



SECURITY GUIDANCE FOR IIS

2026



AIRA
AMERICAN IMMUNIZATION
REGISTRY ASSOCIATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3	Security Controls for IIS: Chapters 4, 5 and 6	41
ACKNOWLEDGMENTS	5	4 OPERATIONAL SECURITY CONTROLS	42
HOW TO USE THIS DOCUMENT	8	5 SPECIAL TOPIC: ARTIFICIAL INTELLIGENCE CONTROLS	72
1 INTRODUCTION	9	6 BUSINESS CONTINUITY, INCIDENT RESPONSE, AND RECOVERY CONTROLS	78
2 SECURITY FUNDAMENTALS	16	7 CONCLUSION	87
3 ESTABLISHING AND MAINTAINING A SECURITY PROGRAM	27	8 APPENDICES	89

APPENDICES

APPENDIX A IIS SECURITY GUIDANCE ACRONYMS	90	APPENDIX C IIS SECURITY RESPONSIBILITIES BY ROLE	97
APPENDIX B CONTROL SELECTION METHODOLOGY	93	APPENDIX D ORIENTATION TO THE SECURE CONTROLS FRAMEWORK (SCF)	101

EXECUTIVE SUMMARY

Immunization information systems (IIS) are critical public health infrastructure that support clinical decision making, vaccine management, public health reporting, and other activities essential to protecting the health of individuals and communities. Maintaining a secure IIS enables IIS to meet the IIS Functional Standards and helps ensure reliable and trusted IIS operations. Because IIS collect, store, and exchange sensitive information, maintaining a secure IIS is fundamental to protecting the confidentiality, integrity, and availability of IIS data. As cybersecurity threats continue to evolve, IIS programs must remain vigilant in managing risk and strengthening security practices.

This Security Guidance for IIS document updates and builds on the 2017 *Security Guidance Considerations for Immunization Information Systems*. This updated guidance reflects current and evolving cybersecurity threats, modern technologies, evolving expectations, and industry-recognized safeguards. It is intended to help IIS programs identify, assess, manage, and reduce cybersecurity risk while supporting operational resilience and continuity of services.

Because IIS programs operate in diverse environments with varying resources and technical capabilities, this guidance is designed to be practical and adaptable. It focuses on high-priority security practices that IIS programs can tailor to their environments and use to strengthen security over time.

The guidance is organized around several core areas that work together to support a comprehensive approach to IIS security:

- **Security Fundamentals** introduces key cybersecurity concepts, terminology, legal and regulatory considerations, and reference resources that support informed decision making.
- **Establishing and Maintaining a Security Program** focuses on leadership, accountability, roles and responsibilities, and making decisions about risk. These activities establish the foundation for a sustainable security program and support ongoing prioritization of security efforts.
- **Operational Security** addresses the day-to-day practices used to protect IIS systems, data, and operations. Topics include human resources security, physical and environmental security, third-party management, system and technical security, secure software development, web application security, configuration and change management, identity and access management, data protection and handling, and logging and monitoring.

- **Artificial Intelligence** discusses this emerging technology as a cross-cutting security topic. As AI becomes increasingly integrated into public health technologies and cybersecurity tools, IIS programs should understand both the risks and opportunities associated with AI.
- **Business Continuity, Incident Response, and Recovery** focuses on preparing for, responding to, and recovering from operational disruptions and cybersecurity incidents. These practices help IIS programs maintain critical functions, restore services, and strengthen resilience over time.

This guidance is intended to support practical, risk-informed decision making and continued improvement over time. For IIS programs looking to begin or advance their cybersecurity efforts, the following actions provide a practical starting point for strengthening security and establishing a foundation for continuous improvement:

-  **Strengthen governance and accountability** by defining and documenting leadership roles, responsibilities, and coordination for IIS security.
-  **Understand your environment** by identifying applicable requirements, critical systems, data, dependencies, and external partners.
-  **Assess and prioritize risks** by evaluating threats, vulnerabilities, and dependencies that could affect IIS operations and data.
-  **Implement prioritized security improvements** that align with organizational needs, available resources, and risk tolerance.
-  **Continuously monitor and improve** security practices as technologies, threats, organizational priorities, and risks evolve.

By applying these practices, IIS programs can strengthen security, improve resilience, and help ensure IIS capabilities continue to support immunization and public health goals.

Disclaimer: This guidance is not a prescriptive standard or compliance requirement, nor does it replace applicable laws, regulations, organizational policies, or jurisdiction-specific security requirements. This document reflects a point-in-time reflection of cybersecurity practices and considerations broadly applicable to IIS. Because cybersecurity continues to evolve, organizations should apply this guidance to their unique environments and supplement it with current standards, best practices, and emerging information as appropriate.

ACKNOWLEDGMENTS

This project is supported by the Centers for Disease Control and Prevention (CDC) through a cooperative agreement, CDC/NCIRD Award No. 6 NH23IP922665-02-01. This project was initiated in response to a recommendation from the 2024–2025 cycle of the Resource Development Recommendations Workgroup, which identified updating the 2017 *Security Guidance Considerations for Immunization Information Systems* as a priority resource development effort.

The American Immunization Registry Association (AIRA) would like to acknowledge and thank the following individuals and organizations for their support and contributions to this project:

SECURITY GUIDANCE FOR IIS ADVISORY PANEL (AP)

Panel members provided subject matter expertise, strategic direction, and iterative review throughout development of this guidance, contributing insights from IIS operations, information security, and related disciplines to ensure the guidance reflects current practices, evolving risks, and practical considerations for implementation across diverse IIS environments.

- **Mike Berry**, Senior Project Manager, HLN
- **Aaron Bieringer**, Operations Technical and Data Unit Supervisor, Minnesota Department of Health
- **Matt Blackmon**, Standards and Conformance Testing Programs Manager, The Sequoia Project
- **Jason Dogariu**, Lead Software Developer, Kunz, Leigh & Associates
- **Austin Fuoco**, IIS Deputy Manager, Philadelphia Department of Public Health
- **Baskar Krishnamoorthy**, IT Business Planning Manager, Florida Department of Health
- **Craig Newman**, Senior Fellow, J Michael Consulting
- **Brian Nicholson**, Information Systems Security Officer, CDC (retired)
- **Nathan Scott**, Chief Technology Officer, Docket
- **Kevin Snow**, Chief Technology Officer, Envision/Inductive Health
- **Mary Woinarowicz**, Immunization Program Manager, North Dakota Department of Health & Human Services

CDC PROJECT STEWARD

- **Jacqueline (“Jackie”) Reyes**, IT Project Manager

SUBJECT MATTER EXPERTS

Additionally, AIRA would like to thank the following individual for contributing expertise and insights as part of the security guidance update process:

- **Tom Cornelius**, Secure Controls Framework (SCF) Founder & Contributor

UNIVERSITY OF TEXAS STUDENT CONTRIBUTORS

AIRA would also like to recognize the University of Texas at Austin students who contributed to the Security Controls Framework control mapping and analysis activities that supported the control selection methodology used for this guidance.

- Ainsley Burns, Deeya Chakrabarti, Monica Garza, Isabelle Huang, Prerana Kalapatapu, Sanya Lalani, Jeniah Landry, Hasya Magesh, Katherine Mercedes Sabino, Meenu Meyyappan, Aarya Nair, Ella Ngo, Riya Patwardhan, Shreyas Sripurushottam, Sabrina Tam, Ryan Tran, Avery Wiley, Noah Yu, Grace Zhou

IIS COMMUNITY REVIEWERS

AIRA would like to thank the IIS community members who participated in the external community review process. Their feedback, insights, and recommendations helped strengthen the content, clarity, and practical applicability of this guidance.

- **Noor Alhayani**, Illinois Department of Public Health
- **Laura Barrett**, Immunization Registry Manager, Kentucky Department for Public Health
- **Josh Davis**, Chief Technology Officer, SSG
- **Kevin Day**, Chief Technology Officer, Rhapsody
- **Janet Fath**, Senior Public Health Advisor, Centers for Disease Control and Prevention (CDC)
- **Kim Gulliver**, CIIS and Data Operations Manager, Colorado Department of Public Health and Environment
- **Jonah Heberlein**, Integration Engineer, Epic
- **Amyanne KeswaniCope**, Illinois Department of Public Health
- **David Lyalin**, Public Health Analyst, Centers for Disease Control and Prevention (CDC)
- **Karyn Lyons**, Immunization Section Chief, Illinois Department of Public Health
- **Sharon Matthies**, Immunization Information System Manager, Idaho Department of Health and Welfare
- **Nancy Sharova**, Health Program Supervisor/IIS Manager, Connecticut Public Health
- **Kimberly S. Spann**, Illinois Department of Public Health
- **Chloe Watts**, Senior HL7 Interoperability Analyst, STChealth
- **Rachel York**, IIS Program Manager, Louisiana Department of Health

AIRA STAFF

- **Skylar Adkins**, Administrative Assistant
- **Franchesca Benjamin**, Program Coordinator
- **Alison Chi**, Senior Director of Education & Organizational Development
- **Rebecca Coyle**, Executive Director
- **Carmela Gupta**, Director of Education & Outreach
- **Eric Heflin**, Consultant, Cybersecurity Expert, Technical Writer, Advisory Panel Co-Chair
- **Jennifer Jubert**, IIP Business Analyst
- **Mary Beth Kurilo**, Senior Director of Health Informatics
- **Eric Larson**, Senior Technical Program Manager
- **Tesha Lucas**, Senior Program Manager
- **Melissa McClung**, Director, Integration & Support
- **Gabriella Pelissier**, Membership Engagement and Communications Specialist
- **Erin Roche**, Consultant, Lead Technical Writer, Advisory Panel Co-Chair
- **Shelby Sandstrom**, Technical Analyst
- **Kristi Siahaya**, Senior Health IT Technical Consultant
- **Chris Sorenson**, Lead Software Engineer

An independent copy editor, Maureen Brody, reviewed and professionally edited the report.

An independent graphic designer, Amy Panzer at Panzer Creative, provided graphic design services.

HOW TO USE THIS DOCUMENT

This document and the companion resources are intended to help IIS programs identify practical cybersecurity practices that can strengthen the security and resilience of IIS environments over time. The recommendations are intended to support risk-informed decision making and should be considered in the context of each organization's operational, technical, and resource environment. The guidance is meant to provide the building blocks for each jurisdiction's unique security road map.

The recommendations are not intended to be implemented all at once or in a prescribed order. IIS programs may use this document to identify priorities, support planning, and guide discussions with enterprise IT, information security teams, and IIS vendors to determine which recommendations are appropriate for their environment.

This document is designed to complement the 2017 *Security Guidance Considerations for Immunization Information Systems*. Together, these resources can help IIS programs assess current capabilities, prioritize improvement efforts, and support ongoing cybersecurity maturity through continuous improvement.

1

INTRODUCTION



CHAPTER 1 INTRODUCTION

SECURITY AS THE FOUNDATION OF IIS OPERATIONS

Maintaining the security of immunization information systems (IIS) is essential to safeguarding the privacy of individuals in these population-based systems. Demonstrating due diligence in security supports compliance with statutory and contractual obligations.

At its core, security practices reduce risk, i.e., the potential for harm arising from unauthorized disclosure, unauthorized modification of data, and/or disruption of system availability. Strong security practices also establish the foundation for patient and user trust in IIS operations. In turn, this foundation enables IIS to meet jurisdictional programmatic goals and the diverse needs of the users and patients they serve.

The importance of maintaining secure systems and ensuring appropriate, authorized access to IIS data is reinforced throughout the Centers for Disease Control and Prevention (CDC) *IIS Functional Standards* and the corresponding *IIS Requirements Traceability Matrix* (RTM). Notably, a primary IIS Functional Standard goal is to “establish and maintain a secure, confidential Immunization Information System” with standards referencing “physical and digital security” and “ensuring authorized access to data.”

As part of the nation’s critical infrastructure, IIS are vital to ensuring public health and safety. As such, IIS, like other health care information systems, have an elevated risk profile and require robust security measures to ensure protection of data, resilience, and continuity of operations. Recent high-profile security incidents highlight the scale and impact of cyber threats in health care.

Recent Health Care Security Incidents

- Yale New Haven Health System: 2025 breach affecting nearly 5.6 million individuals¹
- Change Healthcare: 2024 ransomware attack affecting nearly 200 million individuals²
- HCA Healthcare: 2023 data theft affecting ~11 million individuals³
- Welltok: 2023 third-party breach affecting ~14.7 million individuals⁴
- Kaiser Permanente: 2017–2024 data exposure affecting ~13 million individuals⁵

Additionally, the U.S. Department of Health and Human Services (HHS) list of breaches of unsecured protected health information illustrates the volume and prevalence of these incidents across different organizations,⁶ with an increasing number of breaches due to the “increasing digitalization of healthcare data and the increasing sophistication of cyberattacks.”⁷

PURPOSE

This guidance is designed to support IIS in maintaining a secure foundation for operations in alignment with security best practices, the IIS Functional Standards, RTM requirements, and IIS community expectations. It is intended to help IIS programs identify, assess, manage, and reduce security risk through structured planning, implementation, and ongoing monitoring of priority security practices (i.e., controls).

¹ Hughes, Jill, “Biggest healthcare data breaches reported in 2025, so far,” Tech Target, September 2, 2025, <https://www.techtarget.com/healthtechsecurity/feature/Biggest-healthcare-data-breaches-reported-in-2025-so-far>.

² McGee, Marianne Kolbasuk, “State AG Sues Change Healthcare in 2024 Ransomware Attack,” GovInfoSecurity, April 2, 2026, <https://www.govinfosecurity.com/state-ag-sues-change-healthcare-in-2024-ransomware-attack-a-31326>.

³ Alder, Steve, “11.27 Million HCA Healthcare Patients Affected by Recent Cyberattack,” HIPAA Journal, July 11, 2023, <https://www.hipaajournal.com/hca-healthcare-cyberattack-data-breach-2023/>.

⁴ Adler, Steve, “Welltok Data Breach Victim Count Rises to 14.76 Million,” HIPAA Journal, August 23, 2024, <https://www.hipaajournal.com/welltok-data-breach/>.

⁵ Lewis, Truman, “Kaiser Permanente Agrees to \$46M Data Privacy Settlement over Alleged Tracking of Patient Information,” ConsumerAffairs, January 16, 2026, <https://www.consumeraffairs.com/news/kaiser-permanente-agrees-to-46m-data-privacy-settlement-over-alleged-tracking-of-patient-information-011626.html>.

⁶ U.S. Department of Health and Human Services, Office for Civil Rights, [Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information](#).

⁷ Alder, Steve, “Healthcare Data Breach Statistics – Updated for 2026,” HIPAA Journal, February 26, 2026, <https://www.hipaajournal.com/healthcare-data-breach-statistics/>.

WHAT'S IN A NAME: CONTROL

A safeguard or countermeasure to protect the confidentiality, integrity, availability of a system, its components, processes, data, and users.⁸ Secure Controls Framework adds the dimensions of “safety” to controls to recognize that the physical world can be impacted by cybersecurity.⁹

This document serves to update and expand upon the 2017 *Security Guidance Considerations for Immunization Information Systems* to reflect current cybersecurity threats, modern technologies, evolving regulatory requirements, and industry best practices. As an update to the 2017 Security Guidance, it also serves as a companion to the following AIRA resources:

- *Confidentiality and Privacy: Considerations for IIS* (2016)
- *Business Continuity Planning for IIS Programs* (2019)

DESIRED OUTCOMES

This guidance is intended to support IIS programs in progressing toward a strengthened, sustainable security posture characterized by the following outcomes:

- **Governance and risk-informed planning:** Roles, responsibilities, and decision-making authority for security are clearly defined; security risks are routinely identified, assessed, and prioritized; and security activities are guided by documented plans, priorities, and resource considerations.
- **Implemented and consistently applied security practices:** Administrative, technical, and physical safeguards are applied across IIS operations.
- **Monitored, measured, and continuously improved security:** Practices are continuously monitored, evaluated, and refined to address evolving threats and vulnerabilities.
- **Resilient operations and sustained trust:** Rapid detection, response, and recovery from security events minimize impact to operations and data and maintain confidence among patients, providers, and partners.

Collectively, these outcomes reflect a comprehensive, risk-informed approach to IIS security that supports resilient operations, protects sensitive data, and sustains IIS community trust.

⁸ National Institute of Standards and Technology (NIST), [Computer Security Resource Center Glossary: Control](#). See also: [Security Control](#).

⁹ Secure Controls Framework, [Start Here: Building Your Cybersecurity & Data Privacy Program](#).

SCOPE

This resource focuses on high-priority, actionable security practices to support the protection and resilience of IIS. Grounded in recognized security standards and frameworks and aligned with security-related requirements in the IIS RTM, the guidance is intended to provide a practical foundation for planning, implementing, and maintaining IIS security controls. Additional information on the methodology used to identify and prioritize IIS security controls is provided in [Appendix B: Control Selection Methodology](#).

The guidance is not intended to provide exhaustive coverage of all security domains or prescribe specific policies, technologies, or implementation approaches. The security practices described in this guide should be tailored to each IIS program's legal and organizational requirements, governance structure, operating environment, technical architecture, risk profile, and available resources. Accordingly, each IIS program should establish policies, procedures, and implementation approaches that best align with its needs. Additional implementation resources are cited throughout the guide where applicable.

INTENDED AUDIENCE



To support governance, ongoing management, and implementation of IIS security practices, this guidance is intended primarily for the following audiences:

- **Jurisdictional executive leadership:** Accountable for IIS security risk and responsible for establishing strategic direction, governance, and oversight of IIS security activities
- **Jurisdictional IIS manager/IIS project manager:** Oversees and coordinates implementation of IIS security practices and supports ongoing risk management and operational security activities
- **IIS technical implementer:** Implements, monitors, and validates security controls

These audiences play complementary roles in a shared-responsibility model for IIS security. They also coordinate with the broader network of the IIS community whose roles and responsibilities influence IIS security outcomes. While not the primary audience for this guidance, IIS and immunization program staff, IT and security teams, legal and compliance staff, procurement and contracting offices, hosting providers, vendors, and other external partners may find this guidance useful for understanding IIS security expectations, roles, and practices.

