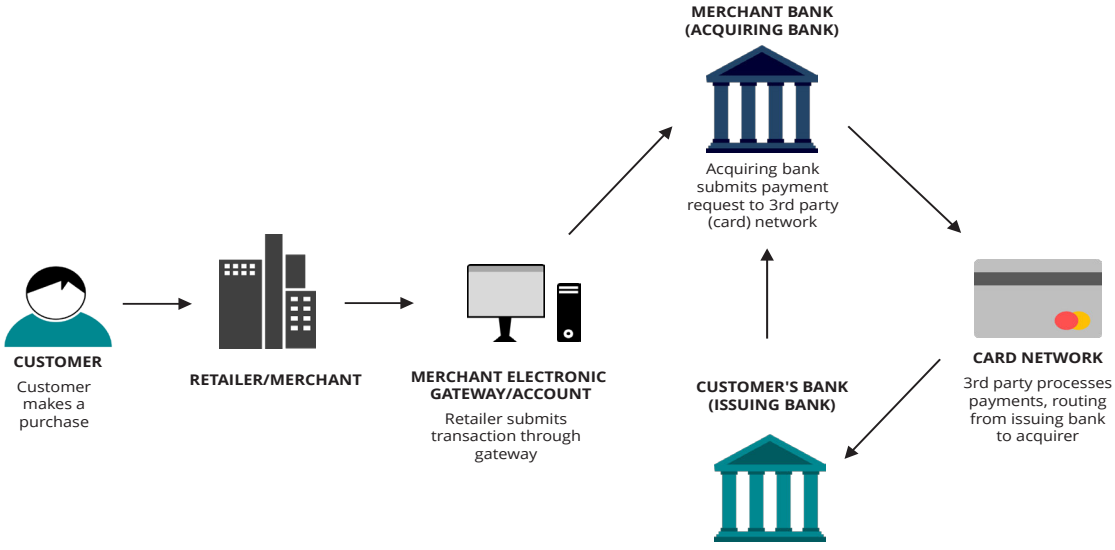
© Becker Professional Education Corporation. All rights reserved.

The PCI DSS provides the following six goals and 12 requirements:

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls. 2. Apply secure configurations to all system components.
Protect Account Data	3. Protect stored account data. 4. Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software. 6. Develop and maintain secure systems and software.
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data through use of need-to-know restrictions. 8. Identify users and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data. 11. Test security of systems and networks regularly.
Maintain an Information Security Policy	12. Support information security with organizational policies and programs.

Source: Material from *PCI DSS v4.0 Quick Reference Guide*, © 2022 PCI Security Standards Council.

The following diagram outlines a typical card payment processing network in which these 12 requirements must be applied, which affects retailers, banks, and the card payment processors themselves. The process starts when a customer makes a purchase at a business using either a physical or virtual debit or credit card that is processed on a third-party payment processor's network (also referred to as a card network). The transaction is sent to the business' bank (acquiring bank) using an electronic gateway supplied by the card network. The acquiring bank then submits a payment request to the card network, which routes payment from the customer's bank (issuing bank) to the acquiring bank. Note that the sequence of these steps may vary depending on the card network and payment processor, with variation in the method of authorization, transmission of data and its encryption, tokenization to mask sensitive data, transaction settlement, and compliance practices.



© Becker Professional Education Corporation. All rights reserved.

Adhering to each of the 12 PCI DSS requirements in the above payment processing network involves the following:

1. Enforcing, for both physical and software-defined networking technologies, network policies that control network traffic between two or more logical or physical network segments.
2. Establishing formalized processes and procedures to apply secure configurations to all system components and wireless environments. Examples include enforcing strict passwords and removing unnecessary software or functions, etc.
3. Minimizing the storage of account data. Sensitive authentication data should not be stored after authorization. Cardholder data, specifically PAN, should be rendered unreadable through means such as cryptography. Cryptographic keys should be secured and their life cycles should be defined and implemented.
4. Encrypting data in transit when transactions are submitted to the card network across the internet and other public networks.
5. Implementing the use of software to protect against malware and phishing attacks.
6. Ensuring all system components have the most recent critical security patches installed. Internally developed software should adhere to secure development and coding practices. Changes to system components are managed securely.
7. Applying strict requirements to grant access to cardholder data on a need-to-know basis, periodically revoking access when applicable.
8. Every user with access to the cardholder data environment (CDE) must have a unique ID. Every user should have a strong authentication mechanism—such as a strong password, biometric, or access token—and use multifactor authentication for all access to the CDE.
9. Physical access to cardholder data or systems that store, process, or transmit cardholder data should be restricted. The point-of-interaction devices utilized should be protected from tampering and unauthorized substitution.
10. Implementing network monitoring that provides audit trails and log activity that are reviewed for suspicious activity.
11. Performing external vulnerability scanning at least once every three months and achieving a passing score. Penetration testing should be performed regularly to identify both external and internal vulnerabilities.
12. Creating, enforcing, and regularly updating the written policy for each stage of the payment process that outlines the sensitivity of account data and employees' responsibilities and procedures to protect account data.

© Becker Professional Education Corporation. All rights reserved.

Center for Internet Security Critical Security Controls: Part 1

1 Center for Internet Security (CIS) Controls

1.1 Overview

The Center for Internet Security (CIS) Controls are a recommended set of actions, processes, and best practices that can be adopted and implemented by organizations to strengthen their cybersecurity defenses. CIS Controls were first developed in 2008 by an international consortium and have evolved over time. The controls are currently supported by the SANS Institute, which provides training, administers certification, and performs research. However, each iteration of control updates involves experts across industries, entity-type (government vs. public companies), and job roles (from operators to policy makers).

The controls are now task-focused and organized by activities. There are 18 CIS controls to reflect shifts in the cybersecurity ecosystem to cloud computing, remote work, and virtualization. Each control has recommendations prescribed to achieve the control objective. These recommendations are referred to as the Safeguards.

1.2 Design Principles

The CIS Controls were designed with the following principles in mind:

- **Context:** An enhancement to the scope and practical applicability of safeguards through incorporation of examples and explanations.
- **Coexistence:** Alignment with evolving industry standards and frameworks, including NIST's CSF 2.0 framework.
- **Consistency:** Disruption to controls users are minimized, limiting the impact on implementation groups.

© Becker Professional Education Corporation. All rights reserved.

1.3 Implementation Groups

The implementation of the CIS Controls can be tailored to an organization's size by using one of three Implementation Groups (IGs). These are self-assessed categories that identify a subset of the CIS Controls, which are critical for companies to adopt, given their size.



Source: CIS Critical Security Controls: Version 8.1

	IG1
	This group is for small or medium-sized organizations that have a limited cybersecurity defense mechanism in place in terms of personnel or IT assets. The main focus of this group is to keep the company operational because their cybersecurity expertise is limited, the data being used is not sensitive, and the company cannot sustain long periods of downtime.
	IG2 (Includes IG1)
	This group is for companies that have IT staff who support multiple departments that have various risk profiles. These organizations typically have sensitive client data, and they can tolerate short interruptions in service. One of the biggest concerns for these entities is loss of trust in the event of a data breach.
	IG3 (Includes IG1 and IG2)
	Organizations in this group have security experts in all the domains within cybersecurity like penetration testing, risk management, and application security. Data assets under management at these companies include those that are sensitive and likely subject to compliance with standards or regulatory oversight. Attacks on these organizations can cause significant damage to the company and the public welfare.

© Becker Professional Education Corporation. All rights reserved.

2 CIS Controls 01–09

2.1 Control 01: Inventory and Control of Enterprise Assets

This control helps organizations actively track and manage all IT assets connected to a company's IT infrastructure physically or virtually within a cloud environment. This allows companies to know the totality of IT assets that should be monitored and protected. Using an IT inventory list, as shown in the following example, will allow organizations to track various data points for company assets:

Asset Description	Serial Number	Model	User	Warranty Expiration	Support End-of-Life Date
Laptop	N4300008A	ProBook 500	Avery Greene	20X5	20X5
Scanner	XCH00R	DesignJet T830	Martin Glenn	20X6	20X7

Having a comprehensive view of company assets will also give visibility into how data flows throughout an organization. Knowing which devices contain sensitive information can help IT managers prioritize the security and maintenance for those devices (e.g., knowing servers and laptops that store employee records should be closely monitored for needed updates, cyber threats, and other irregularities so that unauthorized access is prevented).

