

Navigating the Unknowns: A Live Mock CMMC Assessment

Fernando Machado
CISSP, CISM, CISA, CCA, CCP, CEH
info@cybersecinvestments.com
<https://cybersecinvestments.com>
(800) 960-8802

Matthew A. Titcombe, CISSP, CCA, CCP
cmmc.services@peakinfosec.us
<https://peakinfosec.com>
(352) 575-9737



Fernando Machado

CISO, Cybersec Investments



- **Cybersecurity Consulting:**

- 10+ years DoD cybersecurity experience
- NIST 800-171: Controlled Unclassified Information (CUI)
- Army, Navy, Air Force customer experience

- **Certified:**

- Certified CMMC Assessor (CCA)
- Certified CMMC Professional (CCP)
- Authorized CMMC 3rd Party Assessment Organization (C3PAO)

- **Awards:**

- President's Volunteer Service Award

1900 S Harbor City Blvd. Suite 328
Melbourne, Florida 32901

info@cybersecinvestments.com

1-800-960-8802

Follow us on LinkedIn:



Attain. Maintain. Prove it Anytime.



A Bit About Me



- Air Force & DoD Enterprise/Information Security Architect
- Air Force Program Manager at SAF/CIO and Air Force Academy
- Started Peak InfoSec in 2016
- CMMC Efforts:
 - Provisional Assessor #17—now a CCA
 - CEO of an Authorized CMMC 3rd Party Assessor Organization (C3PAO)
 - CMMC Training Curriculum Developer
 - Including Peak InfoSec, involved in 4 DoD Audits related to NIST SP 800-171/CMMC in 2022
 - Serve as the Information System Security Officer for Coalfire Federal & led them through their CMMC audit



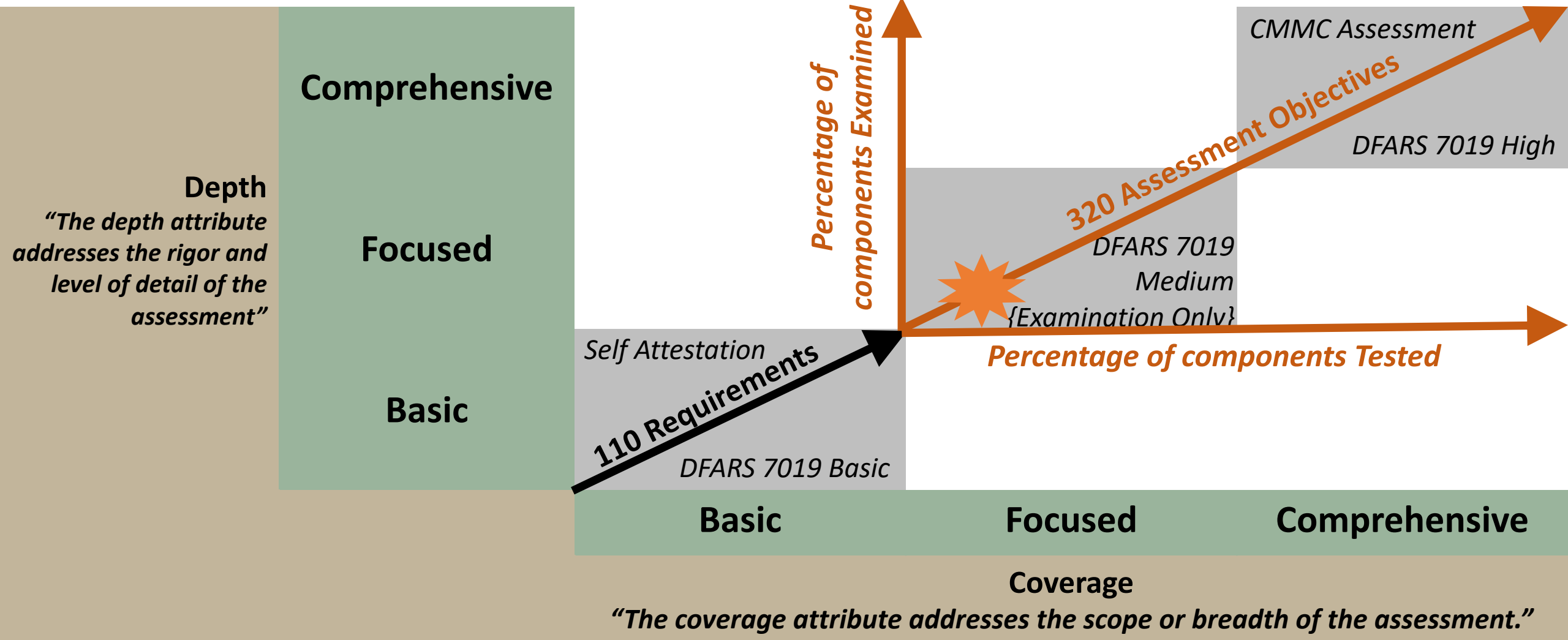
Conformity Assessment Purpose

- *Assessment* means the testing or evaluation of 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
 - Draft 32 CFR Part 170, §170.4, Acronyms and definitions

