Health Care and Public Health Sector

Cybersecurity Framework Implementation Guide

Version 2

March 2023

CAUTIONARY NOTE

This publication is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that Health Care and Public Health (HPH) Sector organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, this publication uses the words "adopt," "use," and "implement" interchangeably. These words are not intended to imply compliance or mandatory requirements.

This document was developed in part based on feedback provided by public and private sector organizations under the Critical Infrastructure Partnership Advisory Council (CIPAC)[1] framework. The U.S. Government has made no representation with respect to the sufficiency of this document in complying with any Federal requirement, nor does the U.S. Government endorse the use of this document or any products or services referenced within, over the use of any other products, services, frameworks, tools, or standards. This document is also considered a "living" document and subject to update, as needed, to best serve the health care industry.

[1] Cybersecurity & Infrastructure Security Agency, CISA (2021a). Critical Infrastructure Partnership Advisory Council. Available from https://www.cisa.gov/critical-infrastructure-partnership-advisory-council.

ACKNOWLEDGEMENTS

In 2015, the National Institute of Standards and Technology (NIST) released the *Framework for Improving Critical Infrastructure Cybersecurity* (“Cybersecurity Framework”) in response to a requirement of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. EO 13636 also called on Sector-specific Agencies (SSAs) like the U.S. Department of Health and Human Services (HHS) to “coordinate with the Sector Coordinating Councils [SCCs] to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.”

The Risk Management (RM) Sub-Working Group (SG) was formally chartered under CIPAC under the Joint HPH Cybersecurity Working Group (WG) in late 2015 to produce the *Health Care Sector Cybersecurity Framework Implementation Guide* (Sector Guide) to help Health Care and Public Health (HPH) Sector organizations implement the NIST Cybersecurity Framework in accordance with EO 13636.

Initially released in Feb 2016 as Version (Ver.) 1, a 508-compliant version, Ver. 1.1, with additional minor updates and corrections was published in May 2016. The Joint HPH Cybersecurity WG was later re-chartered under CIPAC as the HPH Sector Coordinating Council (HSCC) Joint Cyber WG (JCWG) and the original RM SG was renamed as Task Group 1A (TG-1A) under the JCWG in 2018.

TG-1A members who assisted with the development and internal review of this major new release, Ver 2.0, of the Sector Guide include:

Alexander Reniers, U.S. Dept. of Homeland Security (DHS)
Anna Verrichia, Merck
Dr. Bryan Cline, HITRUST (TG-1A Chair)
Cathlynn Nigh, Beyond LLC
Dr. Claude Council, Shriner’s Hospitals for Children
Clay Ramsey, Health Management Systems
Clyde Hewitt, CynergisTek / NCHICA
David Leonard, Anthem Inc.
Dwayne Stevens, Westcare Foundation
Gagandeep Goyal, Idaho College of Osteopathic Medicine
Greg Garcia, HSCC (JCWG Cybersecurity Director)
Henry Sprafkin, Clearwater Compliance
Jon Moore, Clearwater Compliance
Kevin Dang, HHS
Larry Tritschuh, Health Equity
Lassine, Cherif, DC Primary Care Association
Leo Dittemore, Agilon Health
Lenny Levy, Unaffiliated (Direct Patient Care)
Marilyn Zigmund Luke, America’s Health Insurance Plans (AHIP)
Michael McNeil, Royal Phillips
Mitchell Parker, Indiana University of Health
Murali Balakrishnan, TIDI Products
Paul Curylo, INOVA Health System
Phil Meadows, Charleston Area Medical Center
Quang Tran, National Committee for Quality Assurance (NCQA)
Ramakrishnan Pillai, Elekta
Rich Curtiss, Coalfire Systems, Inc.
Ron Yeager, HonorHealth
Sonia Sadana, PNC Bank
Steve Abrahamson, GE Healthcare
Ty Greenhalgh, Cyber Tyger, LLC

Government Coordinating Council (GCC) organizations that conducted formal reviews of this document include the U.S. Food and Drug Administration (FDA), Office for Civil Rights (OCR), HHS Office of the Assistant Secretary for Preparedness and response, HHS Office of the CIO, the Centers for Medicare & Medicaid Services, the Office of the National Coordinator for Health Information Technology (ONC), NIST, and the HHS Office for Civil Rights (OCR).

FOREWORD

Today's climate of increasingly sophisticated cyberattacks exploit fragmented hospital infrastructures, an often-unwieldy number of applications and legacy, and network-connected medical devices, which can negatively impact patient care, cripple business operations, expose sensitive health data, and negatively impact a company's reputation and market value. Additionally, lack of attention to the regulatory compliance increases the risk of to the delivery care in addition to fines and other penalties, these risks drive corporate boards and executive management teams to adapt to this ever-changing threat landscape and improve their overall approach to cyber governance and security.

Many, if not most, health care organizations struggle with managing cybersecurity effectively. OCR's HIPAA Audits Industry Report found that 86% of Covered Entities (CEs) and 83% of Business Associates (BAs) (85% collectively) did not meet expectations for a Risk Assessment. For Risk Management, 94% of CEs and 88% of BAs (91% collectively) did not meet expectations.[2] In 2019, as reported, OCR continued to find the failure to conduct an accurate and thorough risk analysis as one of the most frequent violations of the HIPAA Security Rule by organizations that OCR has entered into resolution agreements with or that have been found to have violated HIPAA.[3] [4] While compliance is an important factor in securing the information technology environment, undertaking a broader collaborative engagement in a risk analysis will enhance the ability to effectively identify and manage organizational risk, safeguard patient privacy, and protect business value.

Federal agencies with regulatory oversight for health care organizations have the ability to hold health care organizations responsible for implementing reasonable and appropriate cybersecurity practices. And, in addition to data centric cyber concerns, health care organizations should be cognizant of Cyber Physical Systems (CPS) and Internet of Things (IoT) security issues[5] that can adversely impact health care operations and patient care.[6]

To be effective in today's constantly evolving threat and regulatory compliance landscape, health care organizations must adopt an approach that goes beyond the threats, vulnerabilities and controls *du jour* and helps communicate how cybersecurity investments result in meaningful risk reduction. Senior leadership has a crucial strategic role to play in developing and managing such an approach, but they are often hampered by their limited understanding of cyber issues, the quality and frequency of the reporting they receive from management, and inadequate governance structures.

One way organizations can improve their ability to manage cyber-related risk is to adopt a comprehensive cybersecurity framework that can provide a common language and structure for discussions around risk and the methods and tools used to manage risk to a level that is not only acceptable to the organization but to other stakeholders such as business partners, customers, and industry and governmental regulators. Basing an organization's cybersecurity program on an industry-recognized cybersecurity framework can also help direct capital, operational, and resource allocations to lines of business generating the greatest return on protecting assets/information and minimizing risk exposure.

[2] OCR (2020, Dec). 2016-2017 HIPAA Audits Industry Report. Available from https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.

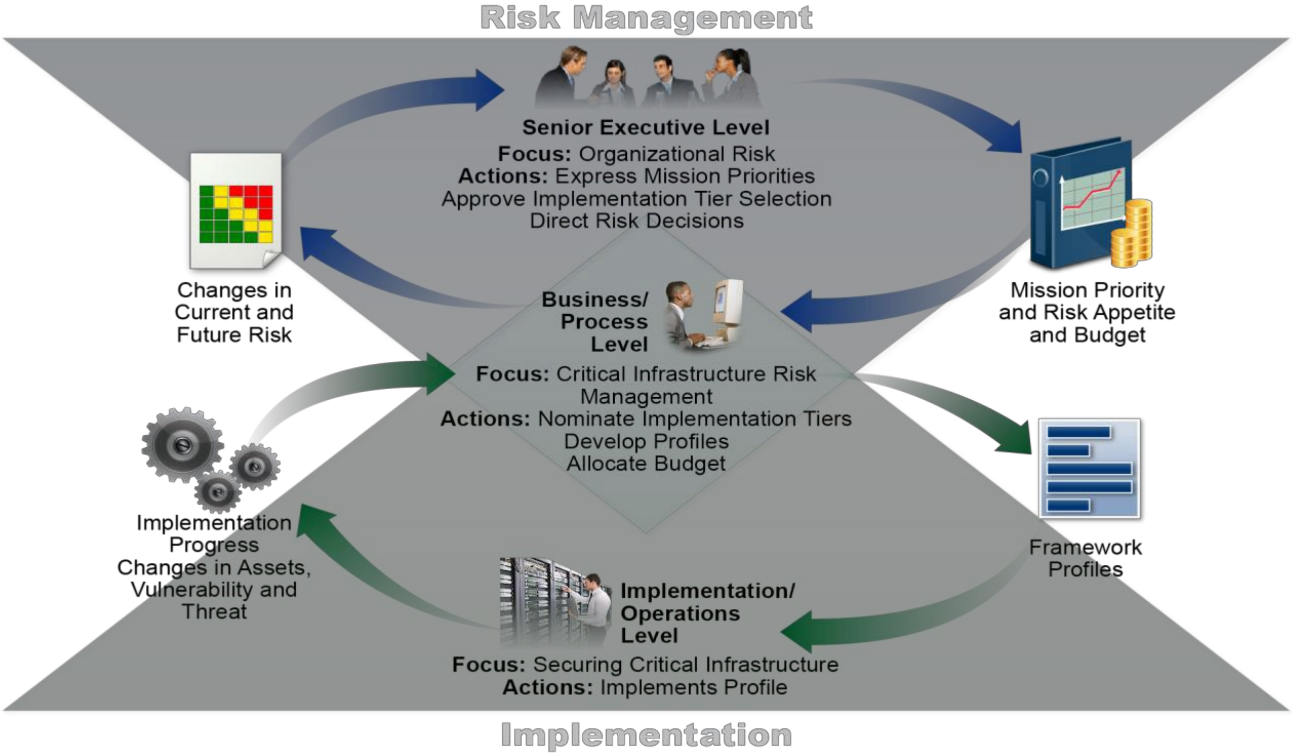
[3] OCR (2019, Feb) OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement. Available from https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf.

[4] For more information on settled enforcement actions, see OCR (2022). Resolution Agreements: Resolution Agreements and Civil Money Penalties. Available from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

[5] National Institute of Standards and Technology, NIST(2021). Cyber-Physical Systems (CPS) and Internet of Things (IoT). Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf.

[6] Parker, S. (2017, Oct 3.). Understanding the Physical Damage of Cybersecurity. In Information Security Magazine. Available from https://www.infosecurity-magazine.com/opinions/physical-damage-cyber-attacks/.

Figure 1. Notional Information and Decision Flows within an Organization[7]


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

The “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients” publication (HICP),[8] recognizes the complexity of cybersecurity threats. This publication, which was developed by the joint public-private 405(d) Task Group, covers the five most prevalent threats in the HPH Sector and ten cybersecurity practices to help mitigate these threats. Within its Technical Volumes, the cybersecurity practices and sub-practices are mapped to the NIST Cybersecurity Framework. Additionally, the Task Group developed a HICP Threat Mitigation Matrix that includes the NIST Cybersecurity Framework and HIPAA Security Rule crosswalk. HHS concurred with the recommendation of the 405(d) Task Group in the report and stated that it would work with appropriate entities to assist in sector adoption.

One of the frameworks recommended by the Task Group to help health care organizations manage cybersecurity and bolster their security posture is the NIST Framework for Improving Critical Infrastructure Cybersecurity (“Cybersecurity Framework”). This document, the *HPH Sector Cybersecurity Framework Implementation Guide*, is intended to help HPH Sector organizations implement the NIST Cybersecurity Framework as an integral part of their cybersecurity and cyber risk management programs.

[7] NIST (2018, Aug 16). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Wash., DC: Author, p. 12. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[8] HHS (2022a). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Available from https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf.

Leveraging the NIST Cybersecurity Framework also aligns with the National Association of Corporate Directors (NACD) Director's Handbook on Cyber-Risk Oversight,[9] which provides five key issues that corporate boards should consider as they oversee cybersecurity and cyber risk management programs:

- Approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.[10]
- Understand the legal implications of cyber risk as they apply to the company's specific circumstances.
- Ensure they have adequate access to cybersecurity expertise and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
- Set the expectation that management will establish an enterprise-wide cyber-risk management framework.
- Include identification of which risks to either avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach, in discussions of cyber risks between the Board and organizational management.

Organizations need a practical approach for addressing cybersecurity challenges. Boards and executive management want better insight into how cybersecurity management decisions are made. The NIST Cybersecurity Framework bridges the communications divide between an organization's leadership and the information technology and security teams, helps define cyber maturity targets, supports complex cyber risk management decisions, and improves Board oversight of cybersecurity and cyber risk management programs.

[9] Clinton, L. (Ed.) (2020). Cyber-Risk Oversight (Director's Handbook Series). Arlington, VA: National Association of Corporate Directors. Available from http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf.

[10] For more information on how to integrate cybersecurity into enterprise risk management, see Stine, K., Quinn, Stephen, Witte, G., and Gardner, R. (2020, Oct). Integrating Cybersecurity and Enterprise Risk Management (ERM) (NISTIR 8286). Gaithersburg, MD: NIST, p. 2. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

BACKGROUND

The National Infrastructure Protection Plan (NIPP), developed under Presidential Policy Directive 21[11] (PPD-21), called for public and private sector collaboration to improve the security and resilience of the nation's critical infrastructure in 16 critical infrastructure sectors. Under the NIPP, HHS is responsible for coordinating critical infrastructure security and resilience activities for the Health Care and Public Health (HPH) Sector. And under the NIPP's Critical Infrastructure Partnership Advisory Council (CIPAC) —a structure administered by DHS to allow for interaction on critical infrastructure security and resilience matters among public and private sector partners—HHS leads a Government Coordinating Council (GCC) of Federal, State, local, Tribal, and Territorial representatives that partners with a self-governed Sector Coordinating Council (SCC) of private sector health care organizations.

The HPH SCC is recognized by the HHS Secretary as the critical infrastructure industry partner with the government under PPD-21 for coordinating strategic and policy approaches to preparing for, responding to, and recovering from significant cyber and physical threats to the sector. These include natural, technological, and manmade disasters, and national or regional health crises. The HPH SCC represents the major health care associations and their stakeholders, including publicly accessible health care facilities and private practices, health plans and payers, blood, lab, pharmacy and other suppliers, funeral homes and mass fatality managers, research centers, manufacturers, and other physical assets and vast, complex public-private information technology systems required to support care delivery and the rapid, secure transmission and storage of large amounts of HPH data.

Together, these public and private sector partners combine to form the HPH Sector Critical Infrastructure Partnership, which established CIPAC and, supporting the work of CIPAC, several joint working groups (WGs), including the HSCC JCWG (formerly the Joint HPH Cybersecurity WG).

The HSCC JCWG collaborates with HHS and other federal agencies (such as DHS) to develop and encourage adoption of recommendations and guidance for policy, regulatory and market-driven strategies to facilitate collective mitigation of cybersecurity threats to the sector that affect patient safety, security, and privacy, and consequently, national confidence in the health care system.

[11] The White House (2013, Feb 12). Presidential Policy Directive—Critical Infrastructure Security and Resilience. Available from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/.

PURPOSE

The HSCC JCWG developed this document in consultation with the SCC and GCC to help Health Care and Public Health sector organizations understand and leverage the NIST Cybersecurity Framework's Informative References in their implementation of sound cybersecurity and cyber risk management programs, address the five Core Function areas of the NIST Cybersecurity Framework to ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with their overall information security and privacy risk management activities.

The guidance will also help an organization's leadership to:

- Understand NIST Cybersecurity Framework terminology, concepts, and benefits,
- Assess their current and targeted cybersecurity posture,
- Identify gaps in their current programs and workforce,
- Identify current practices that help address recommended NIST Cybersecurity Framework outcomes.

VERSION HISTORY

Version	Date	Drafted By	Description
1.0	31 Dec 2015	HPH Joint Cybersecurity WG, Risk Management SG	Final document consolidating content from multiple documents/resources to support intent of broader implementation guidance for the HPH sector and incorporating comments from the Risk Mgmt. Sub-working Group, the Public, and a final review by HHS. Contains placeholders for additional content being developed by the Risk Mgmt. Sub-Working Group for the next version of the Guide.
1.1	15 May 2016	HPH Joint Cybersecurity WG, Risk Management SG	Incorporates OCR's NIST Cybersecurity Framework-to-HIPAA crosswalk, updates CNSSI No. 4009 definitions to reflect its 2015 release; and makes other minor corrections.
2.0	20 Apr 2022	HSCC CWG TG-1A and HHS CWG	Generalizes the implementation approach to reflect how tailored overlays of one or more NIST Cybersecurity Framework Informative References can be leveraged to create an organization or industry sector-specific control overlay. Expands on the framework-based approach to risk analysis. Removes/adds various appendices to accommodate work performed elsewhere in the JCWG. Includes additional updates stemming from the release of v1.1 of the NIST Cybersecurity Framework.

TABLE OF CONTENTS

List of Tables

List of Figures

INTRODUCTION

The United States has seen a marked increase in the use of digital technologies and cyber-physical systems (CPS), which in health care are critical integration of a network of medical devices. These systems are progressively used in hospitals to achieve a continuous high-quality health care. and a resulting increase in the level of exposure to cyber-attacks, which target an organization's use of cyberspace for the purpose of stealing information or disrupting, disabling, or destroying related information resources. As a result of these ever-increasing cyber threats, President Barack Obama directed the NIST to work with the private sector to develop the *Framework for Improving Critical Infrastructure Cybersecurity*,[12] also known as the Cybersecurity Framework. The NIST Cybersecurity Framework provides an organizational cybersecurity risk management model that industries, industry sectors, or organizations can leverage to identify opportunities for improving their management of cybersecurity risk.

Security controls are the safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risks. Privacy controls are the administrative, technical, and physical safeguards employed within a system or an organization to manage privacy risks and to ensure compliance with applicable privacy requirements. Security and privacy controls are selected and implemented to satisfy security and privacy requirements levied on a system or organization. Security and privacy requirements are derived from applicable laws, executive orders, directives, regulations, policies, standards, and mission needs to ensure the confidentiality, integrity, and availability of information processed, stored, or transmitted and to manage risks to individual privacy. This document seeks to help Health Care and Public Health (HPH) Sector organizations understand and use NIST Cybersecurity Framework's Informative References to achieve the goals of the NIST Cybersecurity Framework. To help further this aim, the document presents an implementation approach that leverages these Informative References, explains the relationship between these Informative References and the NIST Cybersecurity Framework, and provides additional implementation guidance.

Executive Orders and Mandates

The following sections discuss the history of the various mandates and executive orders pertaining to the use of a voluntary Cybersecurity Framework in securing the critical infrastructures.

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

In its December 2011 report, "Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use"[13], the Government Accountability Office (GAO) found similarities in cybersecurity guidance and practices across multiple sectors. Much of the guidance is tailored to business needs or to address unique risks and operations and recommends promoting existing guidance to assist individual entities within a sector to identify "the guidance that is most applicable and effective in improving their security posture."[14]

[12] NIST (2018, Aug 16).

[13] GAO (2011). Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use, Wash., DC: Author Available from http://www.gao.gov/products/GAO-12-92

[14] Ibid., p. i.

Less than a year later, President Obama issued Executive Order (EO) 13636,[15] "Improving Critical Infrastructure[16] Cybersecurity," which called for the development of a voluntary Cybersecurity Framework to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for the management of cybersecurity risks to critical infrastructure.

The Executive Order directed NIST to develop the Cybersecurity Framework and to incorporate industry best practices "to the fullest extent possible." The Department of Homeland Security (DHS) was tasked with establishing performance goals and, in collaboration with sector-specific agencies, supporting the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities through a voluntary program.

After three cybersecurity framework workshops, NIST published its August 28, 2013 discussion draft of the Preliminary Cybersecurity Framework. The draft, which was also made available to the public for review, was published in advance of its Fourth Cybersecurity Framework workshop in September 2013. NIST released a 'final' public draft of the Preliminary Cybersecurity Framework in October of 2013, and the final Framework for Improving Critical Infrastructure Cybersecurity, Version 1 was released in February of 2014.[17,18] The Framework has been updated by NIST with extensive private sector input since it issued in February 2014. An updated version of the Framework, Version 1.1, was released in 2018.

EO 13636 also directed development of a program to serve as a central repository for government and private sector tools and resources. This Critical Infrastructure Cyber Community (C^3) Voluntary Program[19] was intended to provide critical infrastructure sectors, academia, state, local, tribal, and territorial governments with businesses tools and resources to use the NIST Cybersecurity Framework and enhance their cyber risk management practices.[20]

Public Law 113-274: Cybersecurity Enhancement Act of 2014

NIST's future Framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274),[21] which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure. This collaboration continues as NIST works with stakeholders from across the country and around the world to raise awareness and encourage use of the Framework.

[15] Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013). Available from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[16] Critical infrastructure is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[17] NIST (2014). NIST Releases Cybersecurity Framework Version 1.0. Available from http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[18] NIST (2014, Feb 12). Framework for Improving Critical Infrastructure Cybersecurity, Version 1. (Updated 2018, Jan 8). Wash., DC: Author.

[19] CISA (2021b). Critical Infrastructure Cyber Community C3 Protection Program. Available from https://www.cisa.gov/ccubedvp.

[20] To access resources related to the former C3 Voluntary Program and the Framework, visit https://www.us-cert.gov/resources

[21] Cybersecurity Enhancement Act of 2014. Public Law 113-274. Available from https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

In May 2017, President Trump issued EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which was intended to focus Federal efforts on supporting "the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure"[22] by securing Federal networks, encouraging collaboration with industry, strengthening the deterrence posture of the United States, and building a stronger cybersecurity workforce.[23] One of the actions taken by Federal agencies in response to this EO was to develop implementation plans for using the NIST Cybersecurity Framework.

Public Law 116-321: Amending the Health Information Technology for Economic and Clinical Health Act

Signed into law by President Trump on January of 2021, Public Law (PL) 116-321[24] amended the Health Information Technology for Economic and Clinical Health Act.[25] This law requires HHS to consider a health care entity's adoption of recognized security practices, as defined by PL 116-321, when determining the length and outcome of audits or the amount of fines or extent of penalties. It is important to note that this law does not help health care covered entities or business associates avoid liability for HIPAA violations as it clearly states that "Nothing in this section shall be construed to limit the Secretary's authority to enforce the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title), or to supersede or conflict with an entity or business associate's obligations under the HIPAA Security Rule." Instead, it requires the HHS Office for Civil Rights to consider if the covered entity or business associate adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place. If so, OCR should consider this when determining the length and outcome of the audit, fines, or resolution agreement terms.

Per PL 116-321, the term "recognized security practices" means "the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities."

Executive Order 14028: Improving the Nation's Cybersecurity

President Biden's 2021 EO 14028, Improving the Nation's Cybersecurity, requires the Federal Government to "improve its efforts to identify, deter, protect against, detect, and respond to [increasingly sophisticated malicious cyber campaigns… and asks the Private Sector to] adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."[26] While the EO does not specifically mention the NIST Cybersecurity Framework, the EO further highlights the need for effective cybersecurity across the Federal Government and the private sector.

[22] Exec. Order No. 13800, 3 C.F.R. 22391-22397 (2017). Available from https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

[23] CISA (2017, 7 Jul). Executive Order 13800 Update Issue 1. Available from https://www.cisa.gov/uscert/eo13800.

[24] Public Law 116-321. https://www.govinfo.gov/content/pkg/PLAW-116publ321/pdf/PLAW-116publ321.pdf.

[25] HHS (2017). HITECH Act Enforcement Interim Final Rule. Available from https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

[26] Exec. Order No. 14028, 3 C.F.R. 26633-26647 (2021). Available from https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

Potential Benefits of Health Care's Implementation of the NIST Cybersecurity Framework

The many cybersecurity-focused executive orders and laws that have been developed in the last 10 years show the importance of strong cybersecurity in protecting critical infrastructure. The NIST Cybersecurity Framework is a powerful tool to help achieve this goal. Since it is based on a collection of cybersecurity standards and industry best practices, the Cybersecurity broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication. Whether an organization has a mature risk management program and processes, is developing a program or processes, or has no program or processes, the Framework can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure.

Specifically, the NIST Cybersecurity Framework:

- Provides guidance on risk management principles and best practices
- Provides common language to address and manage cybersecurity risk
- Outlines a structure for organizations to understand and apply cybersecurity risk management, and
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs.

Beyond the stated goals and benefits of the NIST Cybersecurity Framework, there are additional potential benefits to organizations that implement information protection programs in alignment with the NIST Cybersecurity Framework, such as those obtained from leveraging a NIST Cybersecurity Framework Informative Reference.

In addition to federal provisions, states such as Ohio[27] and Connecticut[28] also offer various forms of 'safe harbor' for organizations that implement various public and private sector cybersecurity frameworks, including the NIST Cybersecurity Framework.[29]

Further benefits for implementing the NIST Cybersecurity Framework follow.

Potential Reductions in Cybersecurity Insurance Premiums

Reductions in cybersecurity insurance premiums are a potential incentive for using the framework. Organizations should consider the impact on their insurance premiums if they do or do not follow sound cybersecurity practices.[30] Furthermore, as cybersecurity continues to grow on the national and international security agenda, insurance underwriters are strongly considering evaluating their client's premiums based on standards, procedures, and other measures consistent with the NIST Cybersecurity Framework. The goal would be to build underwriting practices that promote the use of cyber risk-reducing measures and risk-based pricing and foster a competitive cyber insurance market.

[27] Ohio Data Protection Act, Senate Bill 220 (2018) Available from https://www.legislature.ohio.gov/legislation/132/sb220/documents.

[28] An Act Incentivizing the Adoption of Cybersecurity Standards for Business, Connecticut Public Act No. 21-119 (2021). Available from https://cga.ct.gov/2021/ACT/PA/PDF/2021PA-00119-R00HB-06607-PA.PDF.

[29] See Appendix K – Frequently Asked Questions.

[30] DOE (n.d.), p. 3.

Prioritized Technical Assistance from the Federal Government

The Federal Government can provide prioritized technical assistance for organizations that seek to leverage the Cybersecurity Framework. The Federal Government provides several hands-on tools that will help organizations assess their current state of cybersecurity practices and identify areas to grow their cybersecurity resilience. HPH Sector organizations are encouraged to visit the Cybersecurity & Infrastructure Security Agency (CISA) webpage at https://us-cert.cisa.gov/resources/assessments for additional information related to both facilitated and self-service risk assessment resources. Based off this assessment, the Federal government helps prioritize next steps for organizations, depending on their level of cybersecurity maturity. For example, the government offers preparedness support, assessments, training of employees, and advice on best practices. Under this incentive, the primary criteria for assistance would be criticality, security, and resilience gaps. However, owners and operators in need of incident response support will never be denied assistance based on cybersecurity maturity and/or level of prior engagement with the use of the NIST Cybersecurity Framework.

Uniformity of Efforts Across the Sector

There are significant potential benefits that could be derived from uniformity of efforts, including conducting national/sector-level cybersecurity activities in parallel with organizational level activities. If an organization conducts cybersecurity activities based on the NIST Cybersecurity Framework, that organization will have a road map for reducing cybersecurity risks that is well aligned with HPH sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Sector efforts can manage these systemic risks that cut across many organizations and also lead to research and development efforts to create new security solutions, policy or legal solutions, and national-level programs. Additionally, HPH sector organizations that adopt the NIST Cybersecurity Framework will be able to take advantage of numerous measurement tools developed and made available by NIST for the generation of metrics, measures, and performance reports facilitating performance improvements in their information security programs and the HPH sector. NIST provides extensive guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures.[31] It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Key Elements of a Cybersecurity Program

The NIST Cybersecurity Framework helps organizations:

- Ensure people, process and technology elements completely and comprehensively address information and cybersecurity risks consistent with their business objectives, including legislative, regulatory, and best practice requirements;
- Identify risks from the use of information by the organization’s business units and facilitate the avoidance, transfer, reduction, or acceptance of risk; and

[31] Chew, E., Swanson, M., Stine, K., Barol, N., Brown, A., and Robinson, W. (2008, July). Performance Measurement Guide for Information Security(NIST SP 800-55 Reision 1). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

- Support policy definition, enforcement, measurement, monitoring, and reporting for each component of the security program and ensure these components are adequately addressed.

(For more information on the NIST Cybersecurity Framework, see Appendix C – NIST Cybersecurity Framework Basics.)

The NIST Cybersecurity Framework also provides the structure needed to ensure industry sectors and organizations address three additional key elements of a robust and comprehensive cybersecurity program: threat modeling, threat intelligence and collaboration.

Threat modeling may be accomplished either through a traditional risk analysis or the selection of a control baseline from an appropriate security framework. Threat intelligence is essential for an organization to understand and proactively address active and emerging cyber threats, and collaboration with other public and private sector entities allows an organization to address cyber threats more efficiently and effectively than it otherwise could.

Organizations have unique cybersecurity risks, including different threats, vulnerabilities, and tolerances, all of which affect benefits from investing in cybersecurity risk management, and they must apply the principles, best practices, standards, and guidelines provided in the NIST Cybersecurity Framework to their specific context and implement practices based on their own needs.

The HPH Sector embraces the flexibility the NIST Cybersecurity Framework offers but recognizes organizations' potential need for more guidance on how to specifically apply the framework to their particular situation. In addition, the HPH Sector recognizes the potential of the NIST Cybersecurity Framework to improve cybersecurity risk management efforts across all critical infrastructure industry sectors.

Ability to Incorporate Cyber-Physical Aspects of Cybersecurity

Cyber physical systems security (CPSSEC) "addresses cybersecurity concerns for cyber-physical systems and internet of things (IoT) devices… [that] play an increasingly important role in critical infrastructure… and everyday life." [32]

One of the examples of CPS in the HPH sector is medical devices, which "are increasingly connected to the Internet, hospital networks, and other medical devices to provide features that improve health care and increase the ability of health care providers to treat patients. These same features also increase the risk of potential cybersecurity threats. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device."[33]

The NIST Cybersecurity Framework, when applied through the lens of a comprehensive risk analysis that specifically includes CPS-related threats, will help further ensure patient safety in addition to protecting sensitive health information and individual privacy.

[32] DHS (2022). Cybersecurity: Cyber Physical Systems Security. Available from https://www.nist.gov/publications/cyber-physical-systems-and-internet-things.

[33] FDA (2022, Nov). Medical Devices: Digital Health Center of Excellence: Cybersecurity. Available from https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

HEALTH SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION

While the generic cybersecurity framework implementation approach outlined in Appendix C – NIST Cybersecurity Framework Basics works well for organizations that design or specify their own controls, it does not work *as well* (i.e., most efficiently) for those organizations that leverage external control frameworks such as those provided by the NIST Cybersecurity Framework's Informative References[34]. Fortunately, this generic implementation approach can be modified to accommodate a control framework-based approach to risk analysis and control specification.

The primary reason for the modification is that, for those organizations that already leverage or intend to leverage one or more Informative References, Target Profiles are easily obtained once organizations are able to scope their organization and systems and then tailor the Informative Reference(s) to address any unique threats/risks. There is no need to develop a Current Profile beforehand. ***Placement of the Current and Target Profiles can subsequently be reversed***, although some basic information about the state of the organization's cybersecurity program will necessarily be ascertained before the Target Profile is complete.

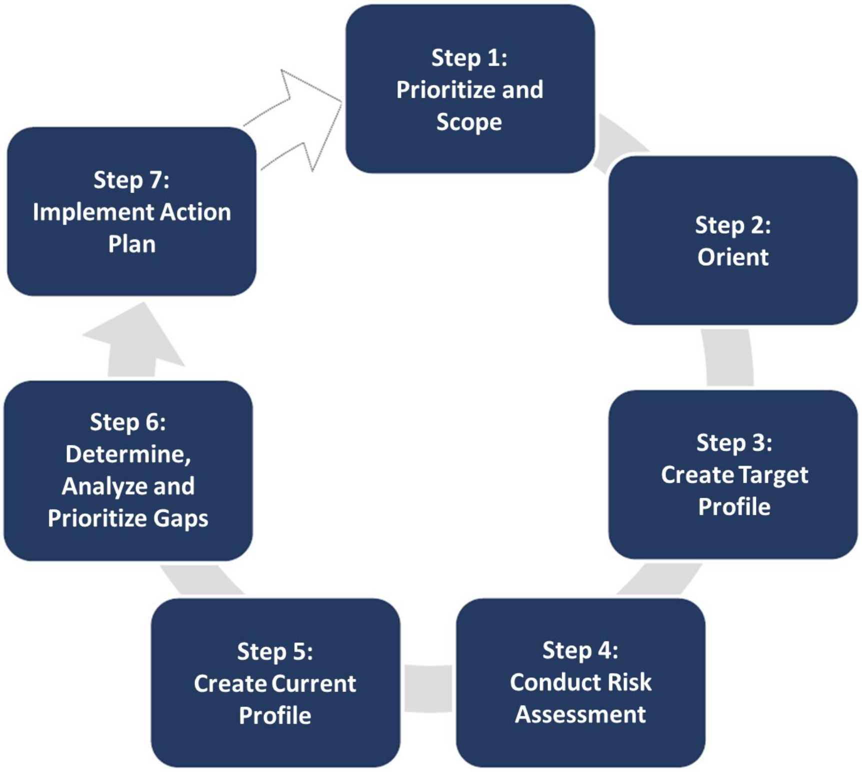
Implementation Process

The Cybersecurity Framework can be used to compare an organization's current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes and use this information to reprioritize resources. Figure 2 on the next page illustrates how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.[35]

[34] NIST (2022a). National Online Informative References Program, Informative Reference Catalog. Available from https://csrc.nist.gov/projects/olir/informative-reference-catalog.

[35] NIST (2018, Aug 16), p. 14.

Figure 2. Health Care Implementation Process



HPH Sector organizations leveraging Informative References[36] as the basis for their cybersecurity programs can use the following seven-step process for implementation depicted in Figure 2 on the previous page, which slightly modifies the general approach outlined in the NIST Cybersecurity Framework.[37]

As with the generic process, it is recommended that implementation include a plan to communicate progress to appropriate stakeholders, such as senior management, as part of its risk management program. In addition, each step of the process should provide feedback and validation to previous steps.

Each step is now discussed in more detail, first introduced by Table 1 describing the step's inputs, activities, and outputs followed by additional explanation.[38] A table of the inputs, activities, and outputs for all seven steps is also included in Appendix G– Summary of Health Care Implementation Activities.

[36] NIST (2021, Dec 8). Cybersecurity Framework: Informative References: What are they, and how are they used? Available from https://www.nist.gov/cyberframework/online-learning/informative-references.

[37] NIST (2018, Apr 16), pp. 13-15.

[38] The tables describing the activities in the 7-step implementation process are derived from DOE (2015).

