STIG Development Process Used by the DoD/DISA

13TH ANNUAL

PEAK CYBER SYMPOSIUM

SEPTEMBER 13-14, 2023
COLORADO SPRINGS, CO

Kevin Rohan

Chief Architect Cybersecurity for Oracle - Retired

STIG’s - What Are They?

The Defense Information Systems Agency (**DISA**) is the entity responsible for maintaining the security posture of the Department of Defense (DoD) IT infrastructure.

One of the ways **DISA** accomplishes this task is by developing and using what is called:

Security **T**echnical **I**mplementation **G**uides or **STIG**”

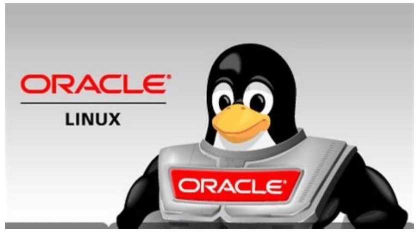
It ***Guides*** the hardening/locking-down of system software

STIG's – My Background

While at Oracle I created or maintained these STIGs:

- Solaris 10
- Solaris 11
- Solaris 12 (before it was cancelled)

- Oracle Linux 6
- Oracle Linux 7
- Oracle Linux 8



(I Never touched the Oracle Database STIGs)

What To Do If No STIG Exists?
(and current hardening is required)

Determine if an *earlier* version of a STIG has been published

- Many checks and fixes in it can be applied
- Review the check and fix procedures to determine which of these still work
- Use that set of checks and fixes
- Evaluate no longer working checks and fixes for each requirement and see if it can be modified
- New product features and configuration settings must also be accounted for based on the relevant Security Requirements Guide (SRG).

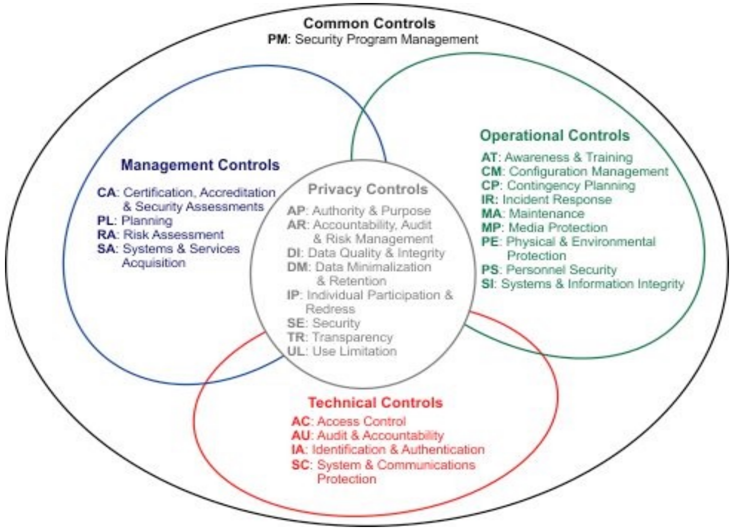
If *no related STIG*, use relevant SRG's to determine compliance with DoD policies.

If assistance is needed with SRG's open a ticket Helpdesk at *disa.stig_spt@mail.mil*

DISA STIG Creation

Path to a STIG'ed Operational System

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


Common Controls
PM: Security Program Management
Management Controls
CA: Certification, Accreditation & Security Assessments
PL: Planning
RA: Risk Assessment
SA: Systems & Services Acquisition
Operational Controls
AT: Awareness & Training
CM: Configuration Management
CP: Contingency Planning
IR: Incident Response
MA: Maintenance
MP: Media Protection
PE: Physical & Environmental Protection
PS: Personnel Security
SI: Systems & Information Integrity
Privacy Controls
AP: Authority & Purpose
AR: Accountability, Audit & Risk Management
DI: Data Quality & Integrity
DM: Data Minimalization & Retention
IP: Individual Participation & Redress
SE: Security
TR: Transparency
UL: Use Limitation
Technical Controls
AC: Access Control
AU: Audit & Accountability
IA: Identification & Authentication
SC: System & Communications Protection

NIST SP 800-53 Catalog
Basis for STIGs, HIPPA, CIS, etc

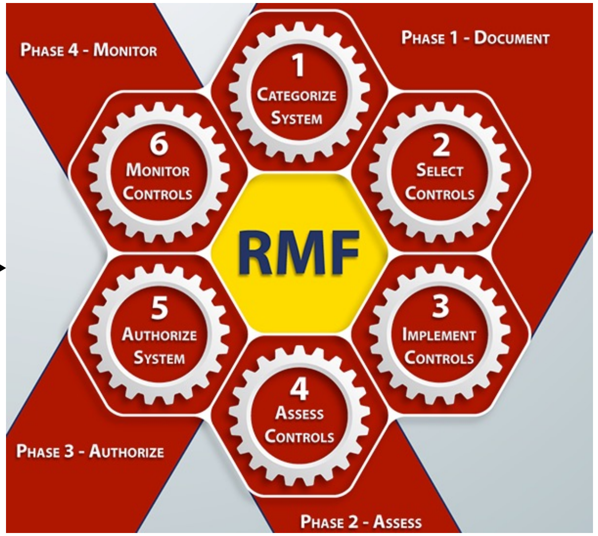
DISA
Defense Information Systems Agency
Department of Defense

Control Correlation Identifier (CCI)
Map NIST Rqmts to SRGs

Security Requirements Guide (SRG)

Security Technical Implementation Guide (**STIG**) - How-To Guide
Work done by **Vendor** & DISA
(SCAP also created by DISA)

NIST
Risk Management Framework



Project Security Evaluators

Authorization to Operate

Getting Started

Staffing levels at DISA are very tight, so they need to know you are serious

Step 1 – Go to the Vendor Process at DISA’s Cyber.mil web site:

https://public.cyber.mil/stigs/vendor-process/

Step 2 – Download and fill out the “**Vendor STIG Intent Form**”

Have a DoD Sponsor (no cost to them, no work for them)

The form tells them **what** you want to STIG (O/S, DB, etc)

There is no cost for doing this

There is no commitment required – so you can change your mind

Step 3 – **Wait** for a Subject Matter Expert (SME) to be assigned

For Solaris 12 (which instead became 11.4), it took about 2 months

For Oracle Linux 7, it took 22 months

Staffing issues, politics, & health issues at DISA delay things

While You Are Waiting – You *Can* Move Forward

Go out to the DISA web site to find the blank STIG template so you can start

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_GPOS_V2R6_SRG.zip

Download the "*General Purpose Operating System SRG Ver 2, Rel 6*"

- With a browser open the file that end in: xccdf.xml
- It shows about ~500 different STIG items of interest for O/S's
- This is what you temporarily will be working from

Also download any similar O/S's for examples and possible reuse

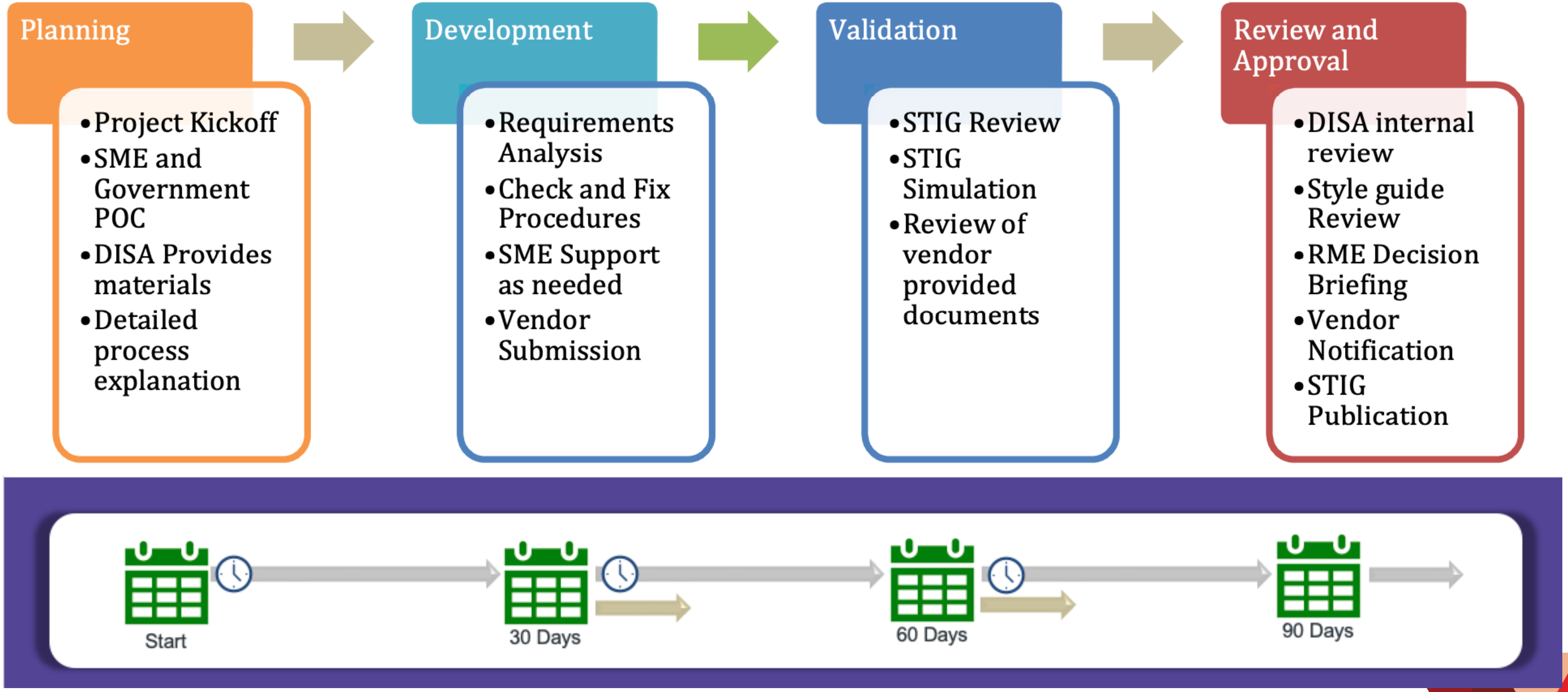
Once you have a SME you can 100% begin

- The SME will provide the spreadsheet version
- It has the STIG development cells in it

A SME Is Assigned

Let The Meetings Begin...

The SME will walk you through the phases that you will be working through what to expect:



Planning

- Project Kickoff
- SME and Government POC
- DISA Provides materials
- Detailed process explanation

Development

- Requirements Analysis
- Check and Fix Procedures
- SME Support as needed
- Vendor Submission

Validation

- STIG Review
- STIG Simulation
- Review of vendor provided documents

Review and Approval

- DISA internal review
- Style guide Review
- RME Decision Briefing
- Vendor Notification
- STIG Publication

Start

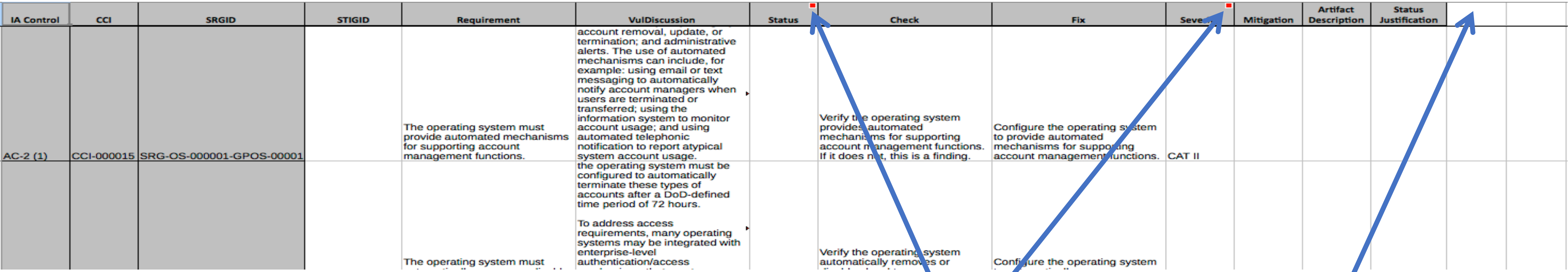
30 Days

60 Days

90 Days

General Purpose Operating System

GPOS Template --- Its Just a Spreadsheet ---



IA Control	CCI	SRGID	STIGID	Requirement	VulDiscussion	Status	Check	Fix	Severity	Mitigation	Artifact Description	Status Justification		
AC-2 (1)	CCI-000015	SRG-OS-000001-GPOS-00001		The operating system must provide automated mechanisms for supporting account management functions.	account removal, update, or termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.		Verify the operating system provides automated mechanisms for supporting account management functions. If it does not, this is a finding.	Configure the operating system to provide automated mechanisms for supporting account management functions.	CAT II					
				The operating system must	the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours. To address access requirements, many operating systems may be integrated with enterprise-level authentication/access		Verify the operating system automatically removes or	Configure the operating system						

Pull Down Menus

Specific Answers / Categories

Gray Cells

Never Edit

Used to provide Guidance and Mapping

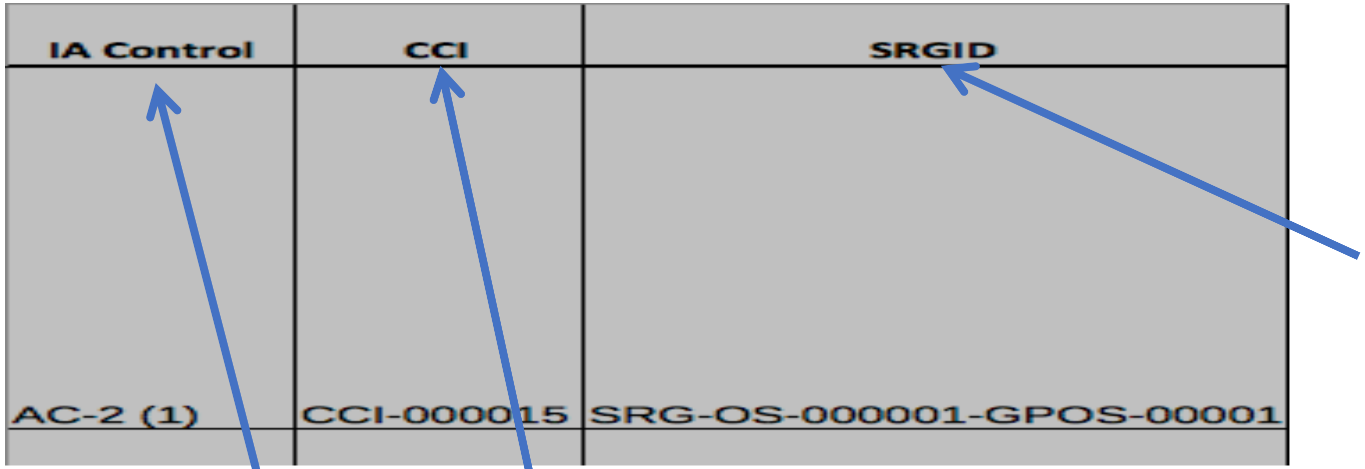
Blank Cells

For us to use

Who's assigned, notes,

Questions, etc

The Gray cells - Not Changeable



IA Control	CCI	SRGID
AC-2 (1)	CCI-000015	SRG-OS-000001-GPOS-00001

DISA Security Recommendation Guides (SRG).

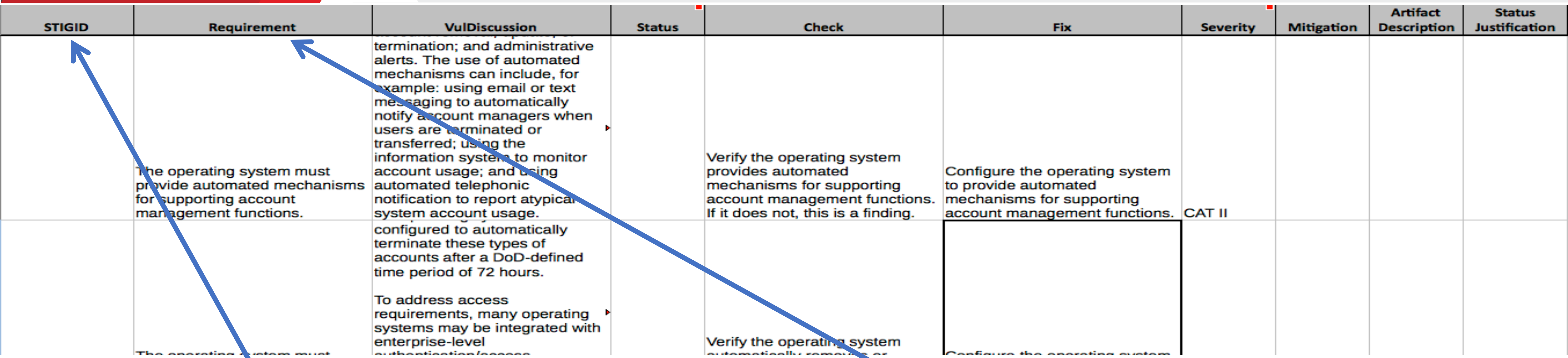
IA control

This is a pre-populated reference to the **NIST SP 800-53** IA control from which this requirement is sourced.

CCI

DISA's Control Correlation Identifier (CCI) enables DoD organizations to **trace** STIG **compliance** to Information Assurance controls specified by NIST and mandated for Federal government agencies

STIGID & Requirement Columns



STIGID	Requirement	VulDiscussion	Status	Check	Fix	Severity	Mitigation	Artifact Description	Status Justification
	The operating system must provide automated mechanisms for supporting account management functions.	termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.		Verify the operating system provides automated mechanisms for supporting account management functions. If it does not, this is a finding.	Configure the operating system to provide automated mechanisms for supporting account management functions.	CAT II			
	The operating system must	configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours. To address access requirements, many operating systems may be integrated with enterprise-level authentication/access		Verify the operating system automatically removes or	Configure the operating system				

STIGID

DISA Most Likely will fill this in

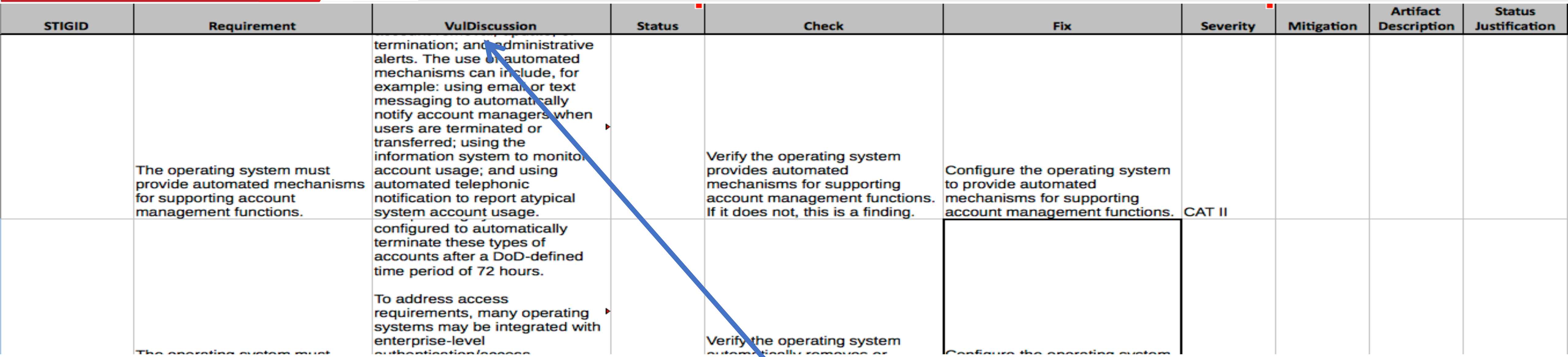
We can offer a naming convention like:

SOL-11-020280

Requirement

This is a sentence stating the requirement. **This will be pre-populated** from the SRG but could be updated to reflect the STIG requirement

The VulDiscussion Column



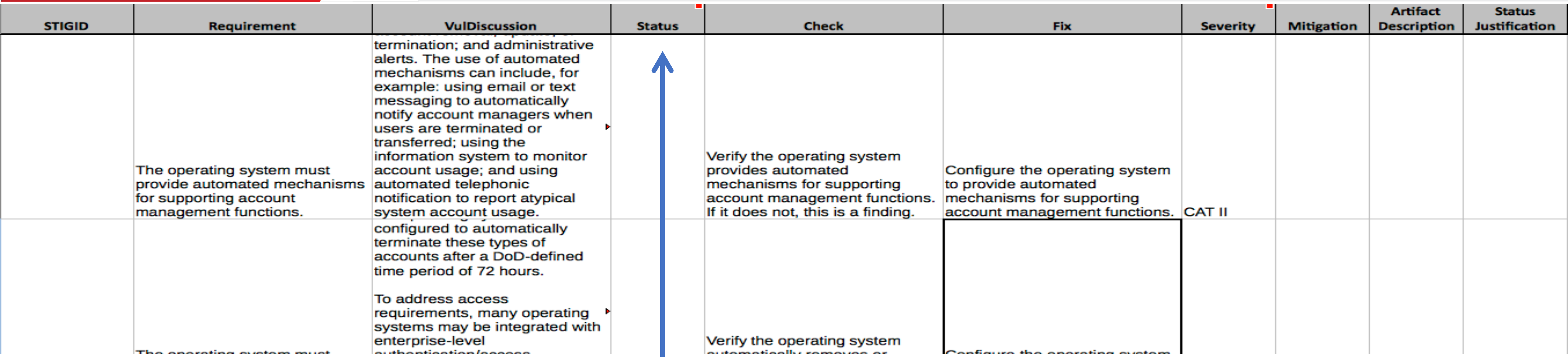
STIGID	Requirement	VulDiscussion	Status	Check	Fix	Severity	Mitigation	Artifact Description	Status Justification
	The operating system must provide automated mechanisms for supporting account management functions.	termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.		Verify the operating system provides automated mechanisms for supporting account management functions. If it does not, this is a finding.	Configure the operating system to provide automated mechanisms for supporting account management functions.	CAT II			
	The operating system must	configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours. To address access requirements, many operating systems may be integrated with enterprise-level authentication/access		Verify the operating system automatically removes or	Configure the operating system				

VulDiscussion

The vulnerability discussion describes the risk associated with not complying with the requirement. The field is not for discussing specifics of particular settings or products. **This will be pre-populated** from the Technology SRG and should be updated only where the associated risk or vulnerability of this product is substantively different from the risk described in the pre-populated text.

The STATUS Column

- A Lot Of Learning Here

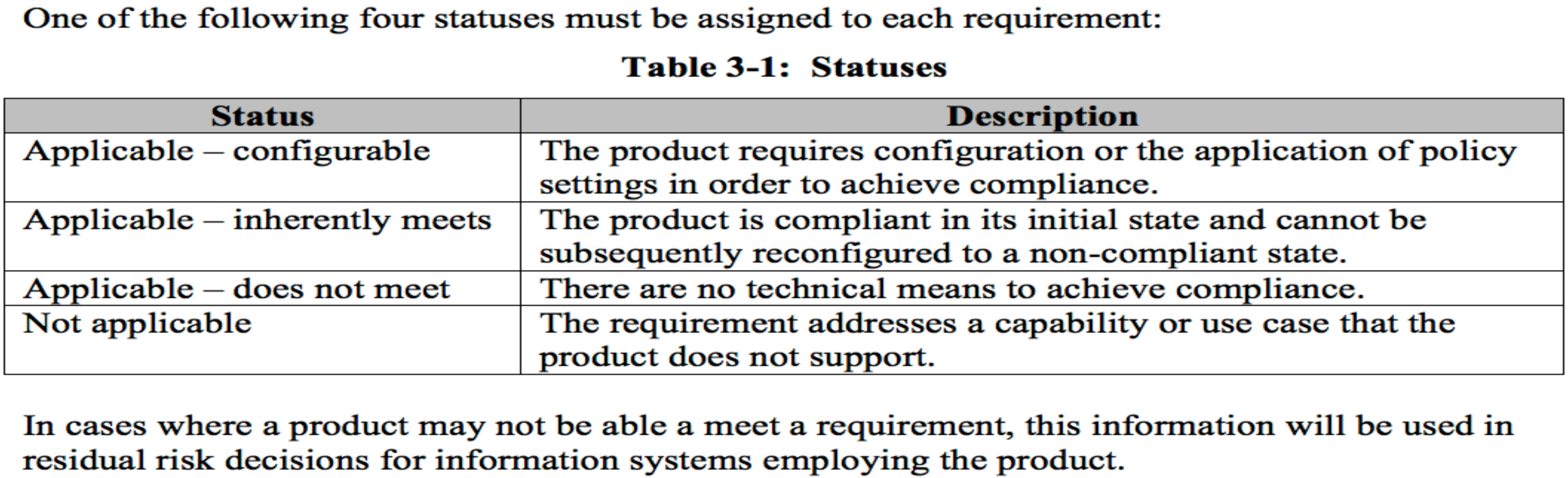


STIGID	Requirement	VulDiscussion	Status	Check	Fix	Severity	Mitigation	Artifact Description	Status Justification
	The operating system must provide automated mechanisms for supporting account management functions.	termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.		Verify the operating system provides automated mechanisms for supporting account management functions. If it does not, this is a finding.	Configure the operating system to provide automated mechanisms for supporting account management functions.	CAT II			
	The operating system must	configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours. To address access requirements, many operating systems may be integrated with enterprise-level authentication/access		Verify the operating system automatically removes or	Configure the operating system				

STATUS – Where the Work Starts

Status is the outcome of the analysis of the Technology SRG requirement as it relates to the product for which the STIG is being written. This is a pull down list.

Using The STATUS Column



One of the following four statuses must be assigned to each requirement:

Table 3-1: Statuses

Status	Description
Applicable – configurable	The product requires configuration or the application of policy settings in order to achieve compliance.
Applicable – inherently meets	The product is compliant in its initial state and cannot be subsequently reconfigured to a non-compliant state.
Applicable – does not meet	There are no technical means to achieve compliance.
Not applicable	The requirement addresses a capability or use case that the product does not support.

In cases where a product may not be able a meet a requirement, this information will be used in residual risk decisions for information systems employing the product.

Submit STATUS Column To DISA

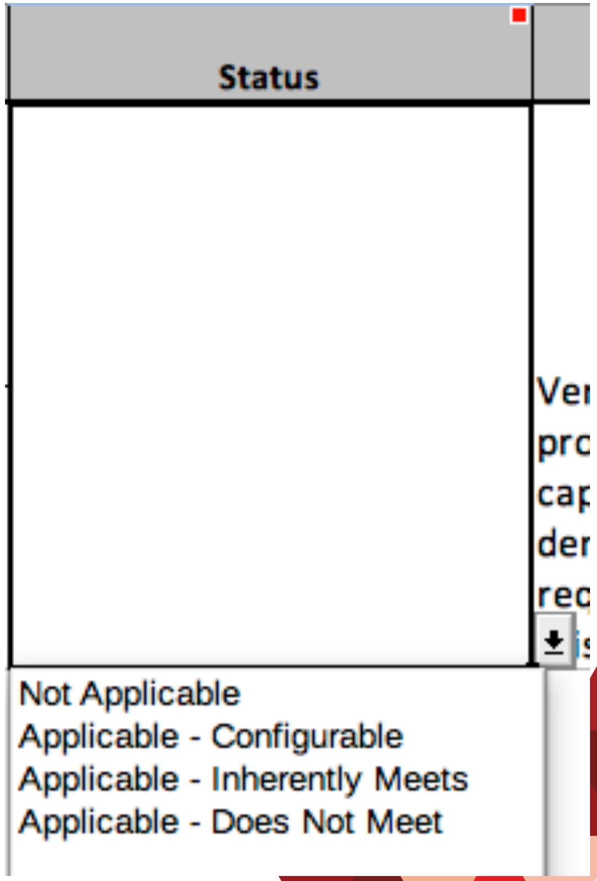
Meetings, meetings, meetings……

This is the Gateway to the next stage

- DISA has to agree to each and every one of the Status selections made
- DISA will *challenge* you on everything that is *not* configurable
  - You need to document WHY its not configurable
  - You will have to defend your position sometimes
- DISA is very good at having you think through things

Legal Cheating:

- Download as many similar and older versions of other STIGs
- They can help guide you through
- Surprise – What was OK before, might not be today…

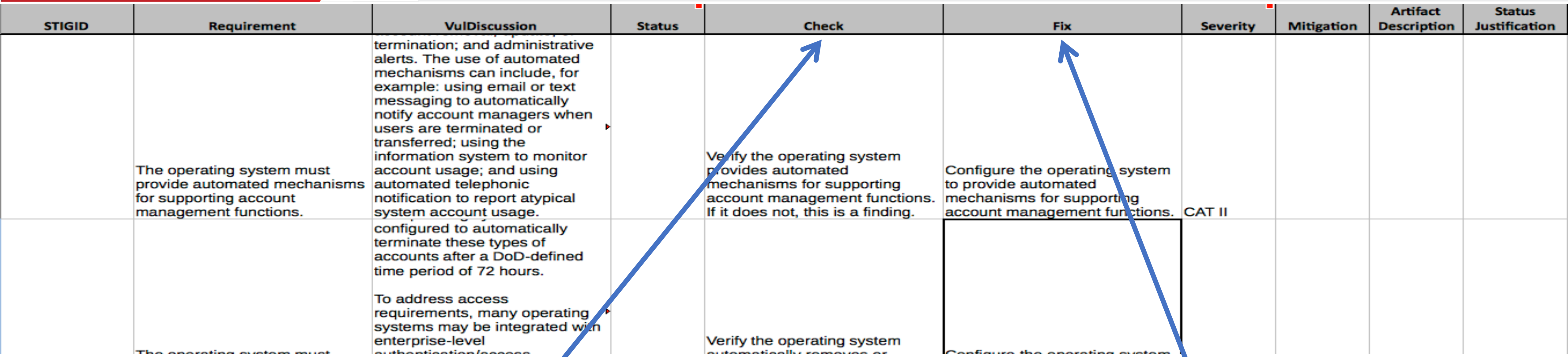


Status

Ver
pro
cap
der
req

Not Applicable
Applicable - Configurable
Applicable - Inherently Meets
Applicable - Does Not Meet

The Check & Fix Columns



STIGID	Requirement	VulDiscussion	Status	Check	Fix	Severity	Mitigation	Artifact Description	Status Justification
	The operating system must provide automated mechanisms for supporting account management functions.	termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.		Verify the operating system provides automated mechanisms for supporting account management functions. If it does not, this is a finding.	Configure the operating system to provide automated mechanisms for supporting account management functions.	CAT II			
	The operating system must	configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours. To address access requirements, many operating systems may be integrated with enterprise-level authentication/access		Verify the operating system automatically removes or	Configure the operating system				

Check

This cell should only be completed for rows where the status is Applicable – configurable.
It should remain blank for all other status types.

Fix

This cell should only be completed for rows where the status is Applicable – configurable.
It should remain blank for all other status types.

Submitting Check / Fix To DISA

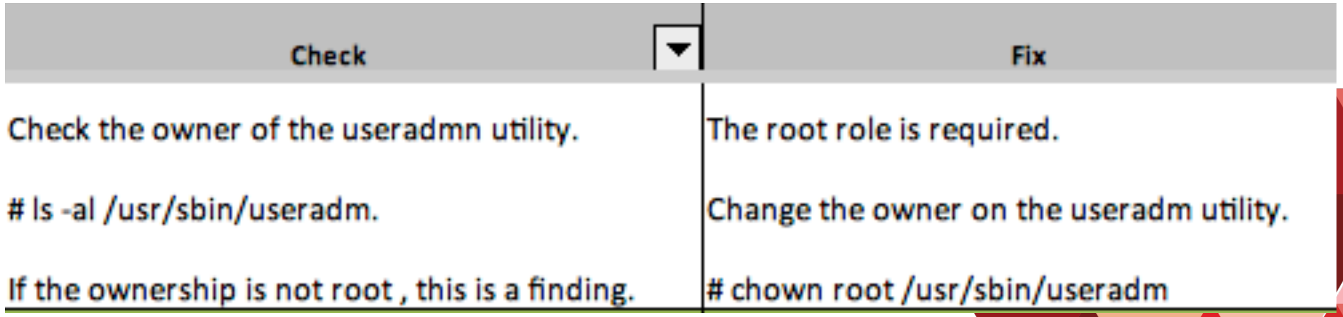
Again, meetings, meetings, meetings...

This is the Gateway to the next stage

- DISA may discuss the Check / Fix wording, commands used, etc.
- You will have to defend your position sometimes
- DISA is very good at having you think through things

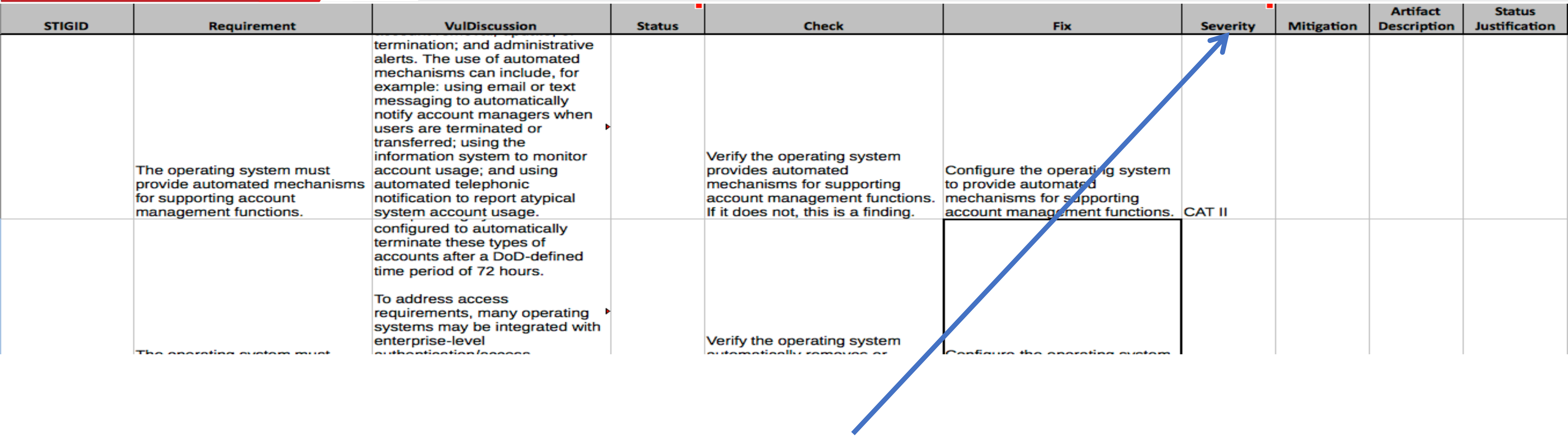
<u>Legal Cheating:</u>

- Download as many similar and older versions of other STIGs
- They can help guide you through
- Surprise – What was OK before, might not be today…



Check	Fix
Check the owner of the useradmn utility.	The root role is required.
# ls -al /usr/sbin/useradm.	Change the owner on the useradm utility.
If the ownership is not root , this is a finding.	# chown root /usr/sbin/useradm

The Severity / CATegory Column



STIGID	Requirement	VulDiscussion	Status	Check	Fix	Severity	Mitigation	Artifact Description	Status Justification
	The operating system must provide automated mechanisms for supporting account management functions.	termination; and administrative alerts. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using automated telephonic notification to report atypical system account usage.		Verify the operating system provides automated mechanisms for supporting account management functions. If it does not, this is a finding.	Configure the operating system to provide automated mechanisms for supporting account management functions.	CAT II			
	The operating system must	configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours. To address access requirements, many operating systems may be integrated with enterprise-level authentication/access		Verify the operating system automatically removes or	Configure the operating system				

Severity

The Severity Category Code (CAT) is an indicator of the risk associated with non-compliance. DoD SMEs may modify the CAT value after considering the impact of non-compliance in the overall security architecture of the product and the environment in which is expected to operate. This is a pull down list.

The Severity / CATegory Column

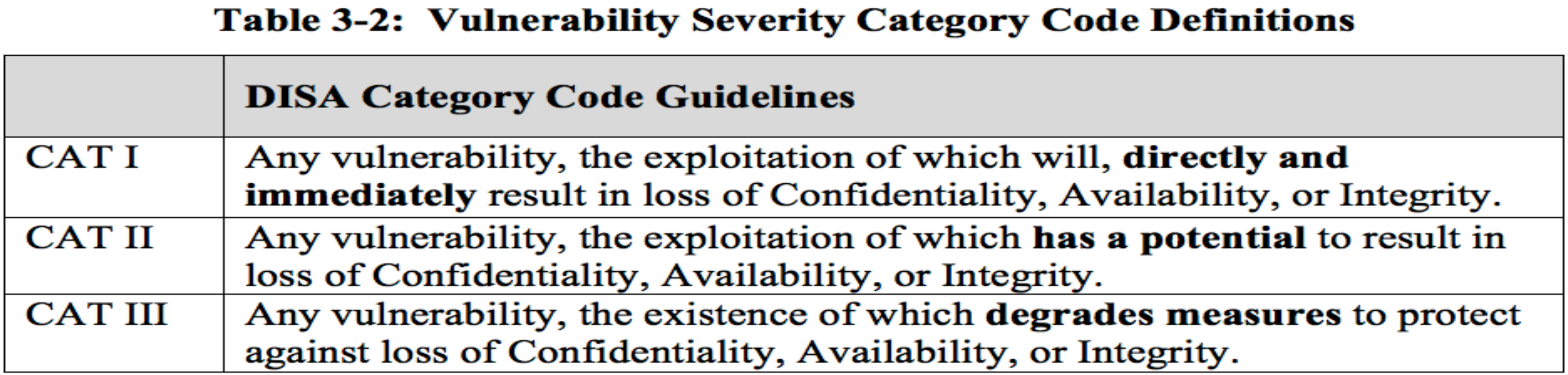


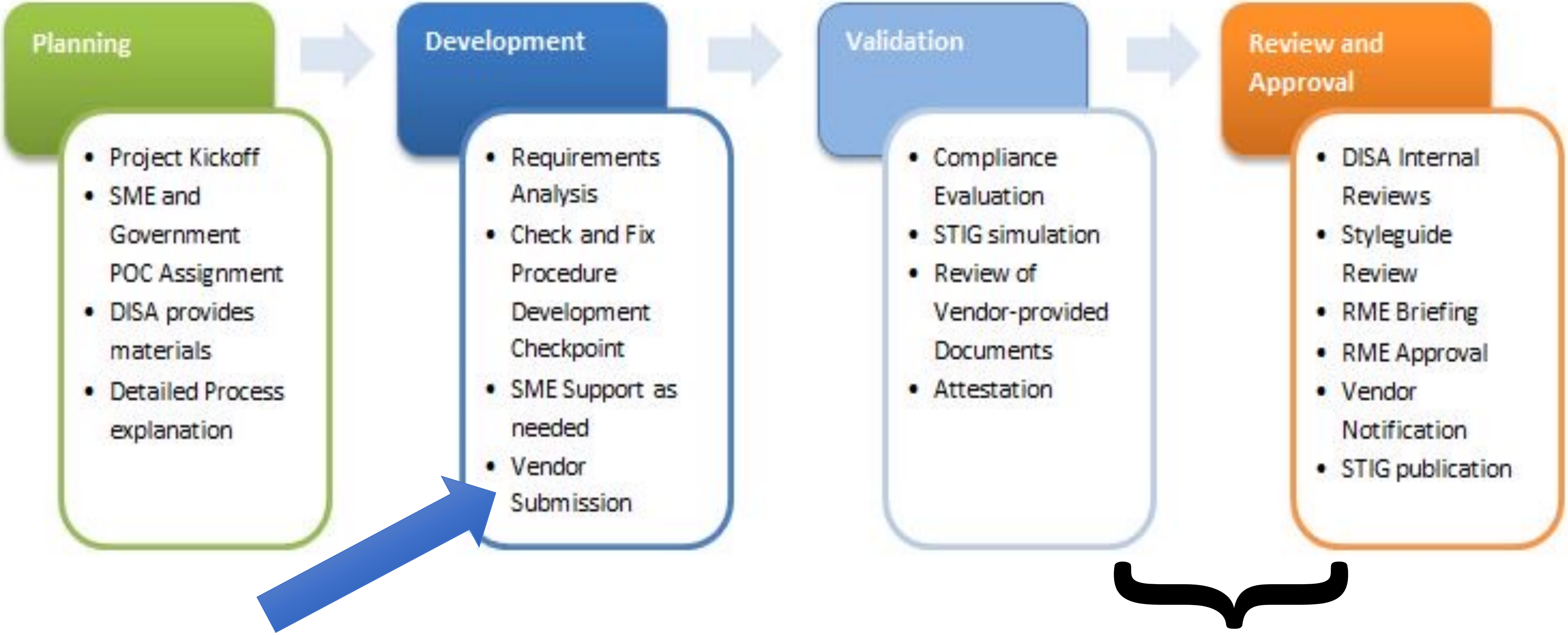
Table 3-2: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

Severity Level = CAT Level   CAT II is default

The Severity Category Code (CAT) is an indicator of the risk associated with non-compliance. DoD SMEs may modify the CAT value after considering the impact of non-compliance in the overall security architecture of the product and the environment in which is expected to operate. This is a pull down list.

Progressing & Finishing



Planning

- Project Kickoff
- SME and Government POC Assignment
- DISA provides materials
- Detailed Process explanation

Development

- Requirements Analysis
- Check and Fix Procedure Development Checkpoint
- SME Support as needed
- Vendor Submission

Validation

- Compliance Evaluation
- STIG simulation
- Review of Vendor-provided Documents
- Attestation

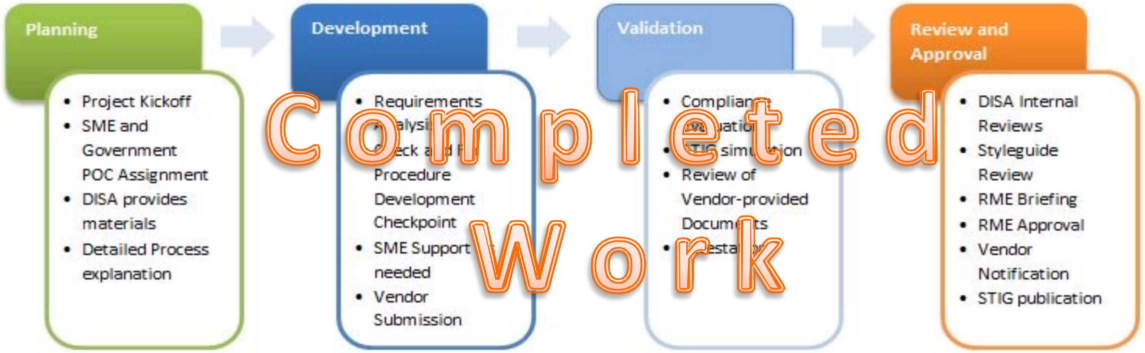
Review and Approval

- DISA Internal Reviews
- Styleguide Review
- RME Briefing
- RME Approval
- Vendor Notification
- STIG publication

Your work is mainly done at this point

The waiting game begins – and you should expect
For many months to go by without much interaction

When STIG Is Completed
– What’s Next



Completed Work

Quarterly Meetings with DISA SME(s) – Prior to each Quarterly Release

- ✓ Add/Delete/Change covered STIGs
- ✓ I get a high level preview of any changes
- ✓ Discuss just about anything (Trains)

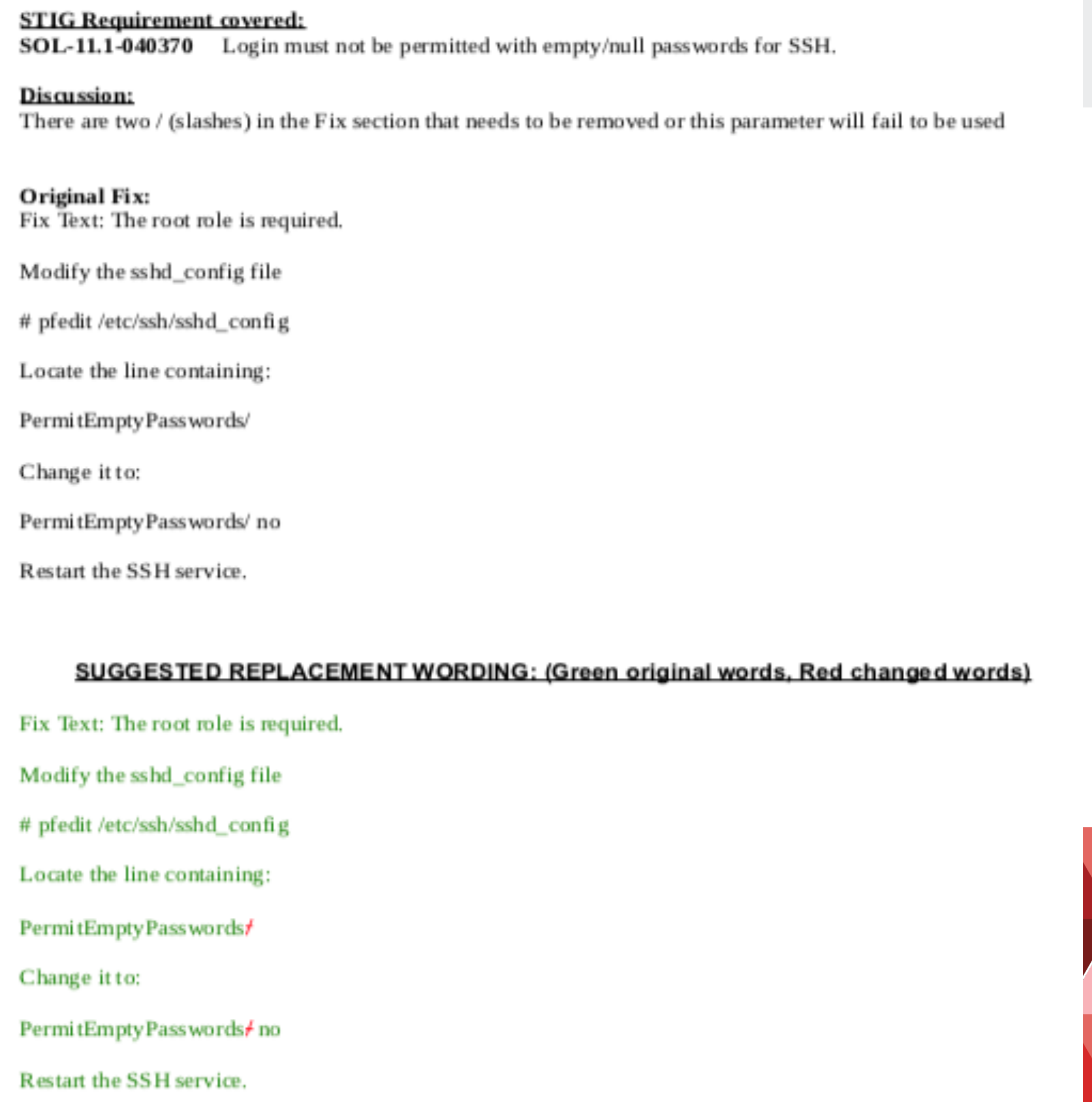
Concerns Or Errors In The STIG ??

<u>Anyone</u> can submit changes

If a problem is found with the STIG, let DISA know. They prefer a well though out case *with a solution.*

Like this:

If a STIG related interpretation or implementation question, contact DISA STIG Customer Support Desk:
disa.stig_spt@mail.mil



STIG Requirement covered:
SOL-11.1-040370 Login must not be permitted with empty/null passwords for SSH.

Discussion:
There are two / (slashes) in the Fix section that needs to be removed or this parameter will fail to be used

Original Fix:
Fix Text: The root role is required.

Modify the sshd_config file

pfedit /etc/ssh/sshd_config

Locate the line containing:

PermitEmptyPasswords/

Change it to:

PermitEmptyPasswords/ no

Restart the SSH service.

SUGGESTED REPLACEMENT WORDING: (Green original words, Red changed words)

Fix Text: The root role is required.

Modify the sshd_config file

pfedit /etc/ssh/sshd_config

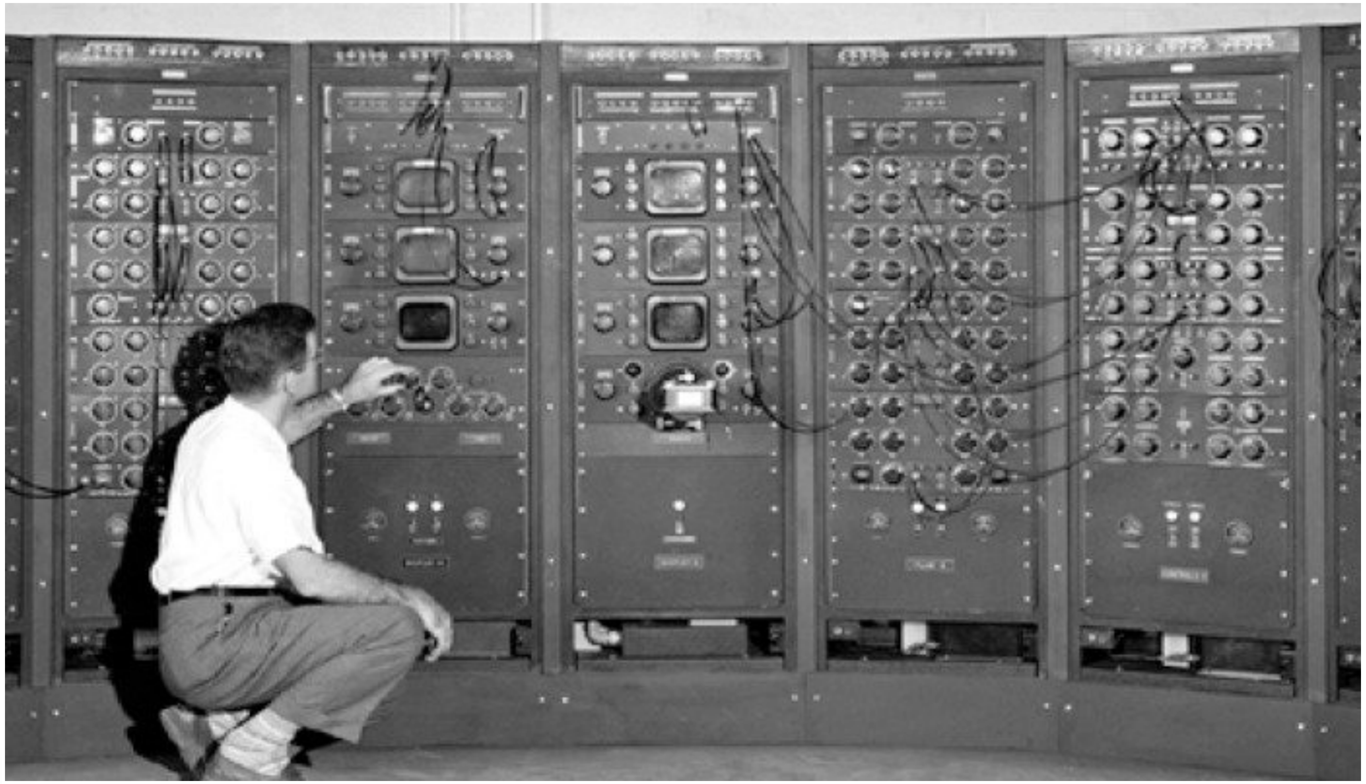
Locate the line containing:

PermitEmptyPasswords~~/~~

Change it to:

PermitEmptyPasswords~~/~~ no

Restart the SSH service.



Questions

THANK YOU FOR YOUR TIME

Kevin Rohan
Chief Architect Cybersecurity for Oracle – Retired
Kevin.Rohan@comcast.net