Overall Schedule

- 6 Weeks Prior to Assessment:
 - Pre-coordination call
 - Scope Validation & Certification Assessment Readiness Review
- 21 Days Prior to Assessment Start:
 - Assessment Plan Finalized
 - Artifact review repository established
- 7 Days Prior to Assessment Start:
 - Artifacts received by C3PAO for examination of artifacts
 - Baseline Freeze begins
- Assessment Week(s)
 - Assessment activities end immediately following last on-site visit
- Assessment End Date:
 - Final Out-Brief
- Appeals Window
 - To be defined in published CMMC Assessment Procedure
 - ~20 Business Days

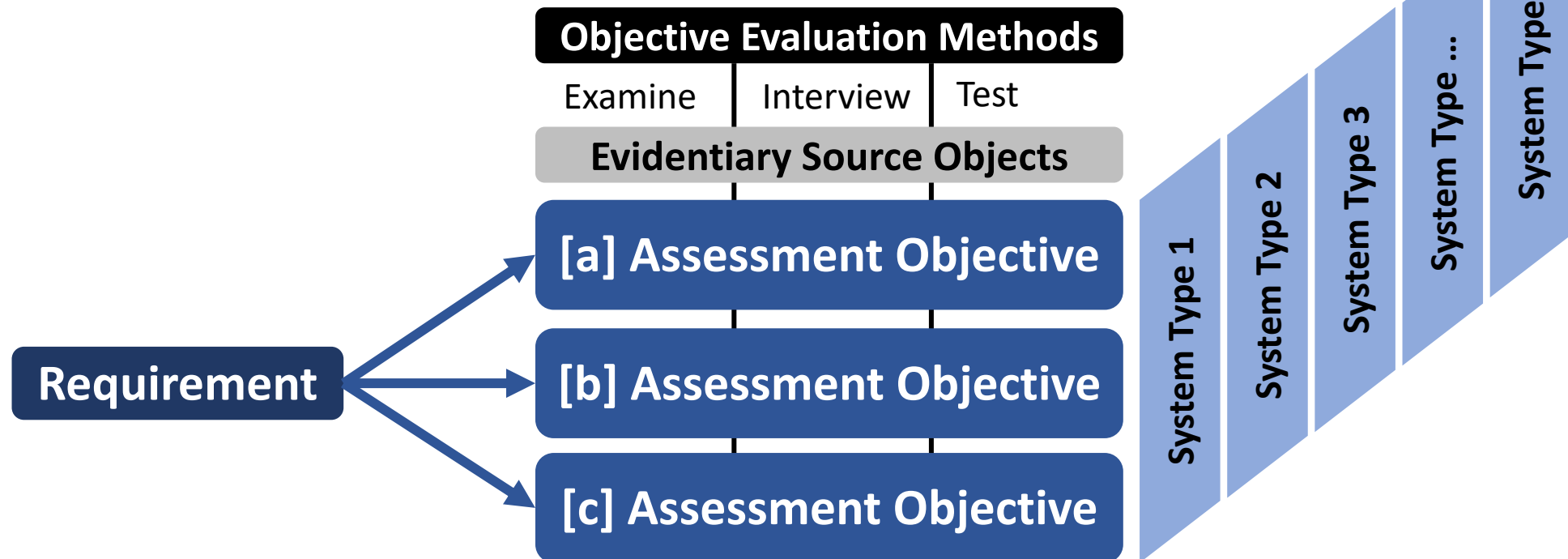
NIST SP 800-171A Appendix D: Assessment Procedure



Crap Rolls Up Hill

Requirement to Objective to System X

- Conformity must be evaluated against all systems of type
- A system of type can inherit controls from another system of type (e.g., using DUO Security)



Where are Assessors coming from?

