CMMC Assessment:
The Assessor's POV

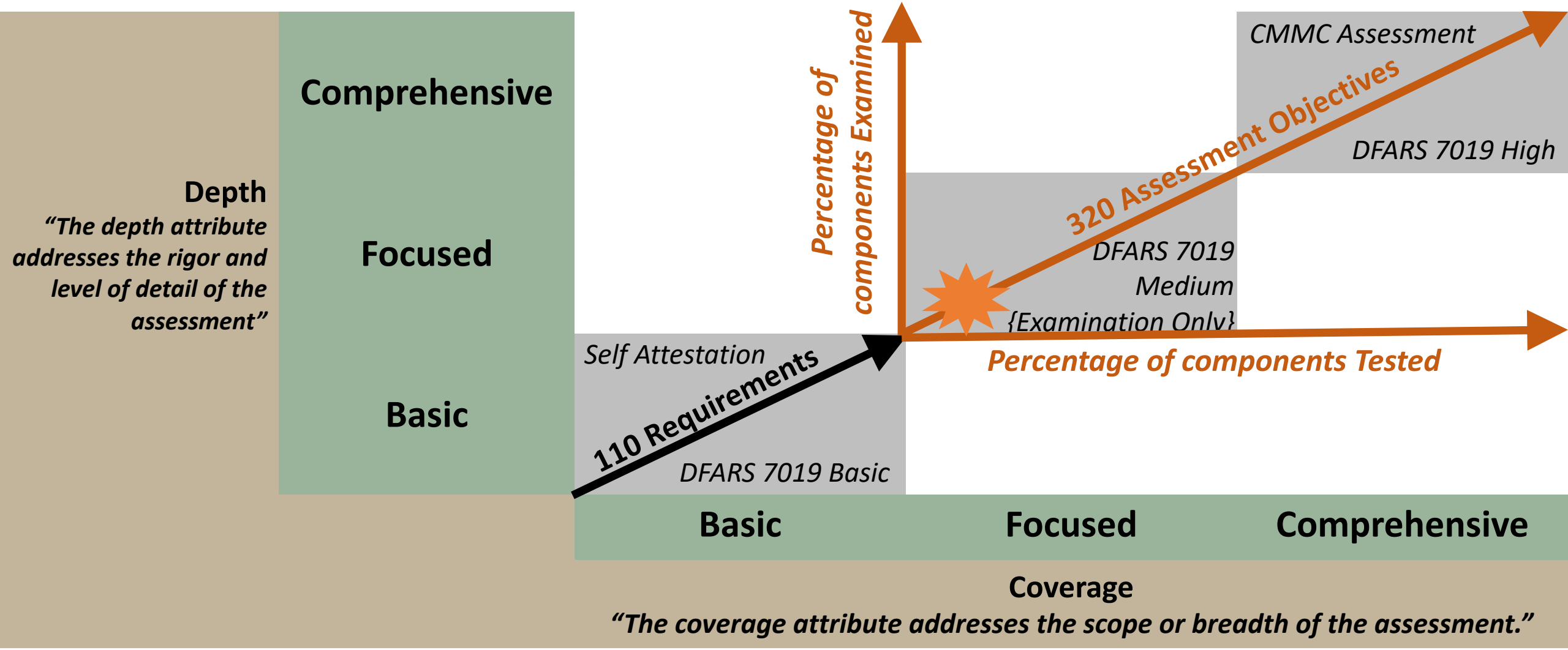
Fernando Machado
CISSP, CISM, CISA, CCA, CCP, CEH
info@cybersecinvestments.com
https://cybersecinvestments.com
(800) 960-8802