Companies should also focus on the potential for external devices to connect to a company's network through means such as guest networks, even if they are segregated from the core network. Other scenarios in which external devices connect to a company's core network include temporary access granted to auditors and permanent access given to managed service providers (MSPs) to manage a company's IT operations.

One challenge organizations face is portable end-user devices that periodically connect to a company's network and then disappear, making it difficult for organizations to have a holistic view of its inventory when devices are off, paused, or otherwise disconnected from the corporate network. Having a robust IT inventory system will mitigate these issues.

The following is a list of the Safeguards (recommendations) within Control 01, along with the asset type associated with the Safeguard, security function, and whether the Safeguard is a priority for an Implementation Group:

Control	Asset Type	Security Function	IG1	IG2	IG3
1.1 Establish and Maintain Detailed Asset Inventory	Devices	Identify	●	●	●
1.2 Address Unauthorized Assets	Devices	Respond	●	●	●
1.3 Utilize an Active Discovery Tool	Devices	Detect		●	●
1.4 Use DHCP Logging to Update Company Inventory—Helps detect which devices are active on the network.	Devices	Identify		●	●
1.5 Use a Passive Asset Discovery Tool—Identifies devices connected to a company's network.	Devices	Detect			●

Source: CIS Critical Security Controls Version 8.1

© Becker Professional Education Corporation. All rights reserved.

2.2 Control 02: Inventory and Control of Software Assets

This control provides recommendations for organizations to track and actively manage all software applications so that only authorized software is installed on company devices. This control also provides guidance on finding unmanaged and unauthorized software already installed so that it can be removed and remediated.

Software within scope consists of operating systems, programming software and library, business applications, drivers, open-source software, application programming interface (API), and some forms of firmware, which is embedded software that comes standard in hardware such as a scanner or printer.

Allowlisting (also known as whitelisting) should be in place so that only approved software is installed on company devices. Maintaining a software inventory list keeps the company informed on whether the most current software patches are installed, applications reaching end-of-life support are renewed or transitioned out, and any additional safeguards needed are in place to compensate for software-related risks.

One popular method of managing software applications is using tools that provide an inventory check against commonly used applications in other companies. Such tools reference information regarding each application's patch level, latest version installed, and naming structure.

Control	Asset Type	Security Function	IG1	IG2	IG3
2.1 Establish and Maintain a Software Inventory	Software	Identify	●	●	●
2.2 Ensure Authorized Software Is Currently Supported	Software	Identify	●	●	●
2.3 Address Unauthorized Software	Software	Respond	●	●	●
2.4 Utilize Automated Software Inventory Tools	Software	Detect		●	●
2.5 Allowlist Authorized Software—Ensures only authorized software can be accessed or executed.	Software	Protect		●	●
2.6 Allowlist Authorized Libraries—Ensures that only specific files can be loaded into a system process.	Software	Protect		●	●
2.7 Allowlist Authorized Scripts—Ensures only authorized scripts, or lines of code, can be executed.	Software	Protect			●

Source: CIS Critical Security Controls Version 8.1

2.3 Control 03: Data Protection

This control helps organizations develop ways to securely manage the entire life cycle of their data, from the initial identification and classification data to its disposal.

Organizations must identify, archive, label, and classify their data to understand the implications of the data being lost or compromised. Classification categories are labeled at the discretion of the enterprise and should be assigned based on sensitivity, such as internal, public, sensitive, and confidential. These labels will vary by industry and each country's relevant regulations, privacy requirements, and compliance obligations.

© Becker Professional Education Corporation. All rights reserved.