Assessors

- Can not trust you
- Need to validate almost everything

Assessors validate your environment via

- Examinations *{Always}*
- Interviews *{Mostly}*
- Tests

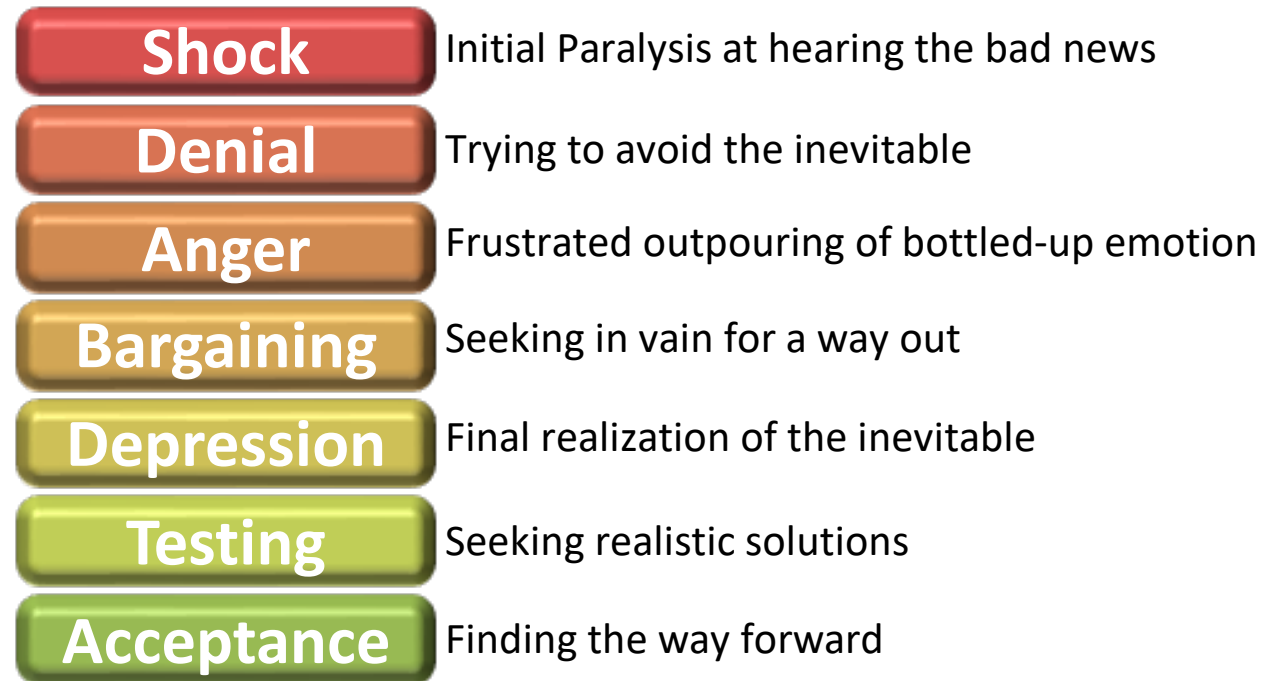
“Organizations [Certified Assessors] are not expected to employ all Assessment methods and objects contained within the Assessment procedures identified in this publication. Rather, organizations [Certified Assessors] have the flexibility to determine the level of effort needed and the assurance required for an Assessment (e.g., which Assessment methods and Assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization [contractor] can accomplish the Assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied”

CMMC Assessment Procedure V1.0 DRAFT, tailored from NIST SP 800-171A, para 2.1

Surgeons General's Warning for CMMC

- Discussing CMMC, NIST SP 800-171, FCI, & CUI have been proven to cause:
 - Anger
 - Anxiety
 - Brain Freezes
 - Confusion
 - Dumbfoundness
 - Mind-numbing pain
 - Panic-attacks
 - Sense of being overwhelmed

CMMC 7 Stages of Grief



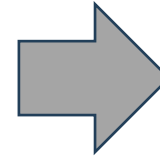


Three Types of Evidentiary Objects

System Design Documentation
"How it should be"



System Configuration
"How it was set up"



Supplemental Artifacts
"Proof it works"

- SSP
- "system design documentation"
- Policies, Plans, & Procedures
- Organization Defined Parameters



- SSP
- "system configuration settings and associated documentation"
- Policies, Plans, & Procedures
- "enterprise architecture documentation"



- Lists of...
- Records of ...
- Screenshots
- Training Content
- ...