Step 1: Prioritize and Scope

Table 1. Step 1: Prioritize and Scope Inputs, Activities, and Outputs

Step 1: Prioritize and Scope		
Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Asset inventory 4. Informative Reference(s)	1. Organization determines where it wants to apply the Informative Reference(s) to evaluate and potentially guide the improvement of the organization's capabilities 2. Threat analysis 3. Business impact analysis 4. System categorization (based on sensitivity & criticality)	1. Usage scope 2. Unique threats

The risk management process should begin with a strategy addressing how to frame, assess, respond to, and monitor risk. For health care organizations, leveraging one or more Informative References is a central component of that strategy as it forms the basis of their risk analysis, informs the organization on the minimum level of due care and due diligence required to meet its multiple compliance obligations, provides for the adequate protection of individually identifiable health information and other sensitive information, and provides a comprehensive and rigorous methodology for control assessment, scoring, and reporting. The organization's risk strategy is also used to inform investment and operational decisions for improving or otherwise remediating gaps in their cybersecurity and information protection program.

In this step, the organization decides how and where it wants to apply the Informative References (its usage scope)—whether in a subset of its operations, in multiple subsets of its operations, or for the entire organization. This decision should be based on risk management considerations, organizational and critical infrastructure objectives, and priorities,[39] availability of resources, and other internal and external factors. Current threat and vulnerability information from a nationally recognized ISAO may also help inform scoping decisions. All types of threats and vulnerabilities, including cyber-physical threats, that are relevant to the organization should be considered.

An organization that is using one or more Informative References for the first time might want to apply it to a small subset of operations to gain familiarity and experience with it. After this activity, the organization can consider applying the Informative References to a broader subset of operations or to additional parts of the organization as appropriate by applying the following elements of a risk analysis:

[39] HHS (2016, May).

- Conduct a complete inventory of where electronic protected health information (ePHI) is created, received, maintained, or transmitted (if not already performed)
- Perform a Business Impact Analysis (BIA) on all systems that create, receive, maintain, or transmit ePHI (criticality)
- Categorize & evaluate these systems based on sensitivity and criticality

Step 2: Orient

Table 2. Step 2: Orient Inputs, Activities, and Outputs

Step 2: Orient		
Inputs	Activities	Outputs
1. Usage scope 2. Risk management strategy 3. Informative Reference(s)	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and other authoritative sources (e.g., cybersecurity and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (e.g., organizational, system, regulatory)

The organization identifies the systems, assets, compliance and best practice requirements, and any additional cybersecurity and risk management approaches that are in scope. This includes standards and practices the organization already uses and could include additional standards and practices that the organization believes would help achieve its critical infrastructure and business objectives for cybersecurity risk management. The organization’s risk management program may already have identified and documented much of this information, or the program can help identify individual outputs. A good general rule is to initially focus on critical systems and assets and then expand the focus to less critical systems and assets as resources permit.

Step 3: Create a Target Profile

Table 3. Step 3: Target Profile Inputs, Activities, and Outputs

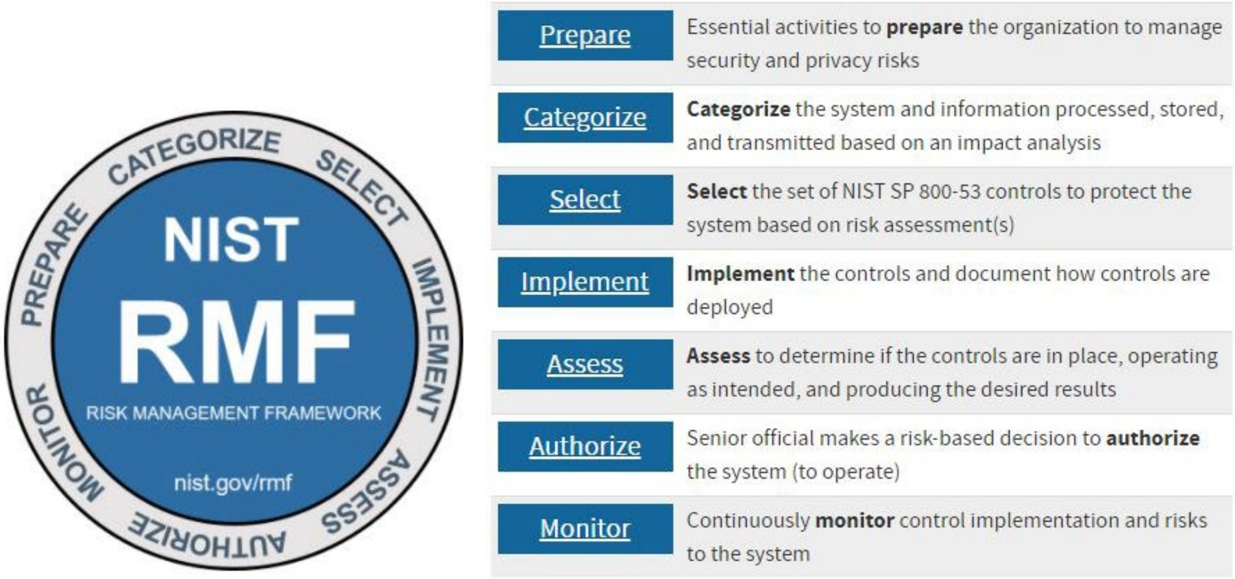
Step 3: Create a Target Profile		
Inputs	Activities	Outputs
1. Organizational objectives 2. Risk management strategy 3. Detailed usage scope 4. Unique threats 5. Informative Reference(s)	1. Organization selects one or more Informative References and creates a tailored overlay based on a risk analysis that considers the unique threats identified in the prioritization and scoping phase 2. Organization determines level of effectiveness or maturity desired in the selected controls	1. Target Profile (Tailored overlay of one or more Informative References) 2. Target Tier

The NIST Risk Management Framework (RMF) shown in Figure 3 on the next page provides organizations an overarching risk management process that integrates security, privacy, and cyber supply chain risk management[40] activities into the system development life cycle. The risk-based approach to control selection and specification provided in the first three steps of the seven-step process—shown in Figure 4 on the following page—considers effectiveness, efficiency, and constraints due to applicable laws, regulations, policies, standards, contractual, and similar obligations. This RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector.[41]

[40] For more information on aligning an enterprise supply chain cyber security program to the NIST CSF, see HSCC CWG (2020, Sep). Health Industry Cybersecurity Supply Chain Risk Management Guide Version 2.0 (HIC-SCRiM v2.0). Available from https://healthsectorcouncil.org/hic-scrim-v2/.

[41] NIST (2022b). NIST Risk Management Framework RMF. Available from https://csrc.nist.gov/Projects/risk-management/about-rmf.

Figure 3. NIST Risk Management Framework



Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

The organization considers the cyber threats and subsequent risk to its operations as determined during the first two steps to create a tailored overlay of its selected Informative Reference(s) to account for any unique threats/risks (as compared to other, similar organizations that are the target(s) of the Informative Reference(s)). The Target Profile should include these practices as well.

However, information protection cannot be a “one size fits all” approach. For example, organizations, more often as not, have different information systems (or different implementations of similar systems), different business and compliance requirements, different cultures, and different risk appetites.[42]

For whatever reason, an organization cannot implement a control specified by its selected Informative Reference(s), one or more compensating controls should be selected to address the risks posed by the threats the originally specified control was meant to address. Note these compensating controls may already exist within the organization and should be leveraged appropriately.)

Organizations should be able to demonstrate the validity of a compensating control by way of a legitimate risk analysis that shows the control has the same level of rigor and addresses a similar type and level of risk as the original. Additionally, the compensating control must be something other than what may be required by other, existing controls specified in the tailored overlay of its selected Informative Reference(s).

The organization should determine the evaluation approach it will use to identify its current cybersecurity and risk management posture. Organizations can use any of several evaluation methods to identify their current cybersecurity posture and create a Current Profile. These include self-evaluations, where an organization may leverage its own resources and expertise; facilitated approaches, where the evaluation is assisted by a third party; or completely

[42] For more information on risk appetite, see Stine, K., Quinn, Stephen, Witte, G., and Gardner, R. (2020, Oct).

independent evaluations, such as those used to support certification or accreditation against the Informative Reference(s) or an American Institute of Certified Public Accountants (AICPA)[43] Service Organization Control 2 (SOC 2)[44] that uses the organization's selected Informative Reference(s) as the basis for assessment.[45]

The organization should also determine its goals for the Target Tier from the NIST Cybersecurity Framework and identify the equivalent levels of control maturity required to achieve those goals. This will generally involve mapping relevant controls from the organization's cybersecurity program to the topical areas (characteristics) addressed by the Tiers (i.e., Risk Management Process, Integrated Risk Management Program, and External Participation) and then evaluating these areas (characteristics) for their respective Tier (i.e., 1 – Partial, 2 – Risk Informed, 3 – Repeatable, and 4 – Adaptive):

- Select an appropriate framework baseline set of controls
- Apply an overlay based on a targeted assessment of threats unique to the organization

Step 4: Conduct a Risk Assessment

Table 4. Step 4: Risk Assessment Inputs, Activities, and Outputs

Step 4: Conduct a Risk Assessment		
Inputs	Activities	Outputs
1. Detailed usage scope 2. Risk management strategy 3. Target Profile 4. Informative Reference(s)	1. Perform a risk assessment for in-scope systems and organizational elements	1. Risk assessment reports

Organizations perform cybersecurity risk assessments to identify and evaluate cybersecurity risks and determine which are outside of current tolerances. The outputs of cybersecurity risk assessment activities assist the organization in developing its Current Profile and Implementation Tier based on control maturity (see Step 5). For organizations that have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist. For example, many organizations perform regular evaluations of their programs through internal audits or other activities, which may describe the controls as implemented within the defined scope of the risk assessment

Note, this step includes the following element of a risk analysis as modified to accommodate the use of one or more

[43] AICPA (2020a). AICPA. Available from https://www.aicpa.org/about/landing/about.

[44] AICPA (2020b). SOC 2® - SOC for Service Organizations: Trust Services Criteria. Available from https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.

[45] AICPA (2020c). SOC 2 Examination That Addresses Additional Subject Matters and Additional Criteria. Available from https://amsuat.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc2additionalsubjectmatter.html.

NIST Cybersecurity Framework Core Informative References: Evaluate residual risk.[46]

Step 5: Create a Current Profile

Table 5. Step 5: Current Profile Inputs, Activities, and Outputs

Step 5: Create a Current Profile		
Inputs	Activities	Outputs
1. Risk assessment reports 2. Informative Reference(s)	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile (Implementation status of selected controls) 2. Current Tier (Implementation maturity of selected controls, mapped to NIST Cybersecurity Framework Implementation Tier model)

A Current Profile is created from the evaluation of the organization's cybersecurity and risk management practices against the Target Profile created in Step 4.

[46] There are multiple approaches to evaluating risk:

– For an example of a qualitative approach, see Alberts, C. and Dorofee, A. (2002). Managing Information Security Risks: The OCTAVE Approach. Boston: Addison-Wesley Professional.

– For examples of a semi- or quasi-quantitative approach, see:
  - Joint Task Force Transformation Initiative (2012, Sep). Guide for Conducting Risk Assessments (NIST SP 800-30 Revision Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
  - Cline, B. (2019, Sep). Risk Analysis Guide for HITRUST Organizations and Assessors. Available from https://hitrustalliance.net/content/uploads/RiskAnalysisGuide.pdf.

– For an example of a quantitative approach, see Freund, J. and Jones, J. (2015). Measuring and Managing Information Risk: A FAIR Approach. Oxford: Elsevier, Inc.

Step 6: Perform Gap Analysis

Table 6. Step 6: Gap Analysis Inputs, Activities, and Outputs

Step 6: Perform Gap Analysis		
Inputs	Activities	Outputs
1. Current Profile 2. Target Profile 3. Organizational objectives 4. Impact to critical infrastructure 5. Gaps and potential consequences 6. Organizational constraints 7. Risk management strategy 8. Risk assessment/analysis reports 9. Informative Reference(s)	1. Analyze gaps between Current and Target Profiles in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) or similar analysis on actions 6. Prioritize actions (CBA or similar analysis) and consequences 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan

The organization evaluates its Current Profile and Implementation Tier against its Target Profile and Target Implementation Tier and identifies any gaps. When mapping back to the NIST Cybersecurity Framework, a gap exists when there is a desired Category or Subcategory outcome in the Target Profile or program characteristic in the Target Implementation Tier that is not currently achieved by the organization's existing cybersecurity and risk management approach, and when current practices do not achieve the outcome to the degree of satisfaction required by the organization's risk management strategy.

After controls are specified by an organization to ensure risk is controlled to a level formally deemed acceptable by executive leadership, the most common way of dealing with (i.e., treating) deficiencies observed with the implementation and management of those controls is to remediate them. This reduces risk to an acceptable level, a process referred to as mitigation.

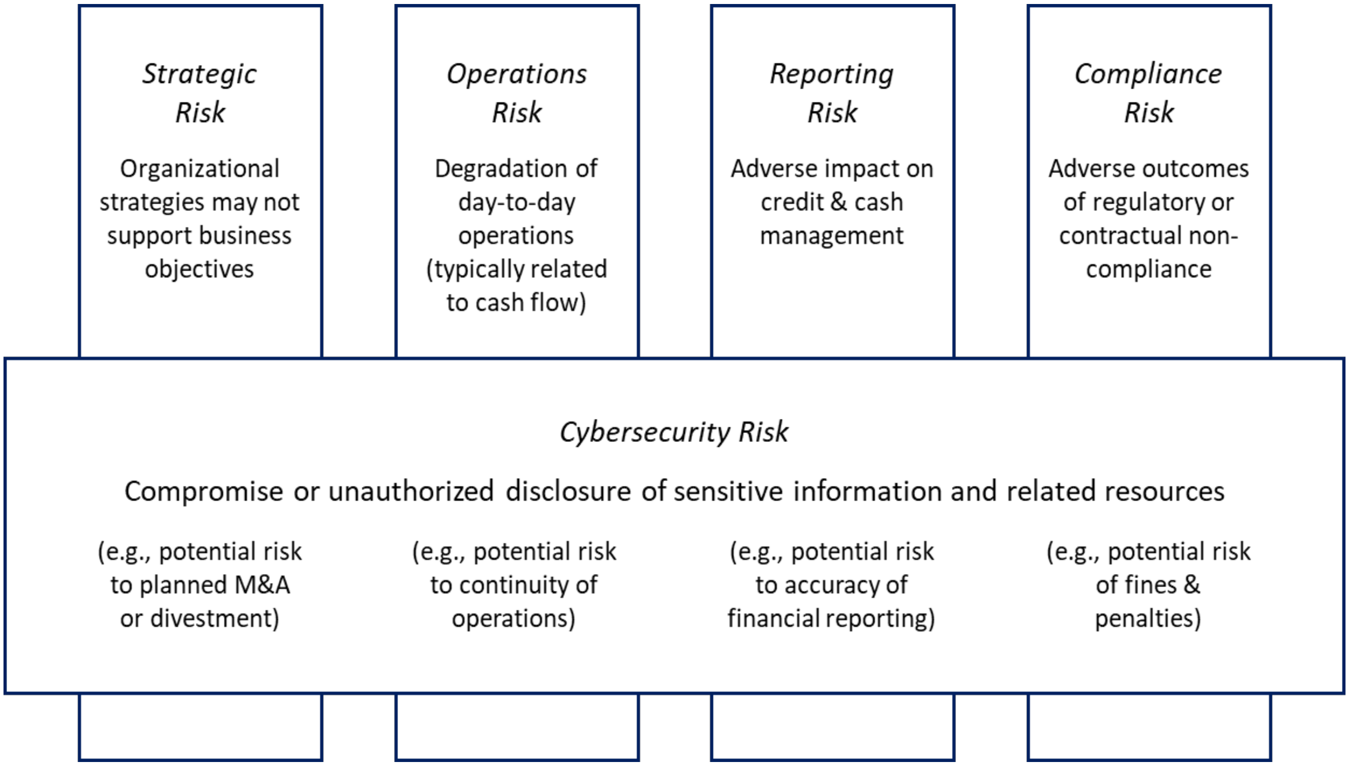
Cybersecurity Risk Management

Although ostensibly intended for U.S. Federal Agencies, NIST provides excellent guidance on how to manage cybersecurity risk that is also applicable to private sector organizations. For example, NIST SP 800-39 provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, and other organizations resulting from the operation and use of information systems. It also provides a structured, yet flexible approach for managing information security risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.[47]

Cybersecurity in Enterprise Risk Management (ERM)

Cybersecurity risk is often managed independently of other types of business risk due to generally dissimilar oversight and reporting requirements;[48] however, it is generally in the best interest of an organization to manage all business risk holistically as part of a broader ERM program, which will help 'min-max' its return on investment and reduce strategic, operations, reporting, and compliance risk, as shown in Figure 4.[49]

Figure 4. Relating Cybersecurity Risk to Other Forms of Business Risk


Strategic Risk
Organizational strategies may not support business objectives
Operations Risk
Degradation of day-to-day operations (typically related to cash flow)
Reporting Risk
Adverse impact on credit & cash management
Compliance Risk
Adverse outcomes of regulatory or contractual non-compliance
Cybersecurity Risk
Compromise or unauthorized disclosure of sensitive information and related resources
(e.g., potential risk to planned M&A or divestment)
(e.g., potential risk to continuity of operations)
(e.g., potential risk to accuracy of financial reporting)
(e.g., potential risk of fines & penalties)

Subsequently, organizations should ensure they identify, evaluate, and communicate cybersecurity risk in the same way other business risks are communicated to senior decision makers. In addition to developing a specific plan of action to address control gaps, organizations should also track associated risks in one or more cybersecurity risk registers, which in turn should be integrated with other risk registers (e.g., financial, and regulatory compliance) to

[47] JTF TI (2011, Mar). Managing Information Security Risk: Organization, Mission, and Information System View (NIST SP 800-39). Gaithersburg, MD: NIST. Available from https://csrc.nist.gov/publications/detail/sp/800-39/final.

[48] Stine, K., Quinn, S., Witte, G., and Gardner, R. (2020, Oct), p. 2.

[49] Ibid., pp. 42-43.

create an Enterprise Risk Register (ERR).[50] The ERR should then be used to create an enterprise risk profile to help senior decision-makers determine which risks should be addressed, to whom responsibilities should be assigned, and how resources should be allocated.[51] Note the risk profile should be updated whenever the underlying cybersecurity risk registers are updated, e.g., after a risk assessment or when risk responses are completed.[52]

Scoring and Reporting

By leveraging an implementation maturity model such as the one presented by NIST[53] and applying an ordinal scoring model, it is possible to evaluate and score how well an organization achieves the outcomes specified by the NIST Cybersecurity Framework's Core Subcategories based on the aggregate of the controls assigned.[54]

The NIST model uses five levels of implementation maturity (ML), as shown in Table 7.

Table 7. NIST Maturity Levels

ML - Name	Maturity Level - Description
1 – Policies	Does the organization know what it needs to do?
2 – Procedures	Does the organization know how to do it?
3 – Implementation	Has the organization done it?
4 – Test	Does the organization keep track of it and fix it if something goes wrong?
5 – Integration	Is it an integrated practice considered 'second nature' to the organization?

We present two types of maturity scales based on a 'traditional' bell-shaped model and a left-skewed bell-shaped 'academic' model based on similar risk reporting models. Although the traditional model is best used for communicating compliance to external stakeholders, the academic model provides a very intuitive approach to understanding compliance when presented as grades, reminiscent of the model used by the federal government to report security status of federal agencies.

[50] Quinn, S., Ivy, N., Barrett, M., Feldman, L. Witte, G., and Gardner, R. (2021, Nov). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (NISTIR 8286A). Available from https://csrc.nist.gov/publications/detail/nistir/8286a/final.

[51] Stine, K., Quinn, Stephen, Witte, G., and Gardner, R. (2020, Oct), pp. 40-42.

[52] Ibid., p. 17.

[53] Bowen, P. and Kissel, R. (2007). Program Review for Information Security Management Assistance (PRISMA), NISTIR 7358, Wash., DC: NIST. Available from http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf.

[54] It is important to note that 'achievement' is measured in terms of the control requirements the organization states it needs to achieve the outcomes specified by the Framework's Core Subcategories, and those requirements should be based on an appropriate risk analysis.

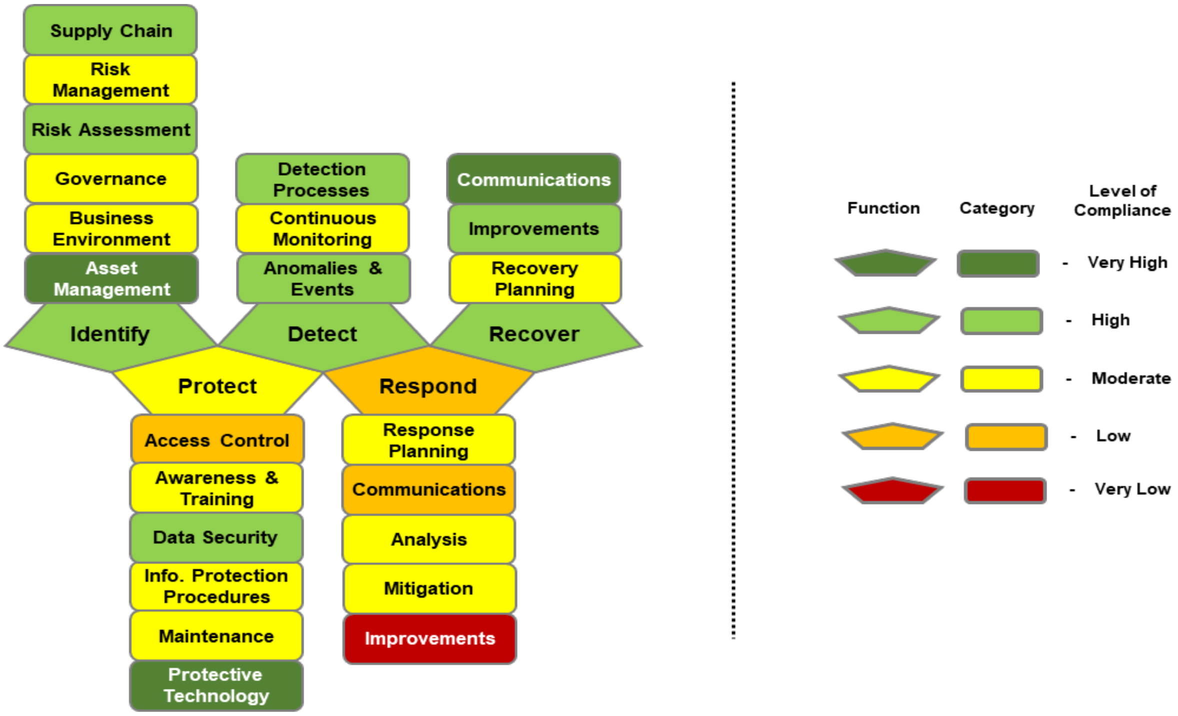
Table 8 below provides the intervals for both models

Table 8. Achievement Scales

'Traditional' Model		'Academic' Model	
Level of Compliance	**Range**	**Level of Compliance**	**Range**
Very High	96-100	'A'	90-100
High	80-95	'B'	80-89
Moderate	21-79	'C'	70-79
Low	5-20	'D'	60-69
Very Low	0-4	'F'	0-59

A manually constructed scorecard based on the NIST Cybersecurity Framework Functions and Categories using a traditional scoring model is provided in Figure 4 on the next page. In this example, specific controls mapped to each of the NIST Cybersecurity Framework's Core Subcategories would have been individually evaluated and scored (potentially using the approach just described), and those scores would be aggregated and averaged according to how they mapped to the Subcategories. The Subcategory scores would then be aggregated and averaged for their 'parent' Categories and reflected as shown in Figure 5. Category scores would be similarly aggregated, averaged, and displayed for their respective Functions.

Figure 5. Example NIST Cybersecurity Framework Scorecard



Corrective Action Plans

Deficiencies or ‘gaps’ in a control’s implementation should be corrected immediately or a Corrective Action Plan (CAP) should be developed that outlines the activities and technology required to remediate the gap.

Step 7: Implement Action Plan

Table 9. Step 7: Implement Action Plan Inputs, Activities, and Outputs

Step 7: Implement Action Plan		
Inputs	Activities	Outputs
1. Prioritized implementation plan 2. Informative Reference(s)	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks using metrics or other suitable performance indicators	1. Project tracking data 2. New security measures implemented

The organization executes the CAP and tracks its progress over time, ensuring that gaps are closed, and risks are monitored. CAPs can be used as the overarching document to track all capital (project) and operational work performed by the organization to address gaps in its Target Profile.

A complete CAP should include, at a minimum, a control gap identifier, description of the control gap, control mapping, point of contact, resources required (dollars, time, and/or personnel), scheduled completion date, corrective actions, how the weakness was identified (assessment, assessor name, date), date identified, and current status.

Note, this step includes the following element of a risk analysis as modified to accommodate use of a control framework: Implement corrective actions and monitor the threat environment.

Implementation Conclusion

This implementation approach can help organizations leverage Informative References to establish a strong cybersecurity program or validate the effectiveness of an existing program. It enables organizations to map their existing program to the NIST Cybersecurity Framework, identify improvements, and communicate results. It can incorporate and align with processes and tools the organization is already using or plans to use.

The process is intended to be continuous, repeated according to organization-defined criteria (such as a specific period or a specific type of event) to address the evolving risk environment. Implementation of this process should include a plan to communicate progress to appropriate stakeholders, such as senior management, as part of its overall risk management program. In addition, each step of the process should provide feedback and validation to previous steps. Validation and feedback provide a mechanism for process improvement and can increase the overall effectiveness and efficiency of the process. Comprehensive and well-structured feedback and communication plans are a critical part of any cybersecurity risk management approach.

Additional Resources to Support Framework Use Goals

The use of the NIST Cybersecurity Framework's Informative References along with other tools and approaches discussed above is an important step that HPH Sector organizations can take to align their cybersecurity programs with existing sector-level goals and guidelines. The approaches below can also be used to increase knowledge and enhance cybersecurity practices. Inclusion of non-federal resources should not imply endorsement by HHS. Use of any of these resources is neither required by, nor guarantees compliance with, federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.

- **Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber Defense:[55]** The Critical Controls for Effective Cyber Defense (the Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses.
- **DHS Cyber Resilience Review (CRR):[56]** The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience and provide a gap analysis for improvement based on recognized best practices.
- **Security Risk Assessment (SRA) Tool:[57]** ONC, in collaboration with the HHS Office for Civil Rights (OCR) developed a downloadable tool to help guide organizations through the HIPAA Security Rule risk assessment/analysis process. The SRA Tool presents a question about an organization's activities for each HIPAA Security Rule standard and implementation specification, and then identifies what is needed to take corrective action for that particular item. Resources for each question help assessors understand the context of the question, consider the potential impacts to ePHI if the requirement is not met, and provides the actual safeguard language The Security Risk Assessment Tool is intended for medium and small providers and is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks of the HIPAA Security Rule. DISCLAIMER: The SRA Tool is provided for informational purposes only. Use of this tool is neither required by, nor guarantees, compliance with federal, state, or local laws. (Note: the information presented may not be applicable or appropriate for all health care providers and organizations.
- **The Health Care and Public Health (HPH) Risk Identification and Site Criticality (RISC)[58] Toolkit** is an objective, data-driven all-hazards risk assessment that can be used by public and private organizations within the HPH Sector to inform emergency preparedness planning, risk management activities, and resource investments. The RISC Toolkit 1.0 contains three self-assessment modules. These allow users to identify external threats and internal hazards specific to their site by using objective national-level data; assess the vulnerability of their site based on industry standards and guidance; and evaluate the criticality of and consequences to their site in the event of an incident. The RISC Toolkit compares multiple facilities across systems, coalitions, and regions to

[55] CIS (2020). CIS Controls®. Available from https://www.cisecurity.org/controls/.

[56] US-CERT (2020a). Assessments: Cyber Resilience Review (CRR). Available from https://www.us-cert.gov/resources/assessments.

[57] Health IT (2020). Security Risk Assessment Tool. Available from http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.

[58] HPH Risk Identification and Site Criticality (RISC) Toolkit 1.0 available from https://www.phe.gov/Preparedness/planning/RISC/Pages/default.aspx.

identify dependencies and interdependencies in a consistent and repeatable method to help create a more resilient health care system. One of the key elements of the RISC Tool is a focus on cyber vulnerabilities.

- **Health Industry Cybersecurity Practices (HICP):**[59] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid health care and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, and resources and templates. The HICP examines cybersecurity threats and vulnerabilities that affect the health care industry. It explores (5) current threats and presents (10) practices to mitigate those threats. Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations discusses the ten Cybersecurity Practices along with Sub-Practices for small health care organizations. Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations does the same for these larger entities. HICP also provides a variety of cybersecurity resources and templates in a separate volume, as well as a HICP Threat Mitigation Matrix intended to help organizations prioritize their cyber threats and develop their own action plans. (As of this writing, the tool is still under development. To receive an advance copy, please contact the developers via email at CISA405d@hhs.gov.)
- **Health Sector Cybersecurity Coordination Center (HC3)**:[60] The Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, health care-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH). Its mission is to support the defense of the health care and public health sector's information technology infrastructure, by strengthening coordination and information sharing within the sector and by cultivating cybersecurity resilience, regardless of organizations' technical capacity. Products developed by the HC3 can be found at www.hhs.gov/hc3.
- **ISO 27799:**[61] ISO 27799:2016 provides technology-neutral implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. By implementing ISO 27799:2016, health care organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity, and availability of personal health information in their care. It applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information should always be appropriately protected. The following areas of information security are outside the scope of ISO 27799:2016:
    - Methodologies and statistical tests for effective anonymization of personal health information;
    - Methodologies for pseudonymization of personal health information (see Bibliography for a brief description of a Technical Specification that deals specifically with this topic);
    - Network quality of service and methods for measuring availability of networks used for health informatics; and
    - Data quality (as distinct from data integrity).

[59] 405(d) (2022). HHS 405(d) Aligning Health Care Industry Security Approaches. Available from https://405d.hhs.gov/.

[60] HHS (2022b). Health Sector Cybersecurity Coordination Center (HC3). Available from www.hhs.gov/hc3.

[61] ISO (2016). Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799: 2016). Available from https://www.iso.org/standard/62777.html.

- **Medical Device and Health IT Joint Security Plan:**[62] The Joint Security Plan (JSP) provides recommendations intended to aid health care organizations (e.g., medical device manufacturers, health IT vendors, and health care providers) in enhancing cybersecurity for their software-based medical technologies (products) irrespective of their size or maturity. It is intended to be globally applicable, inspire organizations to 'raise the bar' for product cybersecurity to meet specific cybersecurity challenges, including but not limited to transparency and disclosure between vendors and end users and security by design throughout the product lifecycle. Specifically, the JSP is a total product lifecycle reference guide to developing, deploying, and supporting cyber secure technology solutions in the health care environment:
  - Cybersecurity practices in design and development of medical technology products.
  - Handling product complaints relating to cybersecurity incidents and vulnerabilities.
  - Managing security risk throughout the lifecycle of medical technology; and
  - Assessing the maturity of a product cybersecurity program.

- **Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM):**[63] The Health Sector Coordinating Council's HIC-SCRiM toolkit is intended for small to mid-sized health care institutions to better ensure the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program that maps to the NIST CSF.

[62] HSCC CWG (2019, Jan). Medical Device and Health IT Joint Security Plan. Available from https://healthsectorcouncil.org/the-joint-security-plan/.

[63] HSCC CWG (2020, Sep).

INFORMING EXISTING SECTOR EFFORTS

This Framework Guidance was developed to be intrinsically backwards compatible, meaning it can be used to enhance the success of existing sector-specific programs and inform sector-level goals and guidelines. The approaches below can be used to increase knowledge and enhance cybersecurity practices; the Framework can make them more effective.

- **Critical Infrastructure Cyber Community (C^3) Voluntary Program:[64]** The Critical Infrastructure Cyber Community (C^3) Voluntary Program was launched in February 2014 in support of Executive Order 13636, which called on the Department of Homeland Security to help organizations use and understand the NIST Cybersecurity Framework. Although no longer active, the US-CERT makes resources related to the former C3 Voluntary Program and the NIST Cybersecurity Framework available on its website.[65]
- **HPH Sector-Specific Plan:[66]** The release of the 2016 HPH Sector-Specific Plan (SSP) reflects the maturation of the HPH Sector public-private partnership, and the progress of the sector programs first outlined in the 2007 and 2010 Sector-Specific Plans (SSPs). Changes from previous SSPs include a streamlined and updated set of goals and objectives and an increased emphasis on priorities such as information sharing and emergency response. The 2016 SSP represents a continued collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to develop specific membership actions over the coming years required to reduce critical infrastructure risk and enhance Sector resilience.
- **NISTIR 8268.[67]** The NIST Interagency Report is intended to help improve communications (including risk information sharing) between and among cybersecurity professionals, high-level executives, and corporate officers at multiple levels. The goal is to assist personnel in these enterprises and their subordinate organizations as well as systems owners to better identify, assess, and manage cybersecurity risks in the context of their broader mission and business objectives. This document will help cybersecurity professionals understand what executives and corporate officers need to carry out ERM. This includes, but is not limited to, what data to collect, what analyses to perform, and how to consolidate and condition this discipline-specific risk information so that it provides useful inputs for ERM programs.
- **NIST SP 800-63-3.[68]** These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks (but may be used by other organizations, e.g., for e-prescription of medication). They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.

[64] US-CERT (2014). DHS Announces Critical Infrastructure Cyber Community [C3] Voluntary Program. Available from https://www.dhs.gov/blog/2014/02/12/dhs-launches-c%C2%B3-voluntary-program.

[65] US-CERT (2020b). Resources. Available from https://www.cisa.gov/uscert/resources/assessments.

[66] HHS (2016, May). Health Care and Public Health Sector-Specific Plan. Washington, DC: Author. Available from https://www.phe.gov/Preparedness/planning/cip/Documents/2016-hph-ssp.pdf.

[67] Stine, K., Quinn, Stephen, Witte, G., and Gardner, R. (2020, Oct).

[68] Grassi, P., Garcia, M., and Fenton, J. (2017, Jun). Digital Identity Guidelines (NIST SP 800-63-3). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

CONCLUSION

This document serves as a foundation for how HPH Sector organizations can leverage the NIST Cybersecurity Framework and its supporting Informative References to increase their overall cybersecurity awareness and implement sound cybersecurity programs to protect patient and other sensitive information. Specifically, the guidance in this document can help an organization determine their cybersecurity goals, assess their current cybersecurity practices, or lack thereof, and help identify gaps for remediation.

The NIST Cybersecurity Framework can be accessed from https://www.nist.gov/cyberframework/framework. Additional risk management resources can be downloaded from NIST at https://www.nist.gov/cyberframework/resources or from the US-CERT from https://www.us-cert.gov/related-resources, including those originally developed for the C^3 Voluntary Program.

Additional copies of this document, as well as other Sector implementation guides, are available from the US-CERT Cybersecurity Website at https://www.us-cert.gov/resources/cybersecurity-framework#framework-guidance. For any questions related to this guidance, please contact the HSCC CWG through their contact page at https://healthsectorcouncil.org/contact/.

APPENDIX A – REFERENCE LIST

AICPA (2020a). AICPA. Available from https://www.aicpa.org/about/landing/about.

AICPA (2020b). SOC 2® - SOC for Service Organizations: Trust Services Criteria. Available from https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.

AICPA (2020c). SOC 2 Examination That Addresses Additional Subject Matters and Additional Criteria. Available from https://amsuat.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc2additionalsubjectmatter.html.

Alberts, C. and Dorofee, A. (2002). Managing Information Security Risks: The OCTAVE Approach. Boston: Addison-Wesley Professional.

An Act Incentivizing the Adoption of Cybersecurity Standards for Business, Connecticut Public Act No. 21-119 (2021). Available from https://cga.ct.gov/2021/ACT/PA/PDF/2021PA-00119-R00HB-06607-PA.PDF.

An Act to amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, Pub. Law 116-321. Available from https://www.govinfo.gov/content/pkg/PLAW-116publ321/pdf/PLAW-116publ321.pdf.

Barrett, M., Keller, N., Quinn, S., Smith, M., and Scarfone, K. (2020, Nov). National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers (NISTIR 8278A), Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278A.pdf.

Barrett, M., Marron, J., Pillitteri, V., Boyens, J., Quinn, S., Witte, G., and Feldman, L. (2020, Mar). Approaches for Federal Agencies to Use the Cybersecurity Framework (NISTIR 8170). Gaithersburg, MD: NIST. Available from https://csrc.nist.gov/publications/detail/nistir/8170/final.

Bowen, P. and Kissel, R. (2007). Program Review for Information Security Management Assistance (PRISMA) (NISTIR 7358). Wash., DC: NIST. Available from http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf.

Bundesampt fur Sicherheit in der Informationstechnic, BSI (2021, 1 Feb). IT-Grundschutz-Compendium, Final Draft. Bonn, GE: Author. Available from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf?__blob=publicationFile&v=4.

Chew, E., Swanson, M., Stine, K., Barol, N., Brown, A., and Robinson, W. (2008, July). Performance Measurement Guide for Information Security (NIST SP 800-55 Reision 1). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf.

CIS (2020). CIS Controls®. Available from https://www.cisecurity.org/controls/.

CISA (2021a). Critical Infrastructure Partnership Advisory Council. Available from https://www.cisa.gov/critical-infrastructure-partnership-advisory-council.

CISA (2021b). Critical Infrastructure Cyber Community C3 Protection Program. Available from https://www.cisa.gov/ccubedvp.

CISA (2017, 7 Jul). Executive Order 13800 Update Issue 1. Available from https://us-cert.cisa.gov/eo13800/Issue-1.

Cline, B. (2019, Sep). Risk Analysis Guide for HITRUST Organizations and Assessors. Available from https://hitrustalliance.net/content/uploads/RiskAnalysisGuide.pdf.

Clinton, L. (Ed.) (2020). Cyber-Risk Oversight (Director's Handbook Series). Arlington, VA: National Association of Corporate Directors. Available from http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf.

CM-SEI (2009). CMMI for Services (CMMI-SVC), V1.2, TR CMU/SEI-2009-TR-001, Hanscom AFB, MA: ESC (DoD), p. 23. Available from http://www.sei.cmu.edu/reports/09tr001.pdf.

CNSS (2015, 6 Apr). Committee on National Security Systems (CNSS) Glossary (CNSSI No. 4009). Available from https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

Cybersecurity Information Sharing Act (CISA), Publ. L. 114-113, Division N (2015). Available from https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

DHS (2022). Cybersecurity: Cyber Physical Systems Security. Available from Cyber-Physical Systems and Internet of Things | NIST. Available from https://www.dhs.gov/science-and-technology/cpssec.

DOE (2015). Energy Sector Cybersecurity Framework Implementation Guidance, Version 4 (DRAFT), Wash., D.C.: Author.

Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013). Available from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Exec. Order No. 13800, 3 C.F.R. 22391-22397 (2017). Available from https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Exec. Order No. 14028, 3 C.F.R. 26633-26647 (2021). Available from https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

European Digital SME Alliance (2020). About: Who we are. Available from https://www.digitalsme.eu/about/european-digital-sme-alliance/.

European Digital SME Alliance (n.d.). SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management. Available from https://www.digitalsme.eu/new-sbs-guide-information-security-management-standard-iso27001-made-easy-smes/.

FDA (2022, Nov). Medical Devices: Digital Health Center of Excellence: Cybersecurity. Available from https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

Freund, J. and Jones, J. (2015). Measuring and Managing Information Risk: A FAIR approach. Oxford: Elsevier, Inc.

GAO (2011, Dec). Report to Congressional Requesters: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use (Publication No. GAO-12-92 Critical Infrastructure Protection). Wash., DC: Author. Available from http://www.gao.gov/products/GAO-12-92.

GAO (2016, Aug). Report to the Committee on Health, Education, Labor, and Pensions, U.S. Senate: HHS Needs to Strengthen Security and Privacy Guidance and Oversight (Publication No. GAO-16-771 Electronic Health Information). Washington, D.C: Author, p.35. Available from https://www.gao.gov/assets/680/679260.pdf.

GAO (2018, February). Report to Congressional Committees on Critical Infrastructure Protection: Additional actions are Essential for assessing Cybersecurity Framework adoption (Publication No. GAO -18-211 Critical Infrastructure Protection). Washington, D.C: Author, p.15. Available from https://www.gao.gov/products/GAO-18-211/.

Grassi, P., Garcia, M., and Fenton, J. (2017, Jun). Digital Identity Guidelines (NIST SP 800-63-3). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification regulations text, 45 CFR Pts 160, 162, and 164 (2013, as amended). Available from http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 11-5, U.S. Statutes at Large 123 (2009): 226-279. Available from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

Health IT (2020). Security Risk Assessment Tool. Available from http://www.healthit.gov/providers-professionals/security-risk-assessment-tool .

HHS (2022a). Public Health Emergency: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Available from https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf.

HHS (2022b). Health Sector Cybersecurity Coordination Center (HC3). Available from www.hhs.gov/hc3.

HHS 405d. (n.d.). Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations. Available from https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf.

HSCC CWG (2019, Jan). Medical Device and Health IT Joint Security Plan. Available from https://healthsectorcouncil.org/the-joint-security-plan/.

ISO (2016). Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799: 2016). Available from https://www.iso.org/standard/62777.html.

JTF TI (2012, Sep). Guide for Conducting Risk Assessments, NIST SP 800-30 r1, Wash., DC: NIST, p. 23. Available from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

Keller, N., Quinn, S., Scarfone, K., Smith, M., and Johnson, V. (2020, Nov). National Online Informative References (OLIR) Program and OLIR Uses (NISTIR 8278). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278.pdf.

National Institute of Standards and Technology Act, 15 USC §§ 271 – 286. Available from https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter7&edition=prelim.

NIST (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199). Gaithersburg, MD: Author. Available from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

NIST (2014). NIST Releases Cybersecurity Framework Version 1.0. Available from http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

NIST (2014, Feb 12). Framework for Improving Critical Infrastructure Cybersecurity, Version 1 (Updated 2018, Jan 8). Wash., DC: Author.

NIST (2018, Apr 16). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NIST (2019, Apr). Cybersecurity Framework Online Informative References (OLIR) Submissions (NISTIR 8204), Gaithersburg, MD: Author. Available from https://csrc.nist.gov/publications/detail/nistir/8204/final.

NIST (2019, Sep 13). Cybersecurity Framework: Frequently Asked Questions. Available from http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm.

NIST (2020a). Cybersecurity Framework: Informative Reference Catalog. Available from https://www.nist.gov/cyberframework/informative-references/informative-reference-catalog.

NIST (2020b). Small Business Security Cybersecurity Corner. Available from https://www.nist.gov/itl/smallbusinesscyber.

NIST (2020c). Glossary: Cybersecurity. Available from https://csrc.nist.gov/glossary/term/cybersecurity.

NIST (2020d). Glossary: Risk Assessment. Available from https://csrc.nist.gov/glossary/term/risk_assessment.

NIST (2020e). Glossary: Security Control Assessment. Available from https://csrc.nist.gov/glossary/term/security_control_assessment.

NIST (2020, Jan). National Cybersecurity Online Informative References (OLIR) Program: Guidelines for OLIR Users and Developers (NISTIR 8278), Gaithersburg, MD: Author. Available from https://csrc.nist.gov/publications/detail/nistir/8278/final.

NIST (2021, Dec 8). Cybersecurity Framework: Informative References: What are they, and how are they used? Available from https://www.nist.gov/cyberframework/online-learning/informative-references.

NIST (2022a). National Online Informative References Program. Available from https://csrc.nist.gov/projects/olir/informative-reference-catalog.

NIST (2022b). NIST Risk Management Framework RMF. Available from https://csrc.nist.gov/Projects/risk-management/about-rmf.

NIST (2022c). Cybersecurity Framework: The Five Functions. Available from https://www.nist.gov/cyberframework/online-learning/five-functions.

OCR (2019, Feb) OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement. Available from https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf.

OCR (2021). About Us. Available from https://www.hhs.gov/ocr/about-us/index.html.

OCR (2020, Dec). 2016-2017 HIPAA Audits Industry Report. Available from https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.

ONC (2020). About ONC: What We Do. Available from https://www.healthit.gov/topic/about-onc.

OCR (2022). Resolution Agreements: Resolution Agreements and Civil Money Penalties. Available from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

Ohio Data Protection Act, Senate Bill 220 (2018). Available from https://www.legislature.ohio.gov/legislation/132/sb220/documents.

Paulsen, C. and Toth, P. (2016, Nov). Small Business Information Security: The Fundamentals (NISTIR 7621, Revision 1). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

Ross, R., Pillitteri, V., Dempsey, K., and Riddle, M., and Guissanie, G. (2016, Dec). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171, Revision 2). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf .

Scholl, M., Stine, K., Hash, J., et al. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, NIST SP 800-66 r1, Wash., DC: NIST. Available from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

Small Business Administration, SBA (2020). Available from https://www.sba.gov/.

Small Business Regulatory Enforcement Flexibility Act (SBREFA), Publ. L. 104-121 (1996; as amended by P.L. 110-28, 2007). Available from https://www.congress.gov/104/bills/s942/BILLS-104s942rfh.pdf.

Stine, K., Quinn, S., Witte, G., and Gardner, R. (2020, Oct). Integrating Cybersecurity and Enterprise Risk Management (ERM) (NISTIR 8286). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

The White House (2013, Feb 12). Presidential Policy Directive—Critical Infrastructure Security and Resilience. Available from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/.

US-CERT (2014). DHS Announces Critical Infrastructure Cyber Community [C3] Voluntary Program. Available from https://www.cisa.gov/uscert/announcements/DHS-Announces-Critical-Infrastructure-Cyber-Community-Voluntary-Program.

US-CERT (2020a). Assessments: Cyber Resilience Review (CRR). Available from https://www.us-cert.gov/resources/assessments.

US-CERT (2020b). Resources. Available from https://www.us-cert.gov/resources.

US-CERT (2020c). Resources for Small and Midsize Businesses (SMB). Available from https://www.us-cert.gov/resources/smb.

APPENDIX B – GLOSSARY OF TERMS

Adequate Security

Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [NIST Glossary]

Adversary

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [NIST Glossary]

Analysis Approach

The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated. [NIST Glossary]

Assessment

See Security Control Assessment or Risk Assessment.

Asset

Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). [NISTIR 7693]

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [NIST Glossary]

Availability

Ensuring timely and reliable access to and use of information. [NIST Glossary]

Compensating Security Control

A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. [NIST Glossary]

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST Glossary]

Corrective Action Plan [CAP]

Corrective actions for an issuer for removing or reducing deficiencies or risks identified by the Assessor during the assessment of issuer operations. The plan identifies actions that need to be performed in order to obtain or sustain authorization. [NIST Glossary]

Criticality

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. Note criticality is often determined by the impact to the organization due to a loss of integrity or availability. [NIST Glossary]

Cyber Attack

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. [NIST Glossary]

Cyber Incident

Actions through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident. [NIST Glossary]

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. [NIST Glossary]

Cyberspace

The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. [NIST Glossary]

Cyber Physical System

A system that includes engineered, interacting networks of physical and computational components. [NIST Glossary]

Defense-in-Breadth

A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). [NIST Glossary]

Defense-in-Depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. [NIST Glossary]

Enhanced Overlay

An overlay that adds controls, enhancements, or additional guidance to security control baselines in order to highlight or address needs specific to the purpose of the overlay. See Overlay. Synonymous with Tailored Overlay. [NIST Glossary]

Enterprise

An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management. [NIST Glossary]

Enterprise Risk Management [ERM]

The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures, as necessary. [NIST Glossary]

Enterprise Risk Register

A risk register at the enterprise level that contains normalized and aggregated inputs from subordinate organizations' risk registers and profiles. [NISTIR 8286]

Impact Level

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [NIST Glossary]

Impact Value

The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high. [NIST Glossary]

Incident

An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [NIST Glossary]

Information Security Risk

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk. [NIST Glossary]

Information System

A discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [NIST Glossary] Information systems also include specialized systems, for example: industrial/process control systems, cyber-physical systems, embedded systems, and devices.[NIST SP 800-171, Rev 2]

Information System-Related Security Risk

Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of Information Security Risk. See Risk. [NIST Glossary]

Integrity

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [NIST Glossary]

Likelihood of Occurrence

A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. [NIST Glossary]

Organization

An entity of any size, complexity, or positioning within an organizational structure. See Enterprise. [NIST Glossary]

Overlay

A fully specified set of security controls, control enhancements, and supplemental guidance derived from tailoring a security baseline to fit the user's specific environment and mission. [NIST Glossary]

Plan of Action and Milestones [POAM]

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. Synonymous with Corrective Action Plan. [NIST Glossary]

Processing

Operation or set of operations performed upon [ePHI] that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of [ePHI]. [NIST Glossary]

Quantitative Assessment

A set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment. [NIST Glossary]

Qualitative Assessment

A set of methods, principles, or rules for assessing risk based on non-numerical categories or levels. [NIST Glossary]

Quasi-quantitative Assessment

See Semi-Quantitative Assessment.

Repeatability

The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments. [NIST Glossary]

Reproducibility

The ability of different experts to produce the same results from the same data. [NIST Glossary]

Residual Risk

Portion of risk remaining after security measures have been applied. [NIST Glossary]

Risk Analysis

The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. [NIST Glossary]

Risk Appetite

The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. [NIST Glossary]

Risk Assessment

The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, resulting from the operation of an information system. Part of risk management, risk assessment incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST Glossary]

Risk Assessment Methodology

A risk assessment process, together with a risk model, assessment approach, and analysis approach. [NIST Glossary]

Risk Factor

A characteristic in a risk model as an input to determining the level of risk in a risk assessment. [NIST Glossary]

Risk Management

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [NIST Glossary]

Risk Management Framework [RMF]

A structured approach used to oversee and manage risk. [NIST Glossary]

Risk Mitigation

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [A subset of Risk Response.] [NIST Glossary]

Risk Model

A key component of a risk assessment methodology—in addition to the assessment approach and analysis approach—that defines key terms and assessable risk factors. [NIST Glossary]

Risk Monitoring

Maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions. [NIST Glossary]

Risk Profile

A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks. [NISTIR 8286]

Risk Register

A central record of current risks, and related information, for a given scope or organization. Current risks are comprised of both accepted risks and risks that have a planned mitigation path. [NIST Glossary]

Risk Response

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, or other organizations. See Course of Action. Synonymous with Risk Treatment. [NIST Glossary]

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result. [NIST Glossary]

Scoping

The act of applying scoping guidance, which consists of specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security and privacy controls in the control baseline. [NIST Glossary, adapted from Scoping Guidance]

Scoping Considerations

A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective. [NIST Glossary]

Security Control(s)

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an organization and/or information system(s) to protect information confidentiality, integrity, and availability. [NIST Glossary, adapted]

Security Control Assessment

The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. [NIST Glossary]

Security Control Baseline

A set of information security controls that has been established through information security strategic planning activities intended to be the initial security control set selected for a specific organization and/or system(s) that provides a starting point for the tailoring process. [NIST Glossary]

Semi-Quantitative Assessment

Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. Synonymous with Quasi-Quantitative Assessment. [NIST Glossary]

Tailored Overlay

See Enhanced Overlay.

Tailored Security Control Baseline

A set of security controls resulting from the application of tailoring guidance to the security control baseline. See Tailoring. [NIST Glossary]

Tailoring

The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. Tailoring [NIST Glossary]

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [NIST Glossary, adapted]

Threat Assessment/Analysis

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. [NIST Glossary]

Threat Event

An event or situation that has the potential for causing undesirable consequences or impact. [NIST Glossary]

Threat Intelligence

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. [NIST Glossary]

Threat Scenario

A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. [NIST Glossary]

Threat Source

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [NIST Glossary]

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [NIST Glossary]

Vulnerability Assessment/ Analysis

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [NIST Glossary]

APPENDIX C – NIST CYBERSECURITY FRAMEWORK BASICS

NIST Cybersecurity Framework Structure and Terminology

For an industry, sector, or organization to implement the NIST Cybersecurity Framework one must understand that it relies on existing standards, guidance, and best practices to achieve specific outcomes meant to help organizations manage their cybersecurity risk.[69] The NIST Cybersecurity Framework provides a common language and mechanism to:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improving the management of risk
- Assess progress toward the target state
- Foster communications among internal and external stakeholders

The NIST Cybersecurity Framework is intended to complement rather than replace an organization's existing business or cybersecurity risk management process and cybersecurity program. Instead, organizations should use its current processes and leverage the framework to identify opportunities to improve an organization's management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use the framework as a reference to establish one. In other words, the NIST Cybersecurity Framework provides an overarching set of guidelines to critical infrastructure industries to provide a minimal level of consistency as well as depth, breadth, and rigor of industry's cybersecurity programs.

The NIST Cybersecurity Framework consists of three main components: Framework Core, Framework Implementation Tiers, and the Framework Profile.[70] Each component is designed to strengthen the connection between business drivers and cybersecurity activities. The Core, Tiers, and Profiles represent the key structure of the Framework, which this document frequently references.

Core

The NIST Cybersecurity Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.[71] The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

[69] NIST (2018, Apr 16), p. 2.

[70] Ibid., pp. 4-5

[71] Ibid., p. 2.

The four Core elements are:[72]

1. **Functions:** Functions provide five focus areas that can shape cybersecurity activities at a strategic level for an organization's cybersecurity management. The Functions aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. Although the NIST Cybersecurity Framework leverages the risk management framework (RMF) outlined in NIST's Special Publication 800-series documents, it is different in several respects. The key difference here is that the NIST Cybersecurity Framework Functions categorize cybersecurity requirements using what is essentially an incident management process. The five Functions are:[73]

   - **Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function lay the foundation for effective Framework use.
   - **Protect** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function limits potential cybersecurity events.
   - **Detect** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, enabling the timely discovery of cybersecurity incidents.
   - **Respond** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event.
   - **Recover** - Develop and implement appropriate activities for resilience planning and restore any capabilities or services impaired by the cybersecurity event.[74]

   When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

2. **Categories:** The Framework decomposes Functions into Categories, which are cybersecurity outcomes that closely relate to programmatic needs and specific activities. Categories add an additional layer of specificity within the Core Functions. In the Identify Function for instance, categories include Governance, Business Environment, and Asset Management.
3. **Subcategories:** Subcategories further break down a particular Category into specific outcomes of a technical or management activity. Subcategories also provide a set of results that help support achievement of each Category's outcomes. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
4. **Informative References:** In a general sense, an informative reference, sometimes called a mapping, indicates how one document relates to another document. The National Cybersecurity Online Informative

[72] Ibid., pp. 4-5.

[73] Ibid., pp. 6.

[74] NIST (2022c). Cybersecurity Framework: The Five Functions. Available from https://www.nist.gov/cyberframework/online-learning/five-functions.

References Program[75] is a NIST effort to facilitate subject matter experts (SMEs) in defining standardized online informative references (OLIRs) between elements of their cybersecurity, privacy, and workforce documents and elements of other cybersecurity, privacy, and workforce documents like the Cybersecurity Framework. The OLIR Catalog provides an interface for Developers and Users to view Informative References and analyze Reference Data between various standards and practices commonly used across the HPH and other critical infrastructure sectors.[76]

Implementation Tiers

Implementation tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.[77] Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

Profiles

NIST Cybersecurity Framework Profiles represent outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories.[78] A profile can be characterized as the alignment of standards, guidelines, and practices to the NIST Cybersecurity Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

Refer to the *Framework for Improving Critical Infrastructure Cybersecurity* for more information on the NIST Cybersecurity Framework.

Generic Implementation

Within the HPH Sector, various organizations already have risk management programs of some type with varying levels of maturity. In many cases, organizations' risk assessment activities already align with the NIST Cybersecurity Framework, and implementation is largely a matter of translating elements of current activities and programs to the

[75] Keller, N., Quinn, S., Scarfone, K., Smith, M., and Johnson, V. (2020, Nov). National Online Informative References (OLIR) Program and OLIR Uses (NISTIR 8278). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278.pdf.

[76] NIST (2022a).

[77] NIST (2018, Apr 16), pp. 8-11.

[78] Ibid., p. 11

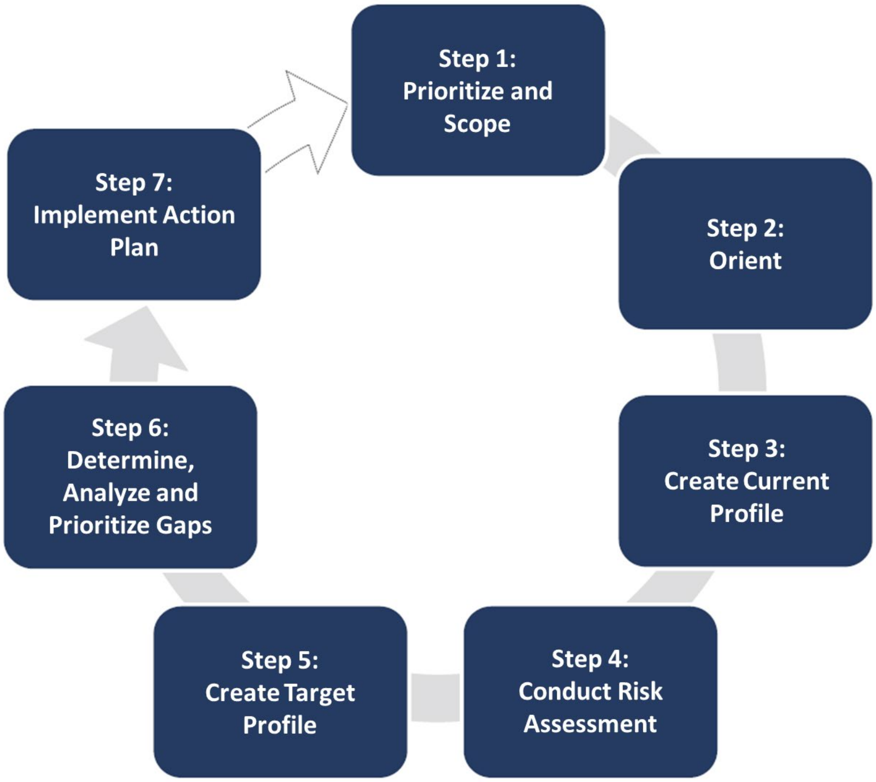
NIST Cybersecurity Framework Core and Implementation Tiers.

NIST recommends using a seven-step process for implementation.[79]

- Step 1: Prioritize and scope organizational components for framework adoption
- Step 2: Identify systems and existing risk management approaches within the scope
- Step 3: Create a current risk management profile (Current Profile)
- Step 4: Conduct a risk assessment
- Step 5: Create a desired risk management profile based on assessment results (Target Profile)
- Step 6: Develop a prioritized action plan of controls and mitigations (Action Plan)
- Step 7: Implement the Action Plan

The diagram provided in Figure 6 on this page shows these steps and the key activities completed within each step. The approach can and should be an iterative process, repeated to address the evolving risk environment.

Figure 6. Generic Implementation Process



[79] Ibid., pp. 13-15

In addition to these steps, implementation should include a plan to communicate progress to appropriate stakeholders, such as senior management, as part of the organization’s risk management program. Each step of the process should provide feedback and validation to previous steps, which can facilitate process improvement and increase the overall effectiveness and efficiency of the process. Comprehensive and well-structured feedback and communication plans are a critical part of any cybersecurity risk management approach.

The following provides additional context, explanation, and guidance from the NIST Cybersecurity Framework document for each step.

Step 1: Prioritize and Scope

The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.[80]

Step 2: Orient

The organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment

The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks along with threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events. This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities.

Step 5: Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization’s desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

[80] For more information on risk tolerance, see NIST (2020, Oct).

Step 6: Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan

The organization determines which actions to take for any existing gaps identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices work best for their needs, including those requirements that are sector or organization specific.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

APPENDIX D – NIST ONLINE INFORMATIVE REFERENCES (OLIR)

In late 2019, NIST began working with members of the NIST Cybersecurity Framework community to create and maintain a more comprehensive Online Informative Reference (OLIR) Catalog[81] to supplement the limited number of Informative References provided in the NIST Cybersecurity Framework document.

The Catalog's Informative References are developed by submitting parties according to NIST Interagency Report (IR) 8278A, *National Online Informative References (OLIR) Program: Submission guidance for OLIR Developers*,[82] and are vetted by NIST for correctness. NIST also works closely with submitters regarding any necessary corrections to these Informative References and hosts links to both public draft and final versions.

Additional information on the NIST OLIR program can be found in NISTIR 8278, *National Cybersecurity Online Informative References (OLIR) Program: Guidelines for OLIR Users and Developers*.[83]

[81] NIST (2020a). Cybersecurity Framework: Informative Reference Catalog. Available from https://www.nist.gov/cyberframework/informative-references/informative-reference-catalog.

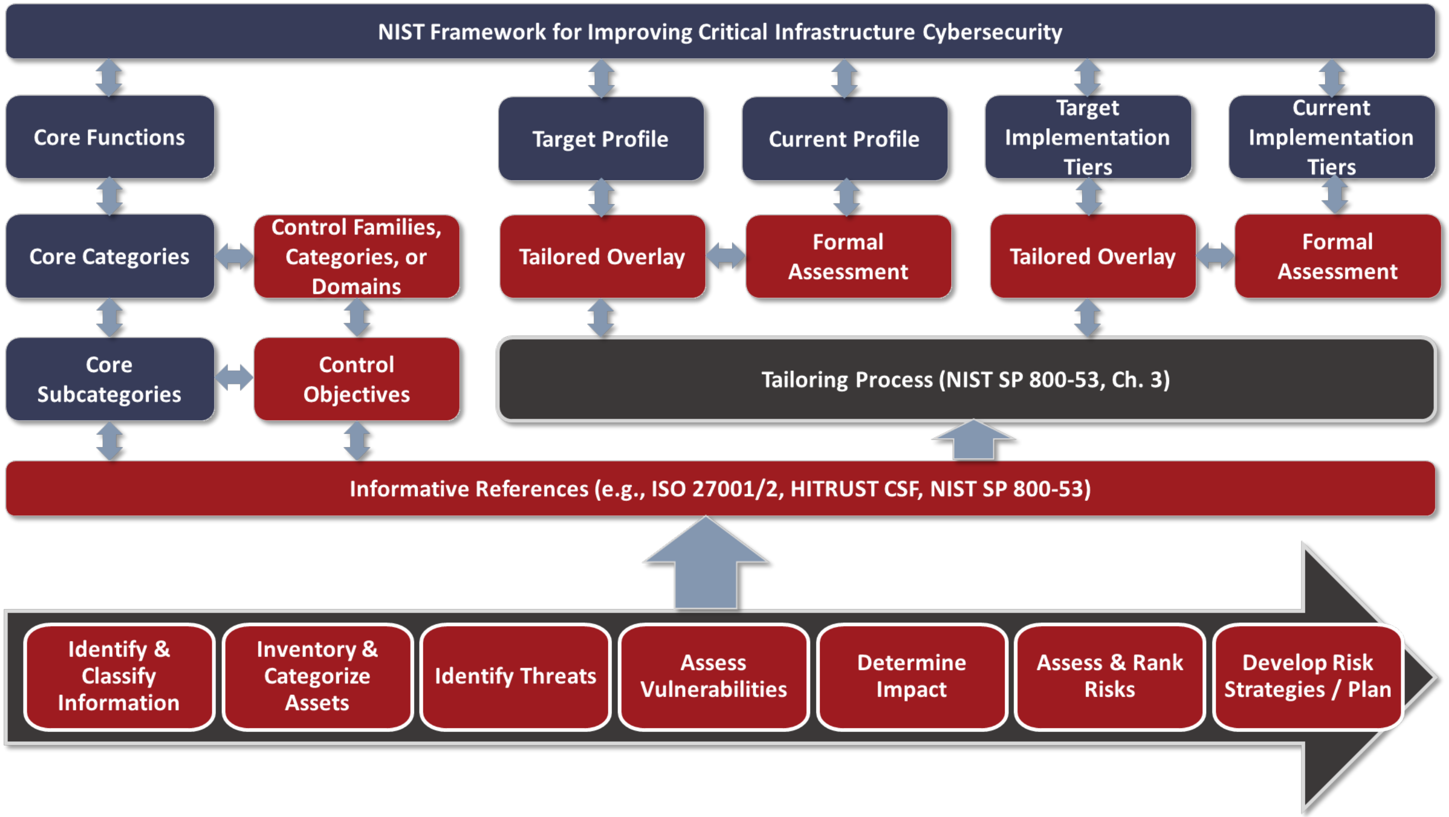
[82] Barrett, M., Keller, N., Quinn, S., Smith, M., and Scarfone, K. (2020, Nov). *National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers* (NISTIR 8278A), Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278A.pdf.

[83] NIST (2020, Jan). National Cybersecurity Online Informative References (OLIR) Program: Guidelines for OLIR Users and Developers (NISTIR 8278), Gaithersburg, MD: Author. Available from https://csrc.nist.gov/publications/detail/nistir/8278/final.

APPENDIX E – HEALTH CARE CYBERSECURITY FRAMEWORK STRUCTURE

The diagram in Figure 6 below is intended to depict the relationship between the underlying Informative References used to support risk analysis and control specification with the NIST Cybersecurity Framework's Core, Profiles, and Implementation Tiers.

Figure 7. Relationship between NIST Cybersecurity Framework and Informative References


NIST Framework for Improving Critical Infrastructure Cybersecurity
Core Functions
Target Profile
Current Profile
Target Implementation Tiers
Current Implementation Tiers
Core Categories
Control Families, Categories, or Domains
Tailored Overlay
Formal Assessment
Tailored Overlay
Formal Assessment
Core Subcategories
Control Objectives
Tailoring Process (NIST SP 800-53, Ch. 3)
Informative References (e.g., ISO 27001/2, HITRUST CSF, NIST SP 800-53)
Identify & Classify Information
Inventory & Categorize Assets
Identify Threats
Assess Vulnerabilities
Determine Impact
Assess & Rank Risks
Develop Risk Strategies / Plan

APPENDIX F – HIPAA SECURITY RULE MAPPING[84]

The sensitive health information maintained by health care providers and health plans has become an increasingly attractive target for cyberattacks. The need for health care organizations to up their game on health data security has never been greater.

To help health care organizations covered by the HIPAA Rules[85] to bolster their security posture, the HHS Office for Civil Rights (OCR)[86] developed a crosswalk[87] with NIST and the Office of the National Coordinator for Health IT (ONC),[88] that identifies "mappings" between the NIST Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework) and the HIPAA Security Rule.[89] The crosswalk also includes mappings to other commonly used security frameworks.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful in identifying potential gaps in their programs. Taking specific action to address these gaps can bolster compliance with the Security Rule and improve an entity's ability to secure ePHI from a broad range of threats. The HIPAA Security Rule is designed to be flexible, scalable, and technology-neutral, which enables it to accommodate integration with more detailed frameworks such as the NIST Cybersecurity Framework. Although the Security Rule does not require use of the NIST Cybersecurity Framework and use of the Framework does not guarantee HIPAA Security Rule compliance, the crosswalk provides an informative tool for entities to use to help them more comprehensively manage security risks in their environments.

In addition, Congress, in both the HITECH Act of 2009[90] as well as the Cybersecurity Information Sharing Act of 2015 (CISA),[91] called for guidance on implementation of NIST frameworks. In response, this crosswalk provides a helpful roadmap for HIPAA covered entities and their business associates to understand the overlap between the NIST Cybersecurity Framework, the HIPAA Security Rule, and other security frameworks that can help entities safeguard health data in a time of increasing risks. The crosswalk also supports and encourages HIPAA Rules covered entities and their business associates to enhance their security programs, increase cybersecurity awareness, and implement appropriate security measures to protect ePHI.

[84] The text for this appendix is an adaptation of the text provided by HHS (2016, Feb 23). Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework. Available from https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html.

[85] HIPAA (2006).

[86] OCR (2021). About Us. Available from https://www.hhs.gov/ocr/about-us/index.html.

[87] HHS (2016, 22 Feb). HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Available from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

[88] ONC (2020). About ONC: What We Do. Available from https://www.healthit.gov/topic/about-onc.

[89] 45 CFR Part 164.

[90] HITECH (2009).

[91] CISA (2015).

APPENDIX G – SUMMARY OF HEALTH CARE IMPLEMENTATION ACTIVITIES

Table 10 consolidates health care implementation activities for all steps in the NIST Cybersecurity Framework implementation process.

Table 10. Health Care Implementation Activities by Step

Implementation Process Steps	Inputs	Activities	Outputs
Step 1: Prioritize and Scope	1. Risk management strategy 2. Organizational objectives and priorities 3. Asset inventory 4. Informative Reference(s)	1. Organization determines where it wants to apply the Informative Reference(s) to evaluate and potentially guide the improvement of the organization's capabilities 2. Threat analysis 3. Business impact analysis 4. System categorization (based on sensitivity & criticality)	1. Usage scope 2. Unique threats
Step 2: Orient	1. Usage scope 2. Risk management strategy 3. Informative Reference(s)	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and other authoritative sources (e.g., cybersecurity and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (e.g., organizational, system, regulatory)
Step 3: Create a Target Profile	1. Organizational objectives 2. Risk management strategy 3. Detailed usage scope 4. Unique threats 5. Informative Reference(s)	1. Organization selects one or more Informative References and creates a tailored overlay based on a risk analysis that considers the unique threats identified in the prioritization and scoping phase 2. Organization determines level of effectiveness or maturity desired in the selected controls	1. Target Profile (Tailored overlay of one or more Informative References) 2. Target Tier

Implementation Process Steps	Inputs	Activities	Outputs
Step 4: Conduct a Risk Assessment	1. Detailed usage scope 2. Risk management strategy 3. Target Profile 4. Informative Reference(s)	1. Perform a risk assessment for in-scope systems and organizational elements	1. Risk assessment reports
Step 5: Create a Current Profile	1. Risk assessment reports 2. Informative Reference(s)	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile (Implementation status of selected controls) 2. Current Tier (Implementation maturity of selected controls, mapped to NIST Cybersecurity Framework Implementation Tier model)
Step 6: Perform Gap Analysis	1. Current Profile 2. Target Profile 3. Organizational objectives 4. Impact to critical infrastructure 5. Gaps and potential consequences 6. Organizational constraints 7. Risk management strategy 8. Risk assessment/analysis reports 9. Informative Reference(s)	1. Analyze gaps between Current and Target Profiles in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) or similar analysis on actions 6. Prioritize actions (CBA or similar analysis and consequences 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan
Step 7: Implement Action Plan	1. Prioritized implementation plan 2. Informative Reference(s)	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks using metrics or other suitable performance indicators	1. Project tracking data 2. New security measures implemented

Table 11 correlates the NIST Cybersecurity Framework implementation process with the elements of a risk analysis that accommodate the use of NIST Cybersecurity Framework Core Informative References.

Table 11. Relationship of Cyber Implementation and HHS Risk Analysis Elements

Cyber Implementation Process	Risk Analysis Elements
1. Prioritize & Scope	• Conduct a complete inventory of where ePHI is processed • Perform a BIA on all systems with ePHI (criticality) • Categorize & evaluate these systems based on sensitivity & criticality
2. Orient	• *Conduct a complete inventory of where ePHI is processed*
3. Create a Target Profile	• Select an appropriate framework baseline set of controls • Apply an overlay based on a targeted assessment of threats unique to the organization
4. Conduct a Risk Assessment	• Evaluate residual risk
5. Create a Current Profile	
6. Perform Gap Analysis	• Rank risks and determine risk treatments • Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process
7. Implement Action Plan	• Implement corrective actions and monitor the threat environment

APPENDIX H – SMALL HEALTH CARE ORGANIZATION CYBERSECURITY GUIDANCE

Industry regulators and standards bodies generally recognize that smaller, resource-constrained organizations do not have the same capability as medium and large enterprises. US legislation requires federal agencies to give special consideration for small businesses around regulatory compliance,[92] and HIPAA in particular allows covered entities and business associates a certain 'flexibility of approach' based on such factors as size, complexity and capability when addressing its standards and implementation specifications.[93]

With respect to standards organizations, NIST provides small business information security guidance[94] in partnership with the U.S. Small Business Administration (SBA)[95] as well as other online resources such as the NIST Small Business Cybersecurity Corner,[96] and HHS provides small and medium business (SMB) guidance[97] as well.

And, through the public-private partnership with the HSCC CWG, HHS jointly developed a cybersecurity publication for health care organizations. The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector[98]. It seeks to aid health care and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, and resources and templates. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP): The HICP examines cybersecurity threats and vulnerabilities that affect the health care industry. It explores (5) current threats and presents (10) practices to mitigate those threats. Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations[99] discusses the ten Cybersecurity Practices along with Sub-Practices for small health care organizations. Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations does the same for these larger entities.

[92] Small Business Regulatory Enforcement Flexibility Act (SBREFA), Publ. L. 104-121 (1996; as amended by P.L. 110-28, 2007). Available from https://www.congress.gov/104/bills/s942/BILLS-104s942rfh.pdf.

[93] HIPAA Administrative Simplification, Regulation Text, 45 CFR Parts 160, 162, and 164 (2013, Mar). § 164.306(b), p. 63. Available from https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

[94] Paulsen, C. and Toth, P. (2016, Nov). Small Business Information Security: The Fundamentals (NISTIR 7621, Revision 1). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[95] Small Business Administration, SBA (2020). Available from https://www.sba.gov/.

[96] NIST (2020b). Small Business Security Cybersecurity Corner. Available from https://www.nist.gov/itl/smallbusinesscyber.

[97] US-CERT (2020c). Resources for Small and Midsize Businesses (SMB). Available from https://www.us-cert.gov/resources/smb.

[98] Stine, K., Quinn, S., Witte, G., and Gardner, R. (2020). Integrating Cybersecurity and Enterprise Risk Management (ERM) (NISTIR 8286). Available from https://csrc.nist.gov/publications/detail/nistir/8286/final

[99] HHS 405d. (n.d.). Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations. Available from https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf.

APPENDIX I – EXECUTIVE MARKETING/SUMMARY TEMPLATE

Cybersecurity – An Increasing Risk

Hackers are increasingly targeting health care organizations to steal information and disrupt operations. Records containing personal, financial, medical and insurance information are among the dark web's most valued records selling for up to $1,000 per record. Health care also suffers from the highest breach cost, with an estimated $408 per record. The question is not if your organization is going to be attacked, it is when.

Today's climate of increasingly sophisticated cyberattacks exploit fragmented hospital infrastructures, impacting hundreds of applications, vulnerable connected medical devices and multiple EMR's, making investment priorities in security approaches extremely complex. This situation can negatively impact patient care, cripple business operations, expose sensitive data and negatively impact a company's reputation and market value. Penalties resulting from non-compliance with regulatory agencies have steadily increased, driving corporate management teams and boards to adapt and improve their approach to cyber governance.

As some health care organizations still struggle to manage a collaborative approach to cybersecurity, they settle for a compliance centric or checklist focused processes, rather than a risk-based approach to cybersecurity. Today, organizations are challenged to coordinate how investments translate into meaningful risk reduction and integrating Cybersecurity and Enterprise Risk Management (ERM), by providing additional detail regarding risk guidance, identification, and analysis. It is increasingly important to illustrate risk tolerance, risk appetite, and methods for determining risks in that context and determine the likelihood and impact of various threat events through cybersecurity risk registers integrated into an enterprise risk profile to help prioritize and communicate enterprise cybersecurity risk response and monitoring.

Reinforcing the need for organizations to take a risk-based approach, in 2020 the HHS Office for Civil Rights (OCR) released the findings of their 2016-2017 HIPAA Rules audits,[100] including the requirements for Risk Management and Risk Analysis. Fully 87% of organizations that underwent a 'Phase 2' HIPAA Rules audit failed to meet its expectations for risk analysis, and that number grows to 93% for risk management.[101] Many times, this is due to organizations settling for compliance centric or checklist focused cybersecurity processes rather than the broader collaborative engagement that should be undertaken in a risk analysis to effectively identify and manage organizational risk, safeguard patient privacy, and protect business value. To be effective in today's constantly evolving threat landscape and compliant with complex regulations, health care organizations must adopt an approach that goes beyond the threats, vulnerabilities, and the controls *du jour*.

[100] OCR (2020, Dec). 2016-2017 HIPAA Audits Industry Report. Available from https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf .

[101] Hales, M. (2017, Oct 8). OCR Audits Reveal Dismal Performance. Available from https://thehipaaetool.com/2017-10-8-ocr-audits-reveal-dismal-results/.

Standing Up a Cybersecurity Program to Reduce Risk

There is mounting pressure on the entire health care ecosystem to improve cybersecurity. Fines, audits, litigation, reputational damage, loss of business and patient safety are powerful catalysts. But fear by itself is no longer the sole motivating factor. Health care executives are beginning to engage cybersecurity from a business and patient safety perspective.

Senior leadership has a crucial strategic role to play regarding cybersecurity. But they can be hampered by their limited understanding of cyber issues, the quality and frequency of the reporting they receive from management, and inadequate governance structures that often hold back key information. Without senior leadership's directive and commitment to an agreed upon enterprise cybersecurity framework, they will lack visibility into the threats and vulnerabilities that may impact the mission of the business, and more importantly, patient safety. Basing the program on a cybersecurity framework can help direct capital, operational, and resource allocations to lines of business generating the greatest return on protecting assets/information and minimizing risk exposure.

Leveraging the NIST Cybersecurity Framework

The Department of Health and Human Services has recommended two voluntary resources to assist health organizations in managing cybersecurity and HIPAA compliance: The *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework)[102] developed by NIST and *Health Industry Cybersecurity Practices* (HICP)[103] developed jointly by the HPH Sector GCC, representing the public sector, and SCC, representing the private sector. The NIST Cybersecurity Framework establishes governance processes to manage cybersecurity through the implementation of an outcome-based risk management framework. HICP offers a practical and focused approach for small, medium, and large organizations to begin addressing their cyber risks and build towards a more comprehensive cybersecurity program. The HICP is mapped to the NIST Cybersecurity Framework, references the crosswalk between the HIPAA Security Rule and the NIST Framework, and provides a Threat Mitigation Matrix that can help users navigate HICP's technical volumes. The HICP Threat Mitigation Matrix is a useful tool to help organizations' IT teams identify the five key cybersecurity threats outlined in the HICP that are most pertinent to the organization and apply controls to mitigate those threats. The controls and sub-controls are categorized based on their applicability to an organization's "size" and mapped to existing NIST CSF Controls.

These documents provide tools that can improve compliance while simultaneously reducing the likelihood and impact of a cyber event. The 2018 HIMSS Cybersecurity Survey showed 58% of health care organizations are leveraging the NIST Cybersecurity Framework.

[102] NIST (2018, Aug 16).

[103] HHS (2022b). Public Health Emergency: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Available from https://405d.hhs.gov/Documents/HICP-Main-508.pdf.

The NIST Cybersecurity Framework can be thought of as a three-legged stool:

- The framework articulates what you are going to do
- The process specifies how you are going to do it
- The maturity model fosters continuous process improvement

The Core of the NIST Cybersecurity Framework is based on a hierarchy of: Functions, Categories and Subcategories. The Functions are broken into 5 key areas, as shown by Table 12 on the following page, which resemble a typical incident response process:

Table 12. NIST Cybersecurity Framework Core Functions

Functions		
ID	Identify	What assets need protection?
PR	Protect	What safeguards are available?
DE	Detect	What techniques can identify incidents?
RS	Respond	What techniques can contain the impact?
RC	Recover	What techniques can restore capabilities?

Below are some of the top business reasons to consider implementation of the NIST Cybersecurity Framework. While nothing is guaranteed, implementation could potentially result in

- Breach Risk Reduction
- Improve Patient Safety
- Increased Compliance
- Civil Litigation Penalties
- Decrease Medical Liability Rates
- Protect Customer Base
- Avoid Fines and Penalties
- M&A Considerations
- Impacting Credit Ratings
- Detailed Documentation
- Reasonableness Standard in Court

Leveraging the NIST Cybersecurity Framework is in alignment with the NACD Director's Handbook on Cyber-Risk Oversight. The NACD provides 5 key issues to take up with an organization's Board of Directors.

1. Approach cybersecurity as part of ERM;[104]
2. Understand the legal implications of cyber particular to one's unique organizational circumstances, to include reporting and disclosure;
3. Engage cybersecurity expertise both internally and externally;
4. Directors need to set expectation that an enterprise cyber risk management framework should be adopted and adequately staffed and budgeted; and
5. Board member discussions should include identification of cyber risk and which risks to accept, mitigate, transfer, and avoid.

Summary

Organizations need a practical approach for addressing cybersecurity challenges. Boards and Executive Steering Committees want better insights into how cybersecurity management decisions are made and often complain of getting briefed with technobabble and operational security metrics instead. Too often a business unit's ownership of risk is nominal, and security responsibility is effectively left with the organization's cybersecurity team. The NIST Cybersecurity Framework bridges the communications divide to improve leadership's oversight and engages individuals at all levels in defining maturity level targets, common nomenclature, and complex cybersecurity decisions to effect measurable outcomes.

[104] For more information on integrating cybersecurity into an organization's ERM program, see NIST (2020, Oct).

APPENDIX J – COMMUNICATIONS PLAN – TEMPLATE

Purpose

This appendix is provided to help health care organizations develop an effective and efficient communications plan and intent is to ensure proper facilitation amongst multiple stakeholders, e.g., the board of directors, executive leadership, business units and technical staff.

Scope

This Communications Plan provides communications strategies, core messages, and performance measures organizations can use for their cybersecurity awareness, implementation, and continual service improvement.

Objectives

There are six objectives for a health care organization's communications around information security.

1. Ensure accurate, cohesive, and frequent messages are delivered in plain language to audience segments.
2. Develop awareness of cybersecurity efforts and encourage active participation and show the benefits (corporate, organizational and employee) – and demonstrate the value of cybersecurity.
3. Identify the tools available to communicate to all audiences, develop a schedule for communications; and define specific guidelines for submitting content.
4. Provide management information necessary to support effective communications.
5. Ensure that resources provide effective information on training, current progress of the Initiative, and best practices to promote improved quality service management.
6. Provide feedback on the level of customer satisfaction, suggested corrective and preventive actions, lessons learned, security incidents response, and specific ideas for improving the quality of service.

Roles and Responsibilities

Table 13 provides the responsibilities for two principal roles in communications.

Table 13. Roles and Responsibilities

Role	Responsibilities
Chief Information Officer **(CIO)**	• Serves as the Information Security champion • Updates the Executive Leadership Team and Board of Directors, as needed • Demonstrates a commitment to and strong support for Information Security initiatives • Acts as an advocate for standardized policies, processes, and procedures • Resolves and escalates Information Security issues as appropriate • Approves and manages Information Security program resources

Role	Responsibilities
Chief Information Security Officer **(CISO)**	• Manages the Information Security Program • Leads information security initiatives • Establishes standards, templates, workflows, processes, policies, and procedures • Validates compliance with regulatory and legal requirements for information security • Develops the communications plan for information security initiatives • Determines appropriate internal and external communications and helps facilitate those communications • Communicates the availability of artifacts, training and guidelines required for secure quality service delivery • Makes sure all communications are accurate and timely, and delivers messages in plain language to targeted audiences using appropriate media

Audience

To effectively communicate the Information Security Program and its initiatives, it is important to tailor the messages to the appropriate audiences (all involved parties), which includes the Leadership Team, vendors, suppliers, and customers.

The information required by these audiences will vary in focus and level of detail. The Security Officer must consider each audience's unique interests and perspectives on issues when developing communications.

There are four phases to achieving effective communications dealing with the rollout and acceptance of information security initiatives.

1. Develop interest and awareness
2. Educate audiences on the value of having a security framework.
3. Create a desire to adopt quality service management methodologies, processes and frameworks and actively participate in the security activities
4. Institutionalize the need for standardized policies, processes, procedures, and measures to improve service delivery and customer satisfaction

Communication Phases of Implementation

For communication to be effective, it must satisfy the specific needs of all involved parties and the target audience(s) in particular. As individual or group needs vary over time, so must the communications. The 'Initiative Phases' outlined above represent stages when fundamental changes in perception occur for some or all stakeholder groups. 'Communication Phases' directly relate to these Initiative Phases.

Table 14 summarizes the areas of concern or interest during each of the Communications Phases lists the communication goals for each phase.

Table 14. Phased Communication Goals

Phase	Anticipated Areas of Concern or Interest	Communication Goals
1. Planning and Preparation	• Unclear about the implications of the security Initiatives • Unaware of the standards and their benefits • Confused as to role in effort and level of change • Concern regarding impact to the organization and initiatives (cost, schedule, and time) • Concern about how changes will impact their work and ability to successfully carry out their assigned tasks • Uncertain about the anticipated changes in business policies, processes, and procedures	• Introduce security standards • Set expectations for what is to come • Seek and act on feedback from target audiences • Develop communication vehicles • Communicate management commitment • Communicate vision for the future • Define parameters of change and initiative scope • Articulate timeline and activities • State compelling reasons for initiative • Enlist support and participation • Identify and empower champions • Share Initiative progress
2. Implementation	• Realization of the impact of security activities on resources and timelines • Staff concern over personal impact • Uncertain of new skill requirements • Rising negativity due to changes and work required to meet Initiative objectives • Need for details about ISMS and what it means for their domain • Concern over impacts of security on operations • Availability and effectiveness of training	• Share initiative progress • Set the expectation for work ahead • Provide guidance and assistance for all initiative activities • Seek and act on feedback from target audiences • Motivate towards the end goal • Reinforce benefits including access to additional business and personal opportunities • Outline phased approach and progress milestones • Recognize champions • Celebrate the current successes • Provide more detail on what change will mean to the different target audiences • Provide updates on constraints and accomplishments • Emphasize available training and support

Phase	Anticipated Areas of Concern or Interest	Communication Goals
3. Validation	• Impatient about the outcome • Apprehensive because things are not perfect the first time • Learning new skills • Recognition of personal benefits • Business benefits understood • Fear of business and personal impact • Apprehensive regarding customer acceptance of changes • Anxiety over internal and external assessment and assessment requirements • Relief when "it works" as perceived following initial assessments	• Share Initiative progress • Set realistic expectations for change • Focus on successes • Continue to communicate timeline • Assess preparedness • Provide training on the tools and methodologies that will be used • Familiarize target audiences with assessment process and expectations • Reinforce training and support availability • Share lessons learned • Seek and act on feedback from target audiences • Celebrate milestones
4. Continual Service Improvement	• Apprehensive over continuous assessment of work and work products • Impatience regarding continual service improvement activities	• Communicate individual contribution to the quality service management • Communicate successes including increased business opportunities and customer satisfaction • Seek and act on feedback from target audiences • Solicit input regarding service improvement and lessons learned • Share lessons learned • Re-emphasize benefits, training, and access to guidance and assistance to facilitate service improvement and "maintaining the gain"

Core Messages and Vehicles

The core message concepts are reinforced with targeted audiences through selected communication activities and vehicles. Core messages are tailored to the audience's role in a successful implementation of security and support ongoing change management objectives. Core messages will be planned for the following targeted audiences:

- Leadership Team
- Customers/Contractors and Suppliers

It is important to communicate core messages through multiple vehicles (tactics) and channels. Vehicles are selected based upon:

- Availability of vehicle
- How effective the vehicle is at reaching audiences?
- The appeal it has to a variety of learning styles
- Individual audience preference

A variety of written and visual communication vehicles, such as newsletters and announcements, e-mails, surveys, and bulletins, plus more personal, two-way vehicles, such as meetings and briefings to various groups should be included. A mechanism allowing the audience to ask questions and receive feedback is critical for the security Initiatives.