After sensitivity is defined, data mapping should be developed that identifies the various software applications that access each of these sensitivity levels. This would allow devices and software to be consolidated into one network so that more sensitive classifications are separate from less sensitive forms of data. Retention requirements, access control lists, access logging mechanisms, and data disposal plans can also be implemented in a tailored fashion once data classification levels are assigned. Encryption can be strategically used to further secure data at rest and in transit so that data compromise is avoided.

Control	Asset Type	Security Function	IG1	IG2	IG3
3.1 Establish and Maintain a Data Management Process	Data	Govern	●	●	●
3.2 Establish and Maintain a Data Inventory	Data	Identify	●	●	●
3.3 Configure Data Access Control Lists	Data	Protect	●	●	●
3.4 Enforce Data Retention	Data	Protect	●	●	●
3.5 Securely Dispose of Data	Data	Protect	●	●	●
3.6 Encrypt Data on End-User Devices	Data	Protect	●	●	●
3.7 Establish and Maintain a Data Classification Scheme	Data	Identify		●	●
3.8 Document Data Flows	Data	Identify		●	●
3.9 Encrypt Data on Removable Media	Data	Protect		●	●
3.10 Encrypt Sensitive Data in Transit	Data	Protect		●	●
3.11 Encrypt Sensitive Data at Rest	Data	Protect		●	●
3.12 Segment Data Processing and Storage Based on Sensitivity	Data	Protect		●	●
3.13 Deploy a Data Loss Prevention Solution	Data	Protect			●
3.14 Log Sensitive Data Access	Data	Detect			●

Source: CIS Critical Security Controls Version 8.1

2.4 Control 04: Secure Configuration of Enterprise Assets and Software

This control helps organizations establish and maintain secure baseline configurations for their enterprise assets, including servers, network devices, mobile and portable end-user devices, non-computing assets such as Internet of Things (IoT) devices, operating systems, and other corporately managed hardware or software.

Many applications are sold preconfigured with default configuration settings that were designed for ease of installation or usage. However, default configurations may present vulnerabilities that can be exploited, allowing unauthorized users to gain access to an organization's core network. This means organizations should implement control activities to assess preconfigured devices at their baseline state, modify vulnerable configuration settings, and eventually move to a continuous review phase.

© Becker Professional Education Corporation. All rights reserved.

It is worth noting that the cloud environment provided by cloud service providers (CSPs) may not be setup in the most secure configuration in order to provide flexibility to their customers. Re-mediating the vulnerability would fall on the enterprises using the platform or services instead of the CSPs.

Publicly available security standards, such as the CIS Benchmarks Program or NIST National Checklist Program Repository, can be used by organizations as a starting point for asset reconfiguration. Adhering to these standards will also assist in complying with any applicable laws and regulations.

Security hardening, which is the process of making an organization less vulnerable to attacks, can be incorporated into adjusting target security configurations so that they are continuously "hardened" against new forms of attack. These improvements may include removing any unused or unnecessary software, closing network ports that are openly exposed to the internet, changing default passwords, and turning off nonessential services.

Security tools such as firewalls, intrusion detection/prevention systems, data loss prevention (DLP) systems, and mobile device management (MDM) software can also be used to secure networks and end-user devices. Organizations with multiple types of environments or data classification levels may have several security baselines that should be addressed. Once target configuration levels have been implemented, they should be continuously monitored for deviations and necessary updates.

Control	Asset Type	Security Function	IG1	IG2	IG3
4.1 Establish and Maintain a Secure Configuration Process	Documentation	Govern	●	●	●
4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure	Documentation	Govern	●	●	●
4.3 Configure Automatic Session Locking on Enterprise Assets	Devices	Protect	●	●	●
4.4 Implement and Manage a Firewall on Servers	Devices	Protect	●	●	●
4.5 Implement and Manage a Firewall on End-User Devices	Devices	Protect	●	●	●
4.6 Securely Manage Enterprise Assets and Software	Devices	Protect	●	●	●
4.7 Manage Default Accounts on Enterprise Assets and Software	Users	Protect	●	●	●
4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Devices	Protect		●	●
4.9 Configure Trust DNS Servers on Enterprise Assets	Devices	Protect		●	●
4.10 Enforce Automatic Device Lockout on Portable End-User Devices	Devices	Protect		●	●
4.11 Enforce Remote Wipe Capability on Portable End-User Devices	Data	Protect		●	●
4.12 Separate Enterprise Workspaces on Mobile End-User Devices	Data	Protect			●

Source: CIS Critical Security Controls Version 8.1

© Becker Professional Education Corporation. All rights reserved.