NIST SP 800-171 Artifact Request Template

A	B	C	D	E	F	G	H	I	J	K	L	M	N
GROUP	FAMILY	SORT	LEVEL	OBJECTIVE	SECURITY REQUIREMENT	VIRTUAL (YES/NO)	EVIDENCE TYPE	TEAM INPUT	ASSESSOR	EVIDENCE EXAMPLES (ASSESSORS ARE NOT LIMITED OR RESTRICTED TO EXAMPLES)	CMMC ASSESSMENT CONSIDERATIONS (CMMC Assessment Guide - Level 2)	CMMC REFERENCES (in addition to NIST SP 800-171A and NIST SP 800-171R2)	Request
1	AC	3.01.09	L2	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Yes							
1	AC	3.01.09[a]	L2	3.1.9[a]	Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.	Yes	Artifact Examination	Document		SPP or policy (documentation) showing CUI-specified rules are identified, consistent, and associated with the specific CUI category.	[i] Are requirements identified for privacy and security notices, and do the implemented practices match those identified requirements? Discrepancies may indicate a deficient process and/or an incomplete practice. [ii] Are there any special requirements associated with the specific CUI category?		*BLUE = NEW REQUEST
1	AC	3.01.09[b]	L2	3.1.9[b]	Privacy and security notices are displayed.	Yes	Artifact Examination	Screen Share		Artifact that shows a consent banner or screen that a user sees as they login to the system	[i] Are requirements identified for privacy and security notices, and do the implemented practices match those identified requirements? Discrepancies may indicate a deficient process and/or an incomplete practice. [ii] Are appropriate notices displayed in areas where paper-based CUI is stored and processed?		*BLUE = NEW REQUEST
1	AC	3.01.10	L2	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Yes							

- Based on DIBCAC's spreadsheet & Publicly available Database <https://www.dcma.mil/DIBCAC/>
- Used to track artifacts
- Informs you of the teams expected assessment methodology

How do Assessors Validate via Examination?

Notice & Consent Banner | Endpoints

Saturday, December 12, 2020 7:40 PM

ODP(s)

Long version

***** WARNING *****

This computer system is the property of the Peak InfoSec LLC. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, Peak Info Sec's Acceptable Use Policy ("AUP"). Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions as set forth in Peak InfoSec's AUP. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

ODP Reviews

Date	Reviewer	Comment
26 August 2020	M. Titcombe	Initial Creation
7 August 2021	M. Titcombe	Conversion to this template

Related Practices

NISP SP 800-171	Description
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.

3.1.9	SECURITY REQUIREMENT Provide privacy and security notices consistent with applicable CUI rules.	
	ASSESSMENT OBJECTIVE Determine if:	
	3.1.9[a]	privacy and security notices required by CUI-specified rules are identified , consistent, and associated with the specific CUI category.
	3.1.9[b]	privacy and security notices are displayed.
POTENTIAL ASSESSMENT METHODS AND OBJECTS		
Examine: [SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners ; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records].		
Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers].		
Test: [SELECT FROM: Mechanisms implementing system use notification].		

How do Assessors Validate via Interviews?

Azure AD || Notice & Consent Banner
Saturday, March 6, 2021 6:09 PM

CI Description
Edit company branding

Sign-in page background image
Image size: 1500x1000px
File size: <300KB
File type: PNG, JPG, or JPEG

Banner logo
Image size: 240x240px
File size: 10KB
File type: Transparent PNG, JPG, or JPEG

Username hint
Sign-in page text
Advanced settings
Sign-in page background color
Square logo image, dark theme
Show option to remain signed in

*******WARNING*******

You are accessing a Peak InfoSec Information System (IS) that is provided for Peak InfoSec authorized use only. By using this system (which includes any device attached to this system), you consent to the following conditions:

- Peak InfoSec actively intercepts and monitors communications on this system
- You should have ****no**** expectation of privacy
- This system is used to handling of Controlled information and is secured accordingly

If you don't like this, sign off immediately.

For more info, contact the CISO @ ciso@peakinfosec.com

A description of the CI
Where possible, the person responsible for creating/maintaining the CI will include screenshots of the configuration
If the CI is related to an exception, document the date, time, and person who granted the exception, and the exception specifics in here

Related System(s)

- Microsoft Azure

CI Reviews

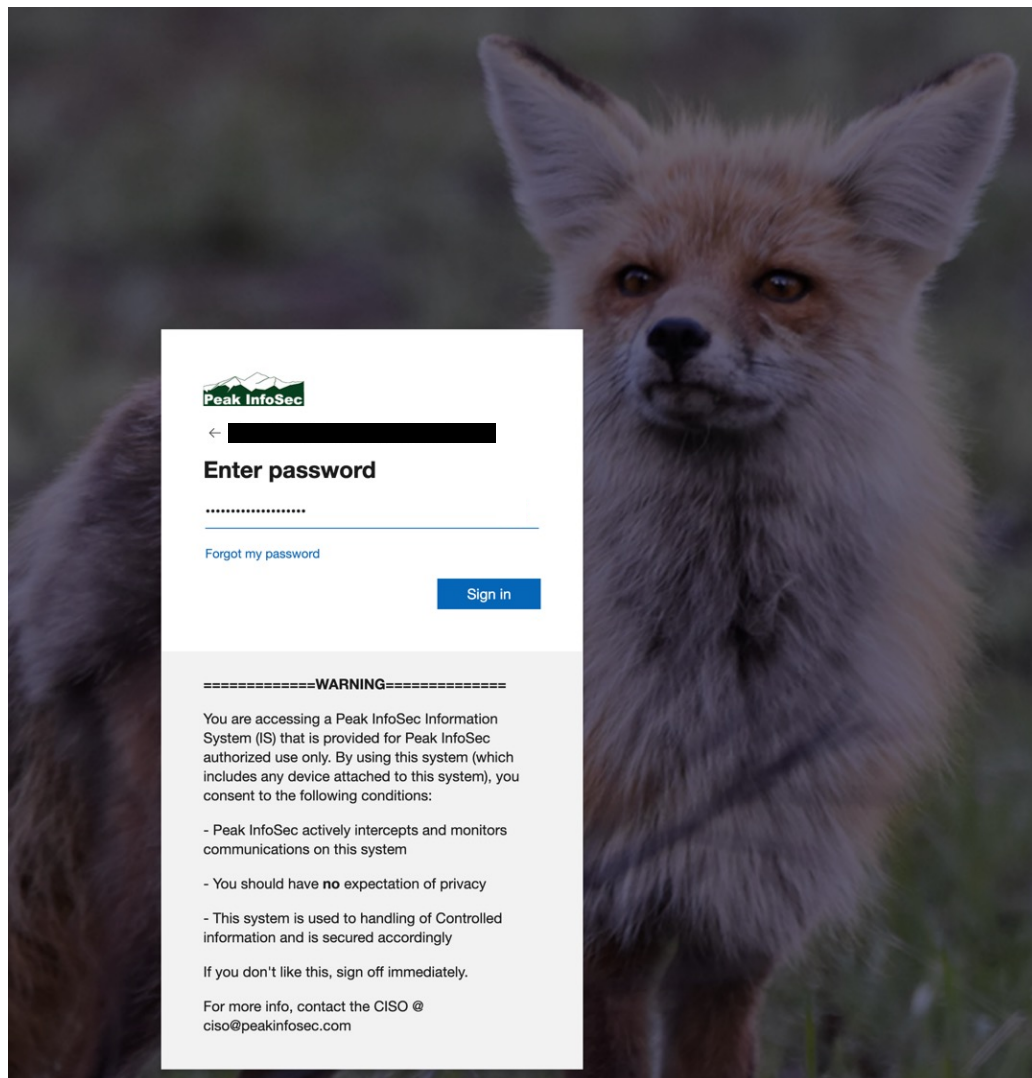
Date	Reviewer	Comment
6 March 2021	M. Titcombe	Initial Creation
28 August 2021	M. Titcombe	Update to CI template

Related Practices

CMMC ID	NISP SP 800-171	Description
AC.2.005	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.

3.1.9	SECURITY REQUIREMENT Provide privacy and security notices consistent with applicable CUI rules.
	ASSESSMENT OBJECTIVE Determine if:
3.1.9[a]	privacy and security notices required by CUI-specified rules are identified, consistent , and associated with the specific CUI category.
3.1.9[b]	privacy and security notices are displayed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS
	Examine: [SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation ; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records].
	Interview: [SELECT FROM: System or network administrators ; personnel with information security responsibilities ; personnel with responsibility for providing legal advice; system developers].
	Test: [SELECT FROM: Mechanisms implementing system use notification].

How do Assessors Validate via Test?



3.1.9	SECURITY REQUIREMENT Provide privacy and security notices consistent with applicable CUI rules.
ASSESSMENT OBJECTIVE Determine if:	
3.1.9[a]	privacy and security notices required by CUI-specified rules are identified, consistent , and associated with the specific CUI category.
3.1.9[b]	privacy and security notices are displayed.
POTENTIAL ASSESSMENT METHODS AND OBJECTS	
Examine: [SELECT FROM: Privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit logs and records; system design documentation; user acknowledgements of notification message or banner; system security plan; system use notification messages; system configuration settings and associated documentation; other relevant documents or records].	
Interview: [SELECT FROM: System or network administrators; personnel with information security responsibilities; personnel with responsibility for providing legal advice; system developers].	
Test: [SELECT FROM: Mechanisms implementing system use notification].	

ODP Disconnect

Notice & Consent Banner | Endpoints

Saturday, December 12, 2020 7:40 PM

ODP(s)

Long version

***** WARNING *****

This computer system is the property of the Peak InfoSec LLC. It is for authorized use only. By using this system, all users acknowledge notice of, and agree to comply with, Peak Info Sec's Acceptable Use Policy ("AUP"). Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions as set forth in Peak InfoSec's AUP. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

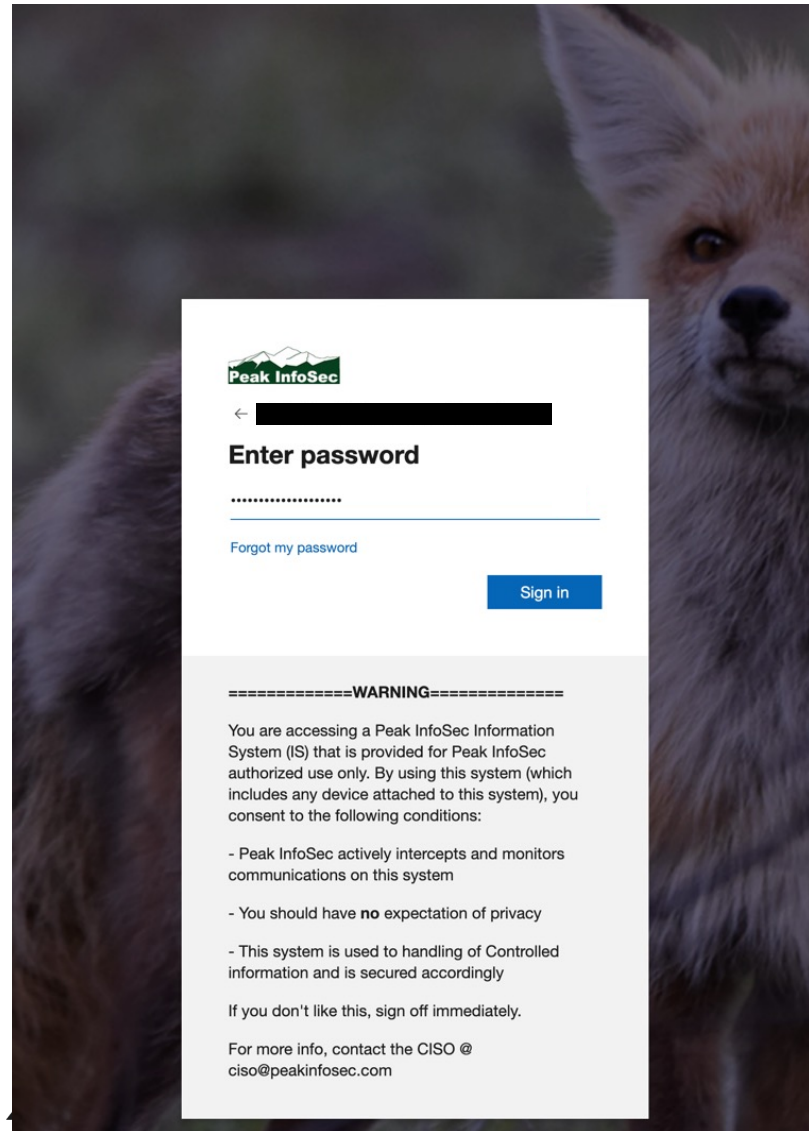
LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

ODP Reviews

Date	Reviewer	Comment
26 August 2020	M. Titcombe	Initial Creation
7 August 2021	M. Titcombe	Conversion to this template

Related Practices

NISP SP 800-171	Description
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.



Notice & Consent Banner | Azure

Saturday, December 12, 2020 7:40 PM

ODP(s)

Long version

*****WARNING*****

You are accessing a Peak InfoSec Information System (IS) that is provided for Peak InfoSec authorized use only. By using this system (which includes any device attached to this system), you consent to the following conditions:

- Peak InfoSec actively intercepts and monitors communications on this system
- You should have ****no**** expectation of privacy
- This system is used to handling of Controlled information and is secured accordingly

If you don't like this, sign off immediately.

For more info, contact the CISO @ ciso@peakinfosec.com

*****WARNING*****

ODP Reviews

Date	Reviewer	Comment
26 August 2020	M. Titcombe	Initial Creation
7 August 2021	M. Titcombe	Conversion to this template

Related Practices

NISP SP 800-171	Description
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.

Controlling the Assessment

- Rule #1: Do Not leave your Assessors alone to figure things out.
 - Point them directly to where the reference is at (e.g., Access Control Policy, Para #1 for 3.1.1)
- Rule #2: Use your SSP, “Document Traceability Matrix,” and supporting artifacts to guide your assessors.
 - “Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained.” *NIST SP 800-171, 3.12.4 Discussion*
- Rule #3: Control the conversation, even in the examination phase
 - Exam: Point to the cited reference
 - Interview: Stay on topic for the AO being addressed
 - Be ready to demonstrate the related components or bring up sample evidence
- Rule #4: Maximize the opportunity for assessors to use Examination only

Document Traceability Matrix

NIST SP 800-171 #	Requirement	Related Policies	Related Organizationally Defined Parameters	Related Plans	Related Procedure(s)	Related Configuration Items	Supporting Evidentiary Artifacts
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	<ul style="list-style-type: none"> Access Control Policy, para 12.3 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> Configuration Management Procedure New Device Authorization Procedure New User Onboarding Procedure Mobile Device Authorization Procedure 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> List of Authorized Users
...							
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	<ul style="list-style-type: none"> Access Control Policy, para 12.1 	<ul style="list-style-type: none"> Notice & Consent Banner Language 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> Configuration Management Procedure 	<ul style="list-style-type: none"> [Component Baseline] [Configuration Item] Azure Active Directory Branding Intune Windows 10/11 Device Settings 	<ul style="list-style-type: none"> Azure AD Branding Screenshot
...							
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	<ul style="list-style-type: none"> Incident Response Policy, para 5.1 	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> Peak InfoSec Audit and Accountability Plan Peak InfoSec Incident Response Plan 	<ul style="list-style-type: none"> Incident Response Plan Incident Response Playbook 		

CyberSec Investments Assessor's Playbook

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

- AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)
- AC.L1-3.1.2: Limit information system access to the types of transactions and functions that authorize users to perform
- AC.L1-3.1.20: Verify and control/limit connections to and use of external information systems
- AC.L1-3.1.22: Control information posted or processed on publicly accessible information systems
- AC.L2-3.1.3: Control the flow of CUI in accordance with approved authorizations
- AC.L2-3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without coll
- AC.L2-3.1.5: Employ the principle of least privilege, including for specific security functions and priv
- AC.L2-3.1.6: Use non-privileged accounts or roles when accessing non-security functions
- AC.L2-3.1.7: Prevent non-privileged users from executing privileged functions and capture the exec
- AC.L2-3.1.8: Limit unsuccessful logon attempts
- AC.L2-3.1.9: Provide privacy and security notices consistent with applicable CUI rules
- AC.L2-3.1.10: Use session lock with pattern-hiding displays to prevent access and viewing of data af
- AC.L2-3.1.11: Terminate (automatically) user sessions after a defined condition
- AC.L2-3.1.12: Monitor and control remote access sessions
- AC.L2-3.1.13: Employ cryptographic mechanisms to protect the confidentiality of remote access ses
- AC.L2-3.1.14: Route remote access via managed access control points
- AC.L2-3.1.15: Authorize remote execution of privileged commands and remote access to security-n
- AC.L2-3.1.16: Authorized wireless access prior to allowing such connections
- AC.L2-3.1.17: Protect wireless access using authentication and encryption
- AC.L2-3.1.18: Control connection of mobile devices
- AC.L2-3.1.19: Encrypt CUI on mobile devices and mobile computing platforms
- AC.L2-3.1.21: Limit use of portable storage devices on external systems

Documenting the Assessment

The screenshot shows the 'ASSESSMENT TOOL v.202402' interface. The top navigation bar includes buttons for 'Open Seven Stages Image', 'Score Assist', 'Open Interviewee(s)', 'Open Components(s)', 'Open Artifacts', and filters for 'Filter to Pending Only', 'Filter to In-Process Only', 'Filter to NOT MET', and 'All Records'. The main content area is divided into several sections:

- Requirement Section:** Shows 'Family 3.1', 'Requirement 3.1.1', and a description: 'Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)'. It also includes 'Review Complete' (Pending), 'Requirement Status' (Pending), and 'Deduction' (5).
- Requirement Notes:** A text area for notes.
- Recommended Remediations / Non-Conformant Components:** Two dropdown menus.
- NIST 800-171 Discussion:** A text block explaining the requirement's focus on account management.
- Potential Examination Objects:** A list of items to be examined, such as 'Access control policy; procedures addressing account management...'. A callout 'Who did we interview?' points to this section.
- Potential Interviewees:** A list of personnel, such as 'Personnel with account management responsibilities...'. A callout 'Who did we interview?' points to this section.
- Potential Test Sources:** A list of organizational processes, such as 'Organizational processes for managing system accounts...'. A callout 'Who did we interview?' points to this section.
- Objective Section:** Shows 'Objective Number 3.1.1[a]', 'Status Pending', and 'Review Method Document'. A callout 'Repeat for each objective' points to this section.
- Assessment Objective Validation Write Up:** A text area containing 'test'. A yellow callout 'Complete after taking notes' points to this section.
- Examination Section:** Includes 'Examination Notes' (containing 'test'), 'Examined Artifacts', and 'Requested Artifacts'. A callout 'Examination notes for citations and disconnects' points to the 'Examination Notes' field.
- Interview Section:** Includes 'Interview Notes' and 'Interviewee(s)'. A callout 'Interview notes' points to the 'Interview Notes' field.
- Test Section:** Includes 'Test Notes' and 'Tested Components'. A callout 'Testing/demonstration result notes' points to the 'Test Notes' field.

What are we examining?

Who did we interview?

Requested artifacts

Who did we interview?

Repeat for each objective

Complete after taking notes

Examination notes for citations and disconnects

Interview notes

Testing/demonstration result notes

What was tested?



Control yourself during the assessment



Rule #5: When we say we are done with a control, stop talking

- Don't let fear "that we don't get it" get you into trouble
- Don't try and show off

RA.L2-3.11.2, Vulnerability Scan

3.11.2	<p>SECURITY REQUIREMENT</p> <p>Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.</p>										
	<p>ASSESSMENT OBJECTIVE</p> <p><i>Determine if:</i></p> <table border="1"> <tr> <td data-bbox="1166 292 1337 396">3.11.2[a]</td> <td data-bbox="1337 292 2537 396"><i>the frequency to scan for vulnerabilities in organizational systems and applications is defined.</i></td> </tr> <tr> <td data-bbox="1166 396 1337 501">3.11.2[b]</td> <td data-bbox="1337 396 2537 501"><i>vulnerability scans are performed on organizational systems with the defined frequency.</i></td> </tr> <tr> <td data-bbox="1166 501 1337 605">3.11.2[c]</td> <td data-bbox="1337 501 2537 605"><i>vulnerability scans are performed on applications with the defined frequency.</i></td> </tr> <tr> <td data-bbox="1166 605 1337 709">3.11.2[d]</td> <td data-bbox="1337 605 2537 709"><i>vulnerability scans are performed on organizational systems when new vulnerabilities are identified.</i></td> </tr> <tr> <td data-bbox="1166 709 1337 813">3.11.2[e]</td> <td data-bbox="1337 709 2537 813"><i>vulnerability scans are performed on applications when new vulnerabilities are identified.</i></td> </tr> </table> <p>POTENTIAL ASSESSMENT METHODS AND OBJECTS</p> <p>Examine: [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].</p> <p>Interview: [SELECT FROM: Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].</p>	3.11.2[a]	<i>the frequency to scan for vulnerabilities in organizational systems and applications is defined.</i>	3.11.2[b]	<i>vulnerability scans are performed on organizational systems with the defined frequency.</i>	3.11.2[c]	<i>vulnerability scans are performed on applications with the defined frequency.</i>	3.11.2[d]	<i>vulnerability scans are performed on organizational systems when new vulnerabilities are identified.</i>	3.11.2[e]	<i>vulnerability scans are performed on applications when new vulnerabilities are identified.</i>
3.11.2[a]	<i>the frequency to scan for vulnerabilities in organizational systems and applications is defined.</i>										
3.11.2[b]	<i>vulnerability scans are performed on organizational systems with the defined frequency.</i>										
3.11.2[c]	<i>vulnerability scans are performed on applications with the defined frequency.</i>										
3.11.2[d]	<i>vulnerability scans are performed on organizational systems when new vulnerabilities are identified.</i>										
3.11.2[e]	<i>vulnerability scans are performed on applications when new vulnerabilities are identified.</i>										
	<p>Test: [SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].</p>										

Fernando Machado

CISSP, CISM, CISA, CCA, CCP, CEH
info@cybersecinvestments.com
https://cybersecinvestments.com
(800) 960-8802



Matthew A. Titcombe

CISSP, CCA, CCP
cmmc.services@peakinfosec.us
https://peakinfosec.com
(352) 575-9737