The following are important guidelines for communications:

- Consistent messaging is always important, especially with a new initiative
- Communications must be ongoing once a new initiative begins
- Recognize that all audiences do not require the same level of detail when receiving the same information

Core Messages for All Audiences

Communicate to *all* audiences, the following core messages:

- Demonstrate organization's commitment to security using a Charter
- Develop interest and awareness in security and the framework selected to achieve it.
- Educate audiences on the value of security; describe the benefits to the organization and the individual
- Create a desire to adopt secure quality service management methodologies, processes and frameworks and actively participate in the security Initiative
- Institutionalize the need for standardized policies, processes, procedures, and measures to improve service delivery and customer satisfaction
- Explain what to do if questions arise regarding security framework, its implementation, rollout, continual service improvement

Core Messages for Leadership Team

The core messages for these audiences focus on team communication and communications with other organizations and individuals involved or interested in security:

- Notify audiences of activities, schedule, progress, successes, artifacts, and events
- Keep team members up to date on all team activities or activities in related programs or initiatives
- Share new ideas, articles, materials related to quality service management and information security
- Review and communicate lessons learned
- Record and review feedback from customers and all involved in or interested in security initiatives
- Emphasize the importance of information security initiatives, training, and awareness
- Detail methods for creating a desire to adopt secure quality service management methodologies, processes and frameworks and actively participate in the security Initiatives
- Reinforce the need to institutionalize standardized policies, processes, procedures, and measures/metrics to improve service delivery and customer satisfaction
- Stress the significance of open communications, matching the communication to the appropriate audience and vehicle

Core Messages for Vendors, Suppliers and Customers

Communicate to vendors, suppliers, and customers the following core messages:

- Announce the results of any information security assessments when applicable
- Describe customer benefits and value of information security by outlining the service improvement and customer focused aspects of relevant information security standards
- Offer options for finding more information about information security and the Information Security Program

Vehicle Selection

A wide range of communications methods or vehicles are available to get information to those who need it, as shown in Table 15. While every vehicle can convey information, some vehicles have greater strengths than others depending on the type of information used.

Table 15. Vehicle Selection

Type of Communication	Possible Vehicle
Internal or external	Corporate communications
Sensitive or restricted material	Email, meeting, one-on-one, paper
Urgent, time critical	Email, meeting, one-on-one
Must reach recipient, a large, targeted audience, and/or be easily understood	Email, paper
Requires dialogue; complex or easily misunderstood	Meeting, conference call, one-on-one
Requires feedback or reply	Email, meeting, teleconference, survey
Large amount of content	SharePoint, Skype Meeting

Type of Communication	Possible Vehicle
Includes special formats	SharePoint, video teleconference, conference call
Large unspecified audience; brief message	SharePoint, survey, email
Team centered	Conference Calls, email, meeting, teleconference, video conference, one-on-one, paper

Table 16 on the next page summarizes the communication tactics that can be used to deliver core messages to targeted audiences, and include the purpose/content of the communications, the intended audience, the timing and frequency of communications, the intended strategy, and responsible party.

Table 16. Communication Vehicles

Vehicle Target	Communication Vehicle	Purpose/Content	Intended Audience	Details	Frequency	Strategy	Responsible Party
All Audiences	*Corporate-wide E-mail*	Framework Announcement Updates	All		Once	Enterprise-wide	
	Web-based Collaborative Platform	Open repository for all project materials, including Processes, workflows, templates, newsletters, contact lists, presentations, and Information Security materials	All employees interested in learning about Information Security Processes		Monitor for updates	Enterprise-wide and targeted	
	Security Training	Information Security Awareness Training	All identified personnel	As scheduled	Initial/Annually	Targeted	
	Security Bulletins	Newsletter announcing successes, activities, items of interest, etc. to be posted to the Portal	All personnel	As scheduled	Ongoing	Corporate-wide and targeted	
Leadership Team	*One-on-One meetings/ conversations*	Two-way exchange on Information Security Initiatives, benefits, and progress (high-level)	Leadership Team	Ongoing	Periodic	Targeted	Executive Sponsor
Customers	*Press Release*	Press Release announcing any applicable Information Security announcements	All	As Applicable	Once	Internal/ External audiences	Communications Team

Vehicle Target	Communication Vehicle	Purpose/Content	Intended Audience	Details	Frequency	Strategy	Responsible Party
Security Assessment Participants	*Templates*	Templates used for Documents	All users	Ongoing	As Needed	Corporate-wide and targeted	Security Officer
	Lessons Learned	Meeting for participants after delivery of critical milestones to discuss what went well, what could have gone better, and what to do differently next time	Assessment Participants	ASAP	As needed	Corporate-wide and targeted	Security Officer
	Post Assessment Reviews	Reviews of assessment outcomes	Assessment Participants	Assessment schedule	As scheduled	Targeted	Security Officer
	E-mail Distribution List	Distribution Lists for targeted communications to be updated frequently and stored on the portal	Assessment Participants	Immediately	Ongoing	Targeted	Security Officer
	SharePoint or Another Repository Platform	Repository for working documents	Targeted	Ongoing	Periodic	Targeted	Security Officer
	Corrective/ Preventive Notification	Notification of service improvement activities (corrective/preventive/non-conformance actions), progress, and status	Assessment Participants	Ongoing	Ongoing	Targeted	Security Officer
	Team Meetings	Forum to share knowledge, status, and to promote coordination	Assessment Participants	Ongoing	As needed	Targeted	Security Officer

Calendar of Events

The tactics listed in this Communication Plan are recommended for all Communications Phases from Planning and Preparation through Continual Service Improvement. This plan is intended to guide the communication effort through the introduction, acceptance, and continual service improvement. It is recommended that a calendar is developed with planned initiatives identified. This will ensure information regarding events will be reviewed and updated periodically.

APPENDIX K – FREQUENTLY ASKED QUESTIONS

Q. Is NIST Cybersecurity Framework implementation a requirement for HPH sector organizations?
A. No, it is voluntary.

Q. Why should I spend the time and effort implementing this framework?
A. See the section, Potential Benefits of Health care's Implementation of the NIST Cybersecurity Framework.

Q. What is the purpose of this guide?
A. The guide is intended to help HPH sector organizations understand and leverage the NIST Cybersecurity Framework's Informative References to support implementation of a sound cybersecurity program that addresses the five core Function areas of the NIST Cybersecurity Framework, ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with their overall information security and privacy risk management activities to the HPH Sector. The guide will also help an organization's leadership to understand NIST Cybersecurity Framework terminology, concepts, and benefits; assess their current and targeted cybersecurity posture, identify gaps in their current programs and workforce, and identify current practices that meet or exceed NIST Cybersecurity Framework requirements.

Q. To what type of organization does this guidance apply?
A. This guide is developed specifically for all HPH sector organizations. However, the NIST framework is not sector specific and can be applied across many organizations.

Q. I am a very small health care organization with few security resources, and this seems like a lot to implement. What can I do?
A. Industry regulators and standards bodies recognize that full implementation of any prescriptive control-based Informative References may be difficult for many small health care organizations. For example, while ISO does not publish its own guidance for small businesses, the European Digital SME Alliance[105] publishes ISO/IEC 27001 implementation guidance for small and medium enterprises (SME).[106] However, NIST does publish its own small business information security guidance[107] in partnership with the U.S. Small Business Administration (SBA)[108] and HHS provides small and medium business (SMB) guidance[109] as well.

Private-public guidance specific to small health care organizations such as physician practices has also been produced and is discussed at more length in Appendix H – Small Health Care Organization Cybersecurity Guidance.

[105] European Digital SME Alliance (2020).

[106] European Digital SME Alliance (n.d.).

[107] Paulsen, C. and Toth, P. (2016, Nov).

[108] SBA (2020).

[109] US-CERT (2020d).

Q. Is the NIST Cybersecurity Framework to be implemented organization-wide or can it be by system/application?
A. The NIST Cybersecurity Framework should be implemented organization-wide; however, controls from one or more Informative References should be tailored and scoped for specific business units and systems/applications (or similar groups of business units and systems/applications) to ensure controls are not specified unnecessarily. In fact, many organizations implement their cybersecurity programs incrementally across their organization and systems/applications over a period of time based on resource (personnel and funding) constraints.

Q. Will there be updates to this guide? If so, how often?
A. Yes, the Joint HPH Cybersecurity WG considers this guide to be a "living" document and subject to update, as needed (e.g., when there are updates to the NIST Cybersecurity Framework), to best serve the health care industry.

Q. If my organization is ISO 27000 certified how does the NIST Cybersecurity compare and/or benefit?
A. An ISO 27000-certified organization will have a mature Information Security Management System in place and should have a basic set of information security controls in place. However, an ISO-certified organization has considerable flexibility in how much risk it is willing to accept; and subsequently the organization may not have implemented an industry-acceptable level of due care. Such an organization's implementation of the NIST Cybersecurity Framework will help ensure it fully addresses the high-level objectives specified by the NIST Cybersecurity Framework's Core Subcategories, and implementation of the NIST Cybersecurity Framework through a tailored control overlay will help ensure the organization meets industry standards for due care and due diligence. See the section, Potential Benefits of Health Care's Implementation of the NIST Cybersecurity Framework for more information.

Q. If I adopt the NIST Cybersecurity Framework, will this ensure full security?
A. No organization is ever "fully secure." However, the NIST Cybersecurity Framework provides high-level guidance for the implementation of an organization's cybersecurity program that will help ensure its comprehensive coverage of information security and privacy; however, the NIST Cybersecurity Framework must be supported by more prescriptive control-based frameworks such as those listed in NIST's Online Informative Reference Catalog[110]. The quality of an organization's cybersecurity program will also depend on other factors, such as the organization's leadership commitment, culture, operational environment, enterprise architecture and available resources (personnel and funding).

Q. How does this Guide compare to other publications?
A. This guide is different in that it shows how a control-based Informative Reference can be used to implement an information protection program fully consistent with and reportable through the NIST Cybersecurity Framework.

Q. What regulatory and legal advantages will this afford?
A. Implementation of the NIST Cybersecurity Framework and the HPH Sector-specific guidance may help support an organization's assertions around meeting a reasonable standard of due diligence and due care with regulators and federal and state judiciaries.

[110] NIST (2020a).

With regard to state-level advantages, the 2018 Ohio Data Protection Act[111] provides a legal safe harbor to covered entities that implement a cybersecurity program[112] … that contains administrative, technical, and physical safeguards for the protection of both personal information and restricted information and that reasonably conforms to the NIST Cybersecurity Framework as well as several other public and private sector frameworks.[113] Ohio was followed by Connecticut in July 2021 with the passage of H.B. No. 6607, An Act Incentivizing the Adoption of Cybersecurity Standards for Business.[114]

Q. How long would it take to fully implement the guidelines outlined in this document?
A. Each organization's cybersecurity resources, capabilities, and needs are different. The time to implement the Framework will vary among organizations, ranging from as short as a few weeks to several years. The Framework Core's hierarchical design enables organizations to apportion steps between current state and desired state that is appropriate to their resources, capabilities, and needs. This allows organizations to develop a realistic action plan to achieve Framework outcomes in a reasonable time frame, and then build upon that success in subsequent activities.

Q. I have hundreds of information systems, some with PHI, some without, do I need to apply this to all systems or only to my major EHRs?
A. The guidance applies to all locations and systems/applications with PHI or any other type of sensitive information that requires similar levels of protection, such as PII, federal tax data, payment card data, corporate financial data, and trade secrets. The organization would simply not apply controls for data types that are not relevant to the business unit or system/application. It is important to note that this statement should not viewed as legal advice regarding the protection of data which has different statutory and regulatory protection mandates. It should also be noted that systems not containing sensitive information can still present risks to the organization and should not be overlooked. Unsecured systems can easily become the “weak link” providing access to a malicious actor or malware that could propagate throughout one’s environment and eventually compromise sensitive information.

Q. This seems like a lot to implement and track, do I need to first implement a GRC tool to track all of this?
A. It depends on the size of an organizations. Small, relatively non-complex organizations with low risk could probably get by with standard office tools such as word processors, spreadsheets, and presentations. However, larger organizations, especially those that are complex and/or have high inherent risks, would benefit from using a GRC-type application early in its cybersecurity program implementation. A good GRC tool will help an organization manage its policies and procedures, controls, control gaps and remediation plans, as well as internal and external reporting requirements. The GRC tool should also support workflow management and provide metrics and dashboards relevant to various stakeholders in the organization (e.g., executive management and the board of directors).

Q. This framework references cybersecurity. Does this mean it only addresses cyber threats or does it apply to an organization’s entire information security program including physical security and insider threats?
A. Actually, the definition of cybersecurity is becoming quite broad. CNSSI No. 4009 defines cybersecurity as:

> *(The) prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication,*

[111] Ohio Data Protection Act, Senate Bill 220 (2018).

[112] Ibid., p. 1.

[113] Ibid., p. 2.

[114] An Act Incentivizing the Adoption of Cybersecurity Standards for Business, Connecticut Public Act No. 21-119 (2021).

> *including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.*[115]

In fact, the DoD has transitioned from the term "information assurance" to the term "cybersecurity."[116] However, there are still some subtle differences. Fortunately, robust Informative References like those listed in NIST's catalog of Informative References[117], provide a complete set of information security controls that address all types of information security threats, not just those traditionally associated with cybersecurity. Therefore, implementing the recommendations in the guide will support a comprehensive as well as robust information protection program. Use of commercial examples should not be construed as HHS endorsement. And readers should refer to NIST OLIR Catalog for further information.

Q. Does NIST offer a certification for organizations that want to demonstrate compliance with the NIST Cybersecurity Framework?
A. NIST does not offer any type of certification for the NIST Cybersecurity Framework; however, commercial, private-sector options are available.

Q. Does the Framework apply to small businesses and, if so, does NIST provide guidance?
A. Yes. The approach was developed for use by organizations that span the largest to the smallest organizations. NIST has a long-standing and on-going effort supporting small business cybersecurity. This is accomplished by providing guidance through websites, publications, meetings, and events. This includes a Small Business Cybersecurity Corner[118] website (https://www.nist.gov/itl/smallbusinesscyber) that puts a variety of government and other cybersecurity resources for small businesses in one site. That includes the FTC's information about how small businesses can make use of the Cybersecurity Framework. Small businesses also may find Small Business Information Security: The Fundamentals (NISTIR 7621 Rev. 1) a valuable publication for understanding important cybersecurity activities. It is recommended as a starter kit for small businesses. The publication works in coordination with the Framework because it is organized according to Framework Functions.

Q. What resources and level of expertise is needed to implement the Framework? What certifications if any exist for IT personnel?
A. The amount and type of financial resources needed to implement the approach outlined in this guide is dependent on the organization's inherent risk and the existing state of its information protection program.

Some organizations may require external support from knowledgeable professionals to implement an efficient and effective cybersecurity program. The authors of this guide concur with HHS' position that provider organizations typically do not have this type of expertise "in house" and we recommend they obtain the necessary expertise from a reputable professional, such as a security consultancy, if it does not have suitable resources available. For example, an evaluation of an entity's security safeguards need not be conducted by an external third-party as an external evaluation could be too costly for a smaller provider.

[115] NIST (2020c). Glossary: Cybersecurity. Available from https://csrc.nist.gov/glossary/term/cybersecurity.

[116] Committee on National Security Systems, CNSS (2015, 6 Apr). Committee on National Security Systems (CNSS) Glossary (CNSSI No. 4009), p. 62. Available from https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf.

[117] NIST (2020a).

[118] NIST (2020b).

Professional certifications include those for general security, such as the Information System Audit and Control Association's (ISACA's) Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) credentials,[119] and the International Information Systems Security Certification Consortium's [(ISC)^2's] Certified Information Systems Security Professional (CISSP) and Information Systems Security Management Professional (CISSP-ISSMP) credentials.[120] Specialized certifications include (ISC)^{2}'s Health Care Information Security and Privacy Professional (HCISPP).

Q. What's the difference between risk assessment and risk analysis?
A. NIST considers the terms synonymous.[121] However, in common usage, risk analysis is often reserved for the HIPAA-required risk analysis as well as more specific or targeted risk analyses, such as those used for the design or selection of alternate (or compensating) controls and risk acceptance. A risk assessment is often used in common practice for the security controls assessment[122] and gap analysis, which are components or activities of the overall risk analysis process.

Q. Are there any other resources I can use to help answer any other questions I may have?
A. Yes. NIST provides a series of Cybersecurity Framework Frequently Asked Questions.[123]

[119] For more information on ISACA security credentials, see ISACA (2020). Credentialing. Available from https://www.isaca.org/credentialing.

[120] For more information on (ISC)2 security and privacy credentials, see ISC2 (2023). Certifications. Available from https://www.isc2.org/certifications.

[121] NIST (2020d). Glossary: Risk Assessment. Available from https://csrc.nist.gov/glossary/term/risk_assessment.

[122] NIST (2020e). Glossary: Security Control Assessment. Available from https://csrc.nist.gov/glossary/term/security_control_assessment.

[123] NIST (2019, Sep 13). Cybersecurity Framework: Frequently Asked Questions**.** Available from http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm