CONNSTEP
a CBIA affiliate

CMMC PREPARATION Webinars: Steps to Take in Preparation for a CMMC Audit

CONNSTEP
6/1/2023

CMMC PREPARATION Webinars

CONNSTEP
a CBIA affiliate

Four Webinar Series

3/9 – 6/1

12 noon – 1 pm

March 9th	Understanding CMMC Timeline & Steps to Compliance
April 6th	How to Develop & Implement Effective CMMC Policies & Procedures
May 4th	How to Leverage Your IT Managed Service Provider (MSP) to Achieve CMMC Compliance
June 1st	Steps to Take in Preparation for a CMMC Audit

Webinar #4 Agenda

CONNSTEP
a CBIA affiliate

Steps to Take in Preparation for a CMMC Audit

- Current State of DoD Rulemaking
- CMMC Assessment Expectations
- Creating Assessment Scope Documentation
- Methods of CMMC Assessment
- Assessment Preparation Best Practices and Success Factors
- Transferring Quality System Expertise into Cybersecurity – Bill Forthofer

CONNSTEP
a CBIA affiliate

Guest Speakers:

Amalia Hilliard
Cybersecurity Provider
CMMC-AB Professional

William Forthofer
Quality Systems/EH&S/CI Manager
Cambridge Specialty Co., Inc.

CONNSTEP
a CBIA affiliate

Presenters:

Anna Mumford
Cybersecurity Consultant

860.305.8880
amumford@connstep.org

Beverly Benson
Cybersecurity Consultant

860.869.2904
bbenson@connstep.org

Jeffrey Orszak
Director, Business Technology and Innovation
860.539.4905
jorszak@connstep.org

Guidance

Nothing in this presentation (written, spoken, expressed, or implied) is legal advice.

Nothing in this presentation (written, spoken, expressed or implied) should be construed as an endorsement of any solution, product, service, or methodology.

Poll

Current State of DoD Rulemaking

- **News from the Cyber AB**
- **Draft NIST SP 800-171r3**
- **Important Insights**

THE CYBER AB
CMMC CERTIFICATION

Current State of Rulemaking

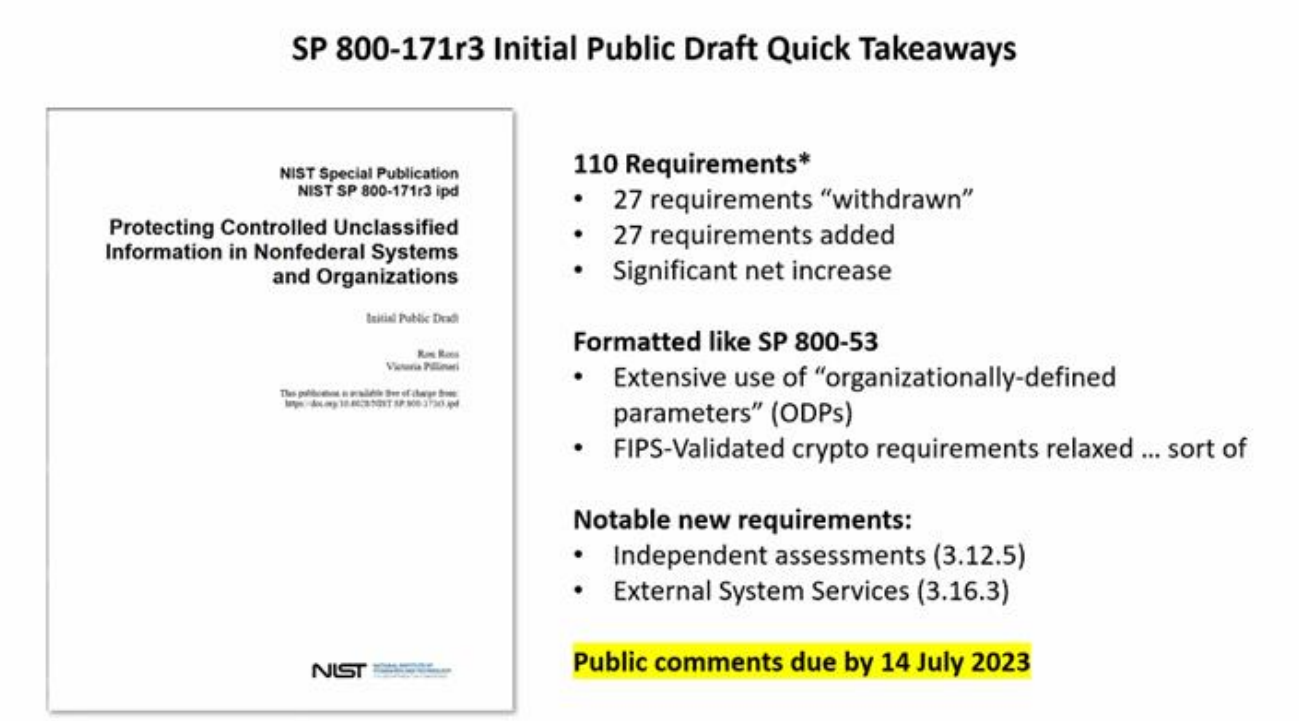
Department of Defense
Chief Information Officer

Now under an upgraded cyber certification program, the Defense Department’s chief information officer said he wants to focus on clarifying requirements and increasing engagements with small to medium-sized companies in hopes of raising the overall “waterline” of the Pentagon’s cybersecurity defenses.

Department of Defense
Senior Information Security Officer, and
Deputy Chief Information Officer for Cybersecurity

Draft NIST SP 800-171r3

On June 6, 2023, NIST will host a webinar to provide an overview of the significant changes in NIST Special Publication (SP) 800-171, Revision 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.



SP 800-171r3 Initial Public Draft Quick Takeaways

NIST Special Publication
NIST SP 800-171r3 ipd

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Initial Public Draft

Ron Ross
Victoria Pillitteri

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

NIST

110 Requirements*

- 27 requirements "withdrawn"
- 27 requirements added
- Significant net increase

Formatted like SP 800-53

- Extensive use of "organizationally-defined parameters" (ODPs)
- FIPS-Validated crypto requirements relaxed … sort of

Notable new requirements:

- Independent assessments (3.12.5)
- External System Services (3.16.3)

Public comments due by 14 July 2023

Important Insights

CONNSTEP
a CBIA affiliate

Why Take Action Now:

- Enhanced Cybersecurity
- Defense Contracting Requirements
- Protection of Controlled Unclassified Information
- Competitive Advantage classified Information (CUI)

About the CMMC Assessments

CMMC Assessments Expectations:

- Testing or evaluation of security controls:
  - implemented correctly
  - operating as intended
  - producing the desired outcome
- Conducted by CMMC Third-Party Assessment Organization (C3PAO) and Certified Assessor
- Certification good for 3 years

CMMC Level 1 vs. Level 2 Assessment

CMMC Level 1

- addresses the protection of Federal Contract Information (FCI)

CMMC Level 2

- addresses the protection of Controlled Unclassified Information (CUI)

Level 2 assessment is **cumulative** - demonstrate achievement of all Level 1 and Level 2 practices

EXAMPLE: CMMC Level 1 self-assessment for the boundary containing FCI (e.g., the enterprise network), but obtain a CMMC Level 2 certification for the boundary or enclave of its network within which all CUI must be processed, stored, or transmitted

Difference Between FCI vs. CUI

Federal Contract Information (FCI)

"Information, not intended for public release, that is provided or generated for the Government under a contract to deliver a product or service to the Government."

– *Official Government Definition of FCI*

- Contract performance reports
- Organizational or programmatic charts
- Process documentation
- Proposal responses
- Past performance information
- Contract information
- Emails exchanged with the DoD or defense contractor

Controlled Unclassified Information (CUI)

"CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."

– *Official Government Definition of CUI*

- Information Systems Vulnerability Information
- Personally Identifiable Information (PII) (Could be your employees, government employees, or even employees of a third party)
- Research and engineering data
- Engineering drawings, Technical reports & Technical orders
- Specifications & Standards
- Process sheets, manuals & catalog: item identification

CUI and CDI

Controlled Unclassified Information (CUI)

Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended

Covered Defense Information (CDI)

Unclassified information that—

(1) Is—

(i) Provided to the contractor by or on behalf of DOD in connection with the performance of the contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract;

AND…

(2) Falls in any of the following categories:

(i) Controlled technical information.

(ii) Critical information

(iii) Export control

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information)

Achieving CMMC Certification

CMMC certification can be achieved for:

- an entire enterprise network,
- for particular segment(s), or
- for a specific enclave

→ It is dependent upon how the CMMC assessment is **scoped**!

Creating Scope Documentation

Which assets within the contractor’s environment will be assessed?

Need to develop Assessment Scoping Documentation :

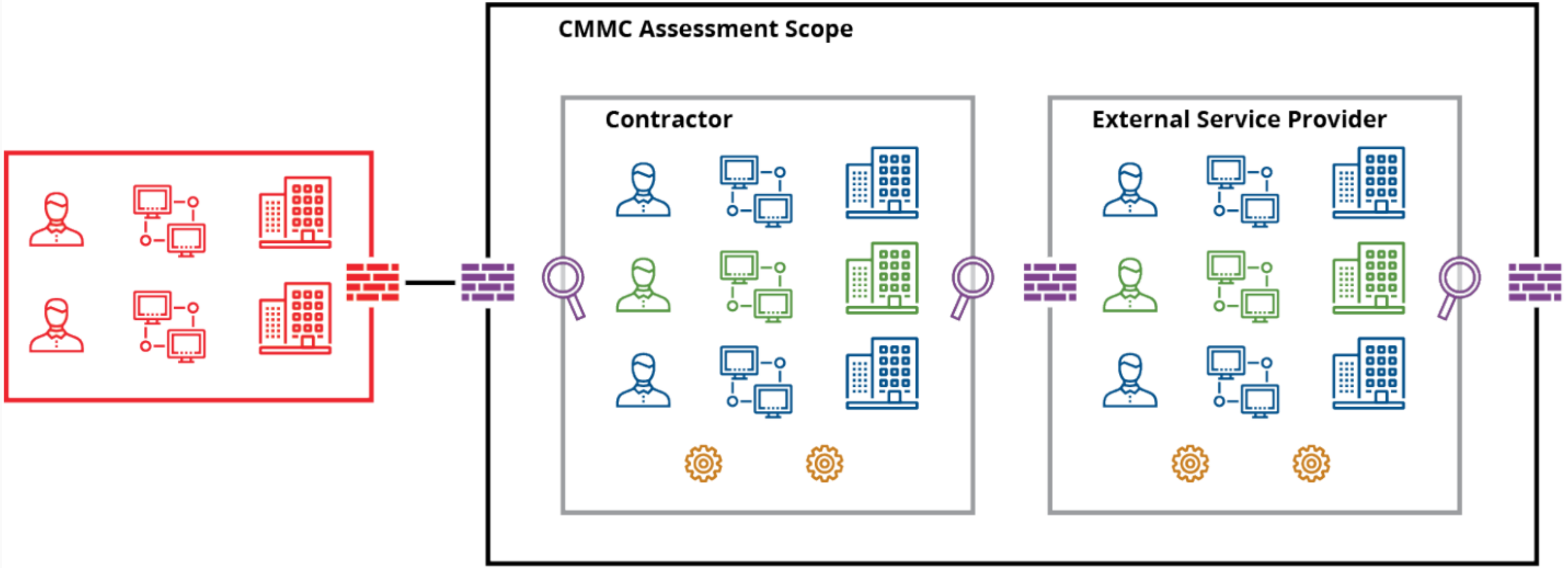
- Scope the environment to be audited
- Map all assets into one of the following five categories:
  1. CUI Assets,
  2. Security Protection Assets,
  3. Contractor Risk Managed Assets,
  4. Specialized Assets, and
  5. Out-of-Scope Assets.

Assets Categorization

Assets can include:

- people
- other organizations
- computing device
- IT system
- IT network
- OT system
- software
- Virtual computing platform (common in the cloud and virtualized computing)
- related hardware (e.g., locks, cabinets, keyboards)

CMMC Assessment Scope



- 🟦 CUI Assets
- 🟪 Security Protection Assets
- 🟩 Contractor Risk Managed Assets
- 🟧 Specialized Assets
- 🟥 Out-of-Scope Assets

Scoping External Service Providers (ESP)

External Service Provider (ESP) may be:

external people, technology, or facilities that the contractor uses

Examples:

including cloud service providers

managed service providers

managed security service providers

cybersecurity-as-a-service providers

For each of the practice objectives that an ESP performs, the SMM can inherit the practice compliance.

The SMM will need to demonstrate the performance of the practice objectives by the ESP and provide adequate evidence of compliance.

Mapping CUI Flow EXERCISE

CONNSTEP
a CBIA affiliate

How CUI flows through the organization?

- CUI is received via (describe client portals)
  - Customer Portals ______________________
  - Email ______________________________
  - Paper ______________________________

- CUI is stored.
  - Paper_____________________________
  - Digital____________________________
  - Encryption__________________________

- CUI is transmitted.
  - Paper_____________________________
  - Digital____________________________
  - Encryption__________________________

- At end of job, CUI is:
  - Stored________________________
  - Destroyed ______________________

- CUI is shared. Please list everyone that has access to the organization's CUI.
  - Internally (Which Employees) _____________________________
  - Externally (Vendors, Customers, etc.) ______________________

Actions to Take

1. Map CUI data flow throughout your organization
2. List assets type and then categorize the assets
3. Document the CMMC Assessment Scope
4. Download the "CMMC Assessment Scope – Level 2" document:

https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf

CMMC Certified Assessor

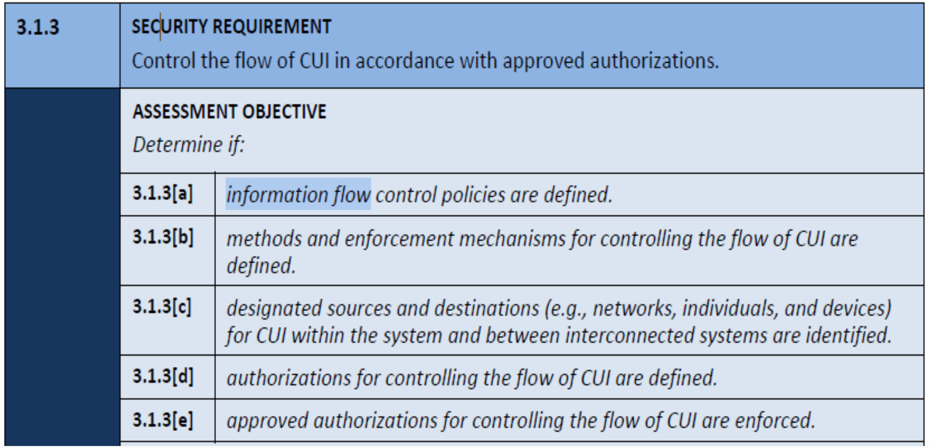
The **Certified Assessor** will:

- Independently verify if the assessment objectives are met

- Evaluate if the controls are:
  - implemented correctly
  - operating as intended
  - producing the desired outcome

- Determine the assessment method most useful in obtaining the desired results

*NIST SP 800-171A



3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*

Methods of CMMC Assessment

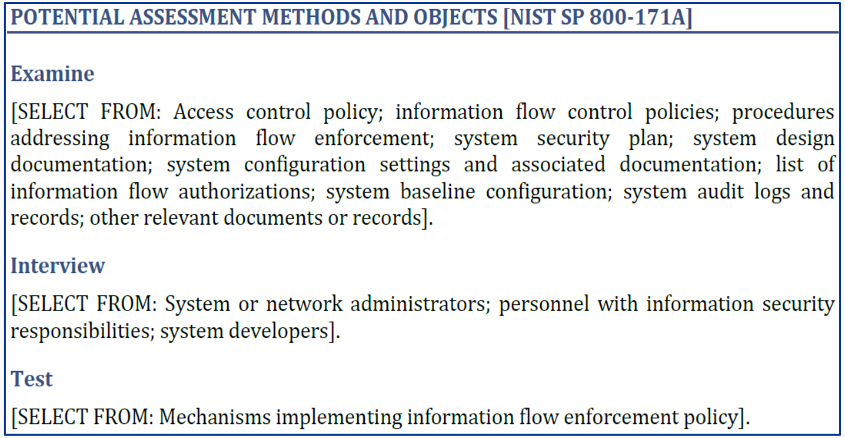
Assessment **Methods of Evaluation**:

1. EXAMINE the assessment objects (*specifications, mechanisms, activities)*

2. INTERVIEW *individuals or groups of individuals discussions*

3. TEST or *exercise assessment objects (activities, mechanism of expected behavior)*

* CMMC Assessor's Guide



POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records].

Interview

[SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers].

Test

[SELECT FROM: Mechanisms implementing information flow enforcement policy].

Assessment Result

Report with each practice's findings - possible findings:

- MET,*
- NOT MET, or
- NOT APPLICABLE

**includes Alternate Solutions*

MET or **NOT APPLICABLE** findings on all CMMC practices are required to meet compliance at a specific CMMC level.

Repository

Assessment Objects Repository - ORGANIZED and READILY AVAILABLE:

- Specifications and document-based artifacts that can include:
  - policies, processes, and procedures documents;
  - security plans and requirements, functional systems specifications, architectural designs
  - training materials and records;
  - plans and planning documents; and
  - Inventories, system-level, network, and data flow diagrams.
- Mechanisms are the hardware, software, or firmware safeguards deployed in a system
- Activities are the actions performed by people to support the systems (performing system backup or monitoring network traffic) that can be examined/observed

Repository (cont.)

Assessment Objects Repository - ORGANIZED and READILY AVAILABLE:

- Individuals or groups of individuals (possibly at different organizational levels) that apply the activities, mechanisms, or specifications:
    - Identify individuals responsible for each activity, mechanism, or specification
    - Ensure those individuals receive proper training on those practices

- External Service Provider (ESP) if it meets CUI asset criteria:
    - Create a shared responsibility matrix with the provider's responsibilities
    - Obtain necessary evidence of inherited compliance (ex. Cloud service provider's configuration settings and parameters)
    - Consider SLAs and contracts to enforce the EPS's security compliance objectives

Schedule

Many practices repeat periodically or need to be reviewed, maintained, and updated frequently

-> **create a SCHEDULE for the sustainment of your cybersecurity practices.**

Ex. risk management, management reviews, training, assessments, etc.

Create a **schedule** that supports Maintenance, Reviews, and Updates:

1. Establish a frequency
2. Assign responsible parties
3. Create a master schedule
4. Update repository

Pre-Assessment Communication

Pre-Assessment Communication with the CMMC Assessor:

Verbal or written communication outlining what the assessor would like to make available for review prior to the assessment, for example:

- Asset inventory
- System Security Plan
- Network diagram of the assessment scope (to include these assets)

Making a Good Impression

Ensure the documents are:

- Well organized and clear to follow
- Complete and up to date
- Visually pleasing
- Impressive in content, as it reflects the state of your cybersecurity posture!

Create a report/presentation that showcases your cybersecurity posture for:

- CMMC Pre-assessment review
- Customers
- DoD/Prime reps

CMMC Assessment Pilot Program

Texas MEP client's CMMC Assessment feedback:

- Importance of documentation
- Using various assessment methods
- Verifying that you live what you built

Success Factors

CMMC Assessment Success Factors:

- Internal pre-audit assessment
- Training employees on what to expect during the assessment
- Ensuring that the appropriate leadership team is available during the assessment
- Get help during the CMMC assessment – assistance that speaks the cybersecurity language to interpret the questions and help you provide the answers

Actions to Take

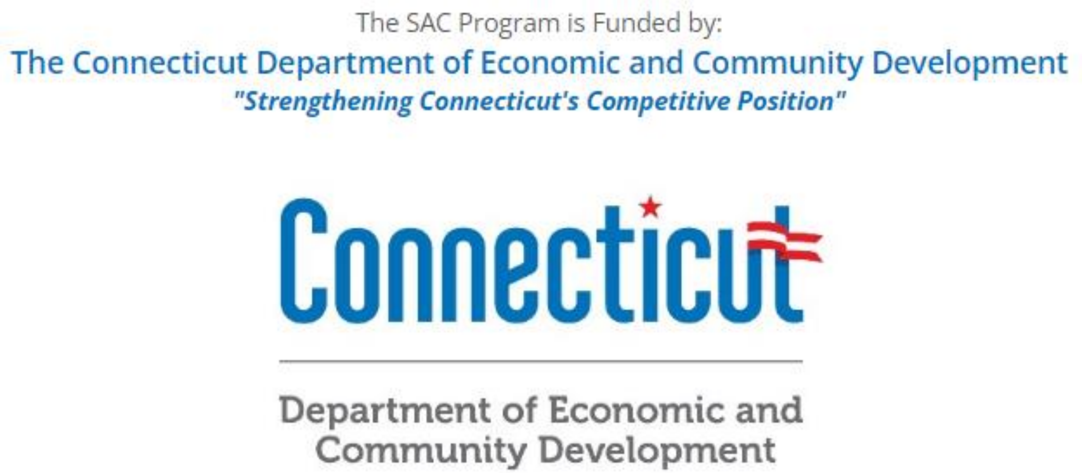
1. Create a repository for your assessment objects
2. Develop a schedule for the sustainment of your cybersecurity practices
3. Prepare documentation for the pre-assessment review

State Funding Available

State funding is available for

Connecticut Manufacturing SIRI and CYBER Assistance Program (SAC)

for manufacturing companies or allied service providers located in Connecticut.



The SAC Program is Funded by:

The Connecticut Department of Economic and Community Development

"Strengthening Connecticut's Competitive Position"

Connecticut

Department of Economic and Community Development

https://ctsac.ccat.us/

Cambridge Specialty Company

New Shepard Rocket

June , 2023

DoD’s Cybersecurity Maturity Model Certification (CMMC) Compliance

Background:

Keeping confidential government/military information Secure from prying eyes is critical to our national sovereignty and economy.

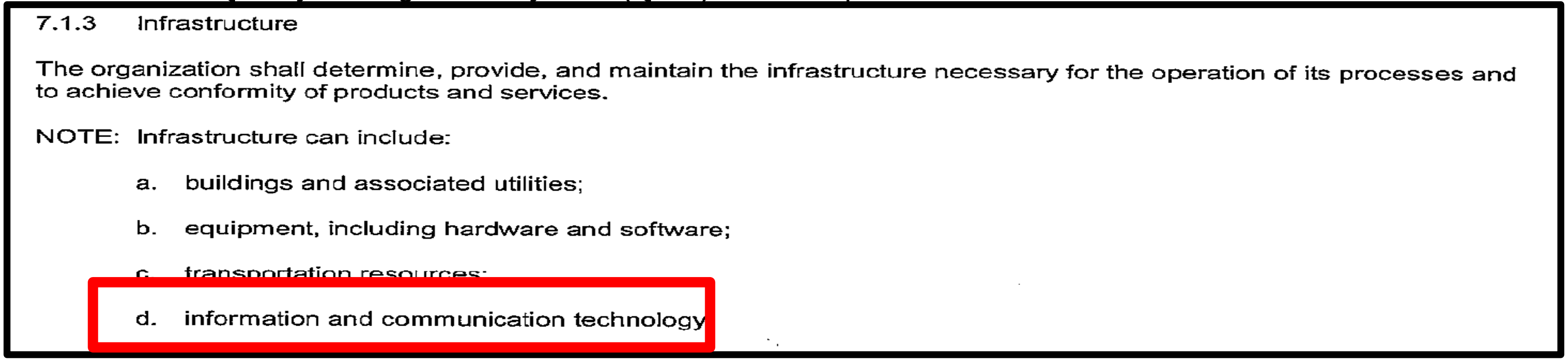
Cambridge Specialty Actions:

- “System Security Plan” in place with Enterprise IT and POAM Provider “TAB” Fully Engaged for the past year
- Working Compliance Requirements to DFAR’s 252.204-7012, 7020 for Solicitations & Contracts and Cybersecurity Compliance to NIST 800- 171,CMMC 2.0
- Required Assessments Complete and Loaded in Government Procurement Integrated Enterprise Environment (PIEE)/Supplier Performance Risk System (SPRS).

Confidentiality Notice: This presentation contains proprietary and privileged information of Cambridge Specialty Company (CSC) Inc. and its component entities. This is intended for use by the original recipient only and is not to be disclosed, copied or distributed, in whole or in part, without the written authorization of CSC. Export Control Notice: this presentation may contain technical data which may be controlled by the US International Trafficking in Arms Regulation (ITAR) 22 CFR part 120-130 or Export Administration Regulation (EAR) 15 CFR part 730-774. If any information is determined to be export controlled it may not be exported, transmitted, shared, disclosed or provided to any non US Persons as defined within ITAR and EAR, either verbally or visually, without first complying with the export requirements of ITAR & EAR. It is the recipients responsibility to assure this item can be legally shared with another party before doing so.

Key Reference Documents/Software

- AS9100 Quality Management System (QMS) for Aerospace



7.1.3 Infrastructure

The organization shall determine, provide, and maintain the infrastructure necessary for the operation of its processes and to achieve conformity of products and services.

NOTE: Infrastructure can include:

a. buildings and associated utilities;

b. equipment, including hardware and software;

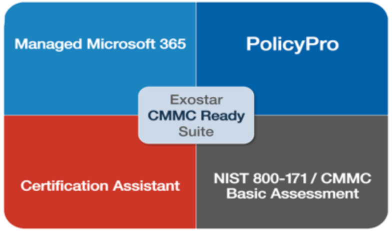
c. transportation resources;

d. information and communication technology

- Working Compliance Requirements to DFAR's 252.204-7012, 7020 for Solicitations & Contracts and Cybersecurity Compliance to NIST 800- 171,CMMC 2.0

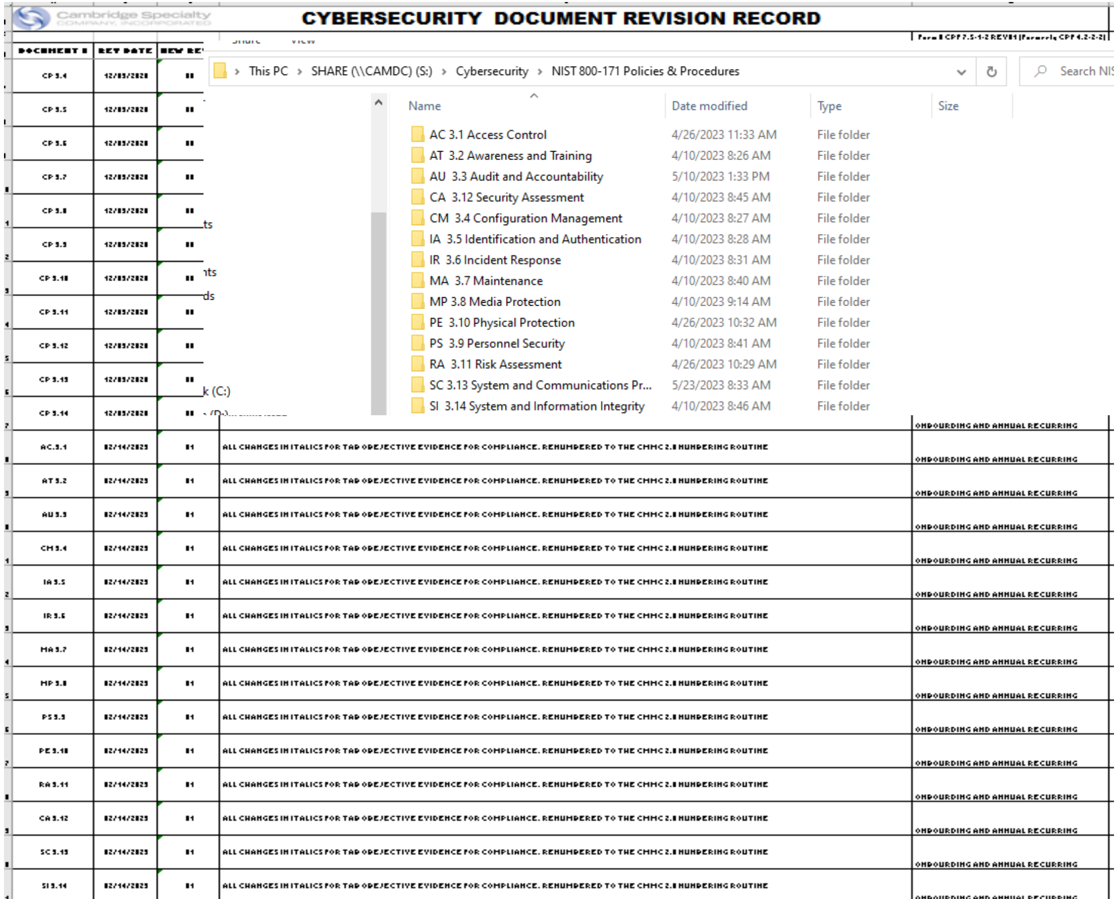
- CONNSTEP - CMMC Assessment Guide Level 2 Version 2.0, December 2021

- Exostar Certification Assistance Software
  - System Security Plan (SSP)
  - Plan Of Actions & Milestones (POAM)



Cybersecurity/QMS Compliance Management Methodology

Document Control



Cambridge Specialty COMPANY, INCORPORATED

CYBERSECURITY DOCUMENT REVISION RECORD

Form # CPF7.5-1-2 REV01 (Formerly CPF4.2-2-2)

This PC › SHARE (\\CAMDC) (S:) › Cybersecurity › NIST 800-171 Policies & Procedures

Name	Date modified	Type	Size
AC 3.1 Access Control	4/26/2023 11:33 AM	File folder	
AT 3.2 Awareness and Training	4/10/2023 8:26 AM	File folder	
AU 3.3 Audit and Accountability	5/10/2023 1:33 PM	File folder	
CA 3.12 Security Assessment	4/10/2023 8:45 AM	File folder	
CM 3.4 Configuration Management	4/10/2023 8:27 AM	File folder	
IA 3.5 Identification and Authentication	4/10/2023 8:28 AM	File folder	
IR 3.6 Incident Response	4/10/2023 8:31 AM	File folder	
MA 3.7 Maintenance	4/10/2023 8:40 AM	File folder	
MP 3.8 Media Protection	4/10/2023 9:14 AM	File folder	
PE 3.10 Physical Protection	4/26/2023 10:32 AM	File folder	
PS 3.9 Personnel Security	4/10/2023 8:41 AM	File folder	
RA 3.11 Risk Assessment	4/26/2023 10:29 AM	File folder	
SC 3.13 System and Communications Pr...	5/23/2023 8:33 AM	File folder	
SI 3.14 System and Information Integrity	4/10/2023 8:46 AM	File folder	

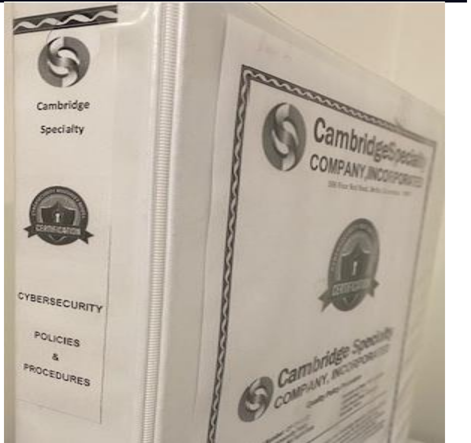
DOCUMENT #	REV DATE	NEW REV		
CP 3.4	12/05/2020	00		
CP 3.5	12/05/2020	00		
CP 3.6	12/05/2020	00		
CP 3.7	12/05/2020	00		
CP 3.8	12/05/2020	00		
CP 3.9	12/05/2020	00		
CP 3.10	12/05/2020	00		
CP 3.11	12/05/2020	00		
CP 3.12	12/05/2020	00		
CP 3.13	12/05/2020	00		
CP 3.14	12/05/2020	00		ONBOARDING AND ANNUAL RECURRING
AC.3.1	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
AT 3.2	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
AU 3.3	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
CM 3.4	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
IA 3.5	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
IR 3.6	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
MA 3.7	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
MP 3.8	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
PS 3.9	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
PE 3.10	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
RA 3.11	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
CA 3.12	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
SC 3.13	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING
SI 3.14	02/14/2023	01	ALL CHANGES IN ITALICS FOR TAP OBJECTIVE EVIDENCE FOR COMPLIANCE. RENUMBERED TO THE CMMC 2.0 NUMBERING ROUTINE	ONBOARDING AND ANNUAL RECURRING

COMMENTS

- **CMMC Practices 3.1-3.14 all under Rev Control**
- **Utilized Exostar Policy Pro as Baseline for Policies & Procedures.**

EXOSTAR POLICYPRO

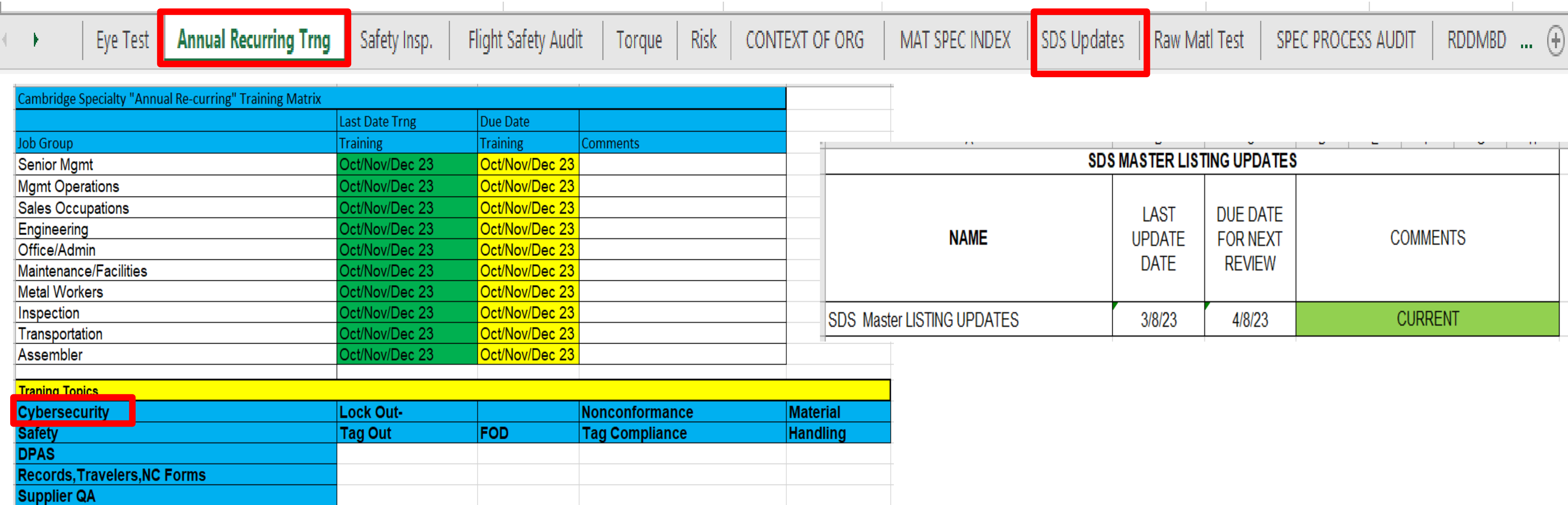
Powered by ISMS APPLICATIONS


Cambridge Specialty
CYBERSECURITY POLICIES & PROCEDURES
Cambridge Specialty COMPANY, INCORPORATED

Cybersecurity/QMS Compliance Management Methodology

- Utilizing AS9100 QMS Compliance Methodology Excel Spreadsheet to ensure Practices are Compliant on a Monthly Basis – Still In Development

AS9100 Spreadsheet



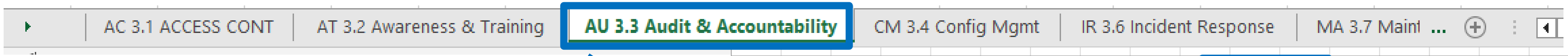
Cambridge Specialty "Annual Re-curring" Training Matrix			
	Last Date Trng	Due Date	
Job Group	Training	Training	Comments
Senior Mgmt	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Mgmt Operations	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Sales Occupations	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Engineering	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Office/Admin	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Maintenance/Facilities	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Metal Workers	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Inspection	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Transportation	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Assembler	Oct/Nov/Dec 23	Oct/Nov/Dec 23	

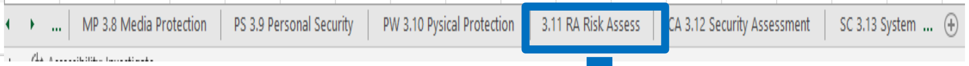
Traning Topics				
Cybersecurity Safety	Lock Out- Tag Out	FOD	Nonconformance Tag Compliance	Material Handling
DPAS				
Records,Travelers,NC Forms				
Supplier QA				

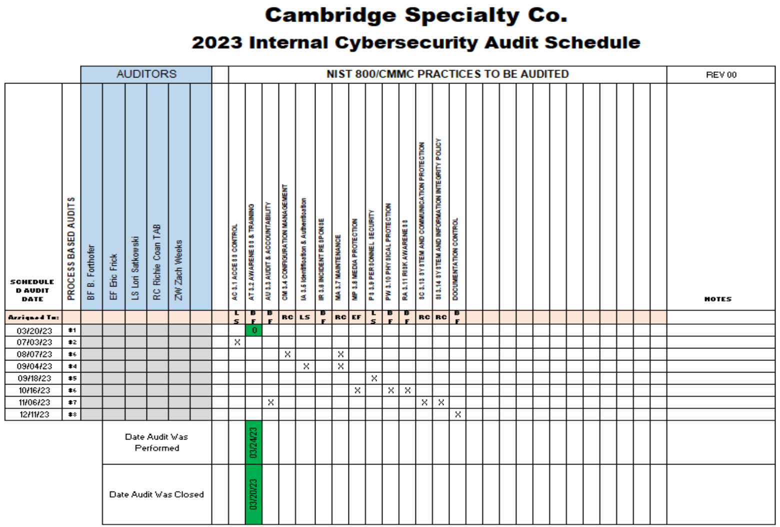
SDS MASTER LISTING UPDATES			
NAME	LAST UPDATE DATE	DUE DATE FOR NEXT REVIEW	COMMENTS
SDS Master LISTING UPDATES	3/8/23	4/8/23	CURRENT

Cybersecurity/QMS Compliance Management Methodology

- Cybersecurity - Utilizing AS9100 QMS Compliance Methodology Excel Spreadsheet to ensure Practices are Compliant on a Monthly Basis – Still In Development
- Utilizing CMMC Assessment Guide and Assessment Objectives



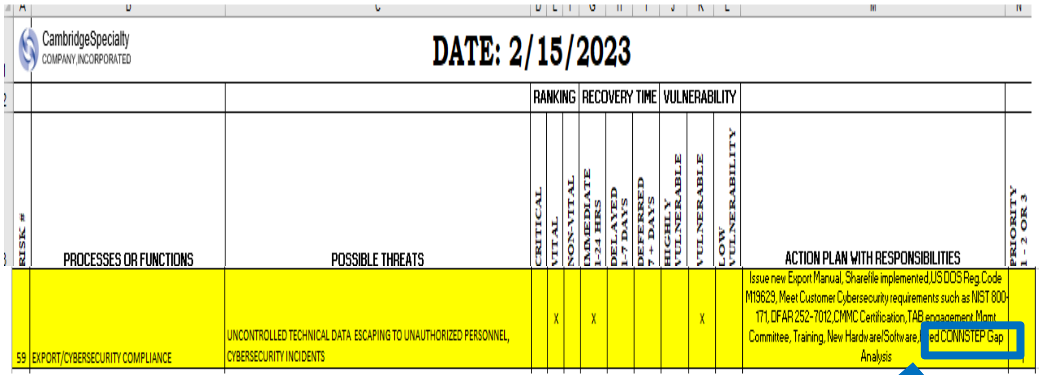




Cambridge Specialty Co.

2023 Internal Cybersecurity Audit Schedule

		AUDITORS						NIST 800/CMMC PRACTICES TO BE AUDITED														REV 00
SCHEDULED AUDIT DATE	PROCESS BASED AUDITS	BF B. Forthofer	EF Eric Frick	LS Lori Satkowski	RC Richie Coan TAB	ZW Zach Weeks		AC 3.1 ACCESS CONTROL	AT 3.2 AWARENESS & TRAINING	AU 3.3 AUDIT & ACCOUNTABILITY	CM 3.4 CONFIGURATION MANAGEMENT	IA 3.5 Identification & Authentication	IR 3.6 INCIDENT RESPONSE	MA 3.7 MAINTENANCE	MP 3.8 MEDIA PROTECTION	PS 3.9 PERSONNEL SECURITY	PW 3.10 PHYSICAL PROTECTION	RA 3.11 RISK AWARENESS	SC 3.13 SYSTEM AND COMMUNICATION PROTECTION	SI 3.14 SYSTEM AND INFORMATION INTEGRITY POLICY	DOCUMENTATION CONTROL	NOTES
Assigned To:								LS	BF	BF	RC	LS	BF	RC	EF	LS	BF	BF	RC	RC	BF	
03/20/23	#1								0													
07/03/23	#2							X														
08/07/23	#6										X			X								
09/04/23	#4											X		X								
09/18/23	#5															X						
10/16/23	#6														X		X	X				
11/06/23	#7									X									X	X		
12/11/23	#8																				X	
			Date Audit Was Performed						03/24/23													
			Date Audit Was Closed						03/20/23													



CambridgeSpecialty COMPANY,INCORPORATED

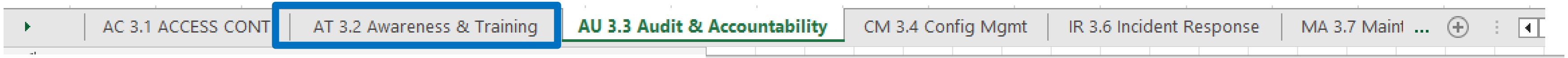
DATE: 2/15/2023

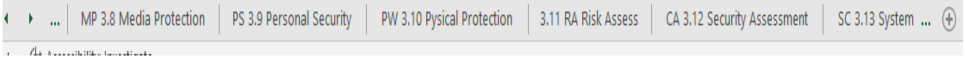
			RANKING			RECOVERY TIME			VULNERABILITY				
RISK #	PROCESSES OR FUNCTIONS	POSSIBLE THREATS	CRITICAL	VITAL	NON-VITAL	IMMEDIATE 1-24 HRS	DELAYED 1-7 DAYS	DEFERRED 7 + DAYS	HIGHLY VULNERABLE	VULNERABLE	LOW VULNERABILITY	ACTION PLAN WITH RESPONSIBILITIES	PRIORITY 1 - 2 OR 3
59	EXPORT/CYBERSECURITY COMPLIANCE	UNCONTROLLED TECHNICAL DATA ESCAPING TO UNAUTHORIZED PERSONNEL, CYBERSECURITY INCIDENTS		X		X				X		Issue new Export Manual, Sharefile implemented,US DOS Reg.Code M19629, Meet Customer Cybersecurity requirements such as NIST 800-171, DFAR 252-7012,CMMC Certification,TAB engagement,Mgmt Committee, Training, New Hardware/Software,Hired CONNSTEP Gap Analysis	

Hired CONNSTEP - Gap Analysis Utilizing the CMMC Assessment Guide Level 2 Version 2.0, December 2021

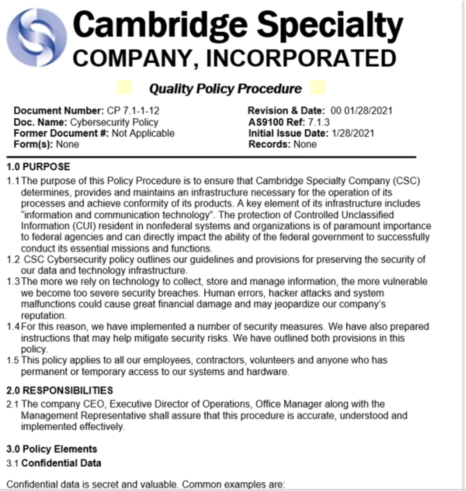
Cybersecurity/QMS Compliance Management Methodology

- Cybersecurity - Utilizing AS9100 QMS Compliance Methodology Excel Spreadsheet to ensure Practices are Compliant on a Monthly Basis – Still In Development
- Utilizing CMMC Assessment Guide and Assessment Objectives





Cybersecurity Procedure



Cambridge Specialty
COMPANY, INCORPORATED

Quality Policy Procedure

Document Number: CP 7.1-1-12
Doc. Name: Cybersecurity Policy
Former Document #: Not Applicable
Form(s): None

Revision & Date: 00 01/28/2021
AS9100 Ref: 7.1.3
Initial Issue Date: 1/28/2021
Records: None

1.0 PURPOSE

1.1 The purpose of this Policy Procedure is to ensure that Cambridge Specialty Company (CSC) determines, provides and maintains an infrastructure necessary for the operation of its processes and achieve conformity of its products. A key element of its infrastructure includes "information and communication technology". The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions.

1.2 CSC Cybersecurity policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

1.3 The more we rely on technology to collect, store and manage information, the more vulnerable we become too severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

1.4 For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

1.5 This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

2.0 RESPONSIBILITIES

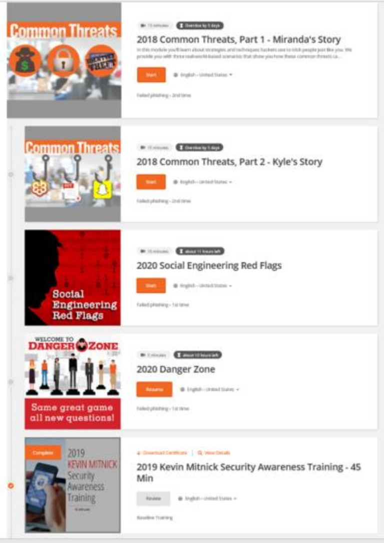
2.1 The company CEO, Executive Director of Operations, Office Manager along with the Management Representative shall assure that this procedure is accurate, understood and implemented effectively.

3.0 Policy Elements

3.1 **Confidential Data**

Confidential data is secret and valuable. Common examples are:

All Personnel with Email Addresses required to read procedure



2018 Common Threats, Part 1 - Miranda's Story

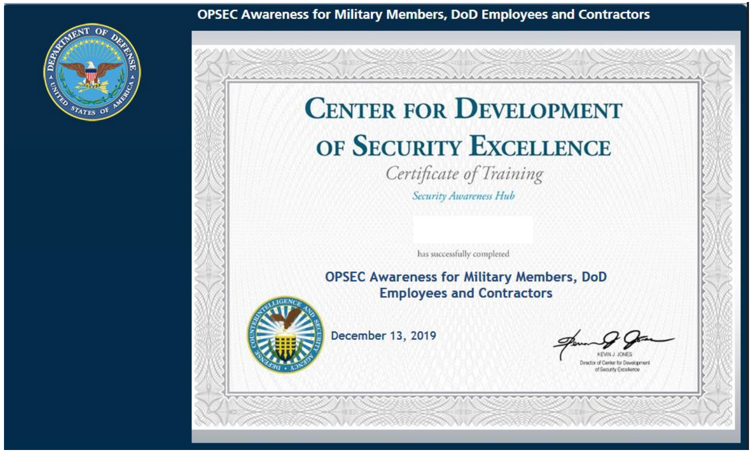
2018 Common Threats, Part 2 - Kyle's Story

2020 Social Engineering Red Flags

2020 Danger Zone

2019 Kevin Mitnick Security Awareness Training - 45 Min

Common Threats
Common Threats
Social Engineering Red Flags
WELCOME TO DANGER ZONE
Same great game all new questions!
2019 KEVIN MITNICK Security Awareness Training



OPSEC Awareness for Military Members, DoD Employees and Contractors

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE
Certificate of Training
Security Awareness Hub

has successfully completed

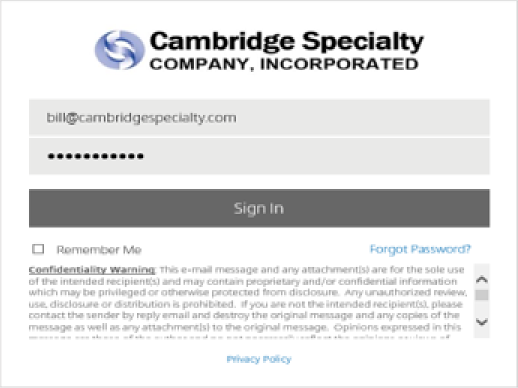
OPSEC Awareness for Military Members, DoD Employees and Contractors

December 13, 2019

KEVIN J. JONES
Director of Center for Development of Security Excellence

Cybersecurity/QMS Compliance Management Methodology
Technical Data Controls

Login Credentials



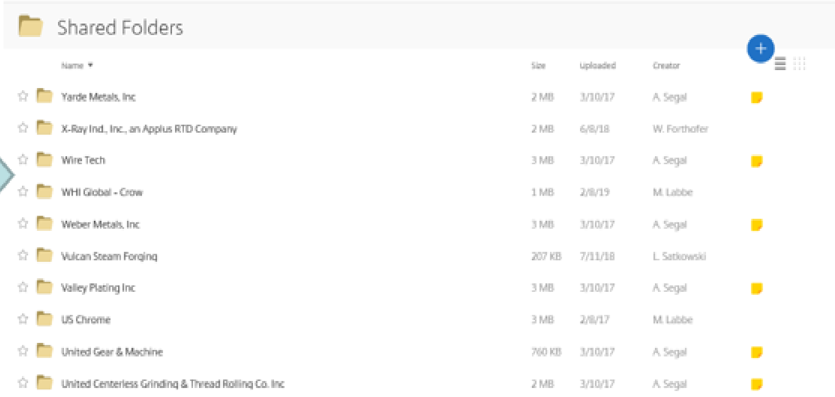
Cambridge Specialty COMPANY, INCORPORATED

bill@cambridgespecialty.com

••••••••••••

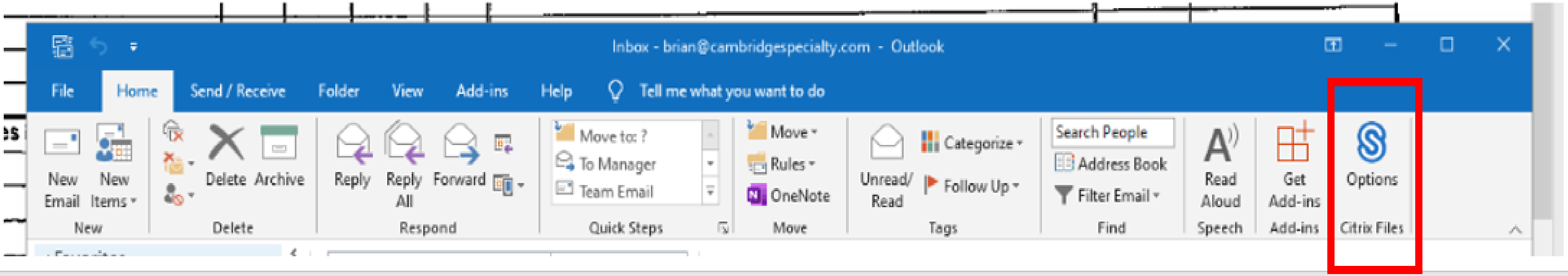
Confidentiality Warning: This e-mail message and any attachment(s) are for the sole use of the intended recipient(s) and may contain proprietary and/or confidential information which may be privileged or otherwise protected from disclosure. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient(s), please contact the sender by reply email and destroy the original message and any copies of the message as well as any attachment(s) to the original message. Opinions expressed in this

Shared Folders

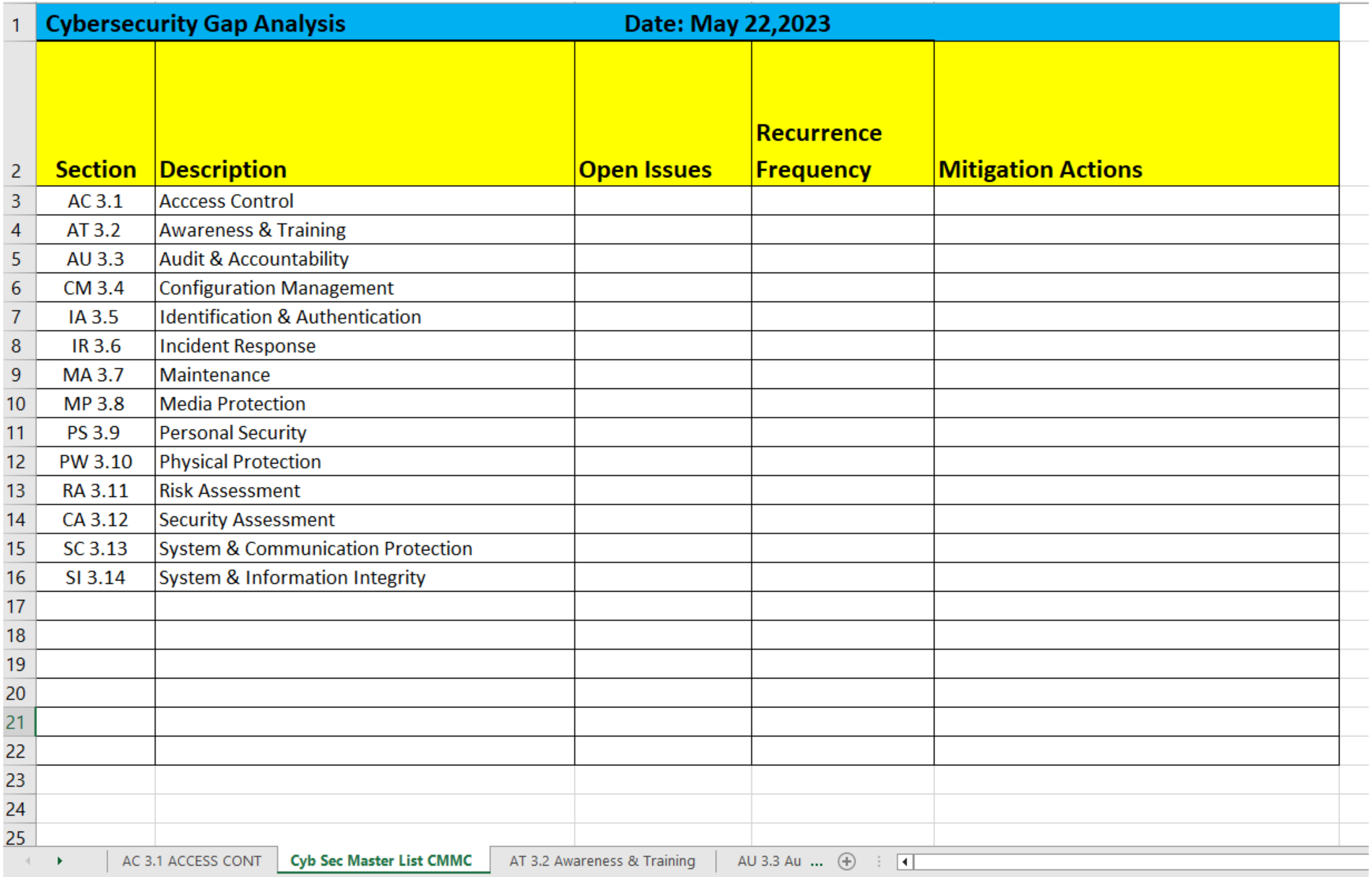


Shared Folders

Name ▾	Size	Uploaded	Creator
Yarde Metals, Inc	2 MB	3/10/17	A. Segal
X-Ray Ind., Inc., an Applus RTD Company	2 MB	6/8/18	W. Forthofer
Wire Tech	3 MB	3/10/17	A. Segal
WHI Global - Crow	1 MB	2/8/19	M. Labbe
Weber Metals, Inc	3 MB	3/10/17	A. Segal
Vulcan Steam Forging	207 KB	7/11/18	L. Satkowski
Valley Plating Inc	3 MB	3/10/17	A. Segal
US Chrome	3 MB	2/8/17	M. Labbe
United Gear & Machine	760 KB	3/10/17	A. Segal
United Centerless Grinding & Thread Rolling Co. Inc	2 MB	3/10/17	A. Segal

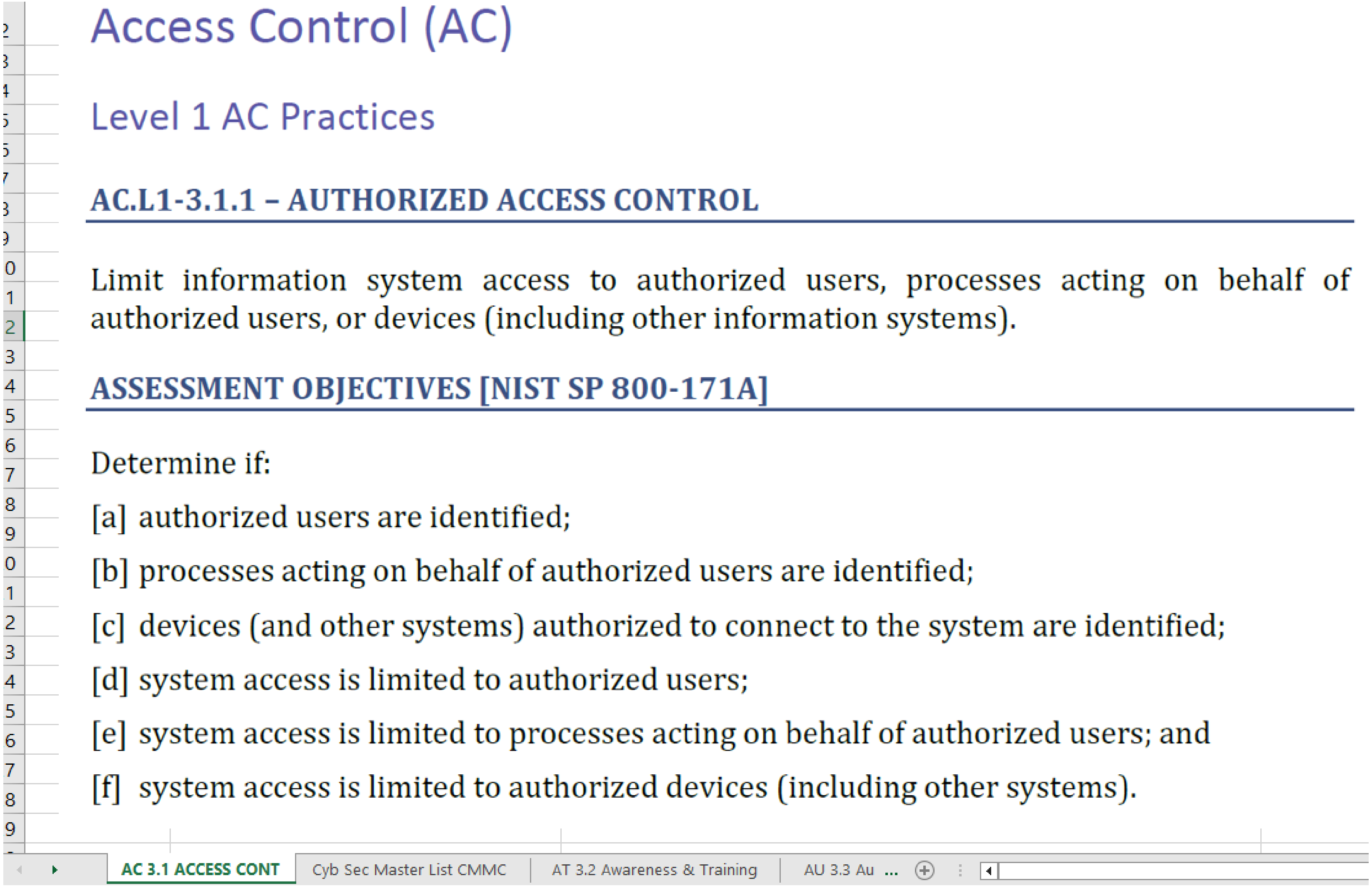


Inbox - brian@cambridgespecialty.com - Outlook



Cybersecurity Gap Analysis Date: May 22,2023

	Section	Description	Open Issues	Recurrence Frequency	Mitigation Actions
3	AC 3.1	Acccess Control			
4	AT 3.2	Awareness & Training			
5	AU 3.3	Audit & Accountability			
6	CM 3.4	Configuration Management			
7	IA 3.5	Identification & Authentication			
8	IR 3.6	Incident Response			
9	MA 3.7	Maintenance			
10	MP 3.8	Media Protection			
11	PS 3.9	Personal Security			
12	PW 3.10	Physical Protection			
13	RA 3.11	Risk Assessment			
14	CA 3.12	Security Assessment			
15	SC 3.13	System & Communication Protection			
16	SI 3.14	System & Information Integrity			
17					
18					
19					
20					
21					
22					



Access Control (AC)

Level 1 AC Practices

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).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

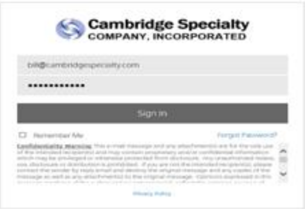
[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

Cambridge Specialty "Annual Re-curring" Training Matrix			
	Last Date Trng	Due Date	
Job Group	Training	Training	Comments
Senior Mgmt	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Mgmt Operations	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Sales Occupations	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Engineering	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Office/Admin	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Maintenance/Facilities	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Metal Workers	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Inspection	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Transportation	Oct/Nov/Dec 23	Oct/Nov/Dec 23	
Assembler	Oct/Nov/Dec 23	Oct/Nov/Dec 23	

Traning Topics				
Cybersecurity	Lock Out-		Nonconformance	Material
Safety	Tag Out	FOD	Tag Compliance	Handling
DPAS				
Records,Travelers,NC Forms				
Supplier QA				

Login Credentials


Cambridge Specialty
COMPANY, INCORPORATED

bill@cambridgespecialty.com
••••••••••••

Sign In

□ Remember Me
Forgot Password?

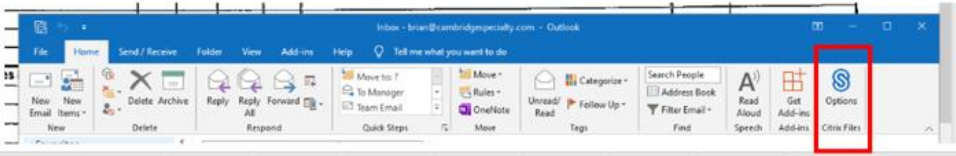
Confidentiality Warning: This e-mail message and any attachment(s) are for the sole use of the intended recipient(s) and may contain proprietary and/or confidential information [illegible]

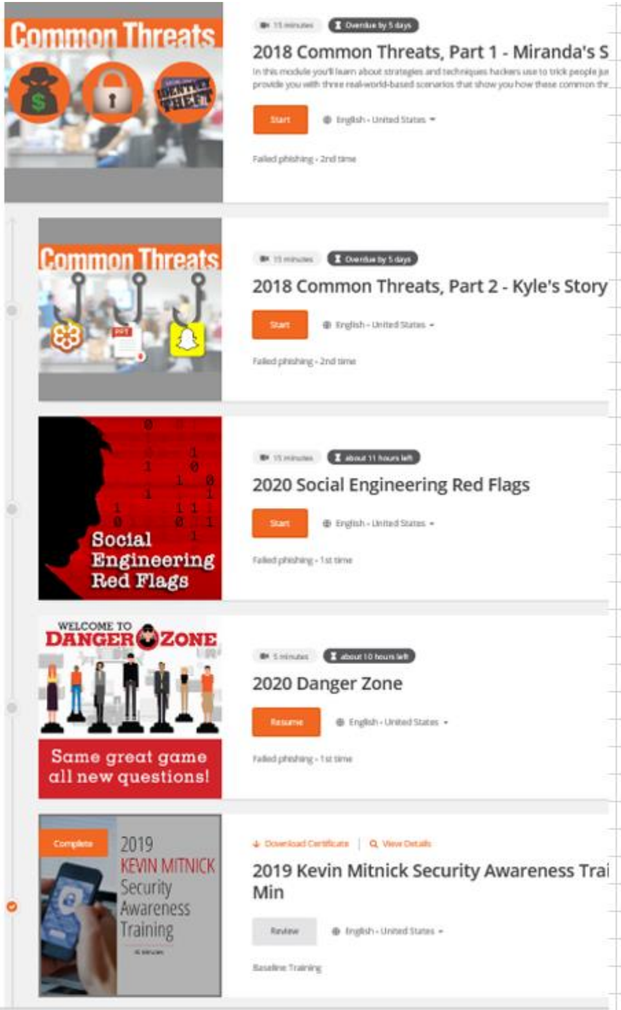
Privacy Policy

Shared Folders

Shared Folders

Name
Yardi Metals, Inc
A-Ray Ind., Inc., an Apollo RTD Company
Wire Tech
WH Global – Crow
Weber Metals, Inc
Vulcan Steam Forging
Valley Plating Inc
US Chrome
United Gear & Machine
United Centerless Grinding & Thread Rolling Co. Inc


Inbox - brian@cambridgespecialty.com - Outlook


Common Threats
Common Threats
Social Engineering Red Flags
WELCOME TO DANGER ZONE
Same great game all new questions!
Complete
2019 KEVIN MITNICK Security Awareness Training

15 minutes | Overdue by 5 days
2018 Common Threats, Part 1 - Miranda's S
In this module you'll learn about strategies and techniques hackers use to trick people ju
provide you with three real-world-based scenarios that show you how these common thr
Start | English - United States
Failed phishing - 2nd time

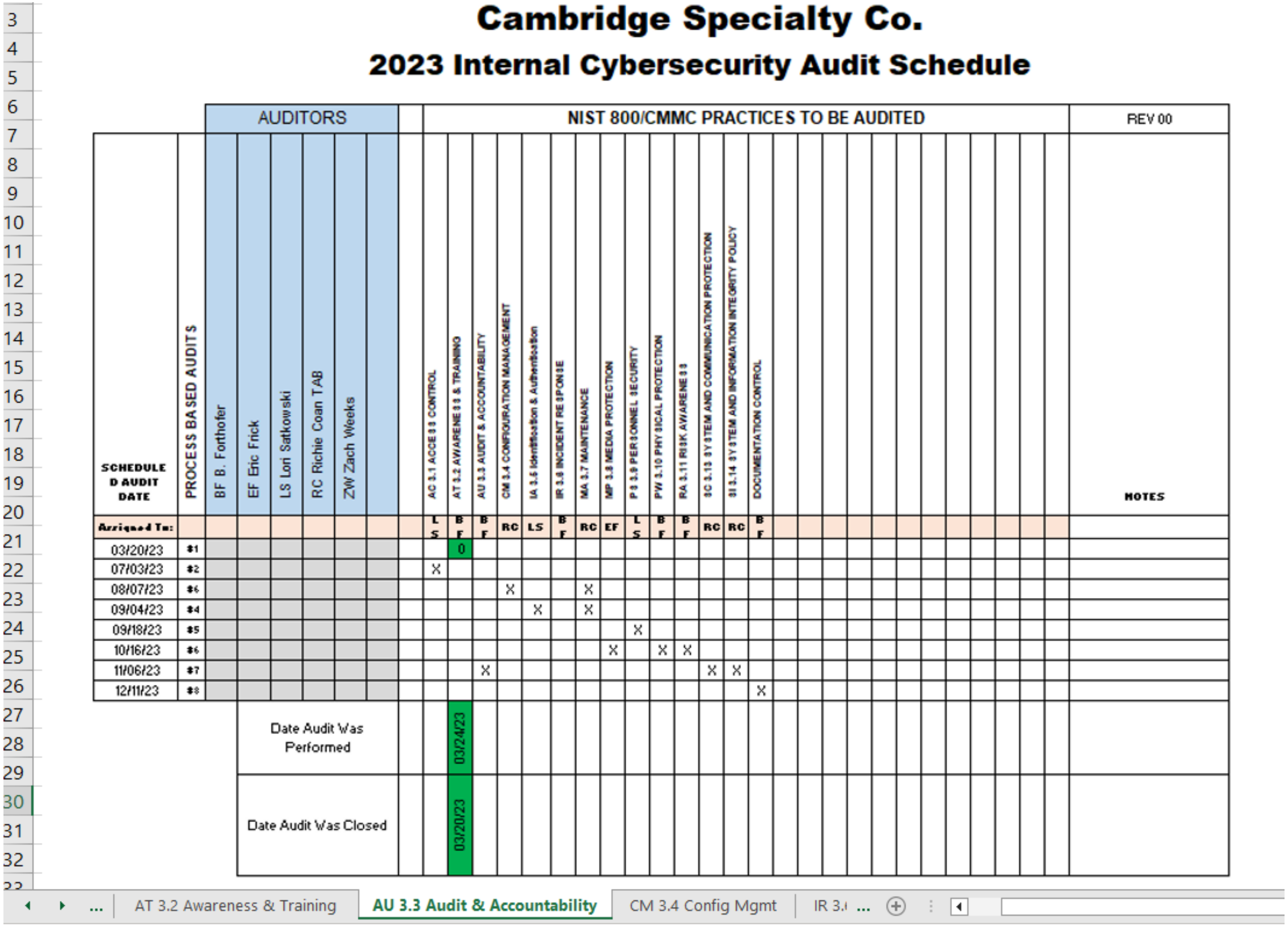
15 minutes | Overdue by 5 days
2018 Common Threats, Part 2 - Kyle's Story
Start | English - United States
Failed phishing - 2nd time

15 minutes | about 11 hours left
2020 Social Engineering Red Flags
Start | English - United States
Failed phishing - 1st time

5 minutes | about 10 hours left
2020 Danger Zone
Resume | English - United States
Failed phishing - 1st time

Download Certificate | View Details
2019 Kevin Mitnick Security Awareness Trai
Min
Review | English - United States
Baseline Training

AC 3.1 ACCESS CONT | Cyb Sec Master List CMMC | AT 3.2 Awareness & Training | AU 3.3 Audit & A ...



Cambridge Specialty Co.

2023 Internal Cybersecurity Audit Schedule

		AUDITORS					NIST 800/CMMC PRACTICES TO BE AUDITED														REV 00
SCHEDULED AUDIT DATE	PROCESS BASED AUDITS	BF B. Forthofer	EF Eric Frick	LS Lori Satkowski	RC Richie Coan TAB	ZW Zach Weeks	AC 3.1 ACCESS CONTROL	AT 3.2 AWARENESS & TRAINING	AU 3.3 AUDIT & ACCOUNTABILITY	CM 3.4 CONFIGURATION MANAGEMENT	IA 3.5 Identification & Authentication	IR 3.6 INCIDENT RESPONSE	MA 3.7 MAINTENANCE	MP 3.8 MEDIA PROTECTION	PS 3.9 PERSONNEL SECURITY	PW 3.10 PHYSICAL PROTECTION	RA 3.11 RISK AWARENESS	SC 3.13 SYSTEM AND COMMUNICATION PROTECTION	SI 3.14 SYSTEM AND INFORMATION INTEGRITY POLICY	DOCUMENTATION CONTROL	NOTES
Assigned To:							LS	BF	BF	RC	LS	BF	RC	EF	LS	BF	BF	RC	RC	BF	
03/20/23	#1							0													
07/03/23	#2						X														
08/07/23	#6									X			X								
09/04/23	#4										X		X								
09/18/23	#5														X						
10/16/23	#6													X		X	X				
11/06/23	#7								X									X	X		
12/11/23	#8																			X	
Date Audit Was Performed								03/24/23													
Date Audit Was Closed								03/20/23													

CONNSTEP
a CBIA affiliate

Questions?

CONNSTEP
350 Church St., Hartford, CT 06103 | 800.266.6672
CBIA & Affiliates | cbia.com | connstep.org | readyct.org

PART OF THE MEP National Network™

Connecticut | Department of Economic and Community Development

Glossary

CMMC – Cybersecurity Maturity Model Certification
CUI - Controlled Unclassified Information
DFARS - Defense Federal Acquisition Regulation Supplement
DIB – Defense Industrial Base
DIBCAC – Defense Industrial Base Cybersecurity Assessment Center
DCMA – Defense Contract Management Agency
IRP – Incident Response Plan
IT – Information Technology
MEP - Hollings Manufacturing Extension Partnership
MSP – Managed Service Provider
MSSP – Managed Security Service Provider
NIST – National Institute of Standards and Technology
NIST SP 800-171 – NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
POAM – Plan of Action and Milestones
SPRS – Supplier Performance Risk System
SSP – System Security Plan