2.5 Control 05: Account Management

This control outlines best practices for companies to manage credentials and authorization for user accounts, privileged user accounts (such as administrator accounts), and service accounts for company hardware and software.

As with other enterprise assets, accounts must be inventoried and tracked so that appropriate controls may be applied. Centralized account management tools and services can be utilized for consolidated account management across the organization. Organizations should develop and communicate an acceptable use policy and account safety guidelines. Credentials should be treated as highly sensitive information, and formal training should be provided to educate users on account safety best practices as well as the organization's account security policies. These may include password requirements, controls for inactivity, and account lockout policies.

Administrator accounts should be restricted to specific use cases. End-users requiring administrator privileges should have separate accounts to run administrative actions to lower the risk of a user's account being compromised because these accounts are more likely to be targeted by attackers. Service accounts used to run systems and services must be well-documented, indicating ownership and purpose.

- **Single Sign-on and Multifactor Authentication**

  One common and convenient form of authentication is single sign-on (SSO). This lets users use a single log-in to securely authenticate across multiple applications. While this increases the number of applications an attacker can gain access to with a single password, security can be enhanced using multifactor authentication (MFA) so that the users must have a secondary point of contact to validate their identity.

Control	Asset Type	Security Function	IG1	IG2	IG3
5.1 Establish and Maintain an Inventory of Accounts	Users	Identify	●	●	●
5.2 Use Unique Passwords	Users	Protect	●	●	●
5.3 Disable Dormant Accounts	Users	Protect	●	●	●
5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts	Users	Protect	●	●	●
5.5 Establish and Maintain an Inventory of Service Accounts	Users	Identify		●	●
5.6 Centralize Account Management	Users	Govern		●	●

Source: CIS Critical Security Controls Version 8.1

© Becker Professional Education Corporation. All rights reserved.

2.6 Control 06: Access Control Management

This control expands on Account Management (Control 05) by specifying the type of access that user accounts should have. Ideally, an organization's users should only have the necessary privileges required for their job role.

Organizations should follow the principles of "least privilege" and "need-to-know" role assignments. These methodologies assist with the goal that users only have access to systems, services, and data needed to perform their job duties. Accounts that do not follow these principles pose a security risk to the organization by allowing unauthorized access.

Protocols should be put in place for granting access and revoking access based on job duties, roles, and responsibilities. Access control models, such as role-based access control (RBAC) or policy-based access control (PBAC), can be utilized to help facilitate this process by defining roles within the organization and assigning appropriate access to each role to provide separation of duties. For accounts with administrator access or remote access, additional controls such as multifactor authentication (MFA) and privileged account management (PAM) can be used as an additional security layer.

A comprehensive solution, ideally centralized, for provisioning and de-provisioning employee access should also be in place. Sophisticated methods allow access to all applications across the organization to be removed synchronously within minutes of initiating such a change in the system.

Control	Asset Type	Security Function	IG1	IG2	IG3
6.1 Establish an Access Granting Process	Documentation	Govern	●	●	●
6.2 Establish an Access Revoking Process	Documentation	Govern	●	●	●
6.3 Require Multifactor Authentication for Externally Exposed Applications	Users	Protect	●	●	●
6.4 Require Multifactor Authentication for Remote Network Access	Users	Protect	●	●	●
6.5 Require Multifactor Authentication for Administrative Access	Users	Protect	●	●	●
6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems	Software	Identify		●	●
6.7 Centralize Access Control	Users	Protect		●	●
6.8 Define and Maintain Role-Based Access Control	Users	Govern			●

Source: CIS Critical Security Controls Version 8.1

© Becker Professional Education Corporation. All rights reserved.

