Welcome To The 10th Annual Hacking Conference

Dungeons and Dragons™

InfoSec Master Edition

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Beyond NIST
CMMC Certification
Options and Opportunities

November 7, 2023 | Chicago, IL

The Institute of Internal Auditors Chicago

ecfirst

ISACA Chicago Chapter

FBI

CISO

MSEE

Author

HITRUST® Assessor Council

CMMC & NIST

U.S. DoD

Keynote Speaker

CLEMSON UNIVERSITY

CISSP®

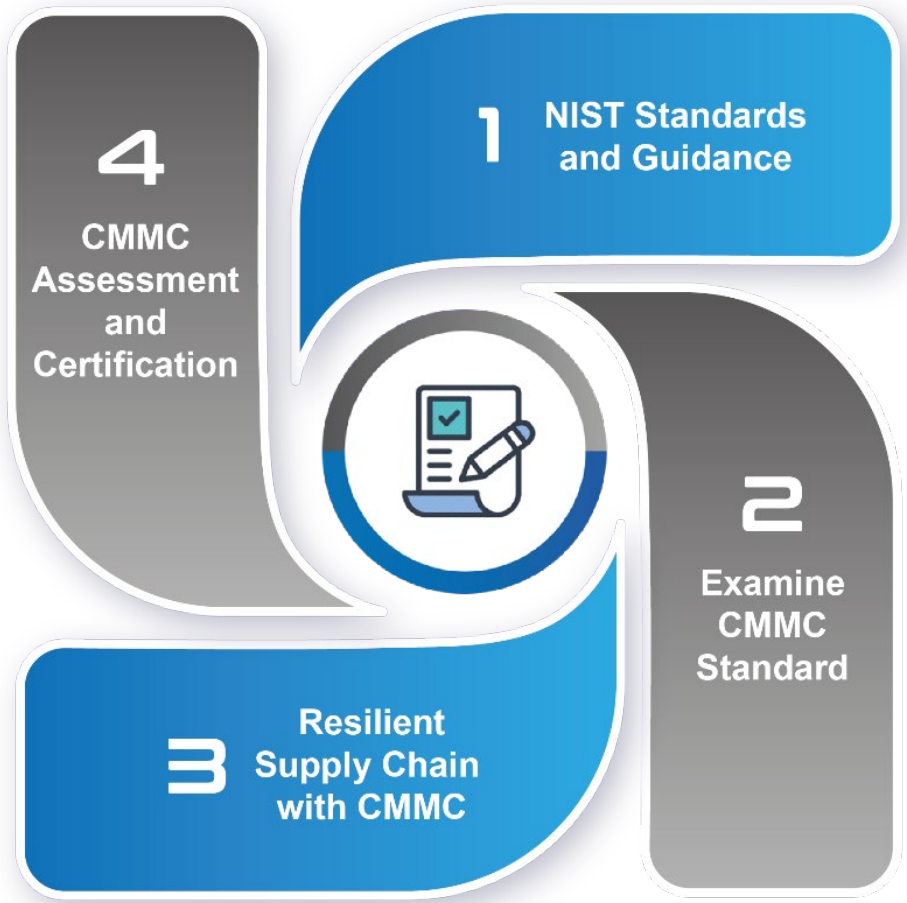
Ali Pabrai

Global Cyber Defense Thought Leader

The Institute of Internal Auditors Chicago

ISACA® Chicago Chapter

Agenda



Learning Objectives

- Learn about NIST standards and guidance, including the NIST SP 800-171r3 Draft
- Examine the CMMC standard and its organization
- Review how to mitigate risks in the cyber supply chain with CMMC
- Step through key phases to successfully achieve CMMC Certification

New AI Tools Could Diagnose the Disease with Visual Scans

THE WALL STREET JOURNAL.

The Future of Everything | Is the Eye the Window to Alzheimer's?

Getting tested for Alzheimer's disease could one day be as easy as checking your eyesight.

The power in AI is that it can help connect the dots.

An AI algorithm that can analyze results from an eye scanner and detect signs of Alzheimer's 20 years before symptoms develop.

The future is bright with AI and Cyber as well!

Future Attacks

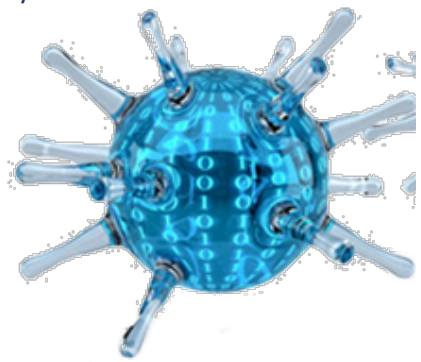
Viruses, Cyber & Biological

THE WALL STREET JOURNAL.

Future Attacks: Viruses, Cyber & Biological

A two-front biological and cyber attack

Hospitals and other critical infrastructure need to harden their cyber defenses.

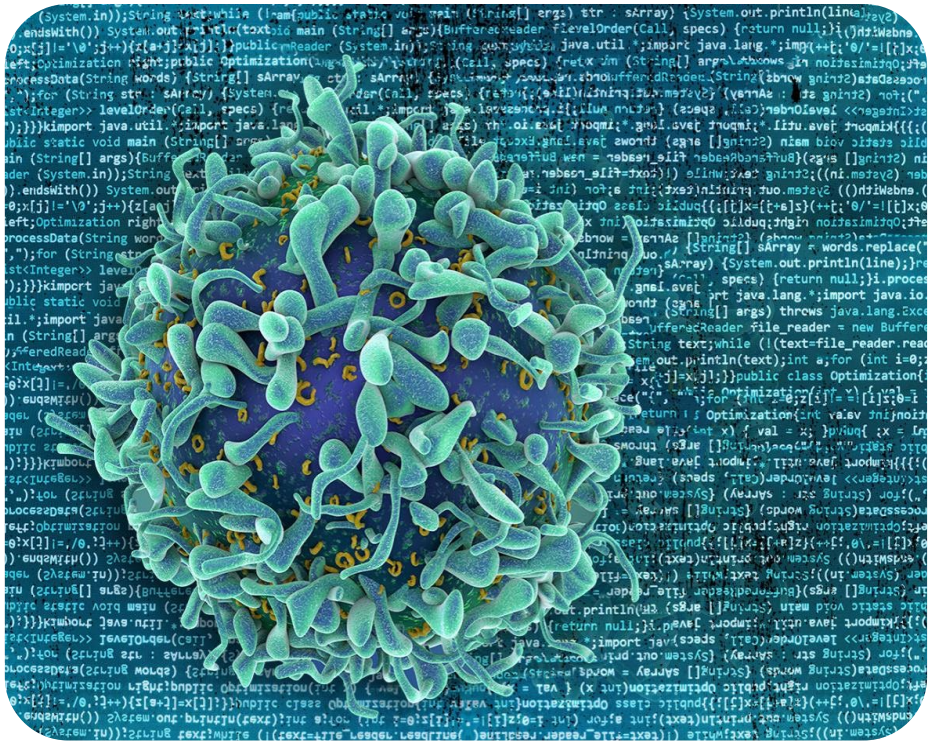


Ransomware could simultaneously target energy grids, power plants, factories, refineries, trains, airlines, shipping, banking, water supplies, sewage-treatment plants and more.

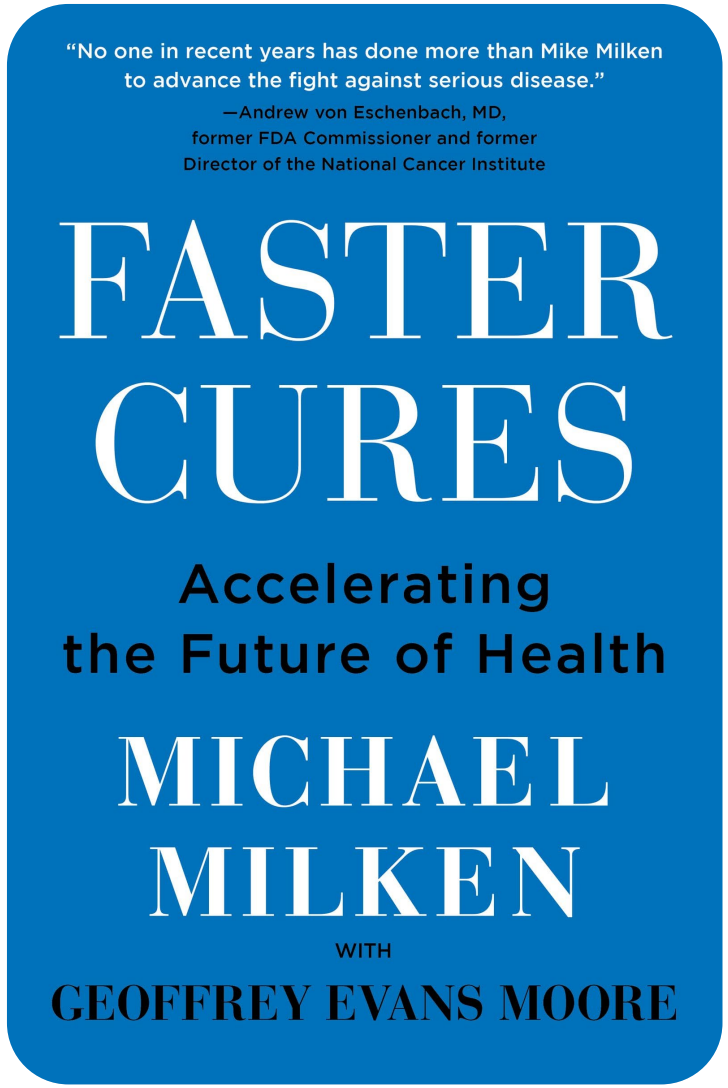
Hospitals would be the most salient targets.

The attacker(s) might falsely claim their own systems are also under siege.

Misdirection can be more effective than a smoke screen.



Dark Past to Bright Future



THE WALL STREET JOURNAL.

Another Medical Revolution Is Under Way

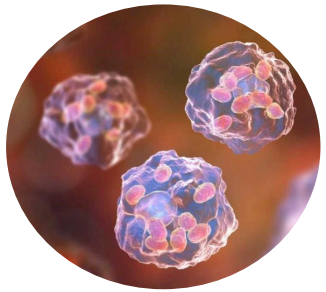
Twenty years ago, the idea of putting a live cell in a human, directing it to travel to a specific location, and having it do a specific task would have been considered impossible.

Today it's reality, and hundreds of companies are working on cell- therapy applications.

What if,

- Cleaning early-stage cancers from your body could become as routine as going to the dentist to clean your teeth
- Or, if a single vaccine could protect you against multiple viruses
- Or if gene editing could eliminate many birth defects and slow the aging process?

These, and many other advances, are within reach.



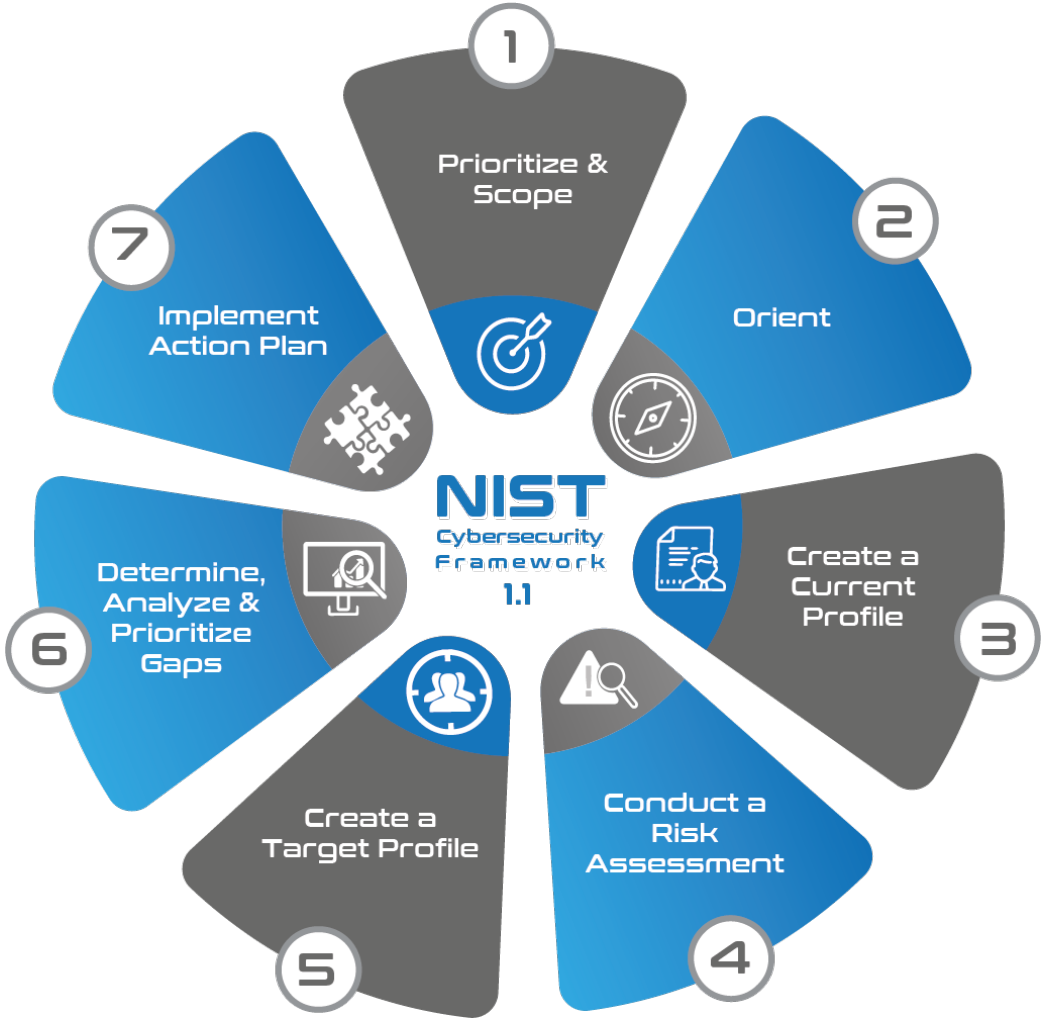
The Institute of Internal Auditors Chicago

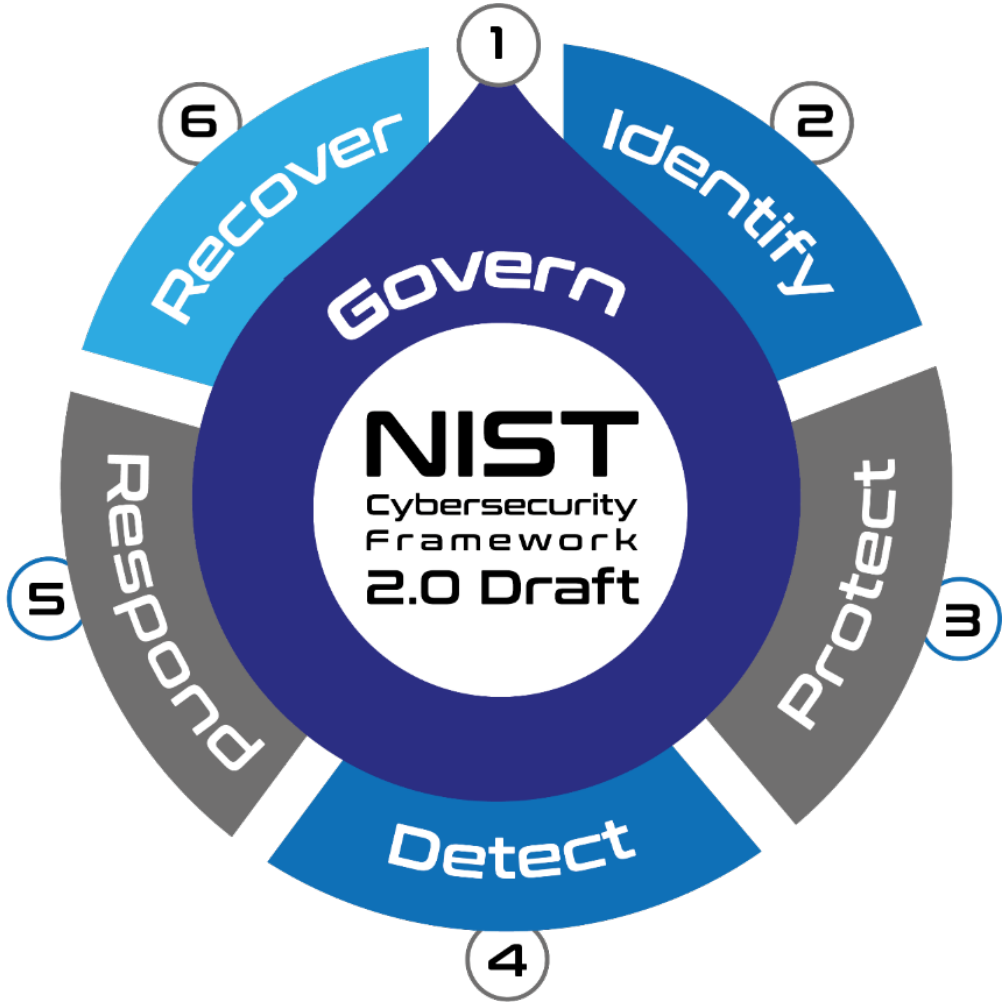
ISACA Chicago Chapter

NIST Standards and Guidance

NIST Cybersecurity Framework

1.1 & 2.0 Draft





The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

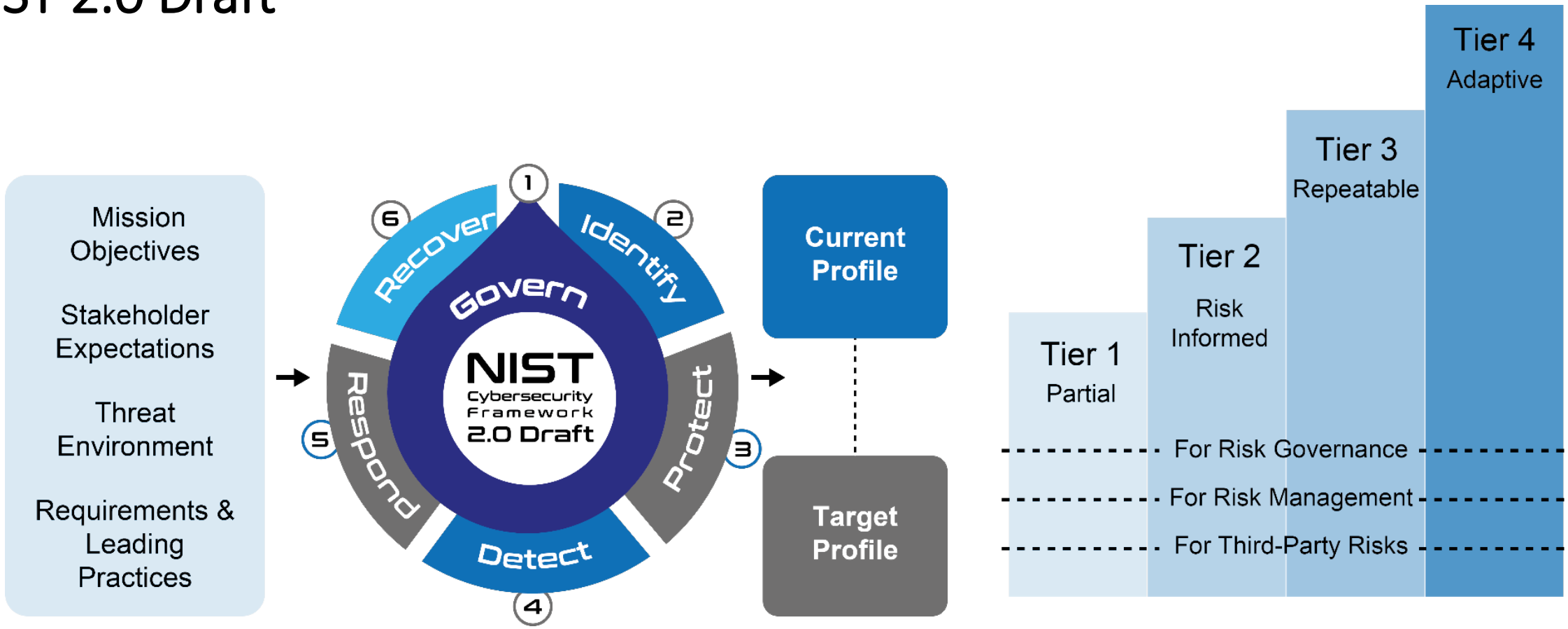
Functions

NIST 2.0 Draft

#	Function	Description	Category
1	**Govern** (GV)	Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy. Provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions.	Organizational Context (GV.OC)
			Risk Management Strategy (GV.RM)
			Roles and Responsibilities (GV.RR)
			Policies and Procedures (GV.PO)
2	**Identify** (ID)	Help determine the current cybersecurity risk to the organization.	Asset Management (ID.AM)
			Risk Assessment (ID.RA)
			Supply Chain Risk Management (ID.SC)
			Improvement (ID.IM)
3	**Protect** (PR)	Use safeguards to prevent or reduce cybersecurity risk	Identity Management, Authentication, and Access Control (PR.AA)
			Awareness and Training (PR.AT)
			Data Security (PR.DS)
			Platform Security (PR.PS)
			Technology Infrastructure Resilience (PR.IR)
4	**Detect** (DE)	Find and analyze possible cybersecurity attacks and compromises.	Adverse Event Analysis (DE.AE)
			Continuous Monitoring (DE.CM)
5	**Respond** (RS)	Take action regarding a detected cybersecurity incident.	Incident Management (RS.MA)
			Incident Analysis (RS.AN)
			Incident Response Reporting and Communication (RS.CO)
			Incident Mitigation (RS.MI)
6	**Recover** (RC)	Restore assets and operations that were impacted by a cybersecurity incident.	Incident Recovery Plan Execution (RC.RP)
			Incident Recovery Communication (RC.CO)

Profile & Tiers

NIST 2.0 Draft



Implementation Examples

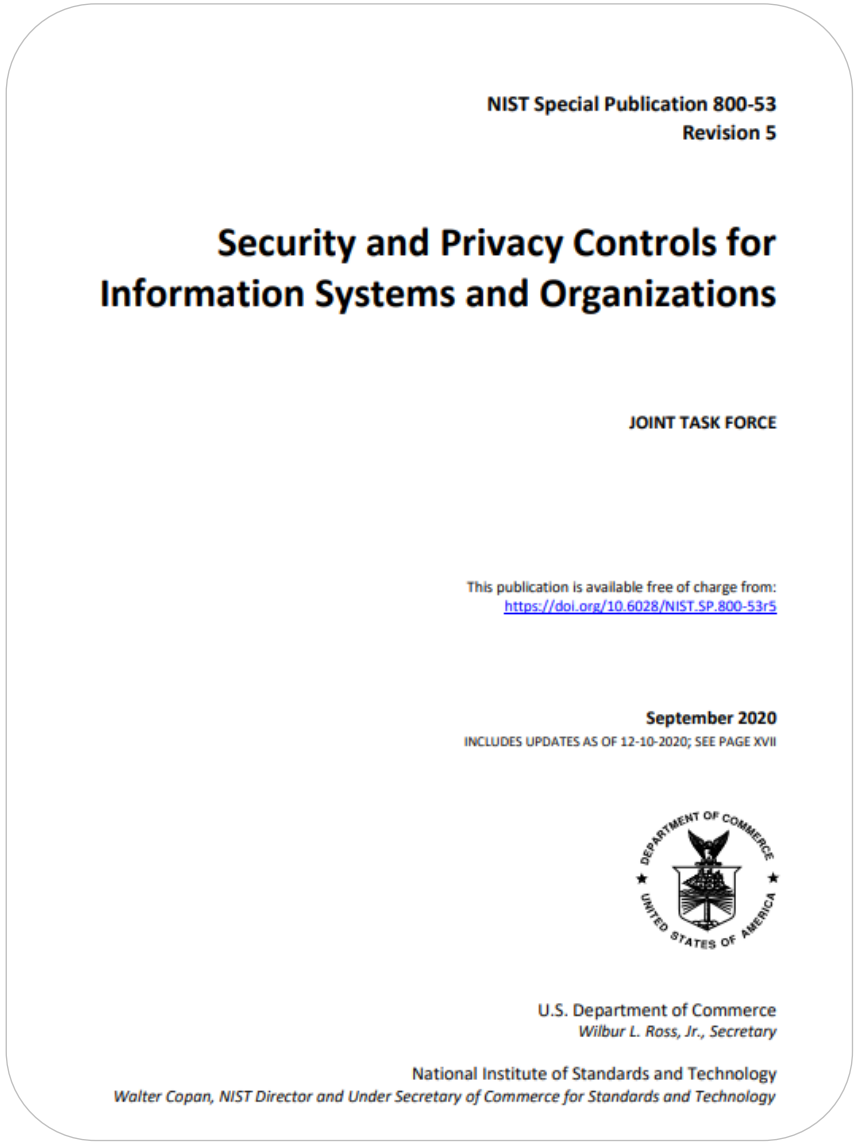
NIST 2.0 Draft

Implementation Examples

- Provide concise, action-oriented steps to help achieve the outcomes of the Subcategories.
- The examples are not a comprehensive list of all actions that could be taken by an organization to achieve an outcome, nor do they represent a baseline of required actions to address cybersecurity risk.

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC) The circumstances — mission, stakeholder expectations, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood (formerly ID.BE)	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)	Ex1: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
Asset Management (ID.AM) Assets (e.g., data, hardware software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	ID.AM-01: Inventories of hardware managed by the organization are maintained	Ex1: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices Ex2: Constantly monitor networks to detect new hardware and automatically update inventories
Identity Management, Authentication, and Access Control (PR.AA) Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access (formerly PR.AC)	PR.AA-03: Users, services, and hardware are authenticated (formerly PR.AC-03, PR.AC-07)	Ex1: Require multifactor authentication Ex2: Enforce policies for the minimum strength of passwords, PINs, and similar authenticators Ex3: Periodically reauthenticate users, services, and hardware based on risk (e.g., in zero trust architectures)

NIST SP 800-53 Rev 5



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

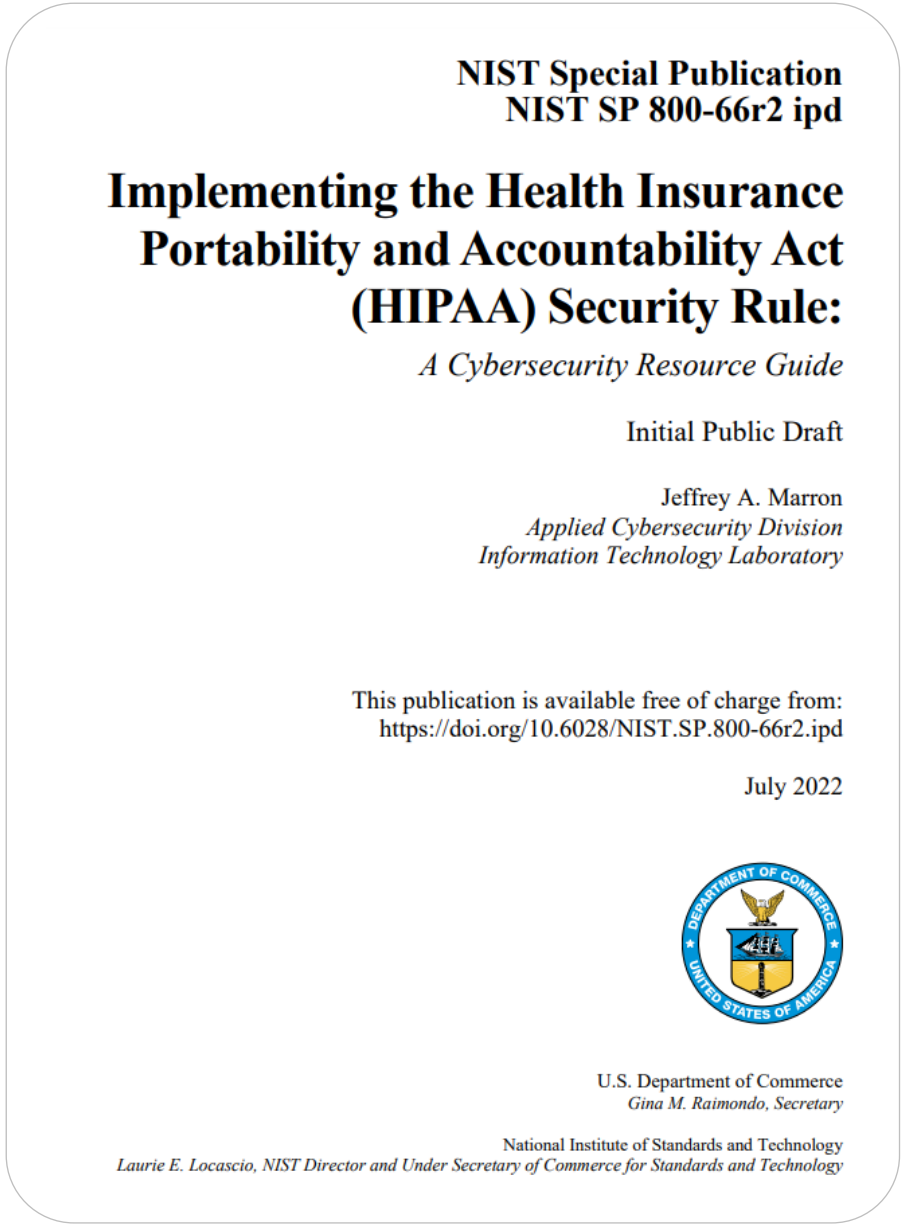
National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

#	Family Name	# of Controls
1	Access Control	25
2	Awareness and Training	4
3	Audit and Accountability	16
4	Assessment, Authorization, and Monitoring	9
5	Configuration Management	12
6	Contingency Planning	13
7	Identification and Authentication	12
8	Individual Participation	6
9	Incident Response	10
10	Maintenance	6

#	Family Name	# of Controls
11	Media Protection	8
12	Privacy Authorization	4
13	Physical and Environmental Protection	22
14	Planning	11
15	Program Management	32
16	Personnel Security	8
17	Risk Assessment	9
18	System and Services Acquisition	22
19	System and Communications Protection	44
20	System and Information Integrity	20

ISACA Chicago Chapter

NIST SP 800-66r2



NIST Special Publication
NIST SP 800-66r2 ipd

Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule:

A Cybersecurity Resource Guide

Initial Public Draft

Jeffrey A. Marron
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-66r2.ipd

July 2022

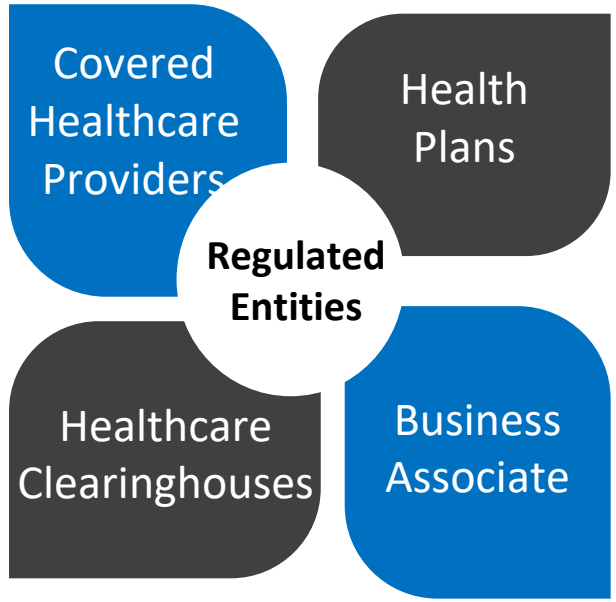
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

- NIST SP 800-66r2 provides practical guidance and resources that can be used by regulated entities of all sizes to protect ePHI and better understand the security concepts discussed in the HIPAA Security Rule.

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and Documentation Requirements

HIPAA Security Rule



ISACA Chicago Chapter

Ransomware Readiness

NISTIR 8374

NISTIR 8374

Ransomware Risk Management:

A Cybersecurity Framework Profile

William C. Barker
Dakota Consulting
Silver Spring, MD

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

William Fisher
Applied Cybersecurity Division
Information Technology Laboratory

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

February 2022

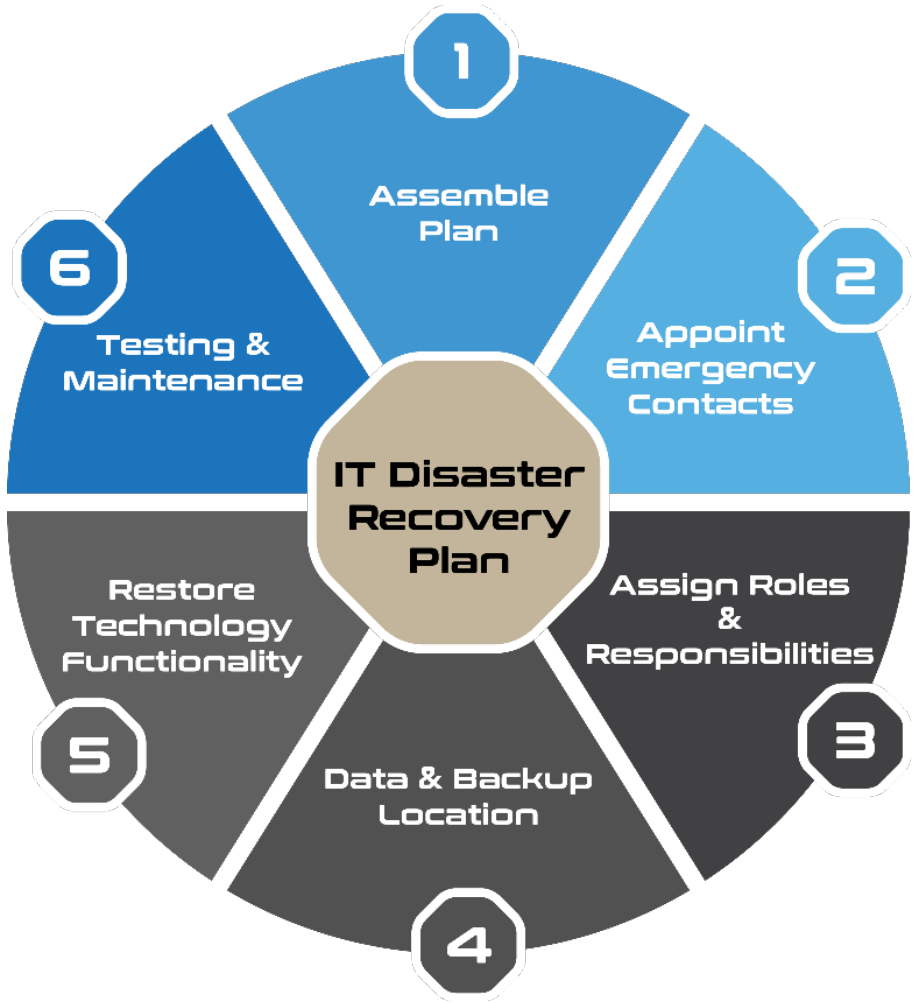
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Table of Contents

ISACA Chicago Chapter

Ransomware Readiness



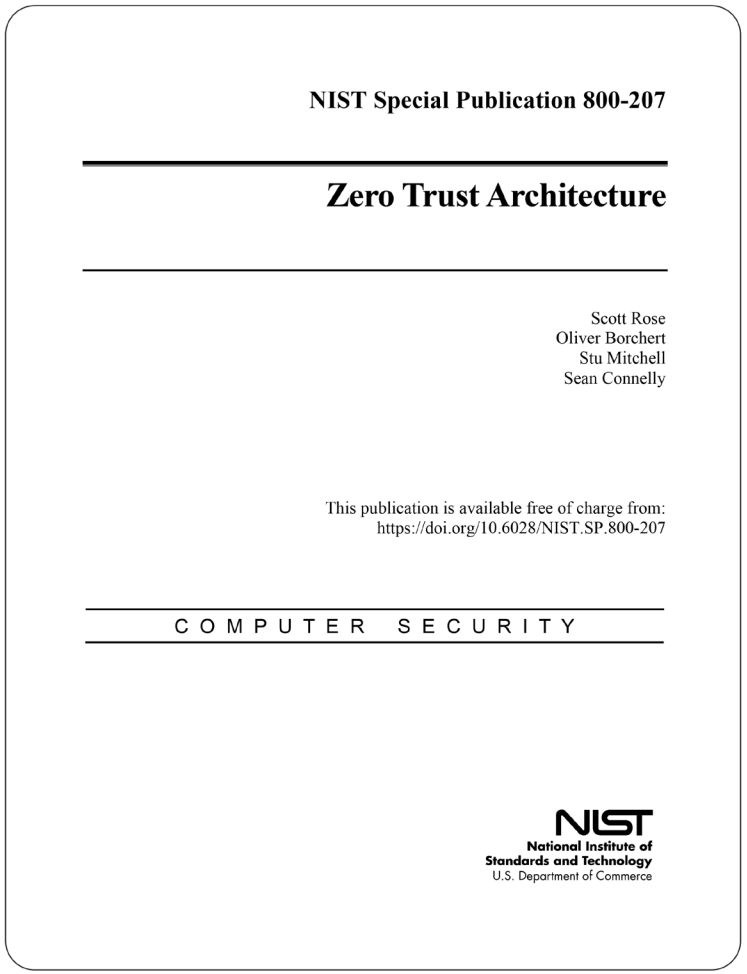
The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

NIST SP 800-207

Zero Trust Architecture

Zero trust is about providing the right user, the right access, to the right data, continuously.


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISACA Chicago Chapter

Zero Trust Facts

1. Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

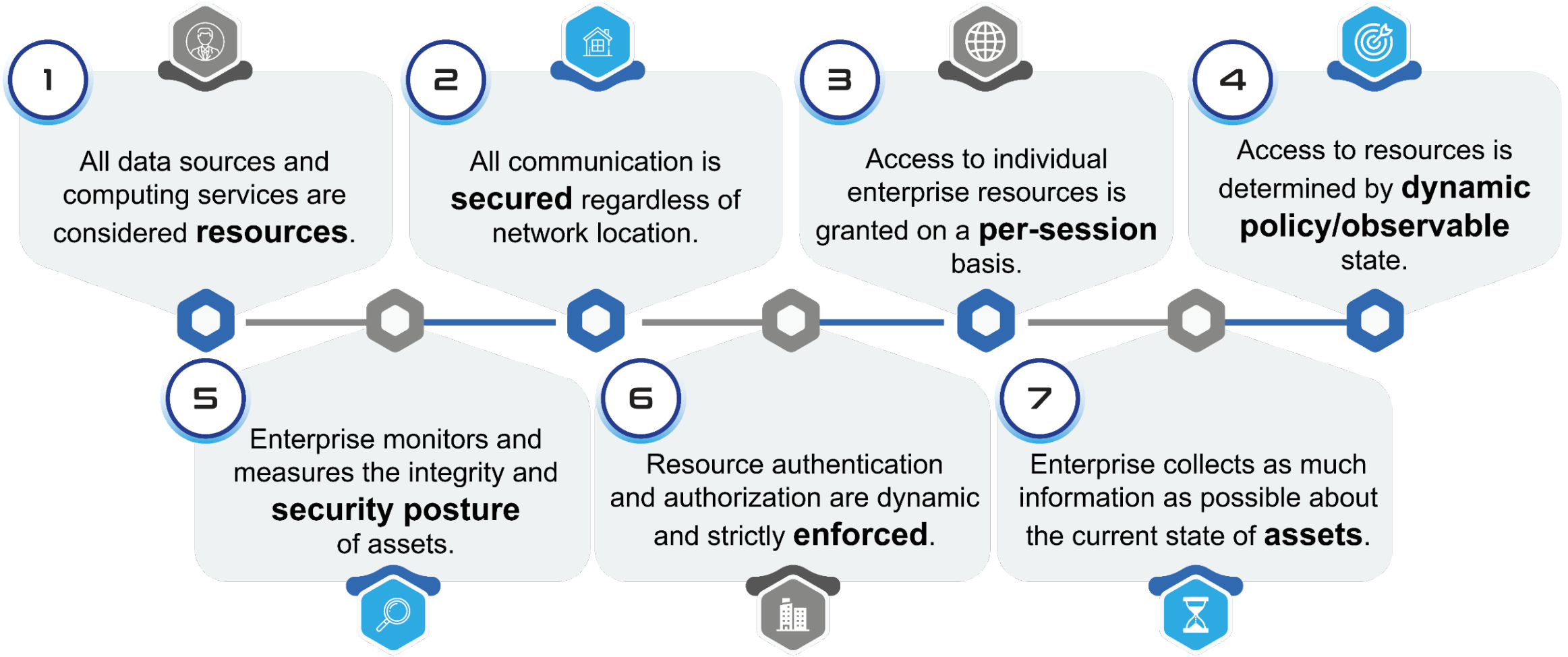
2. Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

3. ZTA is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

4. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.

ZTA
Zero Trust Architecture

Zero Trust Basic Tenets Defined by NIST SP 800-207



NIST SP 800-171 r2

NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
Computer Security Division
National Institute of Standards and Technology

MARK RIDDLE
Information Security Oversight Office
National Archives and Records Administration

GARY GUISSANIE
Institute for Defense Analyses

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

February 2020
INCLUDES UPDATES AS OF 01-28-2021; SEE PAGE X

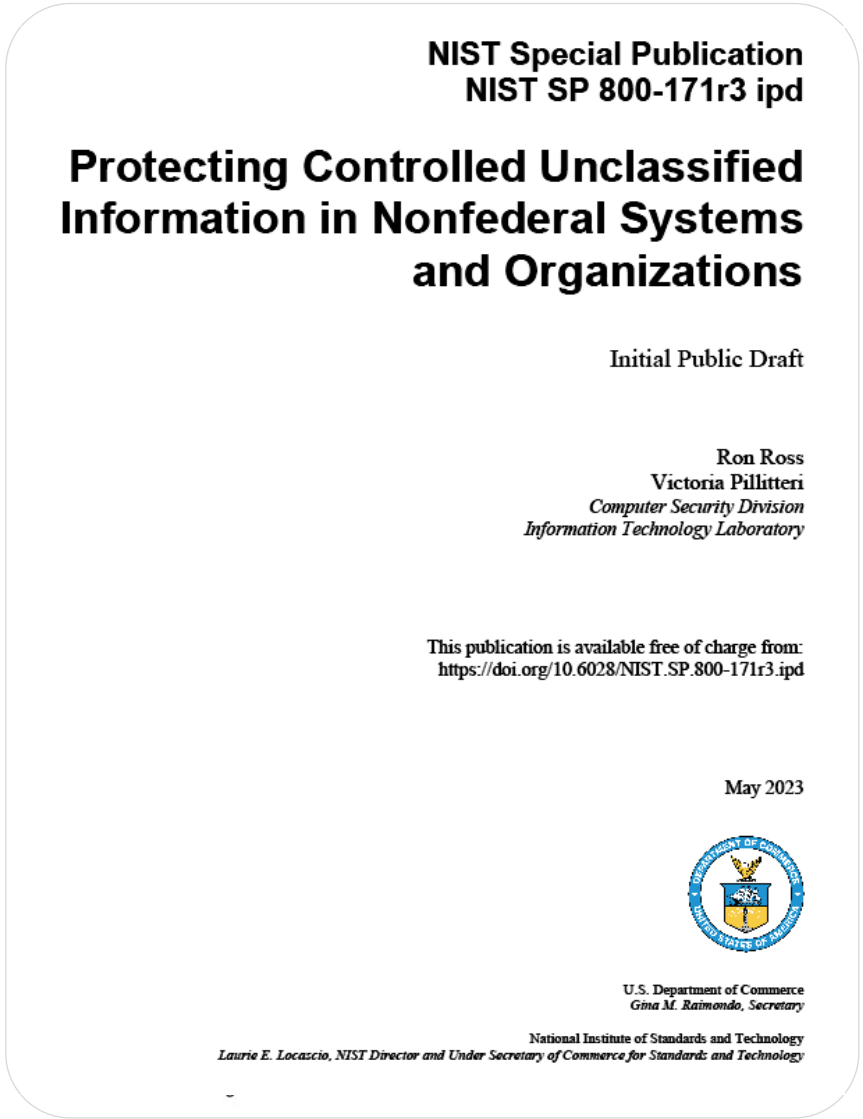
U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Table of Contents

ISACA
Chicago Chapter

NIST SP 800-171 r3 Draft



NIST Special Publication
NIST SP 800-171r3 ipd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Initial Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3.ipd

May 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

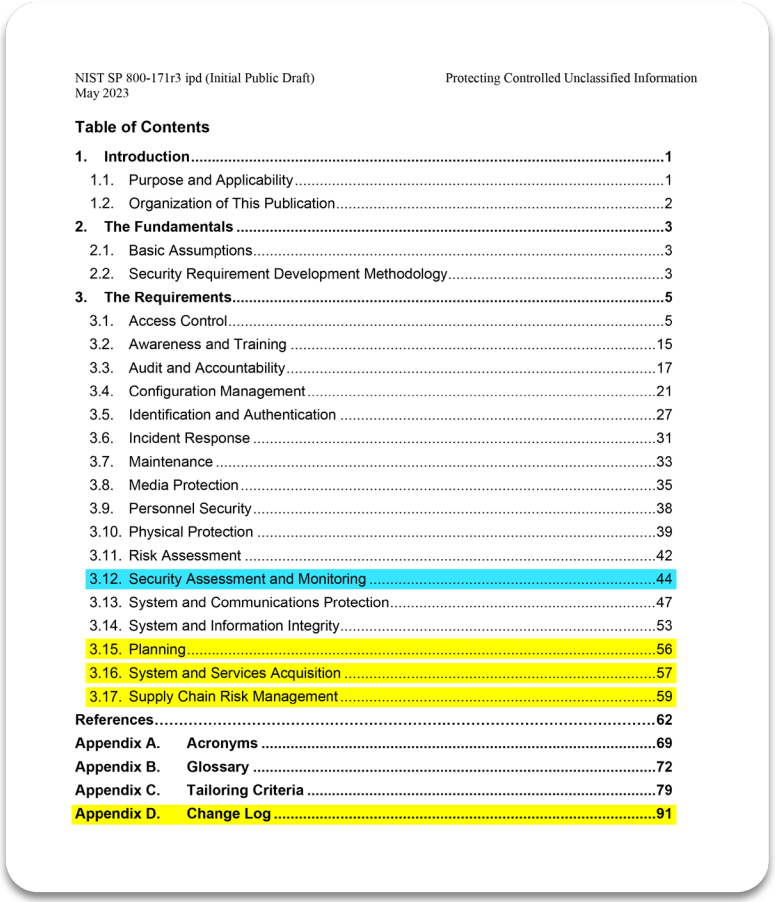
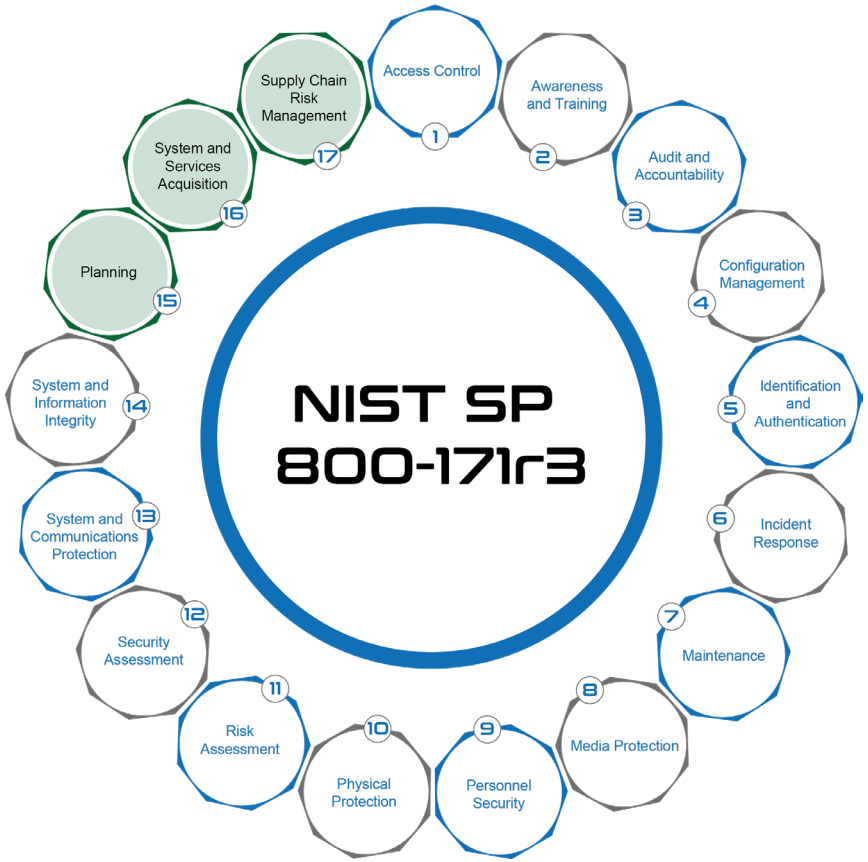


Table of Contents



New Addition Modification

ISACA Chicago Chapter

NIST SP 800-171 r3 Draft

Facts

EO 13556 established a governmentwide CUI program.

NARA provides information, guidance, policy, and requirements on handling CUI.

The CUI federal regulation provides guidance to federal agencies on the designation, safeguarding, marking, dissemination, decontrolling, and disposition of CUI.

The security requirements in ***NIST SP 800-171r3*** are only applicable to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components.

EO
Executive Order

CUI
Controlled Unclassified Information

NARA
National Archives and Records Administration

NIST SP 800-171 r3 Draft

Key Updates

NIST SP 800-171 r2

- A federal information system is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
- A system that does not meet such criteria is a non-federal system.

System components include mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.

Describes **14 families** of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.

Non-existent

Appendix E – Tailoring Criteria. NFO: Expected to be routinely satisfied by nonfederal organizations without specification.

NIST SP 800-171 r3 Draft

Information Technology (IT) systems → Operational Technology (OT) systems → Internet of Things (IoT) devices → Nonfederal Systems

System components include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, and applications.

- The security requirements are organized into **17 families**.
- New security requirement families include Planning, System and Services Acquisition, and Supply Chain Risk Management

Requirement 3.12.5 – Use independent assessors or assessment teams to assess controls.

Appendix C – Tailoring Criteria. NFO: Expected to be ***implemented*** by nonfederal organizations without specification.

Polling Question 1

Identify the key NIST reference that addresses ransomware.

A. NIST SP 800-207

B. NIST SP 800-171 r2

C. NIST SP 800-53 r5

D. NISTIR 8374

Polling Question 2

Identify the NIST reference focused on ZTA.

A. NIST SP 800-171 r2

B. NIST SP 800-207

C. NIST SP 800-53 r5

D. NISTIR 8374

Examine CMMC Standard

https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

CMMC Ecosystem

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

CMMC Facts

- Malicious cyber actors have target the DIB sector and the supply chain of the DoD.
- The DIB sector consists of more than 300,000 companies that support the warfighter and contribute toward the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services.
- Th OUSD (A&S) has developed the CMMC framework.
- The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21 and the security requirements for CUI specified in National Institute of Standards and Technology NIST SP 800-171 R2 per DFARS Clause 252.204-7012.
- DFARS clause 252.204-7012 specifies additional requirements beyond the NIST SP 800-171 security requirements, such as incident reporting.
- When implementing the CMMC model, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s), depending on where the information to be protected is handled and stored.

DIB

Defense Industrial Base

DoD

U.S. Department of Defense

OUSD (A&S)

Under Secretary of Defense for Acquisition and Sustainment

CMMC

Cybersecurity Maturity Model Certification

FCI

Federal Contract Information

CUI

Controlled Unclassified Information

DFARS

Defense Federal Acquisition Regulation Supplement

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

CMMC Data Types

Federal Contract Information (FCI) is information provided by or generated for the Government under contract not intended for public release.

Controlled Unclassified Information (CUI) established by Executive Order 13556, is an umbrella term for all unclassified information that requires safeguarding.

Controlled Technical Information (CTI) is defined as technical information with a military or space application that is marked with a distribution statement in accordance with DoDI 530.24 (Distribution Statements on Technical Documents).

Covered Defense Information (CDI) is used to describe information that requires protection under DFARS Clause 252.204-7012. It is defined as unclassified CTI or other information as described in the CUI Registry.

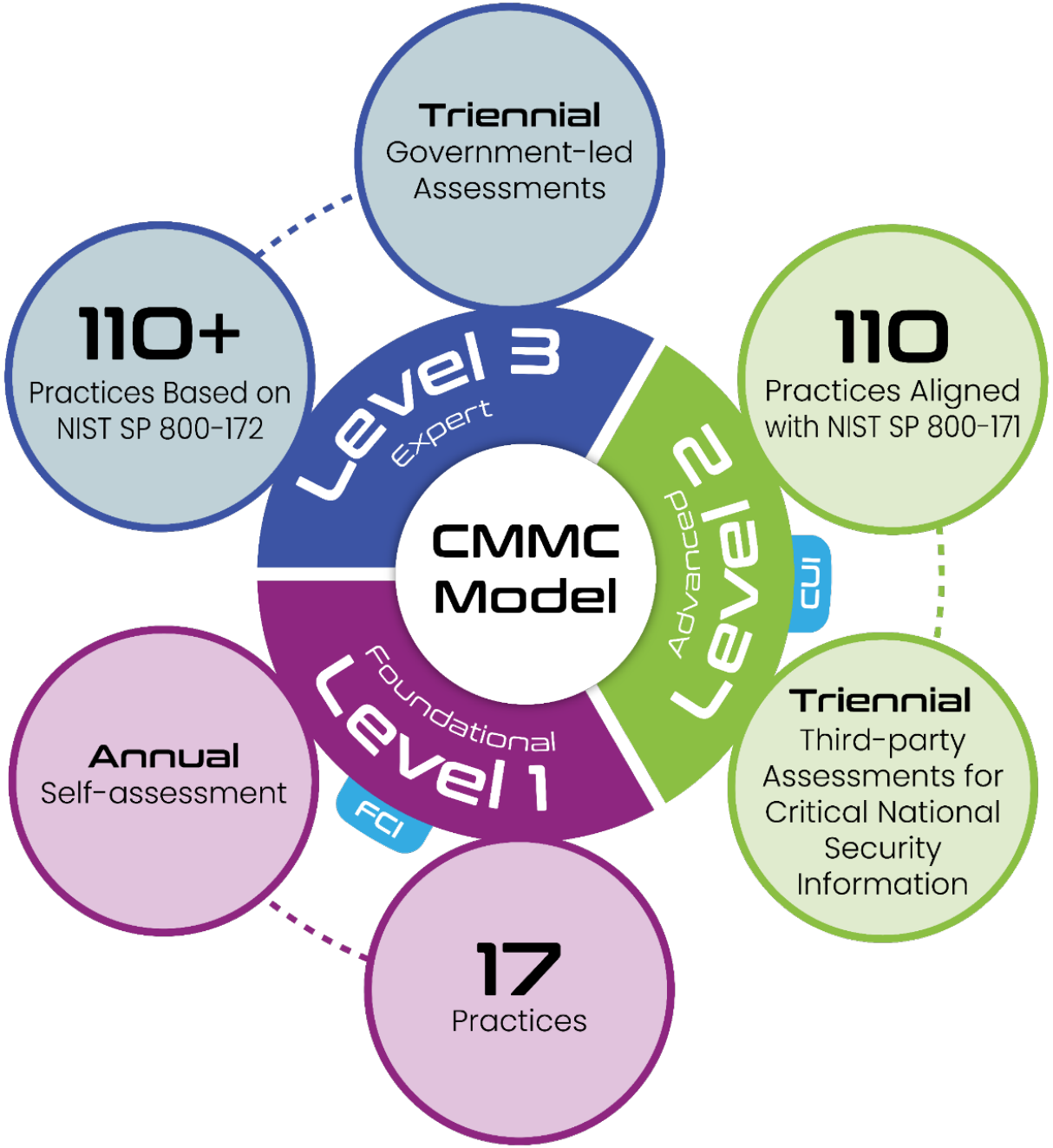
Export Controlled Information (ECI) or material is any information or material that cannot be released to foreign nationals or representatives of a foreign entity, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR).

Resilient Supply Chain with CMMC

The Institute of Internal Auditors Chicago

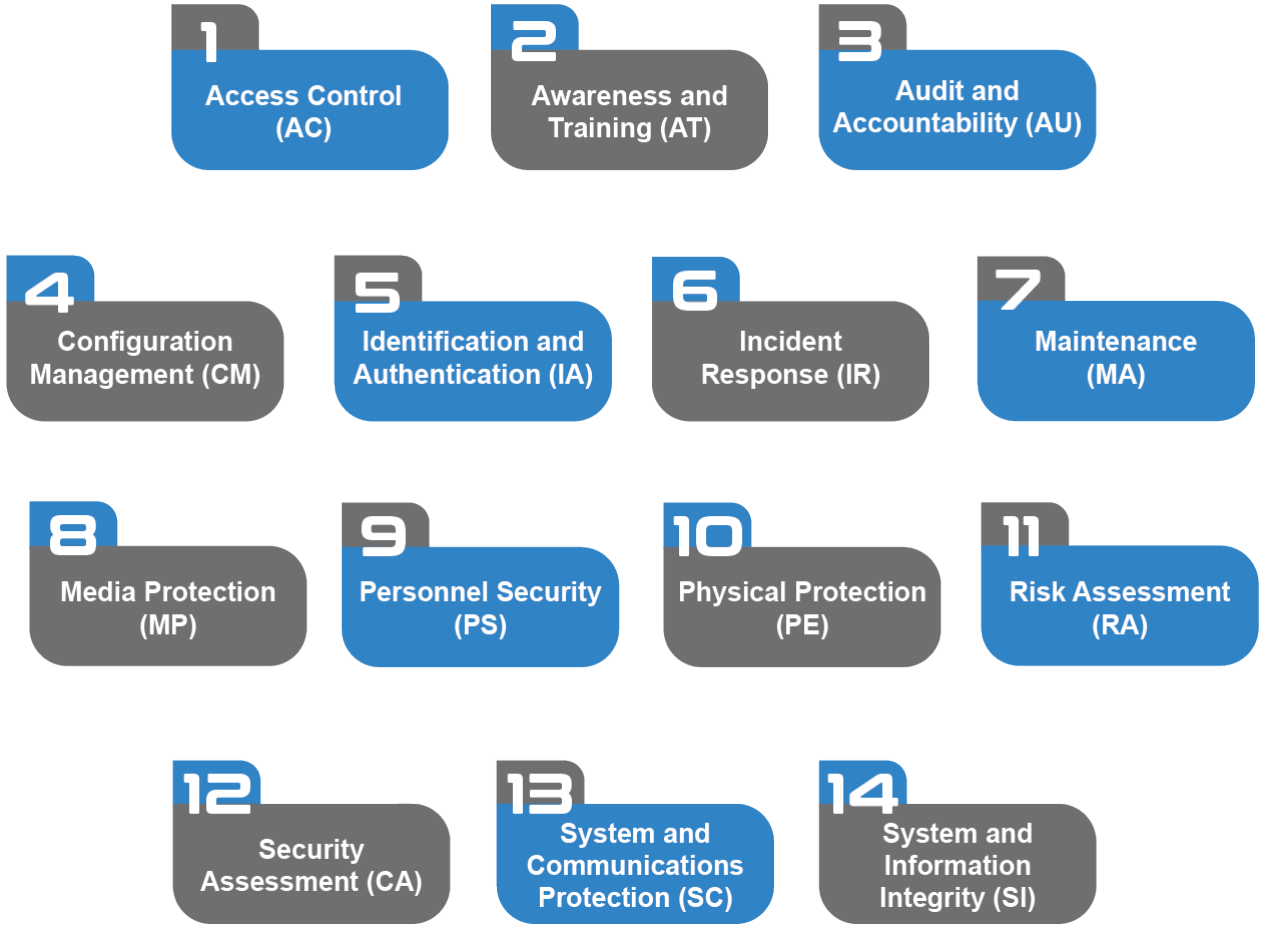
ISACA Chicago Chapter

CMMC Model


Triennial
Government-led Assessments
110+
Practices Based on NIST SP 800-172
Level 3
Expert
110
Practices Aligned with NIST SP 800-171
CMMC Model
Advanced
Level 2
CUI
Triennial
Third-party Assessments for Critical National Security Information
Foundational
Level 1
FCI
Annual
Self-assessment
17
Practices

CMMC Domains

- The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171.



CMMC Practices

- The CMMC model measures the implementation of the NIST SP 800-171 Rev 2 security requirements.
- The practices originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 and DFARS Clause 252.204-7012, respectively.
  - Level 1 is equivalent to all of the safeguarding requirements from FAR Clause 52.20421.
  - Level 2 is equivalent to all of the security requirements in NIST SP 800-171 Rev 2.
  - Level 3 will be based on a subset of NIST SP 800-172 and more detailed information will be released at a later date.
- Each practice has a practice identification number in the format- DD.L#-REQ - where:
  - DD is the two-letter domain abbreviation.
  - L# is the level number.
  - REQ is the NIST SP 800-171 Rev 2 or NIST SP 800-172 security requirement number.
- Below the identification number, a short name identifier is provided for each practice, meant to be used for quick reference only.

Domain 1

Access Control (AC)

Practice

Access Control (AC)			
Level 1			
#	CMMC Practice ID	Practice Description	Reference
1	**AC.L1-3.1.1** Authorized Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	• FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 2 3.1.1
2	**AC.L1-3.1.2** Transaction & Function Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	• FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 2 3.1.2
3	**AC.L1-3.1.20** External Connections	Verify and control/limit connections to and use of external information systems.	• FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 Rev 2 3.1.20
4	**AC. L1-3.1.22** Control Public Information	Control information posted or processed or publicly accessible information systems.	• FAR Clause 52.204-21 b.1.iv • NIST SP 800-171 Rev 2 3.1.22

Polling Question

The focus of the CMMC cyber standard is to secure,

A. FCI and CUI

B. PHI and PII

C. PCI CDE

D. EUPD

CMMC Assessment and Certification

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

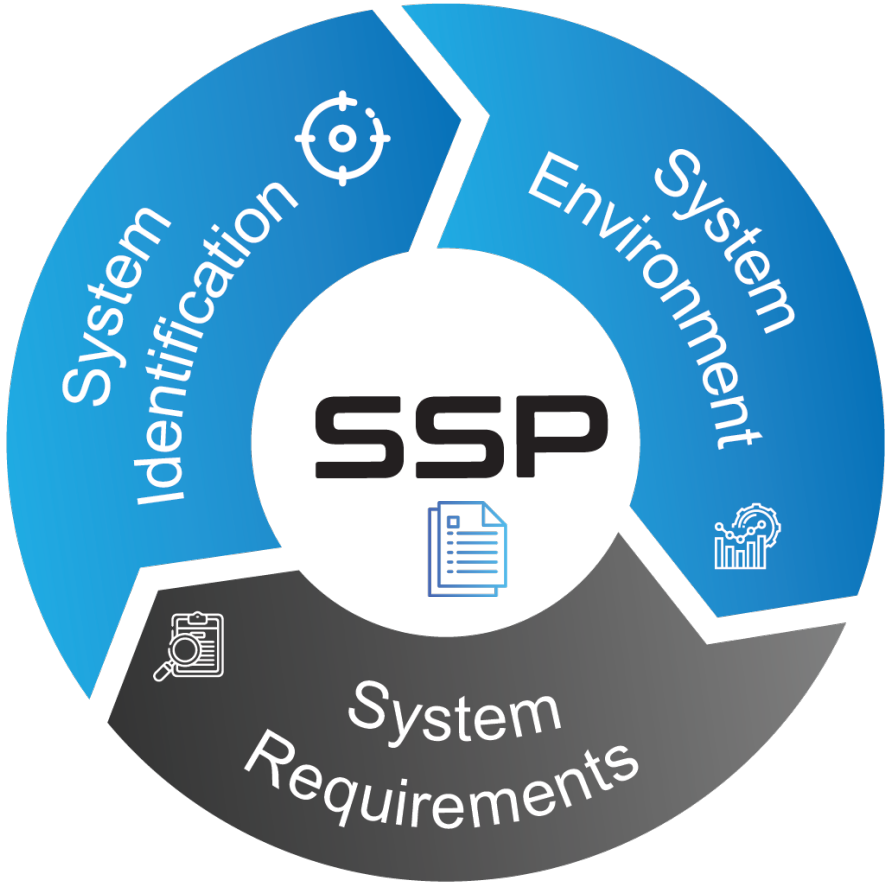
Getting Started

System Security Plan (SSP)

Develop, document, and periodically update the SSP document.

SSP document describes system boundaries, system environments of operation.

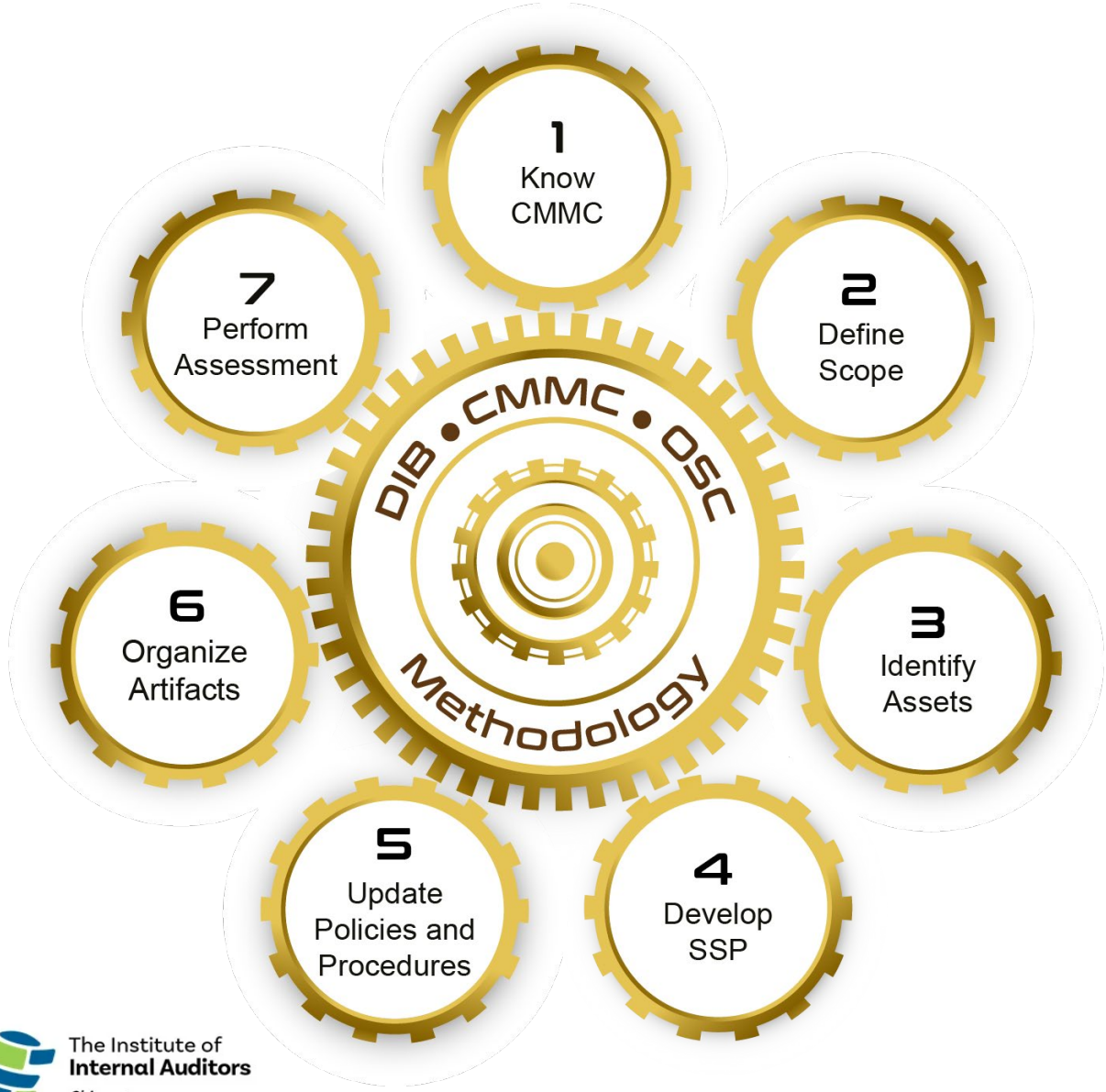
SSP further describes how security requirements are implemented, and the relationships with or connections to other systems.

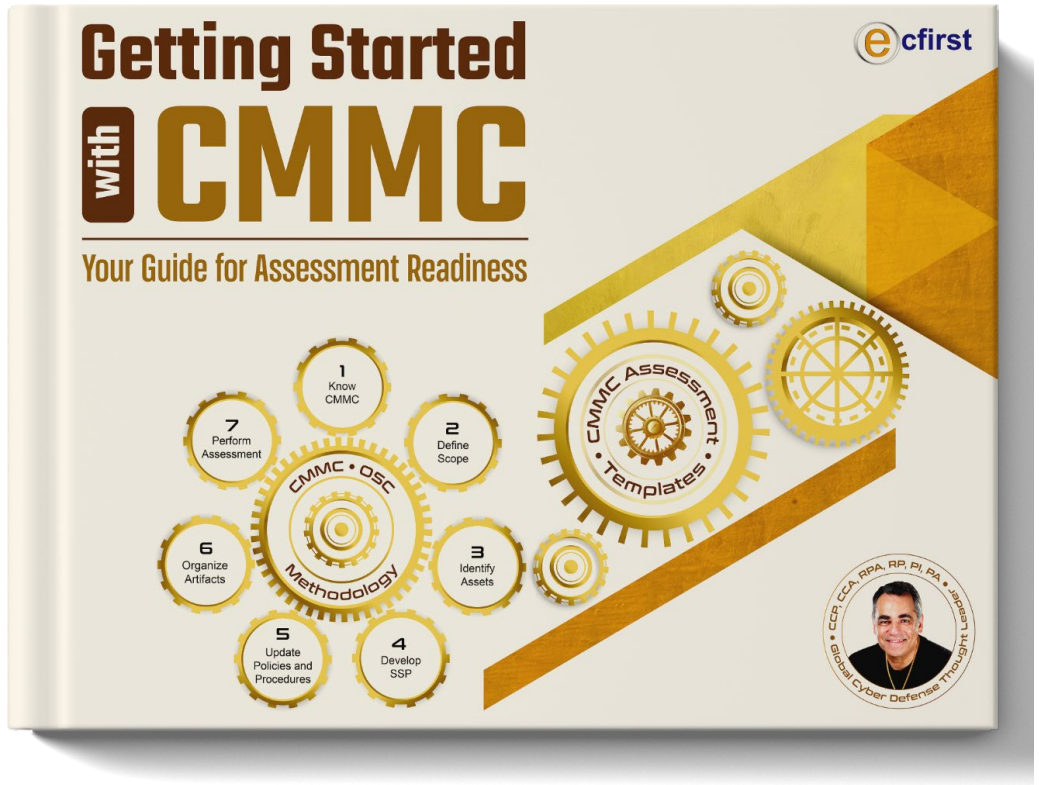


The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

CMMC Methodology





A Must-have Reference for OSCs & DIB

Place Order

https://ecfirst.biz/CMMCbook

The Institute of Internal Auditors Chicago

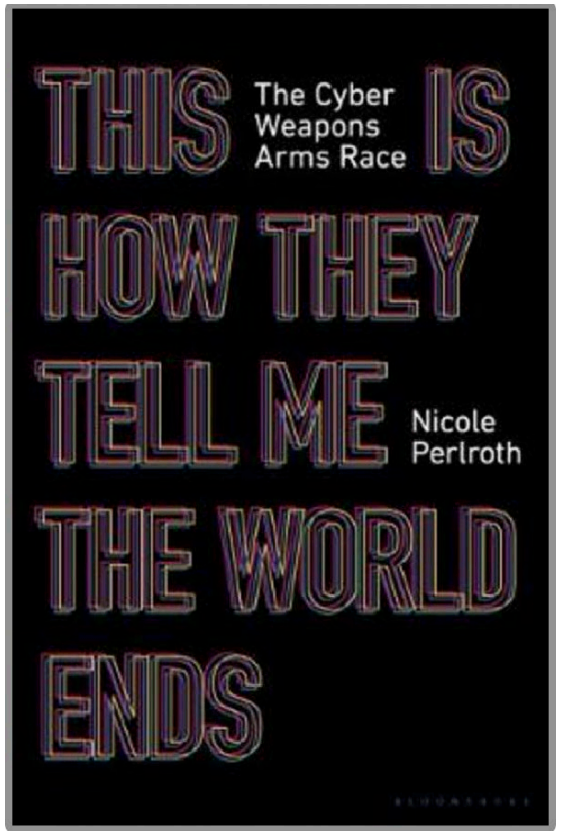
ISACA Chicago Chapter

NIST and CMMC Readiness

NIST Fusion | CMMC Future

ISACA Chicago Chapter

Past = A Mirror to the Future



> “Now zero-days are in the hands of hostile nations and mercenaries who do not care if your vote goes missing, your clean water is contaminated, or our nuclear plants melt down.”

> “Americans are plugging anything we can into the Internet, at a rate of 127 devices a SECOND! The American society is on the cusp of a digital tsunami called the Internet of Things (IoT). There isn’t a single area of our lives that isn’t touched by the web. We have not paused to think that, along the way, we were creating the world’s largest attack surface.”

- Nicole Perlroth

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Certified CMMC Professional

Virtual

January 9 – 12, 2024
March 4 – 7, 2024
March 12 – 15, 2024
May 14 – 17, 2024
June 11 – 14, 2024

Public

December 5 – 8, 2023 | Las Vegas, NV

Columbia, MD

January 9 – 12, 2024
March 4 – 7, 2024
March 12 – 15, 2024
May 14 - 17, 2024
June 11 - 14, 2024

Certified CMMC Assessor

Virtual

December 12 – 15, 2023
January 23 – 26, 2024
February 27 – March 1, 2024
March 26 – 29, 2024
May 21 – 24, 2024
June 25 – 28, 2024

Public

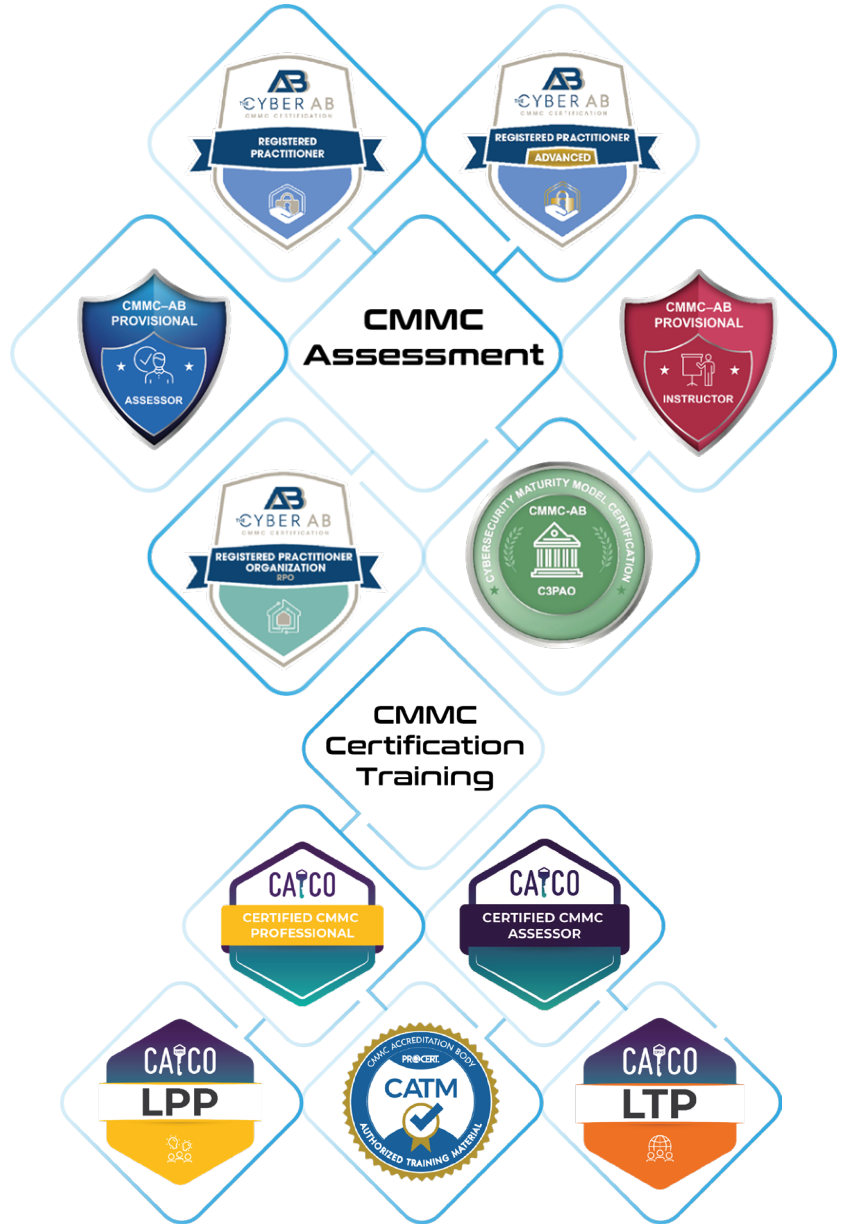
Columbia, MD

January 23 – 26, 2024
February 27 – March 1, 2024
March 26 – 29, 2024
May 28 – 31, 2024
June 25 – 28, 2024

ISACA Chicago Chapter

Thank You!

Ali Pabrai | Ali.Pabrai@ecfirst.com | +1.949.528.5224



The Institute of Internal Auditors
Chicago

ISACA
Chicago Chapter

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter