

# Behind the Failures: Why Companies Still Miss the Mark on CMMC

Matthew A. Titcombe, CCA, CCP, PI, CISSP  
President



# Assessment

- ***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, as defined in [§§ 170.15](#) through [170.18](#). (CMMC-custom term)
  - 32 CFR 170.4(b) “Assessment”

# Know your Scope



**Out-of-Scope "External"**

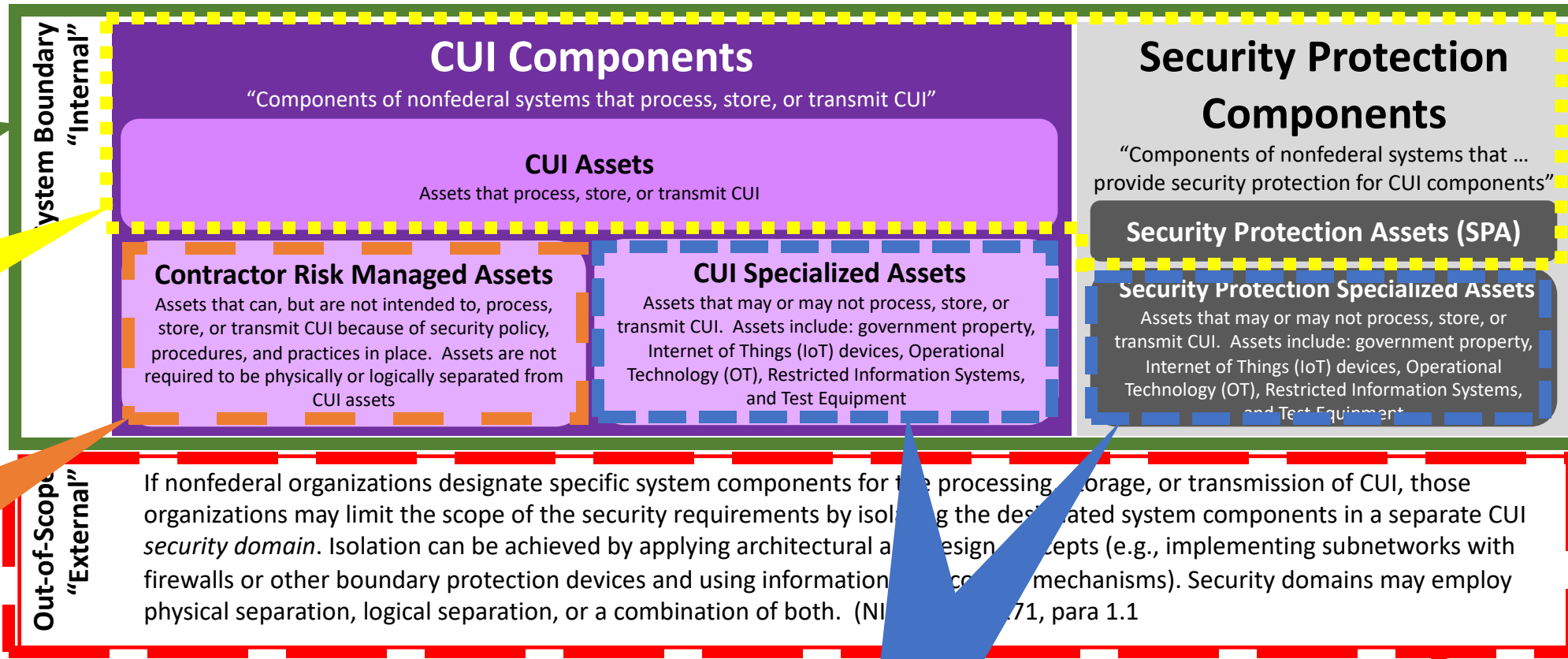
If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. (NIST SP 800-171, para 1.1)

# Know your Scope

**NIST SP 800-171  
Scope of  
Applicability**

**Primary CMMC  
Assessment  
Scope**

**Subject to spot  
checking in  
CMMC  
Assessment**



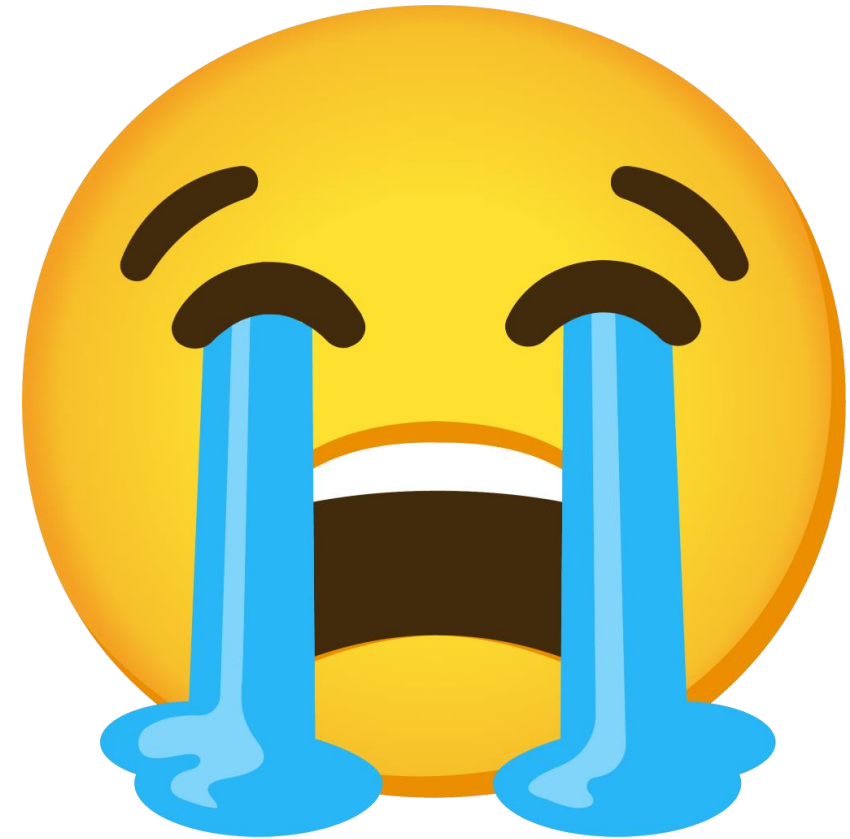
**Reviewed in  
your SSP Only**

**Subject to  
Negative Testing**

# Know thy ESP...

# 32 CFR Part 170 Draft Rule

- **§170.19(c) “CMMC Level 2 Scoping” (2)**
  - If the OSA utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. If using a CSP for Level 2 Self-Assessment, see § 170.16(c)(2). If using a CSP for Level 2 Certification Assessment, see § 170.17(c)(5).



# Ya got what you wanted... BUT

## COMMENT 17.a:

- DoD received numerous comments about the implications of using an ESP while seeking to comply with CMMC requirements. Many comments were concerns that the ESP assessment requirements expanded the scope and cost of the CMMC program. Additionally, some comments described overarching concerns about applicability of CMMC requirements to an ESP when it only provided a Security Protection Asset or processed Security Protection Data.
- **Response:**
  - The DoD has revised the rule to reduce the assessment burden on External Service Providers (ESP). ESP assessment, certification, and authorization requirements in §§ 170.19(c)(2) and (d)(2) have been updated. The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided. ESPs that are CSPs and do NOT process, store, or transmit CUI, are not required to meet FedRAMP requirements in DFARS clause 252.204-7012. Services provided by the CSP are in the OSA's scope. When ESPs that are not CSPs, process, store, or transmit CUI, a CMMC assessment is required to verify compliance with requirements for safeguarding CUI. Any ESP services used to meet OSA requirements are within the scope of the OSA's CMMC assessment.
  - When ESPs that are not CSPs do NOT process, store, or transmit CUI, they do not require CMMC assessment or certification, **however, services they provide are in the OSA's assessment scope**. There is nothing in the rule that precludes an ESP, that is not a CSP, from voluntarily requesting a C3PAO assessment. A C3PAO may perform such an assessment if the ESP makes that business decision.



# ESP Scoping requirements per §170.19(c)(2)(i)

When the ESP processes, stores, or transmits:	When utilizing an ESP that is:	
	A CSP	Not a CSP
<b>CUI (with or without SPD)</b>	The CSP shall meet the FedRAMP requirements in <a href="#">48 CFR 252.204-7012</a>	The services provided by the ESP are in the OSA's assessment scope and <b><u>shall be assessed</u></b> as part of the OSA's assessment.
<b>SPD (without CUI)</b>	The services provided by the CSP are in the OSA's assessment scope and <b><u>shall be assessed</u></b> as Security Protection Assets	The services provided by the ESP are in the OSA's assessment scope and <b><u>shall be assessed</u></b> as Security Protection Assets.
<b>Neither CUI nor SPD</b>	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP	A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

**External Service Provider (ESP)** means external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.

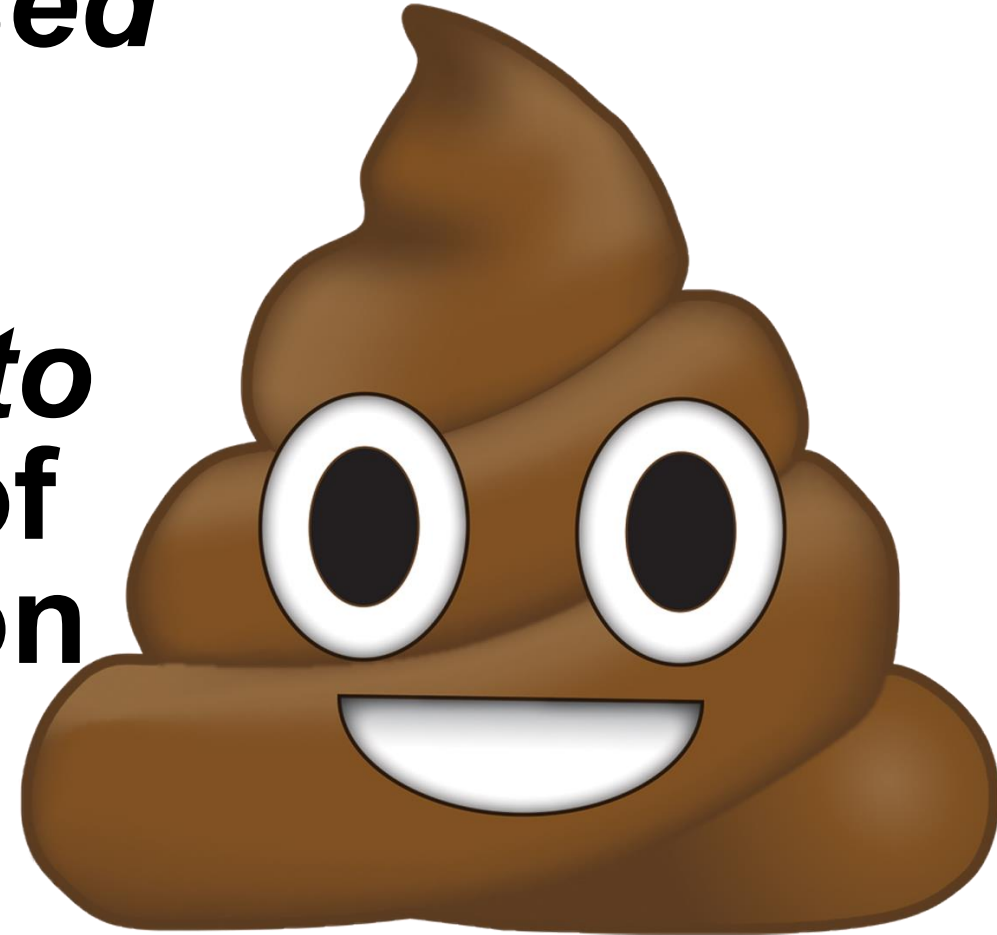
**Cloud Service Provider (CSP)** means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145 Sept 2011.

# ESPs & CMMC per §170.19(c)(2)(ii)

- The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA's SSP and described in the ESP's service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided.
- Note that the ESP may voluntarily undergo a CMMC certification assessment to reduce the ESP's effort required during the OSA's assessment. The minimum assessment type for the ESP is dictated by the OSA's DoD contract requirement.

# Here is what you really got...

**DoD [dumped on, foisted, imposed, inflicted, passed off, forced, fobbed off, palmed off or whatever #####ing term you want to use] the business risk of your ESP failing back on your shoulders.**

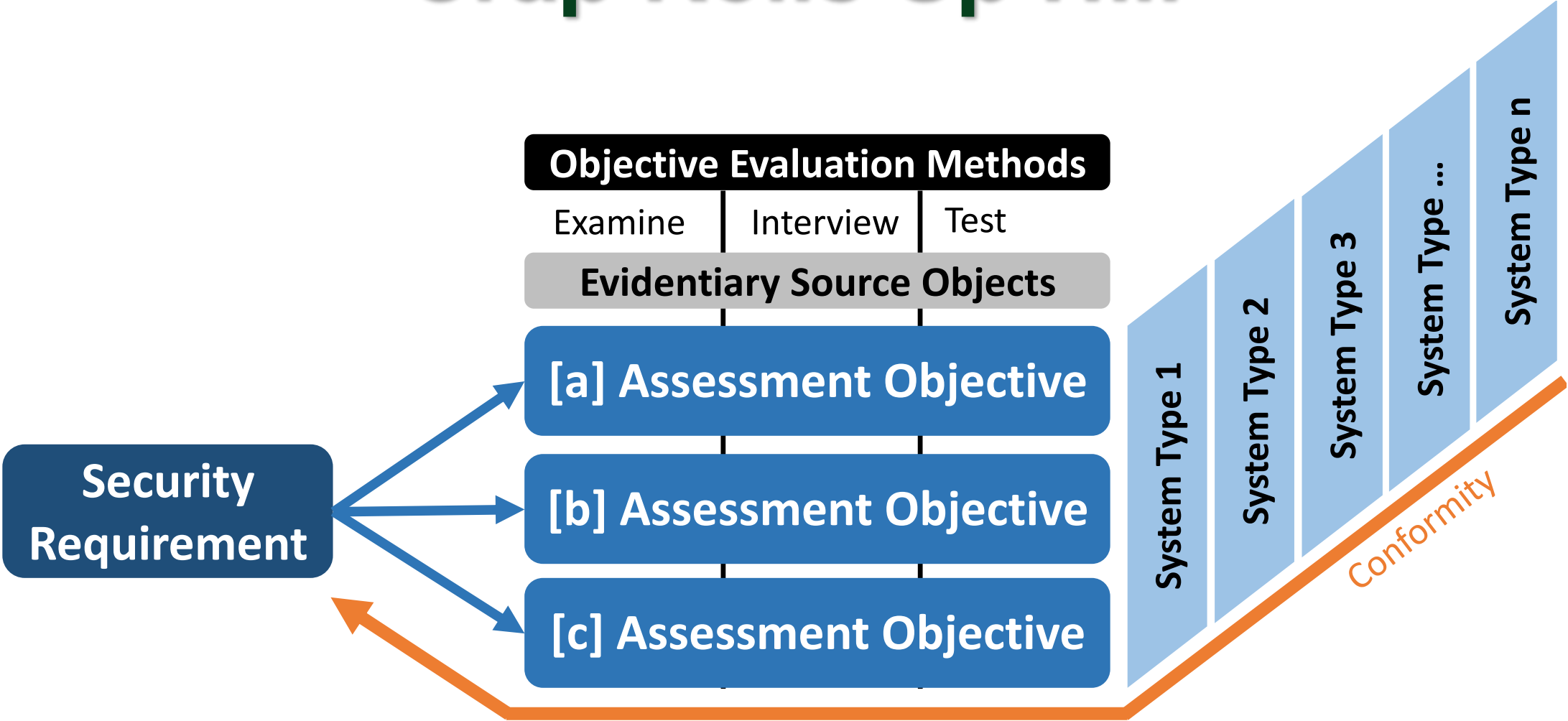


# Know thy ESP...

# Work at least at the Assessment Objective Level

<b>3.3.1</b>	<b>SECURITY REQUIREMENT</b> Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>	
	<b>3.3.1[a]</b>	<i>audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.</i>
	<b>3.3.1[b]</b>	<i>the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.</i>
	<b>3.3.1[c]</b>	<i>audit records are created (generated).</i>
	<b>3.3.1[d]</b>	<i>audit records, once created, contain the defined content.</i>
	<b>3.3.1[e]</b>	<i>retention requirements for audit records are defined.</i>
	<b>3.3.1[f]</b>	<i>audit records are retained as defined.</i>

# Crap Rolls Up Hill



# Answer the Verbs



Organizationally Defined  
“Tell me what is should be”

Organizationally Implemented  
“Tell me how you did it”

# The Configuration <> The ODP



“Self-licking  
ice cream cone”

- **Ask your self?**
  - Can we prove this configuration was approved?
  - Can we prove this configuration is what it should be?

# Define your Functionality(s)

- **Functionality Implicit ODPs**

- 3.1.2[a] the types of transactions and functions that authorized users are permitted to execute are defined.
- 3.1.5[c] security functions are identified.
- 3.1.6[a] nonsecurity functions are identified.
- 3.1.7[a] privileged functions are defined.
- 3.3.9[a] a subset of privileged users granted access to manage audit logging functionality is defined.
- 3.4.6[a] essential system capabilities are defined based on the principle of least functionality.
- 3.4.7[a] essential programs are defined.
- 3.4.7[b] the use of nonessential programs is defined.
- 3.4.7[d] essential functions are defined.
- 3.4.7[e] the use of nonessential functions is defined.
- 3.13.3[a] user functionality is identified.
- 3.13.3[b] system management functionality is identified.

# The Functionality Big Rocks

**3.4.6[a] essential system capabilities are defined based on the principle of least functionality.**



**3.1.2[a] the types of transactions and functions that authorized users are permitted to execute are defined.**

# How did you determine allowed functionality?

**3.4.6[a] essential system capabilities are defined based on the principle of least functionality.**

**3.4.7[a] essential programs**

**3.4.7[d] essential functions**

Essential Capabilities

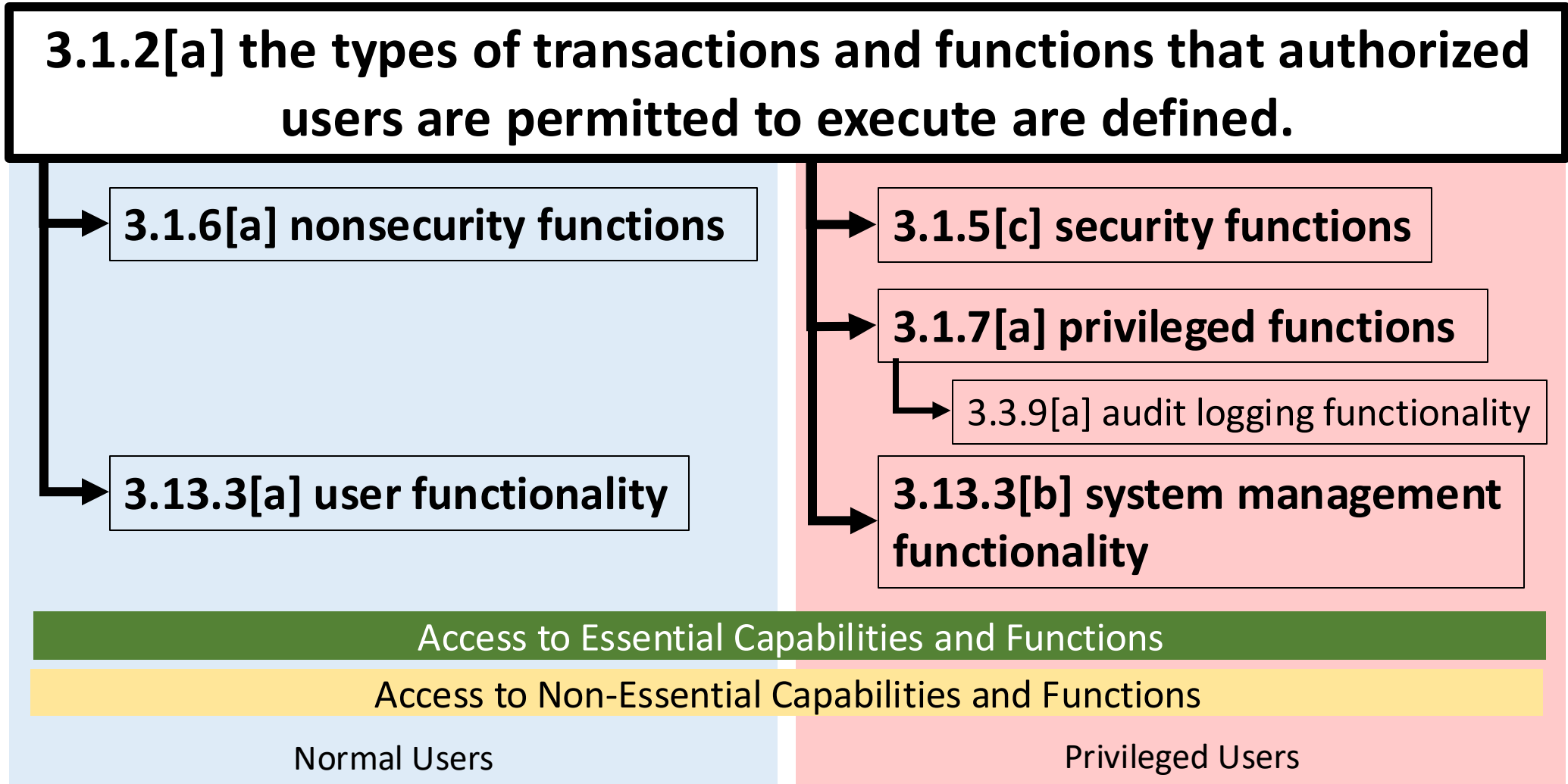
**3.4.7[b] the use of nonessential programs**

**3.4.7[e] the use of nonessential functions**

Non-Essential Capabilities

**3.1.2[a] the types of transactions and functions that authorized users are permitted to execute are defined.**

# Defining Functionality by User Class



# Define your Functionality(s)

- **Ask your self?**

- Can we identify what an authorized normal user can do for each component in scope?
- Can we identify what a privileged user can do for each component in scope?
- Have we defined what the security functions are for each component in scope?
- Has all of this been approved????

# 3.3.1 & Audit Log Specifications

<b>3.3.1</b>		<b>SECURITY REQUIREMENT</b> Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
		<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
<b>3.3.1[a]</b>		<i>audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.</i>
<b>3.3.1[b]</b>		<i>the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.</i>
<b>3.3.1[c]</b>		<i>audit records are created (generated).</i>
<b>3.3.1[d]</b>		<i>audit records, once created, contain the defined content.</i>
<b>3.3.1[e]</b>		<i>retention requirements for audit records are defined.</i>
<b>3.3.1[f]</b>		<i>audit records are retained as defined.</i>

03.03.01.a

[Assignment:  
organization-defined  
event types]

- at a minimum and where applicable:
- 1) Authentication events:
    - a) Logons (Success/Failure)
    - b) Logoffs (Success)
  - 2) Security Relevant File and Objects events:
    - a) Create (Success/Failure)
    - b) Access (Success/Failure)
    - c) Delete (Success/Failure)
    - d) Modify (Success/Failure)
    - e) Permission Modification (Success/Failure)
    - f) Ownership Modification (Success/Failure)
  - 3) Export/Writes/downloads to devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure)
  - 4) Import/Uploads from devices/digital media (e.g., CD/DVD, USB, SD) (Success/Failure)
  - 5) User and Group Management events:
    - a) User add, delete, modify, disable, lock (Success/Failure)
    - b) Group/Role add, delete, modify (Success/Failure)
  - 6) Use of Privileged/Special Rights events:
    - a) Security or audit policy changes (Success/Failure)
    - b) Configuration changes (Success/Failure)
  - 7) Admin or root-level access (Success/Failure)
  - 8) Privilege/Role escalation (Success/Failure)
  - 9) Audit and security relevant log data accesses (Success/Failure)

**Do you have a List of Audit Log Sources and that source specification for COTS?**

# 3.3.3

- **3.3.3 Review and update logged events.**

- DISCUSSION

- The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

**Do you have a process to validate Log Sources are still appropriate and functioning**

# 3.1.22

3.1.22	<b>SECURITY REQUIREMENT</b> Control CUI posted or processed on publicly accessible systems.
	<b>ASSESSMENT OBJECTIVE</b> <i>Determine if:</i>
3.1.22[a]	<i>individuals authorized to post or process information on publicly accessible systems are identified.</i>
3.1.22[b]	<i>procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.</i>
3.1.22[c]	<i>a review process is in place prior to posting of any content to publicly accessible systems.</i>
3.1.22[d]	<i>content on publicly accessible systems is reviewed to ensure that it does not include CUI.</i>
3.1.22[e]	<i>mechanisms are in place to remove and address improper posting of CUI.</i>
	<b>POTENTIAL ASSESSMENT METHODS AND OBJECTS</b> <b>Examine:</b> [SELECT FROM: Access control policy; procedures addressing publicly accessible content; system security plan; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs and records; security awareness training records; other relevant documents or records]. <b>Interview:</b> [SELECT FROM: Personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities]. <b>Test:</b> [SELECT FROM: Mechanisms implementing management of publicly accessible content].

**This is about your out-of-scope public web-site, LinkedIn, et al.**

**This is about PREVENTING data leaks**

# How to prevent a Failed Assessment

- **Do a “True Mock Pre-Assessment” with a C3PAO**
  - a) “the non-certification assessment shall be conducted in a formal fashion and in accordance with the assessment procedures established in 32 CFR Part 170 and the relevant non-certification, non-reporting aspects of the CMMC Assessment Process (CAP), or to the conformity requirements of other cybersecurity standards;
  - b) the C3PAO shall not provide any recommendations, advice, or consultative information as to how the OSA might remediate any discrepancies or improve their security posture for an official CMMC assessment or for conformity to any other cybersecurity standard; and
  - c) the OSA shall receive a deliverable documenting the official results of the non-certification assessment.”

(c.f., Code of Professional Conduct, para 3.4)





Trusted Guides For  
Your CMMC Journey

Matthew A. Titcombe  
matt@ascendcyber.com  
(352)575-9737