2.7 Control 07: Continuous Vulnerability Management

This control assists organizations in continuously identifying and tracking vulnerabilities within their infrastructure so that they can remediate and eliminate weak points or windows of opportunity for bad actors.

An evolving cybersecurity landscape requires organizations to keep abreast of threats and vulnerabilities to be able to defend against them. Attackers can exploit and leverage vulnerabilities to compromise assets and gain a foothold into a company's network. Unknown vulnerabilities, referred to as zero-day exploits, occur when there is no known solution to a weak point. In these instances, attackers can carry out attacks for which there is not yet any remediation.

Organizations must remain proactive in scanning, monitoring, and managing vulnerabilities to reduce the window of opportunity for attackers to capitalize on them. As new vulnerabilities are discovered, they should be assessed for their likelihood of exploitation and impact if they occur so that they can be ranked and prioritized. It is preferable to use vulnerability scanning tools that map vulnerabilities to industry-recognized publications such as Common Vulnerabilities and Exposures (CVE®), Common Configuration Enumeration (CCE), Open Vulnerability and Assessment Language (OVAL®), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS), and/or Extensible Configuration Checklist Description Format (XCCDF).

Control	Asset Type	Security Function	IG1	IG2	IG3
7.1 Establish and Maintain a Vulnerability Management Process	Documentation	Govern	●	●	●
7.2 Establish and Maintain a Remediation Process	Documentation	Govern	●	●	●
7.3 Perform Automated Operating System Patch Management	Software	Protect	●	●	●
7.4 Perform Automated Application Patch Management	Software	Protect	●	●	●
7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets	Software	Identify		●	●
7.6 Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets	Software	Identify		●	●
7.7 Remediate Detected Vulnerabilities	Software	Respond		●	●

Source: CIS Critical Security Controls Version 8.1

© Becker Professional Education Corporation. All rights reserved.

2.8 Control 08: Audit Log Management

This control establishes an enterprise log management process so that organizations can be alerted and recover from an attack in real time, or near real time, using log collection and analytic features. There are two log categories that are frequently configured independently, system logs and audit logs, which provide valuable information that can be used for prevention, troubleshooting, incident response, discovering patterns, and detecting anomalies.

System logs provide a list of events such as start and end times, points of restoration, and system crashes. Audit logs are tied to a specific user, recording when a person logs in or out, accesses a file, or opens an application.

- **Event Logs**

  Having access to event logs is critical to incident response, and it can also facilitate processes for legal matters, such as eDiscovery, accountability for auditing, lessons learned for process improvement, and data retention for compliance requirements. An enterprise log management process should address the entire life cycle of audit logs beginning with log collection and ending with log disposal. Audit logs may be captured from a variety of connection methods, whether directly to a company's network via a hard-wired connection, wirelessly, or using a virtual private network (VPN). Organizations should also be notified when failed user attempts are made to connect to resources without the appropriate privileges.

Control	Asset Type	Security Function	IG1	IG2	IG3
8.1 Establish and Maintain an Audit Log Management Process	Documentation	Govern	●	●	●
8.2 Collect Audit Logs	Data	Detect	●	●	●
8.3 Ensure Adequate Audit Log Storage	Data	Protect	●	●	●
8.4 Standardize Time Synchronization	Data	Protect		●	●
8.5 Collect Detailed Audit Logs	Data	Detect		●	●
8.6 Collect DNS Query Audit Logs	Data	Detect		●	●
8.7 Collect URL Request Audit Logs	Data	Detect		●	●
8.8 Collect Command-Line Audit Logs	Data	Detect		●	●
8.9 Centralize Audit Logs	Data	Detect		●	●
8.10 Retain Audit Logs	Data	Protect		●	●
8.11 Conduct Audit Log Reviews	Data	Detect		●	●
8.12 Collect Service Provider Logs	Data	Detect			●

Source: CIS Critical Security Controls Version 8.1

© Becker Professional Education Corporation. All rights reserved.