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

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

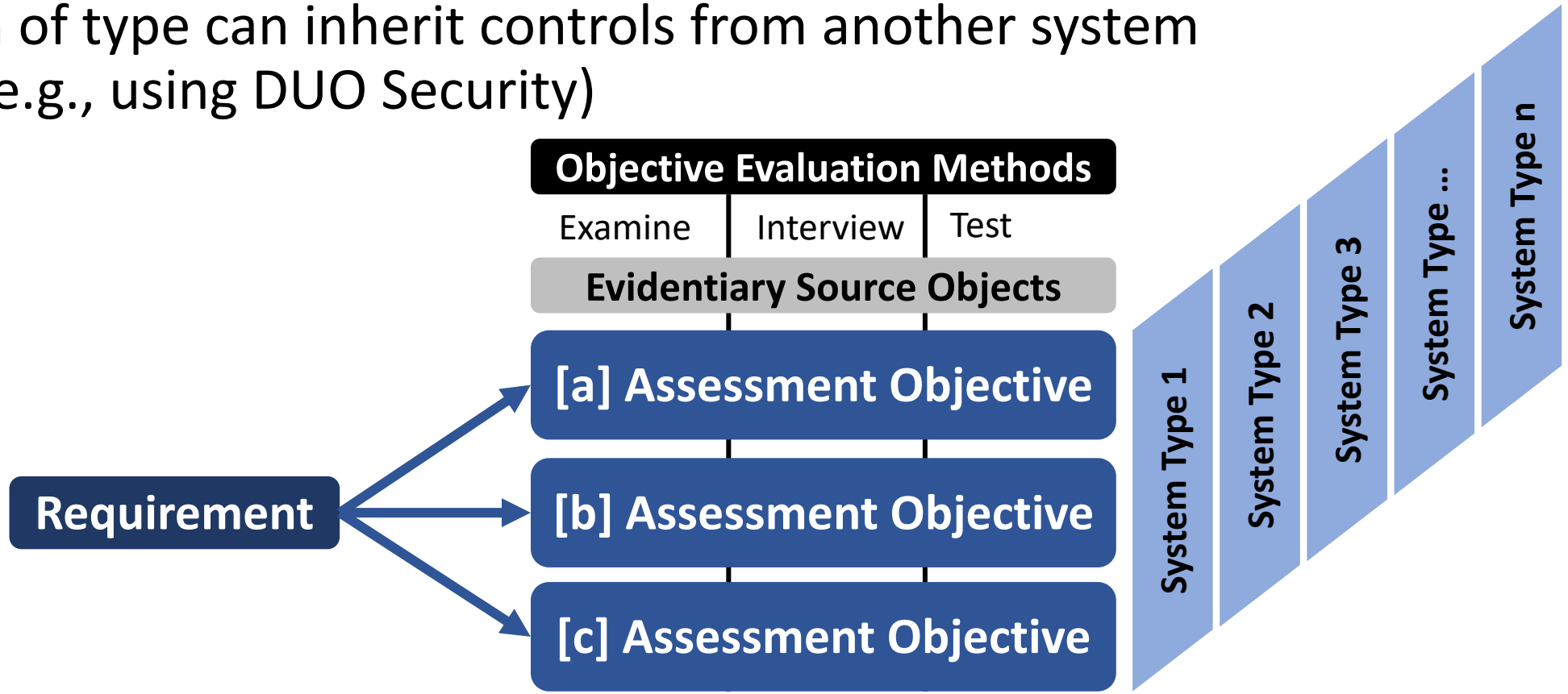
NIST SP 800-171A Appendix D: Assessment Procedure



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

Shock	Initial Paralysis at hearing the bad news
Denial	Trying to avoid the inevitable
Anger	Frustrated outpouring of bottled-up emotion
Bargaining	Seeking in vain for a way out
Depression	Final realization of the inevitable
Testing	Seeking realistic solutions
Acceptance	Finding the way forward

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		SSP 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 s forth in Peak InfoSec's AUP. By continuing to use this system you indicate your awareness of 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.