Broad awareness across IIS teams supports coordinated execution, more consistent application of security procedures, and secure day-to-day operations across organizational boundaries.

INTENDED USE

IIS programs should use this guidance in conjunction with applicable legal, regulatory, contractual, and organizational risk-informed requirements to determine appropriate security obligations and implementation approaches for their environments.

This document is intended to support both the ongoing management of an IIS security program and targeted, topic-based guidance. Key characteristics of this guide include:

- **Action-oriented:** Focused on practical considerations and implementation guidance that support meaningful security improvement
- **Self-contained and extensible:** Designed to function as a stand-alone resource while also supporting more detailed exploration of security through alignment with SCF, a mostly free, open-source security meta-framework
- **Tailorable:** Intended to be adapted to each IIS environment based on governance, legal authority, technical architecture, available resources, risk profile, and program maturity



ORGANIZATION

This document is organized into chapters that may be used independently to address specific needs or together as part of a comprehensive approach to strengthening IIS security. Because security responsibilities vary across roles, targeted primary audiences are identified for each chapter, as indicated in Table 1.

Table 1 | Targeted primary audiences by chapter

CHAPTER	EXECUTIVE LEADERSHIP	IIS MANAGER	IIS IT IMPLEMENTER
1. Introduction: Why IIS security matters and an overview of the guidance document			
2. Security Fundamentals: Foundational concepts and reference resources			
3. Establishing and Maintaining a Security Program: Governance, roles and responsibilities, and risk management practices to oversee and improve security			
4. Operational Security Controls: Practices related to the day-to-day operation of an IIS			
5. Special Topic: Artificial Intelligence (AI) Controls: Practices related to the use of AI			
6. Business Continuity, Incident Response and Recovery Controls: Practices to prepare for, respond to, and recover from disruptions and security events			
7. Conclusion: Key concepts and the importance of continuous improvement			
8. Appendices: Supporting materials and templates for implementation			

LIMITATIONS

This document reflects a point-in-time review of security practices and considerations to provide a practical foundation for strengthening IIS security. Because IIS environments vary, this guidance should be tailored to each jurisdiction’s legal, technical, organizational, and operational needs and should be augmented as needed. SCF is updated quarterly and can serve as a resource for identifying emerging best practices, evolving risks, and other security considerations.

**SECURITY
FUNDAMENTALS**

2



CHAPTER 2 SECURITY FUNDAMENTALS

PURPOSE

This chapter introduces foundational security concepts, terminology, applicable legal and regulatory considerations, and key reference resources relevant to IIS security.

Together, these elements establish a shared vocabulary and common understanding to support informed decision making and application of risk-based security practices.



TARGETED PRIMARY AUDIENCE:

- IIS manager/IIS project manager
- Executive leadership

KEY TERMS AND DEFINITIONS

The following definitions are derived from the National Institute of Standards and Technology (NIST) Glossary¹⁰ and additional sources as noted to support a consistent understanding of the terms used throughout the document.

SECURITY AND PRIVACY

- **Security:** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction; achieved through safeguards to ensure confidentiality, integrity, and availability
- **Privacy:** The protection of individuals' personal information from unauthorized or inappropriate use and disclosure, in accordance with applicable laws and regulations

Security encompasses the safeguards used to protect systems, data, and operations, while cybersecurity focuses specifically on protecting computer systems and networks from attack. For purposes of this guidance, the terms are used interchangeably.

¹⁰ National Institute of Standards and Technology (NIST), Glossary, <https://csrc.nist.gov/glossary>. Note: This glossary provides a compilation of definitions for key terms as used across NIST publications.

Security focuses on protecting information and systems, while privacy focuses on appropriate use and disclosure of personal information. Security practices support privacy by helping safeguard sensitive data.

RISK AND THREAT CONCEPTS

- **Threat:** A potential cause of harm to operations, assets, and/or individuals
- **Vulnerability:** A weakness in a system, security procedures, internal controls, or implementation that could be exploited or triggered by a threat
- **Risk:** A measure of the potential for harm, considering the likelihood and impact of occurrence

For example, an unauthorized access attempt (threat) combined with weak authentication (vulnerability) increases the potential for unauthorized access (risk).

Risk reflects the likelihood and impact of harm when a threat exploits a vulnerability. Security practices aim to defend against threats, reduce vulnerabilities, and minimize risk.

RISK MANAGEMENT

- **Risk management:** The overall, ongoing process of identifying, assessing, prioritizing, and responding to risk through coordinated governance, operational, and technical activities
- **Control (also referred to as “security control”):** A safeguard or countermeasure implemented to manage risk and protect the confidentiality, integrity, and availability of systems, processes, and data

Risk management establishes how risks are identified, evaluated, prioritized, and addressed. Controls are the specific measures implemented to manage those risks and strengthen security outcomes.

OBJECTIVES OF RISK MANAGEMENT

Effective risk management supports the risk management objectives noted below as well as the broader security outcomes described in Chapter 1's Introduction.

Information and system security objectives

Risk management helps protect the confidentiality, integrity, and availability (CIA) of information and systems. SCF also recognizes safety as an additional security objective.

- **Confidentiality:** Information is not disclosed to unauthorized entities or processes.
- **Integrity:** Information is protected from unauthorized modification.
- **Availability:** Information and systems are accessible and usable by authorized entities when needed.
- **Safety:** Information and systems are managed to reduce the risk of harm to individuals, organizations, or the public.¹¹

Operational objectives

Effective risk management also contributes to broader operational objectives:

- **Security:** Implementation of applicable controls, with defined policies, documented procedures, trained personnel, and verified technical controls that address the organization's identified threats and vulnerabilities¹²
- **Resilience:** Ability to adapt to changing conditions and withstand and recover rapidly from disruptions while maintaining critical operations
- **Compliance:** Adherence to external requirements (i.e., applicable statutory, regulatory, and contractual obligations) through the implementation and maintenance of appropriate controls

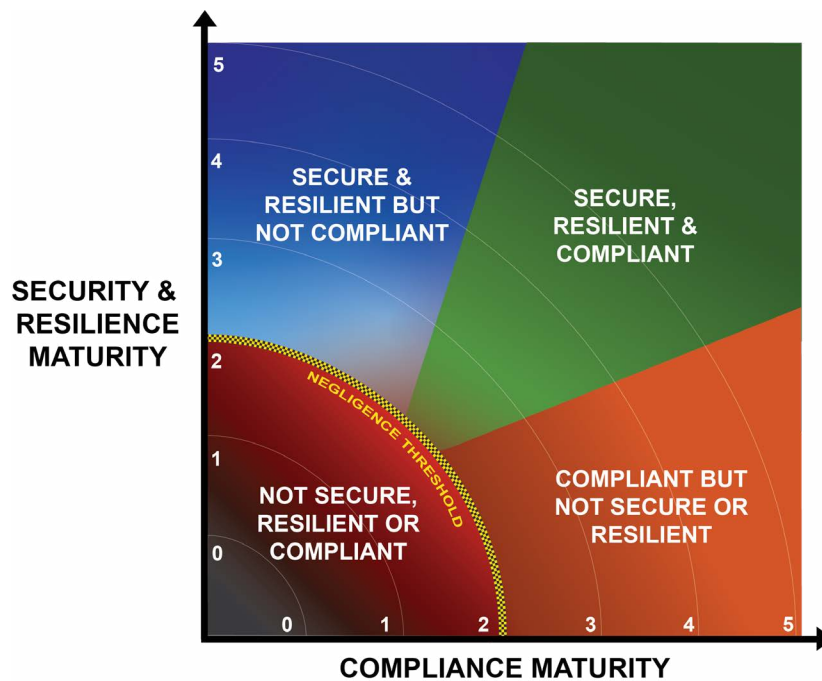


¹¹ SCF, <https://content.securecontrolsframework.com/pdf/scf-recommended-practices.pdf>.

¹² SCF. Security, Compliance & Resilience Management System (SCRMS), <https://securecontrolsframework.com/start-here/security-compliance-resilience-management-system-scrms>.

SCF visualizes the relationship between security, resilience, and compliance as indicated in Figure 1.

Figure 1 | Assessing an organization's security, compliance, and resilience



Source: <https://securecontrolsframework.com/start-here/security-compliance-resilience-management-system-scrms>

FEDERAL LAWS AND REGULATIONS

The following U.S. federal laws and associated implementing regulations help establish the broader legal and regulatory context in which IIS operate. While IIS are primarily governed by state and local laws, familiarity with federal requirements can help IIS programs better understand common security expectations, inform risk management decisions, and support security planning efforts. These federal requirements also provide important context for understanding security expectations, common practices, and supporting resources across the health IT ecosystem.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA) establishes national standards that form a baseline for health information privacy and security protections. Covered entities (CEs) and their business associates (BAs)¹³ are required by law to comply with HIPAA. IIS are commonly recognized as public health authorities under HIPAA; whether the covered entity designation applies to an IIS depends on jurisdictional interpretation. However, *all IIS can benefit from the adoption and implementation of many of the HIPAA privacy and security practices* as reflected in the HIPAA Privacy Rule and HIPAA Security Rule.

- The **HIPAA Privacy Rule** establishes standards for the protection of individuals' health information. This rule "defines and limits the circumstances in which an individual's protected health information may be used or disclosed by covered entities." Notably, CEs may disclose protected health information without an individual's authorization in support of public health activities.¹⁴
- The **HIPAA Security Rule** establishes standards for the security of electronic protected health information (ePHI) that is created, received, used, or maintained by a covered entity or its business associate. Specifically, the rule requires implementation of administrative, physical, and technical safeguards to ensure the security of ePHI.^{15,16}

The U.S. Department of Health and Human Services (HHS) is the federal agency responsible for maintaining, administering, and enforcing HIPAA provisions. Additional information about HIPAA and HIPAA-defined terms as they relate to IIS is available in the *Confidentiality and Privacy Considerations for IIS* document.

¹³ HHS, Covered Entities and Business Associates, <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.

¹⁴ U.S. Department of Health and Human Services (HHS), *The HIPAA Privacy Rule*.

¹⁵ HHS, *The Security Rule*.

¹⁶ Note: At the time of publication, updates to the HIPAA Security Rule have been proposed but have not been finalized. IIS programs should monitor applicable federal guidance and regulatory updates and assess whether changes affect their privacy and security practices. Additional information on the HHS notice of proposed rulemaking for the Security Rule is available at <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>.

ADDITIONAL FEDERAL LAWS

In addition to HIPAA, the **Federal Information Security Modernization Act (FISMA)** and the **Cybersecurity Act of 2015** have influenced the nation's approach to cybersecurity by advancing risk management practices, standardized security frameworks, and information sharing across government and critical infrastructure sectors. Although both apply primarily to federal agencies, the standards, guidance, and resources issued by Cybersecurity and Infrastructure Security Agency (CISA) and the NIST in support of these laws offer valuable information to guide IIS security efforts.

The practices and frameworks developed under these laws, including those highlighted below, can inform risk-based decision making, strengthen security controls, and support alignment with widely recognized security approaches across the health IT ecosystem.

Together, these laws and regulations help establish the broader context for protecting health information and managing security risk and provide IIS programs with a foundation for understanding many of the security practice, frameworks, and resources referenced throughout this guidance.



■ KEY RESOURCES

The legal and regulatory landscape described above establishes important expectations for protecting health information, while implementation approaches and recommended safeguards are addressed across a broad set of frameworks, standards, and reference materials. One challenge of maintaining effective security practices is keeping pace with evolving threats, expectations, and guidance issued by multiple authorities (e.g., HHS, NIST, and CISA). To support navigation of these resources, the following sections highlight select materials intended to provide baseline familiarity and support informed security planning and implementation decisions.

META-FRAMEWORKS

Security “meta-frameworks” consolidate and harmonize requirements, standards, and guidance from multiple sources. Examples of security meta-frameworks include:

- **HITRUST Common Security Framework (CSF):** A widely used framework in health care to support security compliance assurance and certification; accessible to HITRUST Qualified Organizations and HITRUST Qualified Individuals per the HITRUST CSF License Agreement.¹⁷
- **Secure Controls Framework (SCF):** A series of resources and program elements and a community that catalogs and maps security controls across NIST and other recognized frameworks, standards, and regulations to support security implementation.

To support IIS in implementing security practices, this guidance uses the SCF as a primary reference resource. The SCF provides a continually updated, consolidated, and cross-mapped set of controls derived from more than 200 laws, regulations, standards, and frameworks. This SCF Control Catalog is open source and freely available under a Creative Commons license.¹⁸ Although the HITRUST Common Security Framework is widely recognized in health care, licensing constraints limited its suitability as the primary reference for this guidance. Both HITRUST and SCF offer optional paid third-party certifications.

Additional information about the selection of the SCF as a primary reference framework is outlined in the accompanying [Cybersecurity Framework Environmental Scan](#) resource. An orientation to the SCF is also provided in [Appendix D](#).

¹⁷ HITRUST Alliance, HITRUST CSF — Our Cybersecurity Framework, <https://hitrustalliance.net/hitrust-framework>.

¹⁸ Secure Controls Framework, [SCF Overview and Practitioner Guidebook](#). Note: AIRA has no financial interest or commercial relationship with SCF.

SELECT SECURITY RESOURCES

While meta-frameworks help organize and align guidance across sources, familiarity with key resources can provide additional context and support more informed security planning and implementation decisions. The following are highlighted to provide baseline awareness of commonly referenced security resources.

Where available, the resources below identify the corresponding SCF “Authoritative Source” identifier. These identifiers demonstrate how source materials are referenced within SCF and may assist readers in locating related controls and cross-mapped guidance within the meta-framework.

HHS

- **Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs):** Voluntary, health-care-specific cybersecurity goals (both “essential” and “enhanced”); intended to help organizations prioritize high-impact cybersecurity practices¹⁹
- **Healthcare and Public Health Cybersecurity Framework Implementation Guide:** Guidance for how to apply the NIST Cybersecurity Framework²⁰
- **Enterprise Performance Life Cycle (EPLC):** A framework for IT governance and lifecycle management that integrates planning, oversight, and risk management across the lifecycle of IT projects²¹

NIST

- **Cybersecurity Framework (CSF) 2.0:** A broadly applicable, high-level framework for understanding, assessing, prioritizing, and communicating cybersecurity risk. Core functions include govern, identify, protect, detect, respond, and recover.²² (SCF: NIST CSF 2.0)

¹⁹ HHS, [Healthcare and Public Health Cybersecurity Performance Goals](#).

²⁰ HHS, Administration for Strategic Preparedness and Response, [Health Care and Public Health Sector Cybersecurity Framework Implementation Guide](#).

²¹ HHS, [Policy for Information Technology \(IT\) Enterprise Performance Life Cycle \(EPLC\)](#).

²² NIST, [Cybersecurity Framework 2.0](#).

NIST Special publications (SP):

- **800-37 Rev. 2, Risk Management Framework (RMF):** A structured process for application of security practices across the system life cycle. The seven-step process includes prepare, categorize, select, implement, assess, authorize, and monitor.²³ (SCF: NIST 800-37 R2)
- **800-53 Rev. 5, Security and Privacy Controls:** A widely used extensive catalog of security and privacy controls. Controls are organized in 20 families, including access control, identification and authentication, audit and accountability, system and communications protection, incident response, and contingency planning.²⁴ (SCF: NIST 800-53 R5)
- **800-66 Rev. 2, Implementing the HIPAA Security Rule:** Guidance specific to implementing NIST 800-53 controls associated with HIPAA Security Rule requirements, including those related to administrative, physical, and technical safeguards.²⁵ (SCF: NIST SP 800-66 R2)
- **800-218, Secure Software Development Framework (SSDF):** Guidance for integrating security into software development practices. Practices are organized in four groups: prepare the organization, protect the software, produce well secured software, and respond to vulnerabilities.²⁶ (SCF: NIST 800-218)

CISA

- **Cross-Sector Cybersecurity Performance Goals (CPGs) 2.0:** Voluntary, baseline cybersecurity practices for critical infrastructure organizations, intended to help organizations prioritize the most impactful and broadly applicable security actions²⁷ (SCF: US CISA CPG 2022)

²³ NIST, [SP 800-37 Rev 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#).

²⁴ NIST, [SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations](#).

²⁵ NIST, [SP 800-66 Rev 2: Implementing the Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule: A Cybersecurity Resource Guide](#).

²⁶ NIST, [SP 800-218: Secure Software Development Framework \(SSDF\) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities](#).

²⁷ Cybersecurity and Infrastructure Security Agency (CISA), [Cybersecurity Performance Goals 2.0](#).

Additional industry standards, guidance, and resources

- **ISO/IEC 27001 and 27002:** International standards for establishing, implementing, and maintaining information security management systems^{28,29} (SCF: ISO 27001 2022; ISO 27002 2022)
- **Open Worldwide Application Security Project (OWASP) Top 10:** Community-driven resource identifying the most critical web application security risks and providing guidance for mitigating common vulnerabilities³⁰ (SCF: OWASP Top 10 2025)

Additionally, independent audit and authorization programs, such as **System and Organization Controls (SOC) 2**³¹ and **GovRAMP**³², serve to evaluate implementation and provide independent assurance regarding select security and privacy controls (SCF: AICPA TSC 2017:2022 (used for SOC 2); GovRAMP). Just as GovRAMP provides an authorization framework for cloud service providers (CSPs) used by state and local governments, **FedRAMP** serves as the equivalent program for federal agencies.³³ (SCF: US FedRAMP R5)

²⁸ International Organization for Standardization (ISO), [27001:2022; Information Security, Cybersecurity, and Privacy Protection—Information Security Management Systems—Requirements](#). [Paywall].

²⁹ ISO, [27002:2022; Information Security, Cybersecurity, and Privacy Protection—Information Security Controls](#). [Paywall].

³⁰ Open Worldwide Application Security Project (OWASP), [OWASP Top Ten Web Application Security Risks](#).

³¹ American Institute of Certified Public Accountants, [SOC 2® - SOC for Service Organizations: Trust Services Criteria](#).

³² GovRAMP, [Rev. 5 Security Templates and Policies](#).

³³ FedRAMP, [FedRAMP Marketplace: Your Fast Track to FedRAMP Certified Cloud Solutions](#).

ESTABLISHING AND MAINTAINING A SECURITY PROGRAM

3



CHAPTER 3 ESTABLISHING AND MAINTAINING A SECURITY PROGRAM

PURPOSE

Chapter 3 focuses on establishing and maintaining an IIS security program through governance, clearly defined responsibilities, and risk-informed decision making.

These activities provide the foundation for implementing, overseeing, and continuously improving the operational security, continuity, incident response, and recovery capabilities described in Chapters 4, 5, and 6.



TARGETED PRIMARY AUDIENCE:

- Executive leadership
- IIS manager/IIS project manager

GOVERNANCE

Governance establishes the leadership, structures, and processes used to direct and oversee IIS security. It defines decision-making authority, accountability, oversight, and risk management expectations necessary to align security activities with legal, organizational, and operational requirements. Governance also helps ensure security is approached as an ongoing organizational responsibility (rather than just a technical activity) and provides the foundation for prioritizing, implementing, and sustaining security practices across IIS operations.

While services or systems may be provided by external vendors or partners, security governance remains the responsibility of the jurisdiction and IIS program. This accountability is essential to implementing safeguards that protect the confidentiality, integrity, and availability of IIS data and systems and support secure, resilient, and compliant operations.

Key components of governance

Key components of governance, as adapted from the NIST Cybersecurity Framework 2.0 “Govern” function,³⁴ are described below:

Leadership and strategic direction

Leadership should be knowledgeable of the specific security laws, policies, and organizational requirements applicable to the IIS. From these requirements, leadership establishes IIS organizational cybersecurity commitment, sets expectations, defines priorities, and reinforces that security is a core organizational responsibility. Through direction and oversight, leadership promotes a culture of security awareness, shared responsibility, and risk-informed decision making and remains accountable for ensuring security practices are implemented and sustained.

EXAMPLE

Establishing expectations for secure onboarding of provider organizations, role-based access to IIS data, and secure consumer access workflows for immunization records and related services.

Oversight and accountability

Governance establishes roles, responsibilities, authority, and oversight mechanisms that support consistent implementation and accountability, including oversight of security activities performed by third parties. Governance also helps prevent negligent behavior by demonstrating due care and due diligence in protecting systems and data.

EXAMPLE

Assigning responsibility for reviewing and approving provider access requests and ensuring onboarding policies are consistently applied.

³⁴ NIST, [Cybersecurity Framework](#).

Regulatory compliance

Governance should ensure that security practices remain aligned with applicable statutory, regulatory, contractual, and organizational requirements and that these obligations are translated into operational practices.

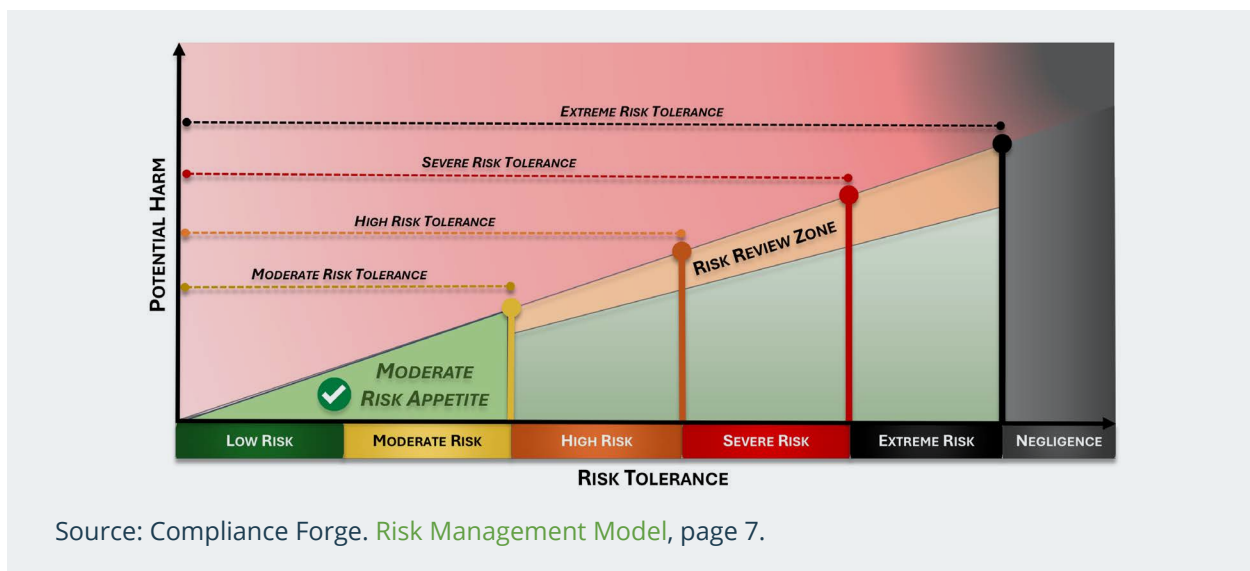
EXAMPLE

Ensuring provider onboarding and access to IIS data comply with HIPAA, state privacy laws, and data-sharing agreements and providing ongoing communication and user training about security requirements.

Risk management strategy and risk tolerance

Governance establishes the risk tolerance and establishes processes to support decision making to guide prioritization of security practices. Figure 2 below indicates the relationship between risk tolerance and potential harm. The SCF Risk Management Model provides additional useful information about identifying risk levels and mitigations.³⁵

Figure 2 | Relationship between risk tolerance and potential harm



³⁵ SCF, Risk Management Model, <https://content.securecontrolsframework.com/projects/cp-rmm.pdf>.

For example, although SCF has approximately 1,500 controls, organizations do not need to implement them all. This guidance was designed, as discussed in [Appendix B: Control Selection Methodology](#), to identify the most applicable and highest-value subset of controls for IIS programs to consider.

The SCF Integrated Controls Management Overview can inform development of a risk management strategy by helping organizations translate governance decisions, risk tolerance, and applicable requirements into an appropriate set of security controls.³⁶

Resource planning and sustainability

Governance supports decision making for priorities, staffing, funding, tools, and time needed to implement and sustain security capabilities.

EXAMPLE

Allocating staff and tools to support provider onboarding, access management, and ongoing monitoring of user activity.

Engaging Leadership on Security

To engage executive leadership on security, consider the following tips:

- Frame security in terms of risk, with a focus on impacts to operations, program continuity, legal and compliance exposure, and public trust rather than technical controls.
- Discuss topics as decisions that require their input and accountability. Present options, associated risks, and tradeoffs, and ask for direction.
- Use concrete scenarios to highlight risk based on prioritized threats.
- Leverage external expectations (e.g., regulatory requirements and funding expectations).

³⁶ SCF, Integrated Controls Management Overview, <https://content.complianceforge.com/Integrated-Controls-Management.pdf>.

Strong governance helps ensure security is approached as an ongoing organizational responsibility rather than solely as a technical activity. Governance decisions shape how security practices are prioritized, implemented, and sustained across IIS operations and provide the foundation for the practices described throughout the remainder of this guidance.

ROLES AND RESPONSIBILITIES

IIS security is a shared responsibility that depends on coordination among IIS programs, enterprise IT teams, security professionals, vendors, hosting providers, and other partners. Although specific responsibilities vary across environments, clearly defined roles, accountability, and communication are essential to effective security governance and operations.

The NIST Risk Management Framework (RMF) reinforces the importance of assigning and maintaining defined functions to support accountability throughout the system lifecycle. Table 2 maps IIS-relevant roles to RMF-aligned functions^{37,38} and summarizes representative responsibilities to support identification and discussion of security functions.



³⁷ NIST, [SP 800-37 Rev 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#).

³⁸ For additional information about the NIST Risk Management Framework roles, see [Appendix D](#), Roles and Responsibilities in the NIST RMF.

Table 2 | *IIS roles as they relate to security functions*

IIS ROLE	NIST RMF ROLE	PRIMARY RESPONSIBILITY	KEY FOCUS AREAS
Jurisdictional Executive Leadership	Authorizing Official (AO)/ Risk Executive	Establish direction and accountability for IIS security	Set risk tolerance; allocate resources; approve strategy; relay priority communications
Jurisdictional IIS Manager/ Project Manager	System Owner/ Business Owner	Coordinate security implementation and execution	Operationalize priorities; manage operations across staff, including ensuring staff training; coordinate with IIS partners (internal and/or external), monitor progress
IIS IT Implementers	Control Implementer	Implement and maintain safeguards	Operate systems; manage change; maintain evidence
Jurisdictional IT Security Professional	Security Officer	Provide security oversight and guidance	Define requirements; monitor security posture ³⁹ and emerging risks; advise on implementation priorities; escalate risks
IT Security Professional (or Independent Assessor) ⁴⁰	Control Assessor	Independently evaluate security effectiveness	Assess controls; validate evidence; report results
Jurisdictional Legal/ Compliance Officer	Supports Risk Executive/ Governance Functions	Interpret obligations and support governance decisions	Advise on requirements; support agreements; guide compliance
IIS Program Staff	System Users/ Operational Support	Support secure and effective operations	Follow procedures; handle data appropriately; identify issues
External Users	System Users	Use IIS capabilities appropriately	Follow access requirements; protect credentials; report issues

*Appendix C provides additional examples of security-related responsibilities that may be associated with these roles.

³⁹ An organization's security posture is a combination of risks, vulnerabilities, and controls.

⁴⁰ Where feasible, assessment activities should be performed independently of those responsible for implementing or operating controls, consistent with the control assessor function described in the RMF. Depending on the structure and resources of the IIS program, assessment activities may be performed through internal audit, by an agency security team, or by external reviewers.

Depending on the environment, functions may be performed by a single individual, distributed across multiple teams, or fulfilled through enterprise, shared-service, cloud, vendor, or other external arrangements. IIS programs should document and maintain a roles and responsibilities matrix (e.g., responsible, accountable, consulted, informed (RACI) matrix or shared responsibility model) to clarify decision-making authority, establish handoff points, and support continuity. IIS programs should clearly define which security activities remain under jurisdictional control and which are performed by external parties. Where feasible, organizations should maintain appropriate separation between control implementation and control assessment, to support independent evaluation of security practices.

Regardless of how activities are distributed or delegated, accountability for IIS security outcomes ultimately remains with the jurisdictional IIS program.

RISK MANAGEMENT FRAMEWORK

Purpose and role of risk management

Once governance expectations and responsibilities are established, IIS programs can apply a structured risk management process to evaluate conditions, make informed decisions, and guide security practices over time. The NIST RMF provides a seven-step process for managing risk: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor.⁴¹ Together, these activities support informed decision making, strengthen accountability, and enable ongoing evaluation and improvement of security practices. The framework is intended to provide a structured approach for understanding risk, prioritizing security activities, and evaluating whether safeguards are achieving their intended outcomes.

Use of a risk management framework helps organizations move from reactive decision making to more consistent, proactive, and risk-informed operations. Table 3 provides an illustrative comparison of how applying a structured risk management approach may influence security operations and decision making in practice.

Applying a structured risk management approach helps organizations move from reactive decision making to more consistent, proactive, and risk-informed operations.

⁴¹ NIST, SP 800-37 Rev 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

Table 3 | *Operating with and without a risk management framework*

OPERATING WITH A RISK MANAGEMENT FRAMEWORK	OPERATING WITHOUT A RISK MANAGEMENT FRAMEWORK
Security is proactive, anticipating and preventing incidents.	Security is reactive, responding after incidents occur or are detected.
Risk management is systematic, documented, and repeatable.	Risk management is inconsistent and ad hoc.
Compliance is integrated into routine operations.	Compliance is reactive and often last-minute.
Operations are conducted with confidence, supported by due care and due diligence.	Operations are characterized by uncertainty, inconsistent decision making, and difficulty demonstrating effective risk management.

Applying RMF concepts to IIS

IIS programs can apply the RMF concepts through four primary activities that support risk-informed decision making: (a) understanding obligations and the operating environment, (b) assessing risks and dependencies, (c) determining and implementing appropriate responses, and (d) continuously monitoring and improving security practices. These activities group related RMF concepts into practical areas of focus and are intended to help IIS programs apply the framework.

Understand obligations, assets, and the operating environment

Related NIST RMF phase: Prepare

Risk management begins with understanding the requirements and operating conditions that shape security expectations and decision making. IIS programs should identify and consider applicable legal, regulatory, contractual, and organizational requirements and maintain an understanding of the systems, data, relationships, and dependencies that influence risk.

This includes maintaining inventories of systems and components that collect, process, store, monitor, secure, recover, or exchange IIS data, as well as the data flows and dependencies that influence security responsibilities and implementation approaches. These obligations establish the context needed to evaluate and manage risk.

Assess risks and dependencies

Related NIST RMF phases: Categorize, Assess

Risk assessment focuses on identifying threats, vulnerabilities, and dependencies and evaluating their potential impacts on IIS operations, services, and information assets. Assessment should consider risks originating internally as well as those introduced through relationships with external entities. External entities may include health care providers, pharmacies, health systems, downstream data consumers, enterprise IT organizations, hosted service providers, cloud vendors, interface and exchange partners, and other parties involved in the collection, transmission, storage, use, or disclosure of IIS data. There are cases where some health care IT systems cannot be updated. These vulnerable systems can be mitigated by micro segmentation and firewall IP allow-listing thus restricting access to only trusted clients. See the [Cybersecurity Tips](#) companion document, tips 5, 7, 10, and 12.

Risk assessment activities should evaluate how these relationships affect confidentiality, integrity, availability, safety, operational resilience, and accountability across the IIS environment. An effective method to assess the risk of a system is to determine if that system contains data classified as a high-value target. For example, an IIS containing Social Security numbers has more value for extortion or identity theft than systems without these data present.

Determine and implement risk responses

Related NIST RMF phases: Select, Implement, Authorize

Risk decisions should be made within the organization's established risk tolerance. These boundaries guide prioritization, resource allocation, and decisions regarding when additional safeguards or corrective actions are warranted.

Based on assessment results, organizations should determine appropriate response strategies, including accepting, avoiding, mitigating, transferring, or sharing risk. The objective is not to eliminate all risk but to manage it at an acceptable level. Risk response decisions should guide implementation priorities, inform where safeguards should be applied, and determine whether residual risk remains acceptable.

EXAMPLE

An IIS may accept risk by onboarding a provider with identified security gaps and address that through compensating controls or avoid risk by delaying IIS access until required safeguards are in place.

*Monitor, evaluate, and improve***Related NIST RMF phase: Monitor**

Applying the RMF is not a one-time activity. Effective risk management requires ongoing monitoring, evaluation, and improvement as systems, threats, dependencies, technologies, and organizational priorities evolve.

Once safeguards are implemented, IIS programs should evaluate whether they are functioning as intended, monitor for changing conditions, and adjust activities as needed. The outputs of these activities should continue to inform implementation priorities, strengthen operational safeguards, and support continuity and resilience planning over time.

For a deeper discussion of the principles and steps involved in a risk management program and how they relate to security controls, refer to the SCF Risk Management Model.⁴²

CONTINUOUS IMPROVEMENT AND MATURITY

The Plan–Do–Check–Act (PDCA) model⁴³ and Capability Maturity Model (CMM)⁴⁴ are broadly applicable management frameworks that can be used to establish, assess, and continuously improve an IIS security risk management program. Together, these approaches help IIS programs determine what actions to take, improve how those actions are performed, and evaluate how effectively capabilities mature over time.

Plan-Do-Check-Act (PDCA) model

The PDCA model supports planning involved in identifying controls and building a road map (Plan), implementation of selected controls (Do), assessment and monitoring (Check), and continued refinement (Act).⁴⁵ SCF provides additional information detailing how the PDCA model maps to its risk management steps to help ensure security is an integrated area of focus.⁴⁶

⁴² SCF, SCR-RMM: Risk Management Model. <https://securecontrolsframework.com/free-content/risk-management-model-scr-rmm>.

⁴³ SCF, <https://content.securecontrolsframework.com/pdf/scf-plan-do-check-act.pdf>.

⁴⁴ SCF, <https://securecontrolsframework.com/free-content/capability-maturity-model-scr-cmm>.

⁴⁵ SCF, What is the Secure Controls Framework: PDCA Approach to Cybersecurity & Data Protection, <https://securecontrolsframework.com/start-here#pdca>.

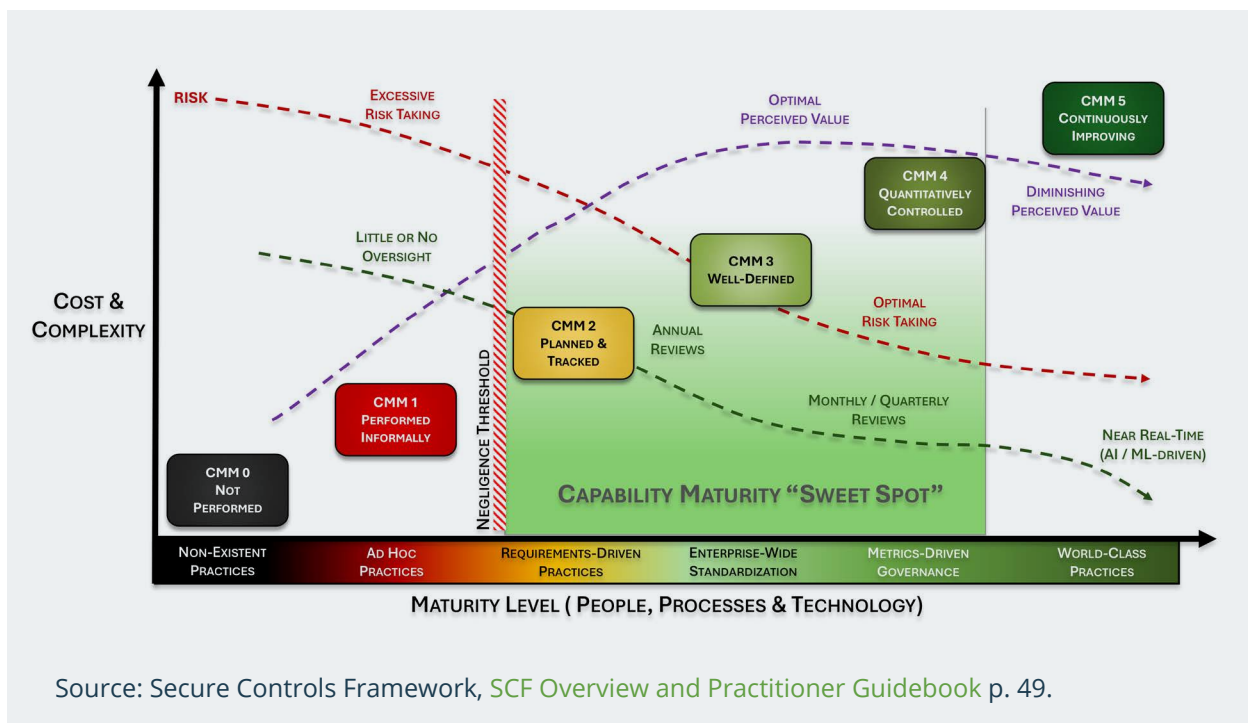
⁴⁶ SCF, Risk Management Model: Plan-Do-Check-Act (PDCA), <https://securecontrolsframework.com/free-content/risk-management-model-scr-rmm#pdca>

Assessing security maturity

The CMM can be applied as part of both the “Plan” and “Check” phases of the PDCA model, to help establish maturity targets and plan and assess progress toward those capabilities.⁴⁷ Capability maturity may be assessed by individual control, by security domain, or across all applicable controls. Overall maturity should reflect the lowest capability maturity achieved among applicable controls, as weaknesses in foundational controls constrain overall program maturity.