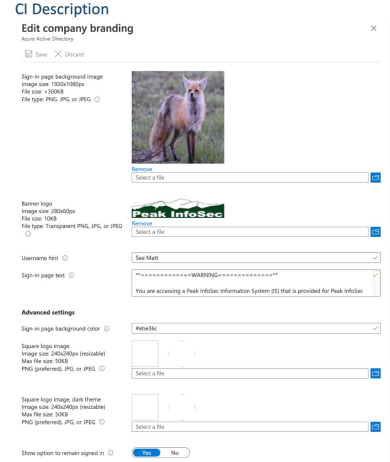
3.1.9	**SECURITY REQUIREMENT** Provide privacy and security notices consistent with applicable CUI rules.
	ASSESSMENT OBJECTIVE Determine if:
	3.1.9[a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.
	3.1.9[b] privacy 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



==========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

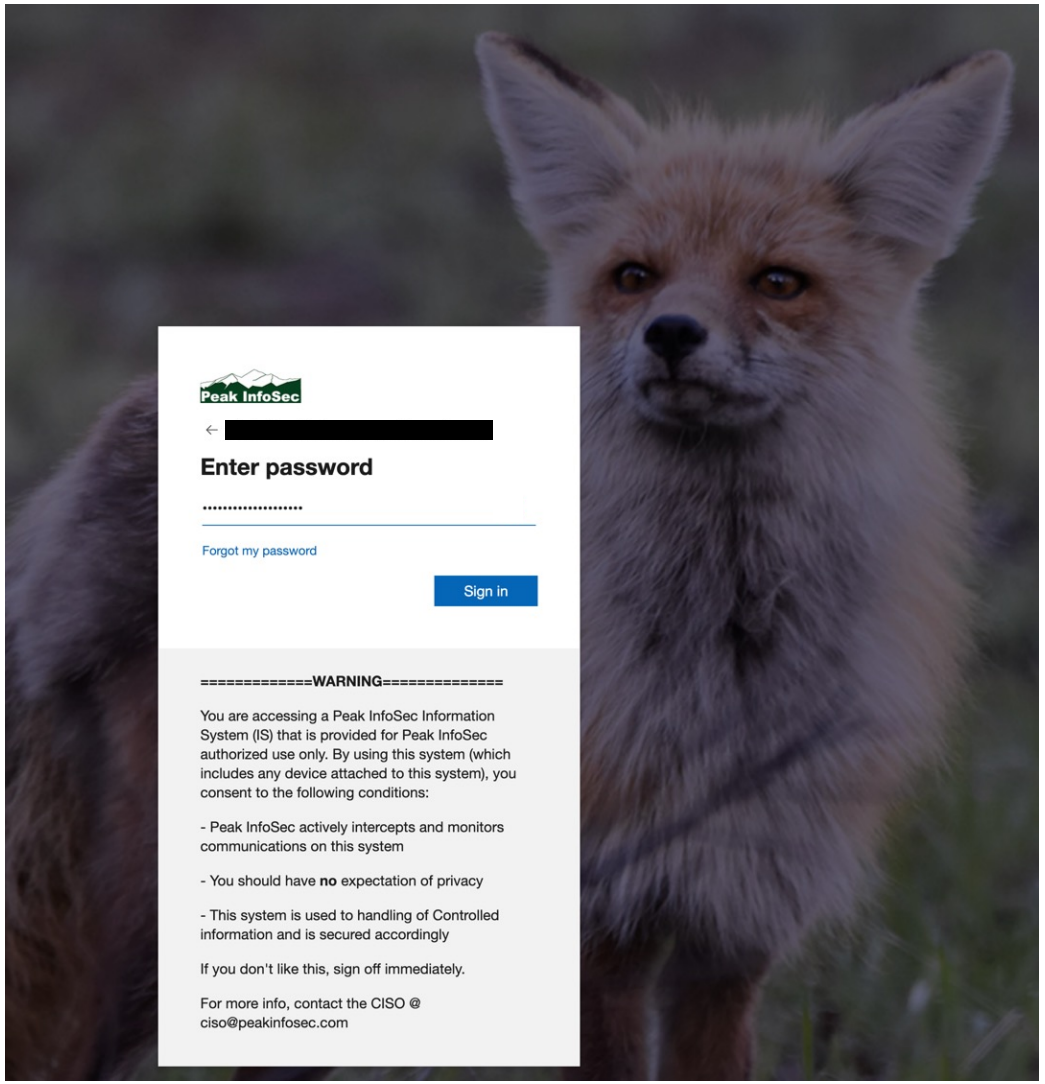
Related Practices

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].

CUI-CON

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.

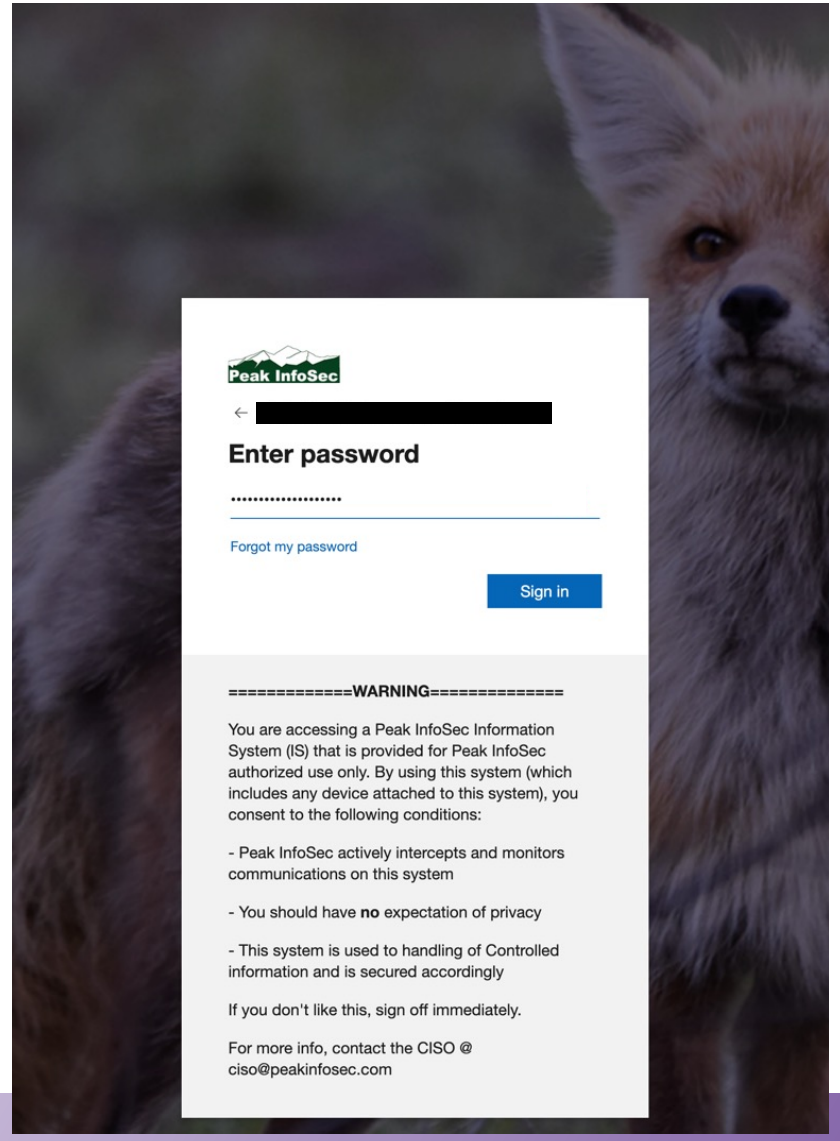
****

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.

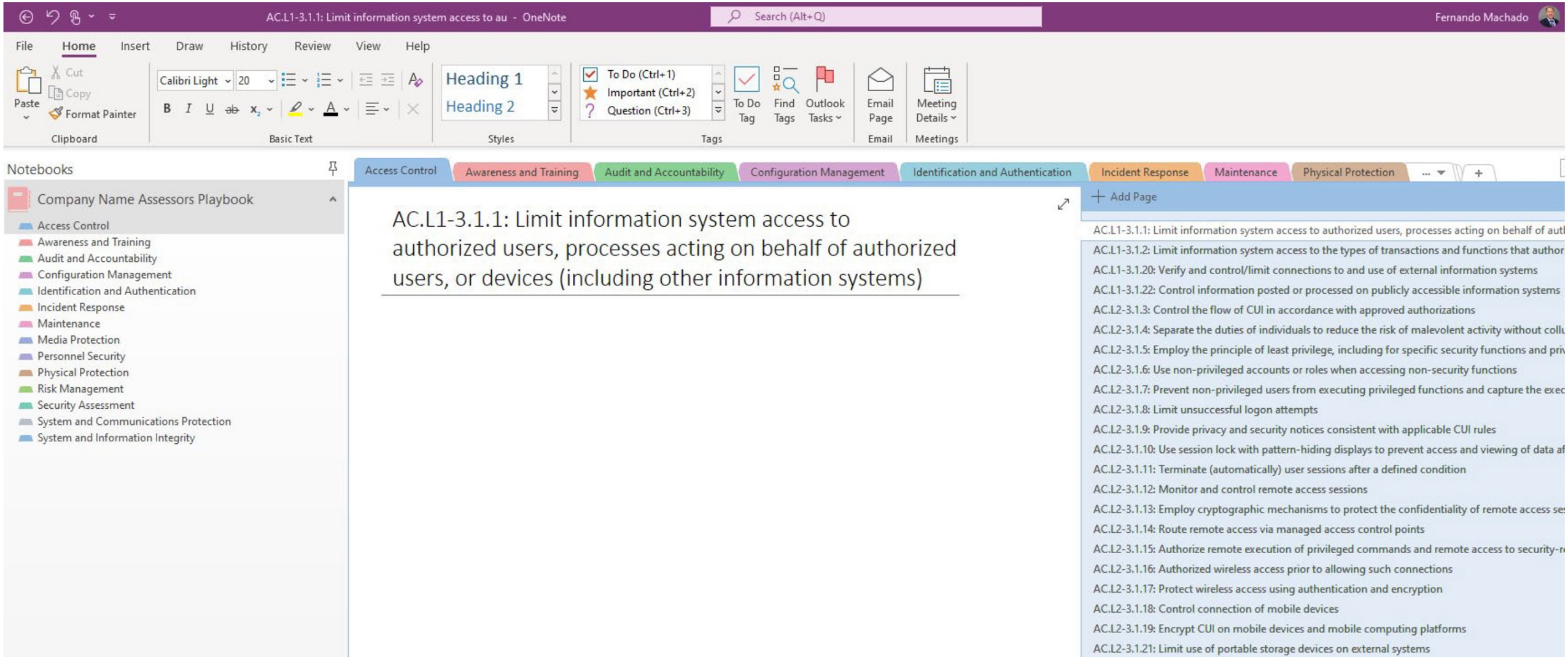
Controlling the Assessment

- 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

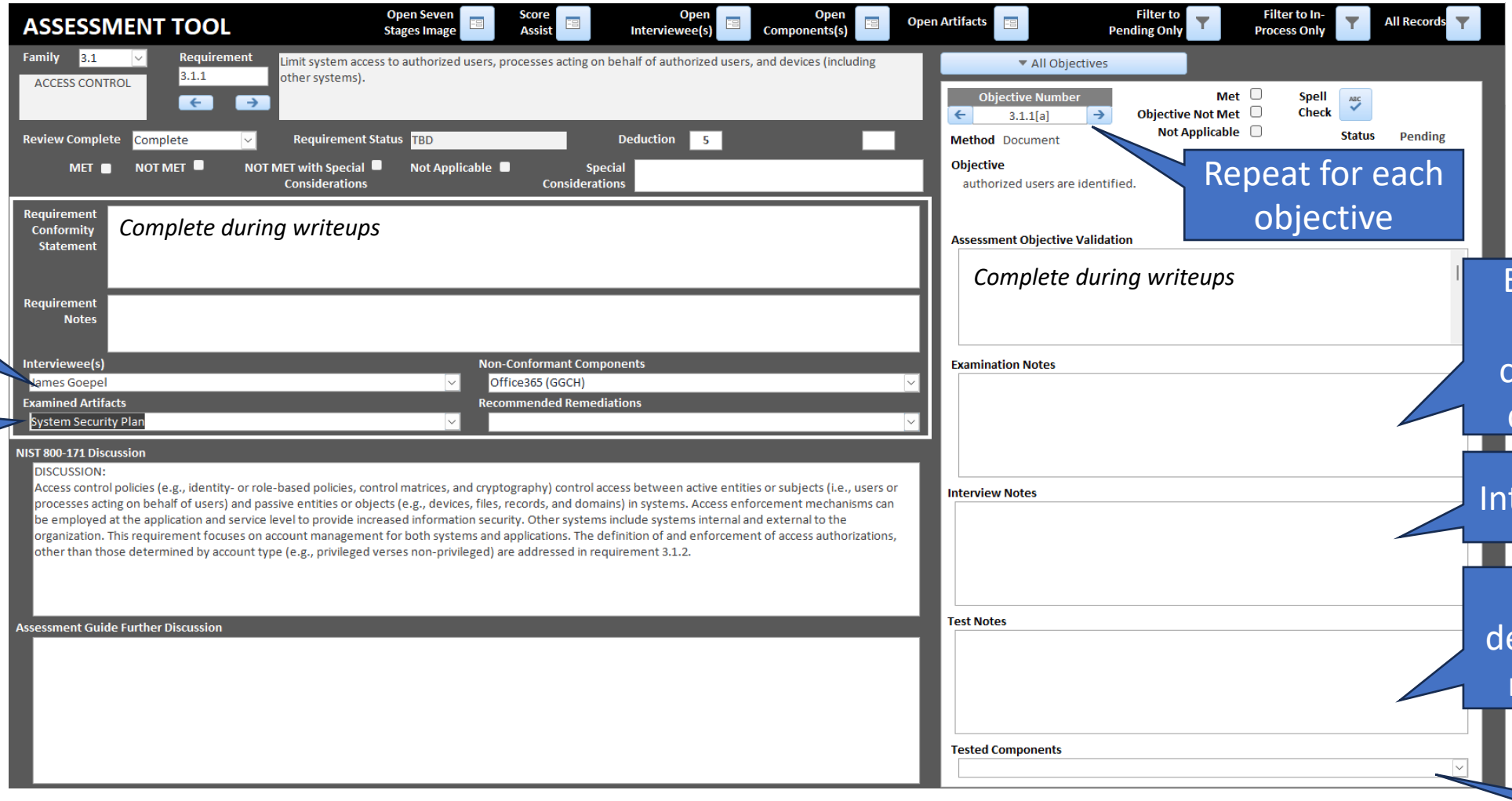
Document Traceability Matrix

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).	• Access Control Policy, para 12.3	•	•	• Configuration Management Procedure • New Device Authorization Procedure • New User Onboarding Procedure • Mobile Device Authorization Procedure	•	• List of Authorized Users
…							
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	• Access Control Policy, para 12.1	• Notice & Consent Banner Language	•	• Configuration Management Procedure	• [Component Baseline] | [Configuration Item] • Azure Active Directory | Branding • Intune | Windows 10/11 Device Settings	• 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.	• Incident Response Policy, para 5.1	•	• Peak InfoSec Audit and Accountability Plan • Peak InfoSec Incident Response Plan	• Incident Response Plan • Incident Response Playbook		

CyberSec Investments Assessor's Playbook



Documenting the Assessment



Who are we interviewing?

What are we examining?

Repeat for each objective

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	**SECURITY REQUIREMENT** Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.11.2[a] *the frequency to scan for vulnerabilities in organizational systems and applications is defined.*
	3.11.2[b] *vulnerability scans are performed on organizational systems with the defined frequency.*
	3.11.2[c] *vulnerability scans are performed on applications with the defined frequency.*
	3.11.2[d] *vulnerability scans are performed on organizational systems when new vulnerabilities are identified.*
	3.11.2[e] *vulnerability scans are performed on applications when new vulnerabilities are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **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]. **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].
	Test: [*SELECT FROM:* Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].