The SCF CMM describes progression through defined levels ranging from no security practices in place (Level 0) to optimized and continuously improving capabilities (Level 5).⁴⁸ Figure 3 maps the spectrum of maturity levels as related to overall cost and complexity in implementation, with Level 0 noted as “CMM 0” and so on.

Figure 3 | Defining a capability maturity target



⁴⁷ SCF, *SCR-CMM: Capability Maturity Model. Measure & Advance Your Cybersecurity Program*.

⁴⁸ Ibid.

As illustrated, Levels 0 and 1 represent insufficient maturity and indicate substantial opportunities to strengthen governance, consistency, and risk management practices. Level 2 reflects emerging and partially implemented practices, but the organization may still be exposed to elevated risk because processes are not yet consistently implemented, measured, or integrated into routine operations.

Level 3 reflects a well-established, security-focused program and serves as a practical baseline target for most IIS environments because practices are defined, implemented consistently, and integrated into routine operations. As mentioned elsewhere, this guidance cites only a subset of all possible SCF controls. Each IIS program should consider if it is optimal, for example, for them to achieve Level 2 on a broader set of controls or Level 3 across a smaller set of controls.

Levels 4 and 5 provide additional advantages through increased measurement, predictability, optimization, and adaptability. These capabilities may enable stronger performance management, more proactive risk reduction, improved resilience, and greater responsiveness to changing conditions. However, progression beyond Level 3 should be guided by organizational priorities, risk exposure, available resources, and expected value rather than assuming all capabilities require maximum maturity.

Subsequent chapters provide considerations and examples that may help IIS programs identify opportunities to strengthen capabilities and progress based on their individual goals and operating environments.

SUMMARY AND KEY ACTIONS

Establishing and maintaining an effective IIS security program requires coordinated leadership, defined accountability, and an ongoing process for understanding and managing risk.

Executive leadership, IIS managers/project managers, IT security professionals, program staff, and supporting partners each play distinct but interconnected roles in implementing and sustaining IIS security.

The RMF provides a structured program for managing risk, PDCA reinforces continuous improvement, and capability maturity concepts help organizations assess progress and define target outcomes. The following actions summarize the governance, risk management, and continuous improvement practices discussed throughout this chapter and provide a practical starting point for establishing and sustaining an IIS security program:

1. Establish governance and accountability by defining roles, responsibilities, and coordination mechanisms.
2. Understand requirements and the operating environment by identifying statutory, regulatory, and contractual obligations, systems, data, dependencies, and external relationships.
3. Assess risks and dependencies to determine priorities and understand potential impacts to IIS operations and data.
4. Develop a security road map to determine and implement risk responses consistent with organizational priorities and risk tolerance.
5. Monitor, evaluate, and improve security practices through ongoing assessment, continuous improvement, and measurement of progress.

Together, these activities provide a practical foundation for establishing and sustaining an effective IIS security program and support the operational security and resilience practices discussed in the chapters that follow.

SECURITY CONTROLS FOR IIS: CHAPTERS 4, 5, AND 6

Chapters 4, 5, and 6 present broadly applicable, priority security controls for IIS, organized into three domains:

- Operational security
- Artificial intelligence
- Business continuity, incident response, and recovery

Within each domain, controls are organized by topic. Each topic includes priority practices and practical considerations to describe what should be in place and how those practices can be applied within IIS environments. Priority practice tables identify the corresponding SCF Control ID and SCF Control Description. Where applicable, the tables also include related requirements from the IIS Requirements Traceability Matrix (RTM) to illustrate alignment between security controls and IIS requirements. For additional information on the SCF and how to interpret the tables, refer to [Appendix D](#).

The guidance presented throughout Chapters 4, 5, and 6 should be applied using a risk-based approach. The security controls described in this guide are broadly applicable to IIS; however, implementation priority and approaches should be based on each IIS program's legal and organizational requirements, operating environment, technical architecture, risks, and available resources. Controls should be implemented through documented policies, procedures, standards, technical safeguards, and defined workforce responsibilities and incorporated into routine operations as part of ongoing security management.

Implementation Resources: Refer to the companion *2026 Security Controls for IIS* workbook for a consolidated list of controls and reference information. Use the "Controls" worksheet to identify implementation priorities and the "Control Documentation Template" worksheet to document implementation status, ownership, evidence, dependencies, and planned improvements. Organizations seeking additional implementation guidance may also refer to the SCF, which provides supplemental information for each control, including control objectives, implementation guidance, example evidence, and capability maturity considerations.



OPERATIONAL SECURITY CONTROLS

4



CHAPTER 4 OPERATIONAL SECURITY CONTROLS

INTRODUCTION



TARGETED PRIMARY AUDIENCE:

- IIS IT implementer
- IIS manager/IIS project manager

Many of the practices discussed in this chapter are led by IIS IT implementers who configure and maintain systems and ensure that security controls function as intended in daily operations.

IIS managers/project managers also play a critical role in understanding risk, coordinating activities, and ensuring security supports operational and program objectives.

This chapter describes the operational security practices used to protect IIS networks, data, and services. These practices represent the day-to-day implementation of the governance and risk management activities described in Chapter 3 and support the continuity and resilience capabilities discussed in Chapter 6. Topics addressed include:

- Human resources security
- Physical and environmental security
- Third-party management
- System and technical security
- Secure development
- Web application security
- Configuration, change, and maintenance management
- Identity and access management
- Data privacy, protection, and handling
- Logging, monitoring, and detection

HUMAN RESOURCES SECURITY

Human resource management (also known as human resources) plays an important role in protecting IIS data, systems, and operations. IIS programs should ensure that staff, contractors, and vendors with access to IIS resources are appropriately vetted, trained, and accountable for safeguarding sensitive information, including protected health information (PHI), within an IIS. This includes establishing confidential and access agreements, providing role-based security training, and overseeing third-party access to IIS systems. Together, these practices reduce operational risk and promote the secure handling of IIS data.

Priority practices

Recommended human resources security controls for IIS are indicated in Table 4.



Table 4 | *Human resources security recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
HRS-02.1	Users With Elevated Privileges: Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive/regulated data is cleared and regularly trained to handle the information in question.	ManOrgs.Enroll
HRS-05.3	Technology Use Restrictions: Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	No corresponding RTM requirement
HRS-06	Access Agreements: Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access. See also: HRS-06.1, Confidentiality Agreements	Admin.SysConfig ManOrgs.Edit ManOrgs.Enroll
HRS-10	Third-Party Personnel: Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	No corresponding RTM requirement

Practical implementation considerations for IIS

Establish security processes

- Ensure that security responsibilities are addressed during employee and contractor onboarding and offboarding processes.

Implement and sustain training

- Provide or ensure role-specific training on IIS security, privacy, confidentiality, appropriate use of IIS data, and incident reporting. Training generally should occur annually or upon staff role changes or new hire onboarding.
- **COST-EFFECTIVE TIP** Provide role-based cybersecurity training to strengthen internal security capabilities over time. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 3.

Maintain ongoing oversight

- Coordinate with vendors and contractors to review and update permissions regularly (note the control cadence column in SCF).

PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and environmental security address how the facilities and infrastructure supporting IIS are protected from unauthorized access, damage, or disruption. Because IIS operations depend on continuous system availability to support clinical care and public health reporting, understanding where systems are hosted and how physical risks are managed is essential to maintaining continuity and trust.

Responsibility for physical security varies depending on the hosting model. Jurisdictions are typically responsible for securing on-premises environments, while cloud providers assume responsibility for the physical security of cloud infrastructure. Regardless of the hosting model, IIS programs remain responsible for understanding which operational and security responsibilities they retain, including oversight of data, user access, vendor management, and compliance requirements.

These physical controls apply to multiple IIS systems, including:

1. Primary IIS hosting environment, whether cloud-based hosting, on premises, or enterprise data centers
2. Backup data center(s) and archival media storage facilities
3. Office and remote work locations used by staff and contractors with privileged access to IIS systems or materials

Cloud services distribute responsibilities depending on the service model:

1. Infrastructure as a Service (IaaS): The IT service provider manages the infrastructure while the customer (such as an IIS program) manages the operating system applications and data.
2. Platform as a Service (PaaS): The IT service provider manages the infrastructure and operating system while the customer manages deployed applications and data.
3. Software as a Service (SaaS): The IT service provider manages the infrastructure and application, while the customer primarily manages users, data, and configuration.

Four newer cloud models are becoming increasingly more common:

1. Container-based
2. Serverless
3. Multi-cloud
4. Hybrid (on-premises and cloud)

Figure 4 illustrates an example of shared cloud security responsibilities across operating models.

Figure 4 | Sample cloud security responsibilities, Microsoft

Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Customer	Customer	Customer	Customer
	Network controls	Customer	Customer	Customer	Customer
	Operating system	Customer	Customer	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

■ Microsoft
 ■ Customer
 ■ Shared

Source: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Priority practices

Recommended physical and environmental security controls for IIS are indicated in Table 5.

Table 5 | *Physical and environmental security recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
PES-03	Physical Access Control: Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	No corresponding RTM requirement
PES-04	Physical Security of Offices, Rooms & Facilities: Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities. See also: PES-04.1, Working in Secure Areas	No corresponding RTM requirement
PES-06.3	Restrict Unescorted Access: Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	No corresponding RTM requirement

Practical implementation considerations for IIS

Define responsibilities and assess risk

- Define ownership of physical risk decisions across the program, jurisdictional IT, and vendors, especially for outages or disruptions tied to facility issues.
- If IIS is vendor or cloud hosted, verify that physical and environmental protections are in place for production, backup, and disaster recovery environments.
- Obtain and periodically review available vendor documentation to understand how physical and environmental risks are managed and verify controls continue to meet IIS security requirements. The review should occur at least annually, or upon (a) contract execution, (b) significant change to the vendor environment such as a new hosting platform, or (c) as determined by IIS staff.

Implement and maintain physical security

- Ensure that physical access controls extend beyond the server room to supporting infrastructure, network equipment, workstations, and administrative areas.
- Include non-production environments, such as testing, backup, and disaster recovery systems, in physical security assessments because they often contain IIS data and are frequently overlooked.
- When infrastructure is shared across programs, confirm how IIS priorities for system availability, facility access, and service restoration will be managed during disruptions.

THIRD-PARTY MANAGEMENT

Third-party management addresses how IIS programs manage relationships with external organizations that support IIS operations or access IIS data. IIS environments depend on a broad ecosystem of partners, including providers, vendors, and public health entities, making it essential to manage these relationships using a consistent, risk-informed approach that protects IIS data and systems. This includes one-way and bidirectional interfaces such as HL7 v2 immunization submissions and queries.

Priority practices

Recommended third-party management controls for IIS are indicated in Table 6.



Table 6 | *Third-party management recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
TPM-04	Third-Party Services: Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD). See also: TPM-04.4, Third-Party Processing, Storage and Service Locations	Nonfunc.Sec.Authentic Nonfunc.Sec.Intact Nonfunc.Sec.NonRepute Nonfunc.Sec.Private Nonfunc.Use Operate
TPM-05	Third-Party Contract Requirements: Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD). See also: TPM-05.5, Third-Party Scope Review	No corresponding RTM requirement
TPM-08	Review of Third-Party Services: Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	No corresponding RTM requirement

Practical implementation considerations for IIS

Establish expectations

- Establish clear policies for organizations accessing IIS data, including requirements for data use, access controls, and protection of shared information. End user agreements and organizational data use agreements can be used to implement third-party control enforcement.
- Define and communicate expectations for how IIS data will be protected and used after it leaves the IIS, through appropriate agreements such as data use agreements.
- For consumer-facing third-party solutions, clearly define responsibilities for identity management, access controls, data handling, and incident response.

Assess and manage risk

- Use standardized security questionnaires, attestations, prescriptive cybersecurity audits, or similar approaches to evaluate organizational readiness and risk.
- Recognize that trusted relationships often extend beyond authorized organizations to their vendors, service providers, and subcontractors, creating an extended web of trust that should be addressed through third-party risk management. Require authorized organizations to contractually flow down applicable security requirements to downstream partners and subcontractors that support IIS-related services or have access to IIS information or systems. Example: An IIS program may require direct data exchange partners to maintain a recognized cybersecurity certification or demonstrate compliance with defined security requirements and require equivalent requirements for supporting subcontractors. Flow-down provisions are typically incorporated into new or renewed contracts.
- Prioritize oversight for third parties with broad access, high data volume, bidirectional exchange, or access to sensitive data.
- Review partner access, agreements, and security expectations, particularly following legal, policy, organizational, or technical changes, at least semiannually (see TPM-08's cadence).

SYSTEM AND TECHNICAL SECURITY

System and technical security focuses on the protective capabilities built into the systems supporting IIS operations, including servers, networks, and endpoints. IIS environments rely on interconnected systems to receive, process, and exchange data across providers, public health partners, and external services. Ensuring these systems are securely designed, managed, deployed, and protected is essential to prevent unauthorized access, limit exposure, and support reliable operations.

Priority practices

Recommended system and technical security controls for IIS are indicated in Table 7.

Table 7 | System and technical security recommended controls

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
AST-02	Asset Inventories: Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: 1 Accurately reflects the current TAASD in use; 2 Identifies authorized software products, including business justification details; 3 Is at the level of granularity deemed necessary for tracking and reporting; 4 Includes organization-defined information deemed necessary to achieve effective property accountability; and 5 Is available for review and audit by designated organizational personnel.	No corresponding RTM requirement
AST-09	Secure Disposal, Destruction or Re-Use of Equipment: Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	No corresponding RTM requirement
EMB-03	Operational Technology (OT): Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	ManOrgs.Enroll
EMB-15	Safety Assessment: Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	No corresponding RTM requirement
EMB-19	Safe Operations: Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured.	No corresponding RTM requirement
END-04	Malicious Code Protection (Anti-Malware): Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	Nonfunc.Sec.Intact
END-08	Phishing & Spam Protection: Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	No corresponding RTM requirement
NET-01.1	Zero Trust Architecture (ZTA): Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	No corresponding RTM requirement

Continued on following page

Table 7 | System and technical security recommended controls (continued)

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
NET-02	Layered Network Defenses: Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	No corresponding RTM requirement
NET-03	Boundary Protection: Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	Nonfunc.Sec.Intact
NET-04	Data Flow Enforcement – Access Control Lists (ACLs): Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized. See also: NET-04.1, Deny Traffic by Default & Allow Traffic by Exception	No corresponding RTM requirement
NET-06	Network Segmentation (macrosegmentation): Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	No corresponding RTM requirement
NET-06.3	Sensitive / Regulated Data Enclave (Secure Zone): Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulated data enclaves (secure zones).	No corresponding RTM requirement
NET-10	Domain Name Service (DNS) Resolution: Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	No corresponding RTM requirement
NET-13	Electronic Messaging: Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	Interop.Onboarding Nonfunc.Rely.Avail Nonfunc.Sec.Private
NET-14	Remote Access: Mechanisms exist to define, control and review organization-approved, secure remote access methods. See also: NET-14.5, Work From Anywhere (WFA) - Telecommuting Security	No corresponding RTM requirement
NET-20	Email Content Protections: Mechanisms exist to implement an email filtering security service to detect malicious attachments in emails and prevent users from accessing them.	No corresponding RTM requirement
SEA-02	Alignment With Enterprise Architecture: Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	No corresponding RTM requirement

Continued on following page

Table 7 | System and technical security recommended controls (continued)

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
SEA-03	Defense-In-Depth (DiD) Architecture: Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	No corresponding RTM requirement
VPM-02	Vulnerability Remediation Process: Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	No corresponding RTM requirement
VPM-05	Software & Firmware Patching: Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	No corresponding RTM requirement
VPM-07	Penetration Testing: Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	No corresponding RTM requirement

Note: Ongoing patching and change management are addressed in the [Configuration, change, and maintenance management](#) section.

Practical implementation considerations for IIS

Document and govern the environment

- Maintain current documentation of IIS architecture, system dependencies, security boundaries, and data flows to understand potential operational and security impacts.
- Evaluate IIS technologies and connections to identify unnecessary exposure and retire outdated configurations, aiming for at least annual review. Where responsibilities are shared across program staff, jurisdictional IT, and vendors, define clear ownership for system-level protections, including network controls and endpoint security.

Implement and strengthen technical protections

- **COST-EFFECTIVE TIP** Restrict IIS data exchange to approved partners and authorized connection points. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 12.
- **COST-EFFECTIVE TIP** Work with enterprise IT and vendors to isolate IIS and PHI from general enterprise networks whenever feasible. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 5.
- **COST-EFFECTIVE TIP** Use layered security controls to reduce risks from vulnerabilities that may be exploited before patches are available. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 7.

Monitor and improve

- **COST-EFFECTIVE TIP** Regularly assess internet-facing IIS components and applications for vulnerabilities and coordinate remediation with enterprise IT, hosting providers, and vendors. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 4.
- **COST-EFFECTIVE TIP** Consider enterprise IT-approved no-cost or open-source tools to identify internal vulnerabilities and support remediation planning. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 11.

SECURE DEVELOPMENT

Many IIS programs rely on vendor-supported solutions and may not directly develop software. However, understanding secure software development practices helps IIS programs evaluate vendor security practices and support informed decision making. For IIS software vendors and jurisdictions that develop or customize their own IIS software, the following controls represent foundational practices that support “privacy by design” and “security by design.” The SCF also includes additional system development lifecycle guidance that organizations can use to supplement the practices described in this guidance.⁴⁹

The software development threat landscape continues to evolve, requiring IIS software developers to incorporate secure development practices and regularly evaluate emerging risks throughout the software lifecycle. As security frameworks evolve, software development organizations continuously update their practices to address emerging threats. These practices help reduce vulnerabilities, protect immunization data, support system availability, and maintain trust in IIS operations.

⁴⁹ See the Technology Development and Acquisition domain in SCF controls catalog.



Priority practices

Recommended controls for IIS vendors and for IIS jurisdictions that develop their own IIS software are indicated in Table 8.

Table 8 | *Secure development recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
TDA-01.1	Product Management: Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: 1 Improve functionality; 2 Enhance security and resiliency capabilities; 3 Correct security deficiencies; and 4 Conform with applicable statutory, regulatory and/or contractual obligations.	No corresponding RTM requirement
TDA-02.7	Security, Compliance & Resilience Representatives For Product Changes: Mechanisms exist to include appropriate security, compliance and resilience representatives in the product feature and/or functionality change control review process.	No corresponding RTM requirement
TDA-06	Secure Software Development Practices (SSDP): Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP). See also: TDA-06.5, Software Design Review	No corresponding RTM requirement
TDA-08	Separation of Development, Testing and Operational Environments: Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	No corresponding RTM requirement
TDA-17	Unsupported Technology Assets, Applications and/or Services (TAAS): Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: 1 Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and 2 Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	No corresponding RTM requirement
PRM-07	Secure Development Life Cycle (SDLC) Management: Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	No corresponding RTM requirement

Practical implementation considerations for IIS

Establish secure development expectations

- Include secure development expectations internally in procurement, contracting, and vendor oversight activities.
- When using vendors, understand how secure development practices are incorporated into implementer development processes and contracts.

Implement secure development practices

- Test software changes before deployment to verify security, privacy, and operational requirements continue to be met.
- Establish processes to address newly identified vulnerabilities, including applying patches, updating software components, and retiring unsupported technologies.
- Although this is an area of active investigation, early research⁵⁰ suggests that software developed with AI assistance may require additional security scrutiny. IIS developers should follow secure development practices, such as human and automated and autonomous cybersecurity code reviews with a special emphasis on AI-developed software.

Maintain ongoing oversight

- Semiannually, review vendor practices to ensure they continue to align with IIS security requirements (see the TPM-08 cadence).
- Maintain documentation to support maintenance and future modernization efforts.

WEB APPLICATION SECURITY

These controls are primarily intended for **IIS vendors and jurisdictions that develop, host, or customize their IIS web application**. IIS programs that rely on vendor-supported solutions should understand these practices and incorporate appropriate security expectations into vendor oversight. Web application security relies on multiple layers of protection across the network, application, and browsers to reduce the likelihood that a single vulnerability will result in a successful cyberattack. Together, these practices help protect immunization data, help support secure data exchange, and strengthen trust in IIS operations.

⁵⁰ ArXiv, Zhao, Song Wen, et al, "Is Vibe Coding Safe? Benchmarking Vulnerability of Agent-Generated Code in Real-World Tasks," v2, Feb. 16, 2026, <https://arxiv.org/abs/2512.03262>.

Priority practices

Recommended controls for IIS web applications are indicated in Table 9.

Table 9 | *Web application security recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
WEB-01.1	Unauthorized Code: Mechanisms exist to prevent unauthorized code from being present in a secure page as it is rendered in a client's browser.	No corresponding RTM requirement
WEB-02	Use of Demilitarized Zones (DMZ): Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	Nonfunc.Sec.Intact
WEB-04	Client-Facing Web Services: Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	ManUsers.AuthAccess Nonfunc.Sec.Intact Nonfunc.Sec.Private
WEB-07	Web Security Standard: Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.	Nonfunc.Use Operate
WEB-08	Web Application Framework: Mechanisms exist to ensure a robust Web Application Framework is used to aid in the development of secure web applications, including web services, web resources and web APIs.	No corresponding RTM requirement
WEB-09	Validation & Sanitization: Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.	Nonfunc.Use.UserErrors
WEB-10	Secure Web Traffic: Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).	Interop.Onboarding Nonfunc.Sec.Private Nonfunc.Use Operate
WEB-11	Output Encoding: Mechanisms exist to ensure output encoding is performed on all content produced by a web application to reduce the likelihood of cross-site scripting and other injection attacks.	Nonfunc.Use Operate
WEB-12	Web Browser Security: Mechanisms exist to ensure web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers to protect both the web application and its users.	Nonfunc.Use Operate



Practical implementation considerations for IIS

Establish security expectations

- Understand how web applications are exposed to external users and systems, including consumer access applications, APIs, and other internet-based services.
- For web-supported solutions, establish clear expectations for web application security practices and incorporate those expectations into procurement, contracting, and oversight activities.

Implement and validate security practices

- Ensure web application controls protect IIS data during transition, processing, and display.
- Test web application changes prior to implementation to help identify potential security, privacy, performance, and usability issues.
- Maintain visibility into third-party components, libraries, and services used by web applications as vulnerabilities that may introduce risk.
- Use a “supply chain firewall” to protect against upstream malicious software.⁵¹

CONFIGURATION, CHANGE, AND MAINTENANCE MANAGEMENT

Configuration, change, and maintenance management focuses on how IIS are configured, updated, and maintained over time. Effective configuration management provides the documentation and processes needed to consistently deploy, maintain, recover, and support IIS environments.

⁵¹ Multiple software supply chain firewalls are now available. Many are free and open source, such as: <https://github.com/DataDog/supply-chain-firewall>.

Priority practices

Recommended configuration, change, and maintenance management controls for IIS are indicated in Table 10.

Table 10 | Configuration, change, and maintenance recommended controls

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
CFG-02	Secure Baseline Configurations: Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	No corresponding RTM requirement
CFG-03	Least Functionality: ⁵² Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	Nonfunc.Sec.Intact
CFG-05	User-Installed Software: Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	No corresponding RTM requirement
CHG-02.1	Prohibition Of Changes: Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	No corresponding RTM requirement
MNT-02	Controlled Maintenance: Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	No corresponding RTM requirement
MNT-03	Timely Maintenance: Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	No corresponding RTM requirement

Practical implementation considerations for IIS

Establish configuration and change management processes

- Use formal configuration packages to ensure changes are controlled, documented, and repeatable. If formal configuration management packages are not yet in place, implement these techniques as soon as practical and improve their completeness over time. Validate configuration packages each time they are used by having different individuals apply the changes across environments, then update the documentation to address any gaps or unclear instructions that are identified.
- Establish a Change Control Board (CCB) appropriate to the organization's size to review, approve, and coordinate system changes. Document system dependencies. Assume that even minor changes can have broad downstream impact, particularly on interfaces and trading partners. Plan changes accordingly.

⁵² Least Functionality is an industry standard term indicating that a system is restricted to those operations necessary for proper operation to reduce that system's ability to be used to cause harm.

Implement and coordinate changes

- Communicate and coordinate configuration (system) changes across program, IT, data exchange partners, and vendors early. Misalignment is a common source of delays, data issues, and unintended disruptions.
- Balance the urgency of updates with operational stability. Some changes may need to be staged, sequenced, or implemented during defined windows to minimize impact.
- Test changes in pre-production environments that reflect real-world IIS conditions, including data exchange scenarios and partner interactions as much as is feasible. Simple tools like open-source interface engines, for example, can be used as test HL7 traffic simulators.
- **COST-EFFECTIVE TIP** Test security controls to identify weaknesses and vulnerabilities before changes are deployed to production and then frequently test post-production deployment. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 9.

Maintain and improve

- Track changes in a way that supports troubleshooting. Many IIS issues surface later and require visibility into what changed and when.
- Maintain awareness of dependencies across systems, interfaces, and external services. Changes in one area may introduce issues elsewhere if dependencies are not fully understood.

IDENTITY AND ACCESS MANAGEMENT

Identity and access management focuses on ensuring users and systems receive appropriate access to IIS data and functionality based on roles and responsibilities. Because IIS support a diverse group of users across organizations, effective identity proofing and access management are essential to support clinical care and public health activities while maintaining accountability and preventing unauthorized access.

Identity proofing, the process of verifying that a user is who they claim to be before granting access, should be aligned with the level of trust and risk associated with different user types.

Classes of Users

In IIS environments, classes of users help define the level of trust, identity assurance, and risk associated with different user types, including:

- **Administrative (privileged) IIS staff users:** Staff users **with** elevated IIS permissions to manage systems, access, or configurations—for example, those users with the ability to add a new organization and user(s) associated with that organization
- **Non-administrative IIS staff users:** IIS staff users **without** the ability to perform administrative functions—for example, an interface engineer who can view the interface engine status but can perform no other functions
- **External end users:** Providers and other authorized external users **without** the ability to perform administrative functions—for example, a clinical user who can view and edit a patient record but can perform no other functions
- **External administrative users:** External users **with** the ability to perform a limited set of administrative functions—for example, a designated administrator of a clinic who can manage the users at that clinic
- **Consumer users:** Individuals accessing their own and/or their family member's records, often through mobile or web-based applications and without organizational affiliation—for example, a parent seeking to determine their child's immunization status
- **System (non-human) users:** System processes that need accounts on other resources to perform useful and authorized activities—for example, the inbound HL7v2 interface engine, which will likely need an account on a database server to write the received messages

These user classes inform how role-based access controls (or attribute-based access controls) are granted and controlled based on trust and risk.

Priority practices

Recommended identity and access management controls for IIS are indicated in Table 11.

Table 11 | *Identity and access management recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
IAC-01.3	User & Service Account Inventories: Mechanisms exist to maintain a current list of authorized users and service accounts.	Admin.UserRoles ManUsers.Search
IAC-07	User Provisioning & De-Provisioning: Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights. See also: • IAC-07.1, Change of Roles & Duties • IAC-07.2, Termination of Employment	Admin.UserRoles
IAC-08	Role-Based Access Control (RBAC): Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	Admin.UserRoles Data.ConsumerAccess
IAC-09	Identifier Management (User Names): Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	No corresponding RTM requirement
IAC-10	Authenticator Management: Mechanisms exist to: 1 Securely manage authenticators for users and devices; and 2 Ensure the strength of authentication is appropriate to the classification of the data being accessed. See also: IAC-10.5, Protection of Authenticators IAC-10.6, No Embedded Unencrypted Static Authenticators IAC-10.8, Default Authenticators	ManUsers.AuthAccess
IAC-15	Account Management: Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts. See also: • IAC-15.3, Disable Inactive Accounts • IAC-15.5, Restrictions on Shared Groups / Accounts • IAC-15.6, Account Disabling for High Risk Individuals • IAC-15.7, System Account Reviews	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search

Continued on following page

Table 11 | Identity and access management recommended controls (continued)

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
IAC-16	Privileged Account Management (PAM): Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). See also: IAC-16.1, Privileged Account Inventories	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search
IAC-17	Periodic Review of Account Privileges: Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search
IAC-18	User Responsibilities for Account Management: Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search
IAC-19	Credential Sharing: Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	No corresponding RTM requirement
IAC-20	Access Enforcement: Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search

Continued on following page

Table 11 | *Identity and access management recommended controls (continued)*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
IAC-20.1	Access To Sensitive / Regulated Data: Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search
IAC-20.2	Database Access: Mechanisms exist to restrict access to databases containing sensitive/regulated data to only necessary Technology Assets, Applications and/or Services (TAAS) or those individuals whose job requires such access.	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search
IAC-21	Least Privilege: Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. See also: IAC-21.3, Management Approval For Privileged Accounts	ManOrgs.Edit ManOrgs.Enroll ManOrgs.Outreach ManOrgs.Search ManUsers.AuthAccess ManUsers.Edit ManUsers.Password ManUsers.Search
IAC-25	Session Termination: Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	Nonfunc.Sec.Intact
IAC-28	Identity Proofing (Identity Verification): Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions. See also: IAC-28.1, Management Approval For New or Changed Accounts	No corresponding RTM requirement

Practical implementation considerations for IIS

Establish identity and access processes

- Align identity proofing with user class and risk. Balance the level of assurance with effort, cost, and usability. Consumer users may require direct identity proofing aligned with NIST SP 800-63 identity assurance levels, while organizational users may rely on affiliation with trusted entities and delegated verification defined in IIS policies or agreements. Note: Most health care broad consensus bodies, such as TECCA⁵³ have selected NIST 800-63 Identity Assurance Level 2 (IAL2) and Authenticator Assurance Level 2 (AAL2) as the minimum criteria for consumer access to health care information technology services and data.
- Recognize that identity proofing depends on the quality of the initial identity verification. If the initial verification, such as an in-person inspection of government-issued identification, results in an inaccurate identity binding (for example, due to a misspelled name or attempted medical identity theft), the identity proofing process may need to be repeated or improved.
- Expect frequent turnover in IIS user populations, especially among providers, pharmacies, and schools. Design onboarding and offboarding processes that can keep pace with these changes.
- Be intentional about delegated administration. Without oversight, local administrators may introduce inconsistencies in how access is granted and managed across organizations.

Implement access controls

- Plan for users who operate across multiple roles or organizations (such as a state IIS coordinating with a city or county IIS). These scenarios often require additional consideration to ensure access remains appropriate.
- Define session timeout policies based on user class, access context, and risk. Shorter timeouts may be appropriate for shared devices, mobile access, and privileged users, consistent with NIST session management guidance.
- **COST-EFFECTIVE TIP** Use approved and monitored access controls, such as bastion hosts, to limit administrative access to sensitive IIS environments. For additional guidance, please see the *Cybersecurity Tips* companion document, Tip 6.

⁵³ See sections 4.2 and 4.3 in <https://rce.sequoiaproject.org/wp-content/uploads/2024/01/Draft-SOP-IAS-Demographic-Matched-508-Compliant.pdf>.



Maintain ongoing oversight

- Establish and document a period of inactivity threshold for disabling inactive user accounts. The threshold should balance security risk with operational considerations, including administrative overhead and typical user access patterns.
- Review user roles and permissions on a quarterly basis to remove unnecessary access (consistent with NIST password and credentials management, access control, and account management practices). (See also the IAC-15 cadence.)

DATA PRIVACY, PROTECTION, AND HANDLING

Data privacy, protection, and handling focus on safeguarding IIS data throughout its lifecycle while ensuring information is collected, used, shared, stored, transmitted, and protected in accordance with applicable laws, policies, agreements, and organizational expectations. While cybersecurity generally focuses on protecting systems and data from unauthorized access, data privacy focuses on appropriate use and disclosure of personal information and protection of individual rights.

IIS data support patient care, Clinical Decision Support, vaccine management, and public health activities and are routinely exchanged with authorized health care providers, pharmacies, health systems, public health agencies, and other approved partners. Protecting this information requires administrative, technical, and operational safeguards that ensure data are accessed, used, shared, retained, and disposed of only as authorized and in accordance with applicable laws, regulations, data-sharing agreements, and organizational policies.

Priority practices

Recommended data privacy, protection, and handling security controls for IIS are indicated in Table 12.

Table 12 | *Data privacy, protection, and handling recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
PRI-07	Information Sharing With Third Parties: Mechanisms exist to disclose Personal Data (PD) ⁵⁴ to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject. See also: PRI-07.1, Data Privacy Requirements for Contractors & Service Providers	ManPtRecord.Consent
CRY-03	Transmission Confidentiality: Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	Nonfunc.Sec.Private
CRY-04	Transmission Integrity: Cryptographic mechanisms exist to protect the integrity of data being transmitted.	Nonfunc.Sec.Private
CRY-05	Encrypting Data At Rest: Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	Nonfunc.Sec.Private
CRY-09	Cryptographic Key Management: Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	Nonfunc.Sec.Private
DCH-01.1	Data Stewardship: Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	No corresponding RTM requirement
DCH-02	Data & Asset Classification: Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	No corresponding RTM requirement
DCH-03.1	Disclosure of Information: Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	Admin.SysConfig Admin.UserRoles Eval.ReminderRecall ManPtRecord.Consent
DCH-08	Physical Media Disposal: Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	No corresponding RTM requirement

Continued on following page

⁵⁴ SCF defines PD, or personal data, in Cybersecurity & Data Privacy by Design (C|P) Principles currently at <https://securecontrolsframework.com/free-content/data-privacy-management-principles-dpmp>.

Table 12 | *Data privacy, protection, and handling recommended controls (continued)*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
DCH-09	System Media Sanitization: Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	No corresponding RTM requirement
DCH-10.1	Limitations on Use: Mechanisms exist to restrict the use and distribution of sensitive/regulated data.	Admin.SysConfig Admin.UserRoles Eval.ReminderRecall ManPtRecord.Consent
DCH-12	Removable Media Security: Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	No corresponding RTM requirement
DCH-13.3	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS): Mechanisms exist to ensure that the requirements for the protection of sensitive/regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.	No corresponding RTM requirement
DCH-15	Publicly Accessible Content: Mechanisms exist to control publicly-accessible content.	Admin.SysConfig Admin.UserRoles Eval.ReminderRecall ManPtRecord.Consent Nonfunc.Use.Operate
DCH-21	Information Disposal: Mechanisms exist to securely dispose of, destroy or erase information.	No corresponding RTM requirement
DCH-24	Information Location: Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	No corresponding RTM requirement

Practical implementation considerations for IIS

Establish privacy and data governance

- Align privacy practices with applicable jurisdictional laws and IIS policies.
- Review data-sharing agreements periodically.
- Use data minimization and minimal data set (MDS) principles to limit disclosure of IIS data to the minimum necessary to accomplish the intended purpose, consistent with applicable legal, regulatory, and operational requirements. Consider the threats associated with each disclosed data element.⁵⁵ Share only the data necessary for the intended purpose, particularly in outbound interfaces and reports.
- Implement training to ensure staff understand IIS policies.
- Use of HIPAA-compliant secured (encrypted) email, such as those based on the DirectTrust open standard, when transmitting PHI or other sensitive information.

Implement data protection practices

- Map data flows over time, not just at a point in time. Interfaces, partners, and use cases evolve, and documentation often lags reality.
- Apply appropriate controls to data exports, downstream systems, backups, and other environments outside of the IIS, recognizing that external handling practices may vary.
- Consider how data integrity is maintained across systems. Errors or inconsistencies introduced during exchange or processing can impact clinical care and public health decision making.
- Pay close attention to high-volume and high-distribution workflows, such as reminder/recall and cross-jurisdiction exchange, HEDIS measure calculations, and data cleansing and address look-up services, where data exposure increases.
- Recognize that consumer access increases the likelihood that IIS data will be viewed, downloaded, or shared outside traditional workflows, requiring additional consideration of how data may be used once it leaves the system.
- **COST-EFFECTIVE TIP** Prioritize security controls for systems that store, process, transmit, or back up PHI and other sensitive IIS data. For additional guidance, see the [Cybersecurity Tips](#) companion document, Tip 10.

⁵⁵ Integrating the Health Enterprise, IHE IT Infrastructure Handbook – De-Identification, June 6, 2014, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Handbook_De-Identification_Rev1.1_2014-06-06.pdf section 2.6.

LOGGING, MONITORING, AND DETECTION

Logging, monitoring, and detection focus on collecting and analyzing system and user activity to identify potential security issues. Examples of unusual activity may include abnormal interface traffic patterns, repeated failed login attempts, or unusual account activity. These practices provide visibility into IIS operations and enable timely detection of unusual, unauthorized, or suspicious activity.

Priority practices

Recommended logging, monitoring, and detection security controls for IIS are indicated in Table 13.

Table 13 | *Logging, monitoring, and detection recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
MON-01.7	File Integrity Monitoring (FIM): Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	No corresponding RTM requirement
MON-01.8	Security Event Monitoring: Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	No corresponding RTM requirement
MON-02	Centralized Collection of Security Event Logs: Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	No corresponding RTM requirement
MON-03	Content of Event Logs: Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: 1 Establish what type of event occurred; 2 When (date and time) the event occurred; 3 Where the event occurred; 4 The source of the event; 5 The outcome (success or failure) of the event; and 6 The identity of any user/subject associated with the event. See also: MON-03.2, Audit Trails	Nonfunc.Maintain.Analyze Nonfunc.Rely.Recover Nonfunc.Sec.Authentic Nonfunc.Sec.Intact Nonfunc.Sec.NonRepute
MON-07	Time Stamps: Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	No corresponding RTM requirement
MON-08	Protection of Event Logs: Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	Nonfunc.Maintain.Analyze

Continued on following page

Table 13 | *Logging, monitoring, and detection recommended controls (continued)*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
MON-10	Event Log Retention: Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	Nonfunc.Sec.NonRepute
MON-16	Anomalous Behavior: Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	No corresponding RTM requirement

Practical implementation considerations for IIS

Define monitoring responsibilities

- Assign clear responsibility for reviewing and acting on log data. Without defined ownership, important signals may be missed.
- Each IIS program should perform an analysis to determine its specific retention requirements for control MON-10. A period of five years is a reasonable minimum retention period for cybersecurity purposes.⁵⁶ Accounting of Disclosures, HIPAA, state regulations, and other legislation may specify longer retention periods, especially for ePHI transactions.

Implement monitoring and detection

- Focus logging and monitoring on high-value activities, including user access, data exchange, and system changes.
- Align monitoring with how the IIS operates day to day so that unusual activity can realistically be recognized and investigated.
- Correlate logs across IIS components to support security investigations. Include consumer-facing activities, such as self-service access and account recovery, when defining monitoring and detection strategies.
- **COST-EFFECTIVE TIP** Incorporate trusted threat intelligence in IIS security planning to improve awareness of emerging risks and vulnerabilities. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 1.
- **COST-EFFECTIVE TIP** Partner with enterprise IT to evaluate detection methods (e.g., decoy systems or “honeypots”) that can identify unauthorized access or scanning activity. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 8.

⁵⁶ The “long-tail” dwell time for cybersecurity attacks is reported to have been 2085 days (about 5 years 7 months). Source Mandiant FireEye MTrends 2018 report, <https://web.archive.org/web/20260714191218/https://static.carahsoft.com/concrete/files/1015/2779/3571/M-Trends-2018-Report.pdf>.

SUMMARY

The practices described in this chapter provide the operational foundation for securing IIS environments. Collectively, they support the implementation and management of administrative, technical, and physical safeguards including system and technical security, identity and access management, data protection, third-party risk management, configuration and change management, and continuous monitoring. Together, these practices help protect IIS systems and data, reduce security risk, and support the secure, reliable operation of IIS services.

**SPECIAL TOPIC:
ARTIFICIAL
INTELLIGENCE
CONTROLS**

5



CHAPTER 5 SPECIAL TOPIC: ARTIFICIAL INTELLIGENCE CONTROLS

INTRODUCTION



TARGETED PRIMARY AUDIENCE:

- IIS manager/IIS project manager
- IIS IT security professional

Artificial Intelligence (AI) is increasingly being used in technologies that support public health programs. While AI creates new opportunities for IIS programs, it also introduces cybersecurity, privacy, and operational risks that must be understood and managed.

This chapter addresses three areas: AI in external-facing applications, use of AI by threat actors, and use of AI to support cybersecurity operations and defenses.

AI FOR PUBLIC-FACING APPLICATIONS

AI governance relies on transparent, risk-based policies and procedures that promote reliable, secure, and explainable AI while protecting IIS data privacy. AI protections should be appropriate for the risks associated with each implementation.

AI technologies should be tested and periodically evaluated to ensure that they continue to operate safely, securely, and as intended. This process includes evaluating trustworthy behavior. To maintain security, strict mechanisms should be employed by IIS to protect source data integrity against accidental contamination or malicious corruption such as data poisoning.

AI systems should safely handle situations outside their intended capabilities by directing users to a human reviewer when appropriate. IIS programs should establish criteria and responsibilities for updating, replacing, disabling, or retiring AI technologies that no longer perform as intended or no longer meet business, privacy, or security requirements.

EXAMPLE

An IIS implements a chatbot to assist with immunization record requests. The IIS program establishes procedures to review chatbot responses, protect sensitive information, and ensure users can escalate questions to a human representative when needed.

EXAMPLE

An IIS help desk solution uses AI to provide initial technical support. Procedures are established to ensure the AI responds to requests only within its intended capabilities.

AI-RELATED THREATS

Attackers are increasingly using AI to improve the scale, speed, and sophistication of cyberattacks. IIS programs should understand how attackers may use AI to target staff, systems, and applications.

1. Targeting people (social engineering and manipulation)—Attackers use AI to create convincing phishing emails, voice impersonations, and deepfake videos. For example, an attacker may impersonate an IIS manager or vendor representative to request sensitive information or system access.
2. Targeting infrastructure (networks and systems)—AI enables attackers to automate vulnerability discovery, adapt to attacks, and evade detection more effectively than traditional methods. IIS programs should maintain layered security controls to reduce these risks.
3. Targeting applications (software and web services)—AI tools are accelerating the discovery and exploitation of software vulnerabilities, reducing the time between identifying a weakness and attempting to exploit it. IIS programs should prioritize timely patching, secure system design, and layered security controls to reduce risk.

AI FOR CYBERSECURITY OPERATIONS AND DEFENSE

AI-enabled cybersecurity tools can help identify unusual activities, prioritize security alerts, detect potential threats, and support incident response activities. These capabilities should complement, not replace, foundational cybersecurity practices. Network segmentation, access management, vulnerability management, and incident response planning remain critical components of a comprehensive cybersecurity program.

Priority practices

Recommended artificial-intelligence related controls for IIS are indicated in Table 14.

Table 14 | Artificial intelligence recommended controls

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
AAT-01	Artificial Intelligence (AI) & Autonomous Technologies Governance: Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively. See also: AAT-01.2, Trustworthy AI & Autonomous Technologies	No corresponding RTM requirement
AAT-02.3	Adequate Protections For AI & Autonomous Technologies: Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) include reasonable security, compliance and resilience protections that are commensurate with assessed risks and threats.	No corresponding RTM requirement
AAT-10	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV): Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT. See also: AAT-10.1, AI TEVV Trustworthiness Assessment AAT-10.4, AI TEVV Safety Demonstration	No corresponding RTM requirement
AAT-12.2	Data Source Integrity: Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	No corresponding RTM requirement

Continued on following page

Table 14 | *Artificial intelligence recommended controls (continued)*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
AAT-15.2	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies: Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	No corresponding RTM requirement
AAT-20	AI & Autonomous Technologies Development Practices: Measures exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed and developed to: 1 Achieve an appropriate level of accuracy, robustness and cybersecurity; 2 Perform consistently in those respects throughout the AAT system's lifecycle; and 3 Be effectively overseen by competent individuals.	No corresponding RTM requirement
BCD-16	AI & Autonomous Technologies Incidents: Mechanisms exist to handle failures or incidents with Artificial Intelligence (AI) and Autonomous Technologies (AAT) deemed to be high-risk.	Nonfunc.Rely. Faults

Practical implementation considerations for IIS

Establish governance and prepare for implementation

- Develop an AI usage policy that defines appropriate, role-based use of AI for staff and contractors.
- Train staff on AI technologies, including benefits, limitations, and cybersecurity risks.
- Evaluate AI technologies before implementation and ensure critical IIS functions can continue if AI systems become unavailable or produce unexpected results.
- Refer to SCF for additional AI-focused cybersecurity controls that can inform IIS considering AI deployments.

Implement and operate AI capabilities

- Build experience by piloting use of AI for selected low-risk internal IIS functions.
- Ensure IIS staff are aware of AI-enabled phishing, deep fake communications, and other emerging threats that may target public health organizations.

Maintain and improve AI capabilities

- **COST-EFFECTIVE TIP** Implement safeguards for AI-enabled solutions to reduce the risk of misuse, data exposure, and unintended outcomes. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 14.

SUMMARY

Artificial intelligence is a cross-cutting topic that influences multiple aspects of IIS security and operations. AI may be implemented by an IIS program, vendors, embedded technologies, or malicious actors. This section highlights selected SCF controls and practical considerations to support risk-informed evaluation, adoption, governance, and use of AI within IIS environments.

**BUSINESS CONTINUITY,
INCIDENT RESPONSE,
AND RECOVERY
CONTROLS**

6



CHAPTER 6 BUSINESS CONTINUITY, INCIDENT RESPONSE, AND RECOVERY CONTROLS

INTRODUCTION



TARGETED PRIMARY AUDIENCE:

- IIS manager/IIS project manager
- IIS IT security professional

This chapter focuses on preparing for, responding to, and recovering from operational disruptions and cybersecurity incidents. Even with strong operational controls in place, disruptions and security events are inevitable.

These practices help IIS programs maintain critical functions, restore services, and strengthen resilience over time. Topics addressed include:

- Business continuity planning
- Cybersecurity incident response
- Disaster recovery
- Post-incident review

Note: Additional IIS-specific guidance and examples of business continuity planning practices are available in the [*Business Continuity Planning for Immunization Information System Programs*](#) guide.

BUSINESS CONTINUITY PLANNING

Business continuity planning focuses on maintaining critical IIS operations during disruptions by defining how essential services continue when systems, personnel, infrastructure, vendors, or external dependencies are degraded or unavailable. While incident response and disaster recovery address managing and restoring systems after an event, business continuity planning defines how operations are sustained.

Continuity planning should prioritize essential business functions before identifying the people, processes, technology, and external resources needed to support those functions. Business continuity and disaster recovery should be developed as complementary components of an overall strategy for resilient IIS operations.

Priority practices

Recommended business continuity planning controls for IIS are indicated in Table 15.

Table 15 | *Business continuity planning recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
BCD-01.7	Business Continuity & Disaster Recovery (BC/DR) Plans: Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	No corresponding RTM requirement
BCD-02	Identify Critical Assets: Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	No corresponding RTM requirement
BCD-08	Alternate Storage Site: Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	Nonfunc.Rely.Recover
BCD-09	Alternate Processing Site: Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	Nonfunc.Rely.Recover Nonfunc.Sec.Intact Nonfunc.Sec.Private

Continued on following page

Table 15 | *Business continuity planning recommended controls (continued)*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
BCD-11	Data Backups: Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). See also: • BCD-11.1, Testing for Reliability & Integrity • BCD-11.4, Cryptographic Protection • BCD-11.9, Backup Access • BCD-11.10, Backup Modification and/or Destruction	Nonfunc.Rely.Recover
	Special note: BCD-16, related to AI, is included in the AI special topics section.	

Practical implementation considerations for IIS

Establish and document continuity processes

- Identify essential IIS business functions and work with IIS community members to establish acceptable downtime and data loss thresholds (recovery point objective and recovery time objective (RPO/RTO)) based on operational needs.
- Define continuity approaches for operating during disruptions, including degraded operating modes, manual processes, alternate workflows, contingency procedures, and queue-based recovery approaches where appropriate.
- Document dependencies across infrastructure, vendors, interface services, cloud, and enterprise environments to ensure recovery expectations and responsibilities are understood.
- Establish communication procedures for outages, including notification expectations, workaround instructions, status updates, guidance for providers and users.

Coordinate with partners

- Contact your jurisdiction's department of emergency management and request IIS participation in annual disaster planning activities, including jurisdiction-wide tabletop exercises (TTEs). Participating in these exercises is a useful, cost-effective way for IIS programs to validate and improve their business continuity plan.
- Ask all IIS data exchange partners to queue inbound messages, in particular submissions (e.g., VXUs), until application-level "ACK" messages are received to minimize data loss during planned or unplanned outages. Coordinating with data exchange partners on message queuing can be manual, or it could be automated by having the sending system use an "exponential backoff" retry pattern where the retry interval increases between attempts.

Maintain and validate the plan

- Business continuity plans should be updated at least annually or upon a significant system change, such as an IIS vendor change.
- Periodically validate continuity plans throughout tabletop exercises, workflow simulations, or other realistic scenarios that reflect IIS operations and align with broader organizational continuity efforts.

INCIDENT RESPONSE

Incident response includes the processes and procedures used to identify, analyze, contain, and respond to cybersecurity incidents in a timely and effective manner.

Priority practices

Recommended incident response controls for IIS are indicated in Table 16.

Table 16 | *Incident response recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
IRO-02	Incident Handling: Mechanisms exist to cover: 1 Preparation; 2 Automated event detection or manual incident report intake; 3 Analysis; 4 Containment; 5 Eradication; and 6 Recovery	No corresponding RTM requirement
IRO-04	Incident Response Plan (IRP): Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders. ⁵⁷	No corresponding RTM requirement
IRO-06	Incident Response Testing: Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	No corresponding RTM requirement

⁵⁷ In this context “Stakeholder” is defined as “IIS Community Member.”

Practical implementation considerations for IIS

Prepare and document response processes

- Define what constitutes an incident in the IIS environment (e.g., unauthorized access, data exposure, credential compromise, interface disruption, system unavailability).
- Align IIS incident response procedures with enterprise, legal, and vendor response processes while clearly defining IIS-specific responsibilities.
- Translate enterprise response activities into IIS operational actions as appropriate, including disabling user accounts, suspending interface access, limiting system functionality, or implementing other containment measures.
- Establish documented procedures and decision-making authority for escalation, containment, service restoration, and reactivation of users, credentials, interfaces, and system functions.
- Maintain communication procedures identifying who must be informed, when communications occur, and what information should be provided to leadership, providers, partners, and other IIS community members.
- Develop and update, on a quarterly basis (see BCD-01.7), supporting resources such as contact lists, checklists, playbooks, and restoration procedures to support consistent execution during disruptions, including after-hours or staff absences.

Strengthen and improve capabilities

- Use incidents as opportunities to strengthen controls, refine operational procedures, improve coordination, and increase future readiness.
- **COST-EFFECTIVE TIP** Participate in information-sharing networks to stay informed of emerging threats and support timely response activities. Communicate those emerging threats to IIS staff and enterprise IT. For additional guidance, please see the [Cybersecurity Tips](#) companion document, Tip 2.

DISASTER RECOVERY

Disaster recovery focuses on restoring IIS systems, data, and supporting services following a disruption to return operations to a secure and reliable state.

Priority practices

Recommended disaster recovery controls for IIS are indicated in Table 17. Please also see related controls under [Business Continuity Planning](#).

Table 17 | *Disaster recovery recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
BCD-07	Alternative Security Measures: Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.	No corresponding RTM requirement
BCD-11	Data Backups: Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	Nonfunc.Rely.Recover
BCD-12	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution: Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure. See also: BCD-12.1, Transaction Recovery	Nonfunc.Rely.Faults Nonfunc.Rely.Recover
	Special note: BCD-16, related to AI, is included in the AI special topics section.	

Practical implementation considerations for IIS

Prepare recovery capabilities

- Prioritize recovery based on essential IIS business functions, such as vaccine ordering, data exchange, or reporting.
- Verify backups are complete, current, and accessible and regularly validate restoration procedures using realistic IIS recovery scenarios.
- Account for dependencies across databases, interface engines, external services, vendors, hosting providers, and jurisdictional IT organizations throughout recovery activities.

Recover and validate

- Communicate recovery status and expected restoration timeline with users and partners throughout the recovery process.
- Perform annual live disaster recovery (DR) failover and restoration exercises to validate recovery capabilities.
- Test backups quarterly by restoring randomly sampled files to verify backup integrity (see BCD-11).

POST-INCIDENT REVIEW AND IMPROVEMENT

Post-incident review focuses on learning from security events to strengthen IIS processes, controls, and organizational resilience.

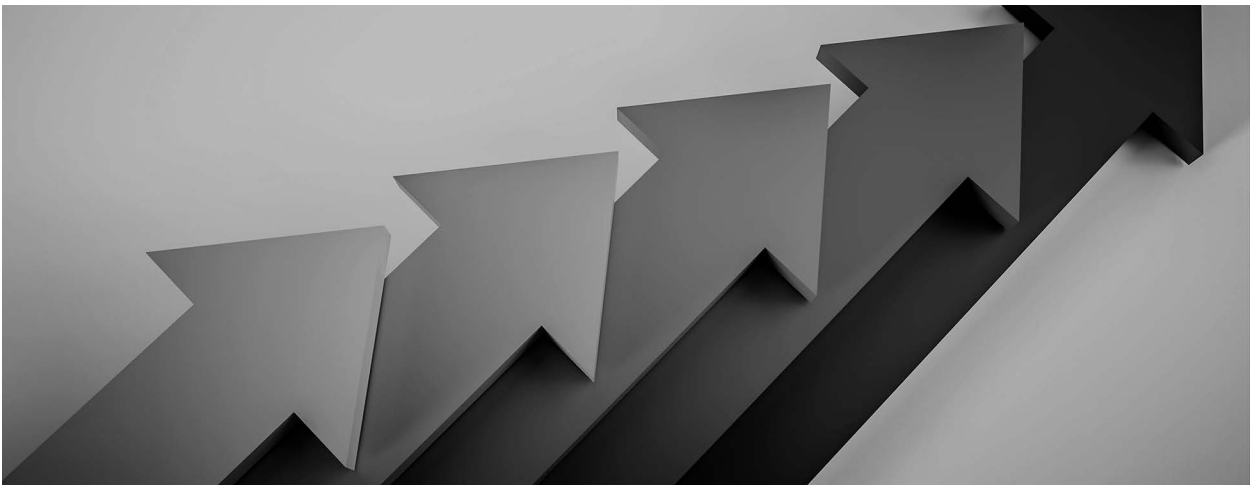
Priority practices

Recommended post-incident review and improvement controls for IIS are indicated in Table 18. Please also see the controls under [Business Continuity Planning](#) and [Disaster Recovery](#).

Table 18 | *Post-incident review recommended controls*

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
BCD-05	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned: Mechanisms exist to conduct a Root Cause Analysis (RCA) and “lessons learned” activity every time the contingency plan is activated.	No corresponding RTM requirement
IRO-10	Incident Stakeholder Reporting: Mechanisms exist to timely-report incidents to applicable: 1 Internal stakeholders; 2 Affected clients & third-parties; and 3 Regulatory authorities.⁵⁸	No corresponding RTM requirement

⁵⁸ In this context, the term “stakeholder” is defined as “IIS community member.”



Practical implementation considerations for IIS

Conduct the review

- Conduct post-incident review following actual incidents and tabletop exercises.
- Include technical staff and IIS program leadership in reviews to identify root causes, contributing factors, operational impacts, and coordination challenges.
- Track corrective actions to completion and share lessons learned with appropriate IIS teams, providers, vendors, and public health partners to reduce recurring issues.

Implement continuous improvement

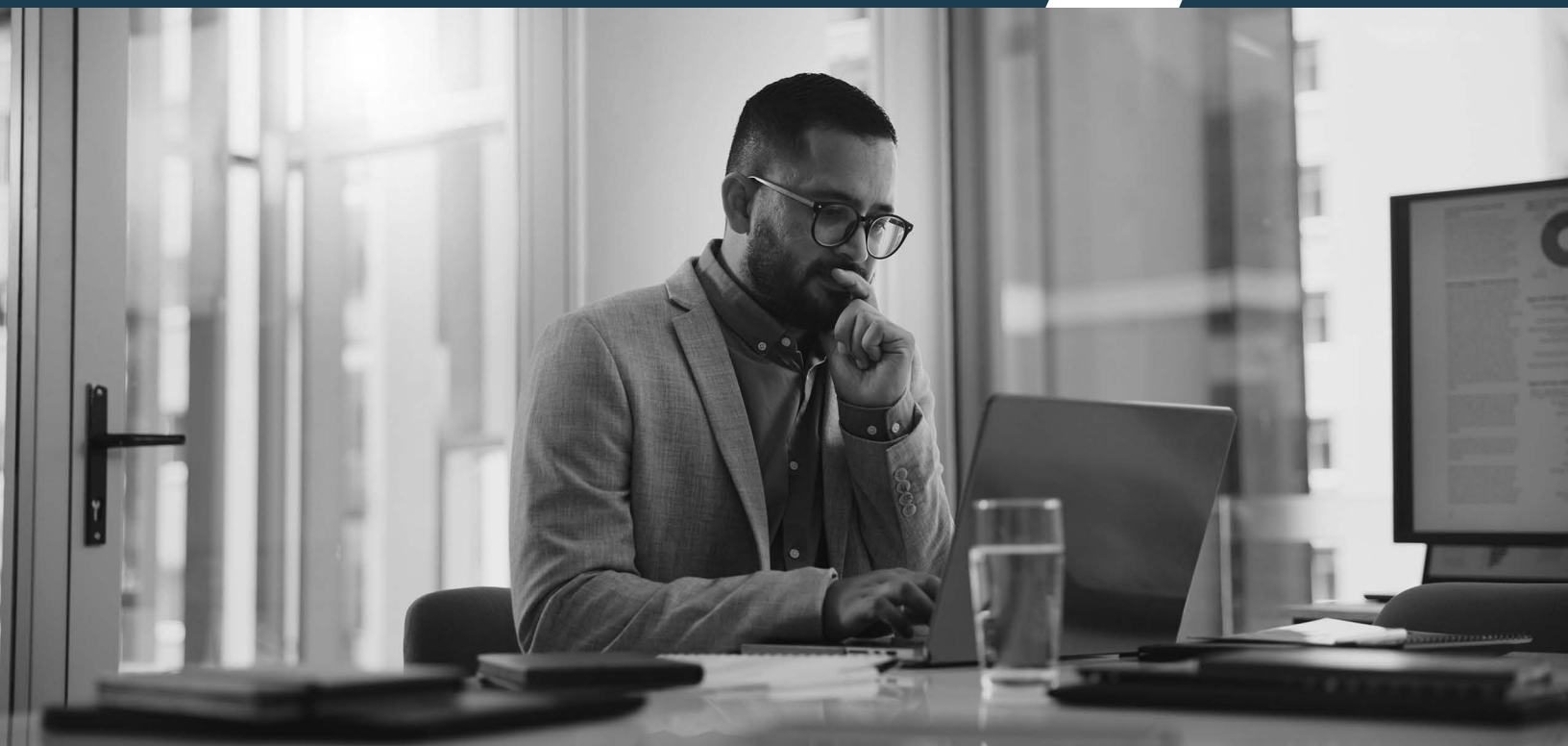
- Use lessons learned to improve security controls, governance, risk management, resource planning, and future security priorities.
- **COST-EFFECTIVE TIP** Conduct IIS security self-assessments and remediate identified gaps. For additional information, please see the [Cybersecurity Tips](#) companion document, Tip 13. Organizations should start with annual self-assessments and then increase the cadence over time to quarterly, monthly, and then ultimately to continuous self-assessments as the IIS attains higher levels of cybersecurity maturity.

SUMMARY

This chapter highlights priority SCF controls and practical IIS considerations for maintaining business continuity, responding to cybersecurity incidents, recovering operations, and strengthening resilience through continuous improvement. These practices help IIS programs sustain essential services, restore operations efficiently, and better prepare for future disruptions.

7

CONCLUSION



CHAPTER 7 CONCLUSION

The practices described throughout this guide are intended to help IIS programs advance IIS Functional Standards Goal A: *Establish and maintain a secure, confidential Immunization Information System.*

Recognized as the foundation of the IIS Functional Standards, system security supports trusted information exchange and helps ensure timely and accurate data are available for consumer, clinical, and public health decision making.

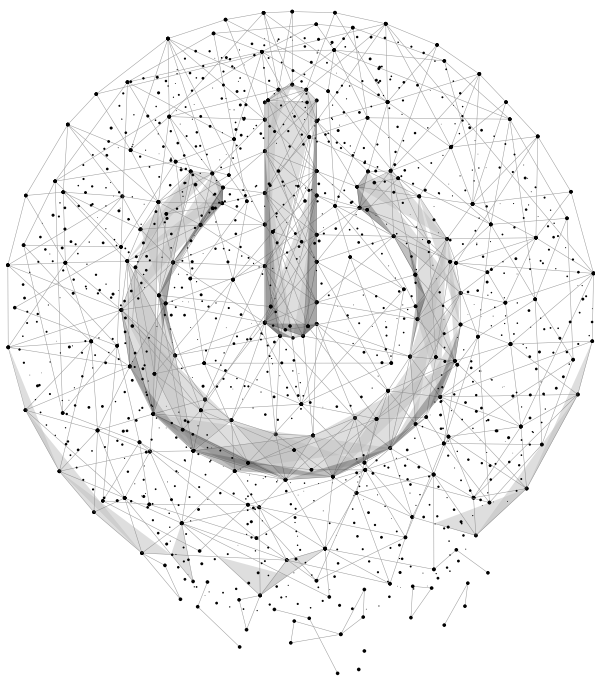
Maintaining a secure IIS requires practices that are implemented, sustained, and continuously monitored and improved in IIS system development and day-to-day operations. Because IIS security responsibilities are often shared across executive leadership, IIS managers, technical implementers, enterprise IT and security teams, vendors, hosting providers, and other partners, jurisdictions remain accountable for ensuring appropriate protections are in place to safeguard IIS systems and data. The priority practices and controls presented throughout this guide help IIS programs and their partners strengthen security while protecting the confidentiality, integrity, and availability of IIS systems and data. They support risk-informed security, secure technical and programmatic operations, and effective business continuity, incident response, and recovery.

Collectively, these practices provide a practical foundation for assessing current capabilities, identifying priorities, and developing a road map for continued improvement. IIS programs should adapt and expand these controls as appropriate to reflect their regulatory environment, organizational requirements, risk management strategy and risk tolerance, and level of cybersecurity maturity. The objective is to understand, prioritize, manage, and reduce risk in a manner consistent with legal obligations and organizational priorities.

As IIS programs apply and refine these practices over time, they can strengthen security, improve resilience, and support reliable and trusted IIS capabilities that support immunization and broader public health goals.

APPENDICES

8



APPENDIX A
IIS SECURITY GUIDANCE
ACRONYMS **90**

APPENDIX B
CONTROL SELECTION
METHODOLOGY **93**

APPENDIX C
IIS SECURITY
RESPONSIBILITIES BY ROLE **97**

APPENDIX D
ORIENTATION TO THE
SECURE CONTROLS
FRAMEWORK (SCF) **101**

APPENDIX A IIS SECURITY GUIDANCE ACRONYMS

ABBREVIATION	DESCRIPTION
AAT	AI and autonomous technologies
ACK	Acknowledgment message
ACL	Access control lists
AI	Artificial intelligence
AI TEVV	Artificial intelligence test, evaluation, validation and verification
AICPA	American Institute of Certified Public Accountants
AIRA	American Immunization Registry Association
AO	Authorizing official
API	Application programming interface
BA	Business associate
BC	Business continuity
CCB	Change control board
CDC	Centers for Disease Control and Prevention
CE	Covered Entity
CISA	Cybersecurity and Infrastructure Security Agency
CMM	Capability Maturity Model
CPG	Cybersecurity performance goals
CSF	Cybersecurity Framework or Common Security Framework (context dependent)
CSP	Cloud service providers
DiD	Defense in depth
DMZ	Demilitarized zones

ABBREVIATION	DESCRIPTION
DNS	Domain name service
DR	Disaster recovery
EPLC	Enterprise performance life cycle
FIM	File integrity monitoring
FISMA	Federal Information Security Modernization Act
HCA	HCA Healthcare
HL7	Health Level Seven
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
HPH CPGs	Healthcare and Public Health Cybersecurity Performance Goals
IaaS	Infrastructure as a service
IIS	Immunization information system(s)
IRP	Incident response plan
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information technology
LAC	Logical access control
NIST	National Institute of Standards and Technology
OCI	Open Container Initiative
OT	Operational technology
OWASP	Open Worldwide Application Security Project
PaaS	Platform as a service
PDCA	Plan-Do-Check-Act
PHI	Protected health information

ABBREVIATION	DESCRIPTION
RACI/RASCI	Responsible, accountable, consulted, informed/ responsible, accountable, support, consulted, informed
RBAC	Role-based access control
RCA	Root cause analysis
RMF	Risk management framework
RPO	Recovery point objective
RTO	Recovery time objective
RTM	Requirements traceability matrix
SaaS	Software as a service
SCF	Secure Controls Framework
SDLC	System development life cycle, software development lifecycle, or secure development life cycle (context dependent)
SIEM	Security incident event manager
SOC 2	System and Organization Controls 2
SP	Special publication
SSDF	Secure Software Development Framework
SSDP	Secure software development practices
TAAS	Technology assets, applications and/or services
TAASD	Technology assets, applications, services and/or data
TLS	Transport layer security
TSC	Trust services criteria
TTE	Tabletop exercise
UAM	User activity monitoring
UEBA	User and entity behavior analytics
ZTA	Zero trust architecture

APPENDIX B CONTROL SELECTION METHODOLOGY

PURPOSE

This appendix describes the methodology used to identify and select cybersecurity controls for this guide.

The objective was to develop a practical, risk-informed set of controls that helps IIS programs protect immunization data while recognizing the varying levels of cybersecurity maturity, staffing, and resources across IIS. Rather than including all 1,500 available cybersecurity controls, the methodology focused on identifying controls that provide the greatest value, align with recognized cybersecurity practices, and address the operational realities of IIS environments.

METHODOLOGY OVERVIEW AND PROCESS

The control selection process combined cybersecurity best practices, health care sector guidance, IIS-specific requirements, and community review to narrow down a large universe of cybersecurity controls into a practical set of recommendations for IIS. The process is summarized below in Figure 5.

Figure 5 | Control selection process

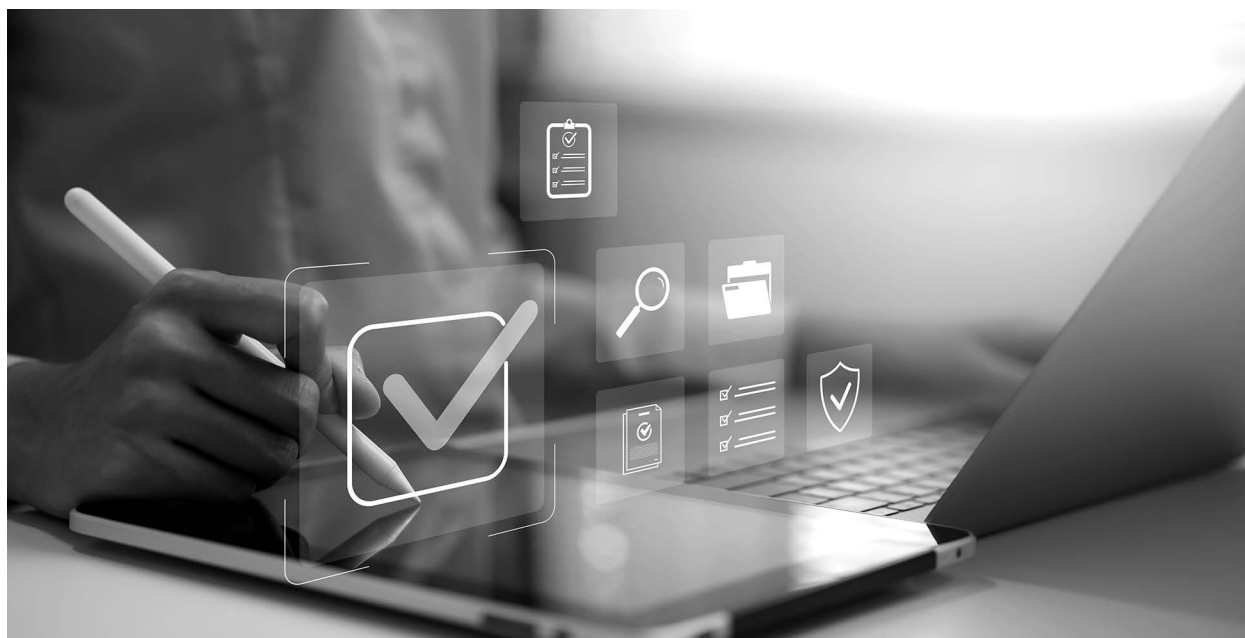


Environmental scan

An environmental scan identified cybersecurity resources most relevant to IIS programs. Twenty-nine resources were reviewed, including federal frameworks, health care sector guidance, industry standards, public health resources, and IIS-specific references. The Secure Controls Framework (SCF) was selected as the foundation for this guidance because it is NIST-aligned and consolidates numerous authoritative cybersecurity, privacy, and compliance frameworks into a single publicly available control catalog (called a “meta framework”). The Security Guidance for IIS Advisory Panel (“Advisory Panel”) and the CDC reviewed and confirmed the SCF was an appropriate foundation for the guidance. The process and outcomes of this scan are further detailed in the [Cybersecurity Framework Environmental Scan](#) companion document.

Development of baseline controls

The SCF served as the primary source of candidate controls because it provides a comprehensive catalog of cybersecurity, privacy, and compliance controls that can be evaluated against operational and security needs of IIS programs. At the time of analysis, the framework contained almost 1,500 controls derived from and cross-referenced with widely adopted cybersecurity, privacy, and compliance sources.





Control prioritization

Because implementing every available control is not practical, a prioritization process identified controls with the greatest potential impact. Controls were evaluated based on their prevalence across all SCF 250 cybersecurity frameworks and standards, helping identify practices that are consistently recognized as important across the cybersecurity community. The selection process focused on SCF-weighted “10” controls and included select SCF-weighted “9” controls when they addressed risks, operational needs, or considerations especially relevant to IIS environments. The goal was to identify controls that provide the greatest risk reduction value relative to the implementation effort.

Framework and IIS validation

Candidate controls were reviewed against key cybersecurity frameworks, health care guidance, and IIS-specific resources (Table 19) to ensure the selected controls align with current cybersecurity expectations and the operational realities of IIS.

Table 19 | *Selected cybersecurity resources and rationale*

RESOURCE	REASON FOR SELECTION
NIST SP 800-53	Widely recognized foundational security controls and control structure
NIST SP 800-66	Health care security and privacy considerations
NIST 800-218	Secure software development practices
OWASP	Web application security and secure development guidance
HHS Healthcare and Public Health Cybersecurity Performance Goals (CPGs)	Practical, high-impact cybersecurity recommendations for health care organizations
IIS Functional Standards and IIS Requirements Traceability Matrix	IIS-specific operational and security requirements
AIRA Security Guidance Considerations for IIS (2017)	Continuity with previous IIS cybersecurity guidance and identification of recommendations that remain relevant today

Community review and refinement

The Advisory Panel, including representatives from IIS programs, CDC, IIS technology vendors, and other subject matter experts, reviewed the draft control set. Feedback was incorporated to confirm relevance, sufficiency, feasibility, effectiveness, and applicability across diverse IIS environments.

Final control set validation

The following activities were completed to validate the final control set and confirm inclusion in the guidance:

- Verified coverage across major cybersecurity and health care frameworks
- Mapped to the Public Health Informatics Institute's IIS Requirements Traceability Matrix (IIS RTM)⁵⁹
- Confirmed alignment with IIS operational and security considerations
- Confirmed that selected controls provide foundational coverage across all applicable cybersecurity domains
- Evaluated implementation feasibility across organizations with varying cybersecurity maturity levels
- Assessed the balance of administrative, operational, and technical controls
- Reviewed community feedback to level-set with current IIS status and improve clarity, applicability, and usability

METHODOLOGY OUTCOMES

The resulting control set represents a carefully selected subset of SCF controls intended to provide IIS programs with a practical foundation for strengthening cybersecurity. The methodology balances security value, implementation effort, regulatory considerations, and operational realities while supporting the protection of immunization and public health data. Organizations may choose to implement additional controls based on their specific risks and requirements, but the selected controls represent practices that are broadly applicable across the IIS community.

⁵⁹ NIST / SCF Set Theory Relationship Mapping template, methodology, and artifacts: <https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm#csrk>

APPENDIX C IIS SECURITY RESPONSIBILITIES BY ROLE

This appendix expands the governance concepts and role descriptions introduced in Chapter 3 by providing additional guidance on security-related responsibilities across roles. These examples support role clarification, accountability, and coordination across executive leadership, IIS program staff, jurisdictional IT, vendors, legal and compliance personnel, and other partners. Effective IIS security depends on collaboration among these roles within the context of the IIS program's operating model, organizational structure, and shared responsibility arrangements.

Jurisdictional executive leadership – Oversight and direction

- Provide executive accountability and strategic direction: Establish governance for IIS security risk, define organizational expectations, and ensure alignment with enterprise priorities, policies, and risk tolerance. Set priorities and allocate resources. Make risk-informed decisions and ensure sufficient funding, staffing, and organizational support for security activities.
- Provide oversight of program execution: Hold program leadership accountable for implementing and sustaining security practices, including approving security priorities and strategic direction.

Jurisdictional IIS manager/IIS project manager – Execution and coordination

- Lead security program execution and operational coordination: Coordinate implementation of IIS security and related activities to promote consistent implementation across the IIS community.
- Operationalize governance and requirements: Translate governance expectations and security requirements into day-to-day procedures, onboarding activities, data use agreements, operational processes, and data exchange activities.
- Manage operational risk and support decision making: Track risks, communicate impacts, escalate issues, and verify that security controls are implemented, monitored, and maintained and support leadership decisions.

IIS IT implementers – Implementation and operations

- Implement and maintain technical safeguards: Configure, deploy, operate, and maintain system, application, infrastructure, and integration controls using secure engineering and operational practices.
- Maintain secure operations: Apply patches, updates, and configuration changes to sustain secure, reliable, and resilient operations.
- Maintain implementation documentation: Document implementation activities and provide evidence that controls are implemented, monitored, and maintained.

Additional responsibilities for vendors (if applicable)

- Define roles and responsibilities: Work with jurisdictional leadership to establish and maintain clear responsibilities between vendor and program staff.
- Deliver secure services: Meet contractual and security requirements by implementing agreed-upon operational, technical, and development controls, supporting assessments and continuous monitoring activities, and providing supporting evidence as requested.
- Report risks and issues: Communicate incidents, vulnerabilities, dependencies, and risks in accordance with contractual and regulatory obligations.

Jurisdictional IT security professional – Oversight and monitoring

Awardee-maintained IIS: Execute the responsibilities below.

Vendor-maintained IIS: Fulfill the responsibilities below through oversight of vendor activities, including obtaining and validating evidence where appropriate.

- Provide technical security leadership: Recommend and prioritize cybersecurity controls, define security requirements, support implementation planning, and maintain security documentation.
- Monitor security posture and identify gaps: Evaluate vulnerabilities, control performance, emerging threats, and alignment with applicable policies, standards, and requirements and communicate impacts.
- Support assessment, continuous monitoring, and incident response: Conduct or coordinate security assessments, continuous monitoring, incident response activities.
- Identify, communicate, and escalate risks: Identify control deficiencies and improvement opportunities and communicate impacts and recommendations to leadership and program staff.

IT security professional (or independent assessor) – Independent assessment

- Maintain independence from the implementation and operation of the controls being assessed (to avoid conflicts of interest).
- Plan and conduct security control assessments.
- Assess whether security controls are implemented correctly, operating as intended, and producing the desired security outcomes.
- Examine and document findings regarding sufficient policies, procedures, system configurations, documentation, and other supporting evidence.⁶⁰
- Interview personnel and observe operational processes, as appropriate.
- Perform or coordinate technical testing, define sampling approaches, and capture evidence to evaluate control effectiveness, where applicable.
- Validate corrective actions and remediation efforts, as appropriate.
- Report assessment results to organizational leadership and the system owner to support risk-informed decision making.

⁶⁰ The Secure Controls Framework Control Catalog lists suggested evidence for each control and references the “Evidence Request List” tab for more detailed information.

Jurisdictional legal/compliance officer – Requirements and risk

- Interpret legal and regulatory requirements: Identify applicable statutory, regulatory, and contractual obligations and translate them into actionable cybersecurity expectations.
- Advise on legal risk and governance: Support executive leadership in understanding legal implications, liability, due diligence, and accountability for protecting IIS data and systems.
- Consult on policy development and updates: Advise on documentation, procedures, agreements, and governance practices needed to demonstrate compliance.
- Advise on data sharing and incident response: Provide guidance on data access, use, disclosure, breach notification, records preservation, communication considerations, and related legal obligations.

IIS program staff – Daily operations

- Promote and demonstrate a culture of shared security responsibility: Demonstrate security awareness and reinforce responsible security practices during daily operations.
- Follow established security and operational procedures: Access and use the IIS in accordance with assigned responsibilities and established organizational requirements.
- Monitor and report security concerns: Monitor for unusual system behavior, data quality concerns, operational disruptions, phishing attempts, suspicious activities, or other potential security issues and report them through established procedures.
- Support responsible data practices: Contribute to appropriate data handling, quality, and responsible use.

External users – Authorized use

- Access IIS appropriately: Use IIS in accordance with defined permissions and applicable requirements.
- Protect credentials and comply with security expectations: Maintain appropriate credential security and use authentication processes as indicated by the IIS.
- Use IIS services and data responsibly and for authorized purposes: Follow authorized workflows and data handling expectations.
- Report user-detected issues: Notify appropriate contacts of suspected security issues or unusual activity.

APPENDIX D ORIENTATION TO THE SECURE CONTROLS FRAMEWORK (SCF)

PURPOSE

This appendix provides a brief introduction to the [Secure Controls Framework \(SCF\)](#) and explains how it is used throughout this guidance.

Familiarity with the SCF is not required to use this guidance. SCF references are included to help IIS programs identify additional implementation considerations, locate related cybersecurity practices, and better understand how selected security recommendations align with recognized standards and guidance.

ABOUT THE SECURE CONTROLS FRAMEWORK

SCF is a series of resources and program elements and a community that catalogs and maps security controls across NIST and other recognized frameworks, standards, and regulations to support security implementation. Rather than establishing new requirements, the SCF aligns guidance across existing authoritative sources to support implementation, assessment, and cross-framework mapping.

Authoritative sources include widely recognized cybersecurity frameworks, standards, regulation, etc. Examples of authoritative sources represented within SCF include:

- NIST Cybersecurity Framework (CSF)
- NIST Special Publications (e.g., SP 800-53)
- HIPAA Security Rule
- HHS cybersecurity guidance
- ISO/IEC standards
- Additional industry and regulatory references

For IIS programs, SCF can serve as a practical reference for exploring additional security practices that support the protection of immunization data, IIS infrastructure, system operations, and other related processes.

WHY THIS GUIDANCE REFERENCES SCF

Security guidance is published across numerous frameworks, standards, regulations, and best-practice documents. Referencing the SCF helps IIS programs:

- Locate more detailed implementation guidance related to referenced controls
- Trace recommendations to authoritative sources
- Explore related SCF domains and additional security practices
- Consider additional controls beyond those highlighted in this guidance
- Promote consistent implementation and assessment of safeguards
- Leverage the SCF evidence list, threat catalog, risk catalog, starter questions, control-maturity assessments, tips for different organization sizes, and more
- Prepare for optional cybersecurity certification

UNDERSTANDING SCF REFERENCES

Readers do not need to fully understand the SCF control numbering system to use this guidance. However, the control identified can be useful for locating additional implementation, assessment, and reference materials.

SCF control identifiers follow the format: **[Domain Prefix] – [Control Number]**

For example, SCF control “PES-03” refers to SCF control domain “PES” (or Physical and Environmental Security). The control number remains consistent across SCF versions. Figure 6 illustrates how this SCF information is referenced in Chapters 4, 5, and 6.

Figure 6 | Sample SCF control table

SCF ID	SCF NAME AND DESCRIPTION	IIS RTM
PES-03	Physical Access Control: Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	No corresponding RTM requirement

Control Name
Control Number
Security Domain

Control Description

IIS RTM Crosswalk (if applicable)

As shown, each SCF reference includes the control ID, control name, and a control description. All IIS-specific controls referenced in this document are also included in the companion [2026 Security Controls for IIS](#) workbook.

Readers may use these SCF control IDs to access additional information within the full SCF control catalog, such as:

- Supporting evidence, sample size, and documentation examples
- Assessment objectives, capability indicators, and validation criteria
- Mappings to authoritative sources
- Suggested threats and risks associated with each control

Readers may also use SCF references to explore related controls within the same domain and identify additional practices that may support their IIS environment beyond those highlighted in this guidance, in alignment with applicable laws, regulations, policies, and organizational expectations.

In addition to the primary SCF control catalog, SCF publishes many no-cost guides and supporting resources. These materials are available through the SCF website and GitHub repository.

SCF CONTROL CATALOG

The following describes key components of the SCF control catalog that IIS programs may use as supplemental implementation guidance.

Compensating controls

If a specific high-priority control cannot be implemented at this time, the SCF identifies compensating controls that may help reduce risk until the primary control can be implemented. A list of these controls may be found on the “Compensating Controls” worksheet as shown below:

SCF Control Name	SCF Control ID	Risk if Primary Control Not Implemented	Possible Compensating Control #1	Compensating Control Name	Compensating Control Justification	Possible Compensating Control #2	Compensating Control Name
Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-01.7	Without Business Continuity & Disaster Recovery (BC/DR) Plans, the organization may be unable to recover from disruptions, resulting in data loss and extended downtime.	BCD-09	Alternate Processing Site	Alternate Processing Site (BCD-09) provides resilience and recovery capability that compensates for the absence of Business Continuity & Disaster Recovery (BC/DR) Plans (BCD-01.7) by ensuring the organization can restore operations and data when the primary control is absent. Given the process-oriented nature of this control, this compensating control targets the same underlying risk objective through an alternative approach, helping to maintain an acceptable level of residual risk until the primary control can be implemented.	RSK-01	Risk Management Program

Evidence request list

The “Evidence Request List” worksheet provides examples of documentation that IIS programs can customize to demonstrate due care and due diligence of control implementation.⁶¹

ERL #	Area of Focus	Documentation Artifact	Artifact Description	SCF Control Mappings	Relevant CMMC 2.0 L Control
229	E-PRI-05	Privacy	Data Sharing Agreement	Documented evidence of formal data sharing practices that address, at a minimum: • The business justification for the data sharing; • The type / category of data being shared; • The third-parties the data is being shared with; • Lawful bases for data sharing; and • Data subject rights.	PRI-01.5 PRI-07 PRI-07.1 PRI-07.2

Assessment objectives

Assessment objectives describe what should be evaluated to determine when a control has been fully implemented effectively and help document assessment results. See the “Assessment Objectives” worksheet for further detail.

SCF #	SCF AO #	SCF Assessment Objective (AO) In addition to relevant policies, standards and procedures, the assessor shall examine, interview, and/or test to determine if appropriately scoped evidence exists to support the claim that:	PERTF Applicability	SCF Assessment Objective (AO) Origin(s)	Notes / Errata	Assessment Rigor (AR)	SCF Defined Parameters (DP)
CFG-03.3	CFG-03.3_A04	registration requirements for functions, ports, protocols and services are defined.	Process	53A_R5_CM-07(03)_ODP		2	
CFG-03.3	CFG-03.3_A05	an allow-all, deny-by-exception policy is employed to prohibit the execution of unauthorized software programs on the system.	Technology	53A_R5_CM-07(04)(b)		2	
CFG-03.3	CFG-03.3_A06	the list of unauthorized software programs is reviewed / updated organization-defined frequency.	Process	53A_R5_CM-07(04)(c)		2	at least quarterly or when there is a change
CFG-03.3	CFG-03.3_A07	organization-defined registration requirements are complied with.	Technology	53A_R5_CM-07(03)		3	
CFG-03.3	CFG-03.3_A08	software programs not authorized to execute on the system are defined.	Process	53A_R5_CM-07(04)_ODP(01)		3	

Threat catalog

The SCF provides a starting point for identifying common cybersecurity threats, which IIS should tailor to their environment. See the “Threat Catalog” worksheet for more information.

Threat Grouping	Threat #	Threat*	Threat Description
Natural Threat			tropical storms.
	NT-6	Landslides & Debris Flow	Landslides occur throughout the world and can be caused by a variety of factors including earthquakes, storms, volcanic eruptions, fire and by human modification of land. Landslides can occur quickly, often with little notice. Location of critical technologies should be considered (e.g., server room is in the basement or first floor of the facility).
	NT-7	Pandemic (Disease) Outbreaks	Due to the wide variety of possible scenarios, consideration should be given both to the magnitude of what can reasonably happen during a pandemic outbreak (e.g., COVID-19, Influenza, SARS, Ebola, etc.) and what actions the business can be taken to help lessen the impact of a pandemic on operations.
	NT-8	Severe Weather	Severe weather is a broad category of meteorological events that include events that range from damaging winds to hail.

⁶¹ More information on use of the evidence request list is available at <https://securecontrolsframework.com/free-content/evidence-request-list-erl>.

Risk catalog

The “Risk Catalog” worksheet provides example risks that an IIS can tailor as part of its risk management activities.

Risk Grouping	Risk #	Risk* Note - Some of these risks may indicate a deficiency that could be considered a failure to meet “reasonable security practices”	Description of Possible Risk Due To Control Deficiency IF THE CONTROL FAILS, RISK THAT THE ORGANIZATION IS EXPOSED TO IS:	NIST CSF Function
Access Control	R-AC-1	Inability to maintain individual accountability	The inability to maintain accountability (e.g., asset ownership, non-repudiation of actions or inactions, etc.).	Protect
	R-AC-2	Improper assignment of privileged functions	The inability to implement least privileges (e.g., Role-Based Access Control (RBAC), Privileged Account Management (PAM), etc.).	Protect
	R-AC-3	Privilege escalation	The inability to restrict access to privileged functions.	Protect
	R-AC-4	Unauthorized access	The inability to restrict access to only authorized individuals, groups or services.	Protect

Additional SCF controls catalog information

Additional columns in the Controls Catalog provide helpful implementation information, including:

- **Conformity Validation Cadence** [Column E] – Recommended control review frequency
- **Possible Solutions & Considerations** [Columns G through K] – Example implementation approaches for organizations of varied sizes
- **SCF Control Question** [Column L] – Sample discussion questions to support implementation
- **SCF Maturity Level Definitions** [Columns S through X] – Criteria for assessing a control’s maturity level, from 0 through 5⁶²

⁶² More information on the SCF Capability Maturity Model is available at:
 • <https://content.securecontrolsframework.com/pdf/scf-capability-maturity-model.pdf>
 • <https://youtu.be/cfjnTAEa5GY> (video tutorial)

LEARN MORE ABOUT SCF

Additional SCF resources, which are available to help IIS learn more about SCF and its implementation guidance, include:

- *Start Here*, which provides a web page, video, and introductory resources:
<https://securecontrolsframework.com/start-here>
- *SCF Overview and Practitioner Guidebook*, which provides an overview of SCF:
<https://content.securecontrolsframework.com/pdf/scf-recommended-practices.pdf>
- *Security Domains*, which lists each of the domains and explains the domain taxonomy of which SCF is composed:
<https://securecontrolsframework.com/start-here/scf-domains-principles>
- The *SCF Control Catalog* (an Excel spreadsheet), which is available in three formats:
 - Registration required (provides notification of new releases):
<https://securecontrolsframework.com/free-content>
 - Anonymous download from the SCF GitHub Repository:
<https://github.com/securecontrolsframework/securecontrolsframework>
 - Download for use in global risk and compliance applications:
<https://tools.scfconnectlabs.com/>
- Free community support, which is available via the official SCF Discord server:
<https://discord.com/invite/8h2twZP2uf>