Automated Assessment Concepts Supporting ISCM

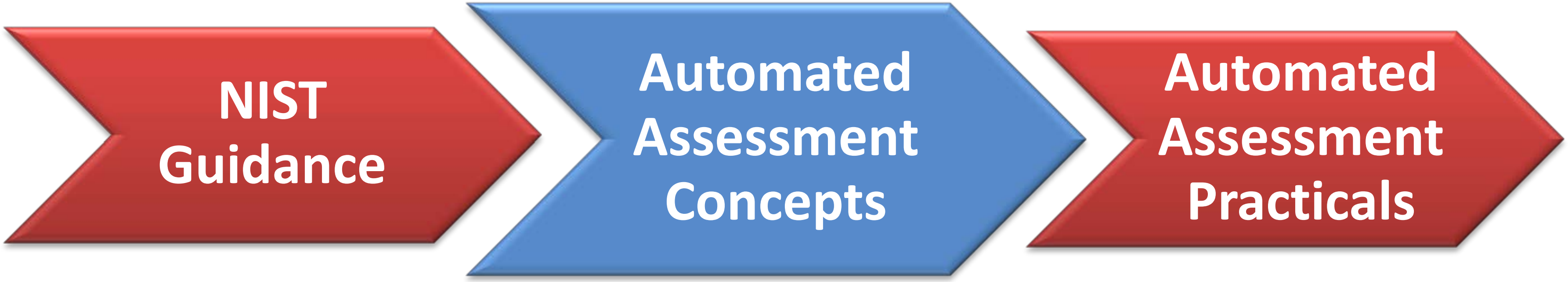
NIST/DHS Workshop

April 10th, 2014

Kelley Dempsey
Dr. George Moore

Module 2: Automated Assessment Concepts

- Where in the training sequence does this module fit?



NIST Guidance

Automated Assessment Concepts

Automated Assessment Practicals

Module 1
1 hour

Module 2
2 hours

Module 3
1 hour

Overview

- ❑ Learning Objectives
- ❑ Section 1: Prerequisites to AUTOMATION of Assessment
- ❑ Section 2: Linking Assessment to Security Results/Outcomes
- ❑ Section 3: Checking Capability Definitions Linking to 800-53 Controls
- ❑ Section 4: Defining Tests (DEFECT CHECKS) that Assess Control Item Effectiveness
- ❑ Section 5: Reporting Discovered Risk

Learning Objectives

- **At the conclusion of this module, the participants will be able to:**
  - Describe the prerequisites for automation.
  - Identify how CDM automates “desired state specifications.”
  - Understand how CDM security capabilities can be linked to 800-53 controls.
  - Describe the purpose of a CDM control item.
  - Define how CDM focuses on “defect checks” for what to test.
  - Describe the purpose of a defect control table.
  - Understand the significance of a Control Allocation Table.
  - Define how a control test narrative is used.
  - Describe the reporting processes used by CDM.
  - Understand the need to conduct and document a root cause analysis.
  - Define the roles and responsibilities that use the CDM reporting capabilities.
  - Understand the role of automation and the assessment boundaries.
  - Learn about the ways to display defects that are found on a system.

INTRODUCTION

SECTION 1: PREREQUISITES TO AUTOMATION OF ASSESSMENT

Areas to cover:

1. Use the NIST “Test” Assessment method.
2. Have data to tell you whether the actual state/behavior of the system is acceptable (called “Desired State Specification” in CDM.

Automating Security Assessment

- Continuous Diagnostics and Mitigation (CDM) promotes the use of automation.
- Benefits of Automated Security Control Assessments
  - With a traditional three year testing cycle, defects may not be detected for 18 months.[1]
  - Manual testing is often more expensive and takes longer.
  - NIST promotes “automation” as recommend guidance in their Continuous Monitoring Special Publication - 800-137.

[1] This assumes defects occur randomly over the 36 month period, and that tests are also occur over the same time, but done every 36 months. IF those assumptions are true, the time between defect and detection is evenly distributed between 0 and 36 months, with an average of 18 months.

NIST Assessment Methods and Automation

- NIST SP 800-53a Potential Control Assessment Methods
  - 800-53a identifies ***potential*** assessment methods
  - so that organizations have flexibility to manage risk

Flexibility & Choice

☑

Method	Definition from 800-53A, Appendix D
Examine	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
Interview	The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence.
Test	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.

Automated Assessment Methods

- Comparing and contrasting Assessment Methods
  - Interview and Examine are difficult to automate.
    - Usually require manual steps, thus expensive and slow
      - Interview - i.e.. person to person
      - Examine – i.e.. manual review of a document, system or environment

Choice for Automation ☑

  - Testing is the easiest method to automate and often the strongest method.
    - More Objective & Detailed
    - More Accurate & Reliable Results (looks at actual system)
    - Find flaws (hopefully faster than the attacker)
    - Saving through automation

> Wherever the Test assessment method can accurately and reliably assess control effectiveness, it can be used as the sole assessment method even when the Examine or Interview methods are listed as potential methods.

Supplementing Automated Assessment Methods

Organizations may still employ the Interview and Examine assessment methods to supplement automated security control assessments when organizations require greater assurance and/or more in-depth assessment rigor.

Defining the Desired State Specification

- NIST assessment guidance deals with concepts which translate to “desired state specification.”

Method	Definition from 800-53A, Appendix D
Test	The process of exercising one or more assessment objects under specified conditions **to compare actual with expected behavior.**

- Actual and expected “state” is also (implicitly) included.
- Desired state is CDM’s name for expected state/behavior (and some other 800-53 concepts).
- Automating “desired state” is key to automating testing.

800-53 Policy and Requirements are in "Desired State Specification"

- **POLICY:** NIST control guidance for "policy" are also examples of desired state specifications
  - [A "Security Policy" is]
    - *The statement of required protection of the information objects.*
    - *A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.*
    - *A set of criteria for the provision of security services.*

    In each of these senses, the security policy can be expressed as a desired state specification.
  - [An informal security policy is a] *Natural language description, possibly supplemented by mathematical arguments, demonstrating the correspondence of the functional specification to the high-level design.*

    This is a desired state specification after being re-expressed in natural language in a report.
  - [An information security policy is an] *aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.*

    This also can be provided through a desired state specification.

Defining the Desired State Specification

- ***Desired State Specification*** - The collection of defect checks to be automatically assessed across an organization/network/system using data.

- ***Defect Check*** - A statement about a particular attribute or behavior of an object type/role that can have security defects, flaws, weaknesses, and/or vulnerabilities; expressed in data;
  - that can be compared to actual state data about the same attribute for each object in that type/role (ideally using automation) to assess whether risk created by the actual state of the attribute is within acceptable limits.
  - And which can be output in human readable form to document the corresponding policy, test, requirement, control, etc.

Desired State is “shorthand” for “Desired/required/prohibited behavior/state”

Type of Desired State Specification	Simplified examples: [actual cases might be more complex]
Desired state	If software product X is present, setting Z should have value X to increase security.
Prohibited state	If software product X is present, the following patch levels have CVEs that produce risk, and are prohibited. List of product patch levels, with associated CVEs and composite risk for each.
Expected state	If software product X is present, the device should have [a list of executables with hashes to identify them]. If may be partially installed.
Desired behavior	Persons receiving e-mail will validate the origin of the e-mail before using links or attachments in the e-mail.
Prohibited behavior	Persons using accounts allowed to install software will not browse the internet or use e-mail from those accounts.
Expected behavior	User Y normally logins in from devices in the [City] area during the period from 8AM to 6PM. Other patterns might indicate account compromise.

Automating "Test" with the Desired State

- CDM uses the "test" assessment method which is easier to automate:
  1. Define the desired state "desired state" in <u>DATA</u> and to reduce risk.
  2. Collect the "actual state" <u>DATA</u> through sensors.
  3. Use automation on the data to test/determine whether desired state = actual state.
  4. When they are not equal we have a security defect with risk.

Can we only Automate Tests of Technical Controls?

- Control Testing Considerations
  - Technical controls can usually be validated through automation via software, tools and technologies.
  - Management and operational controls can often be tested through automation by placing the desired state specification (for example policy) in data.
  - The key to automation of assessment is a good desired state specification (automated specification of the policy/requirement).

The operational key is developing an adequate desired state specification.

Putting the Desired State in "Data"

- Control Testing Considerations (continued)
  - Data needs to be easily accessible for CDM use
    - Quantifiable
    - Accessible
    - Comparable to the actual state data
      - Same device ID in both.
  - What we mean by "data" for desired and actual state
    - In a database format that can be used for computation and can be queried.
    - Not in an unstructured file – thus designed (just) for people to read.
      - Microsoft Word
      - Adobe PDF
      - Spreadsheet

RECAP

SECTION 1: PREREQUISITES TO AUTOMATION OF ASSESSMENT

Areas that were covered:

1. Use the NIST "Test" Assessment method.
   a. NIST allows this choice
   b. Better Supports Automation
2. Have a "Desired State Specification" in data to tell you whether the actual state/behavior of the system is secure.
   a. Aligns with the NIST test method definition.
   b. Supports Automation.

INTRODUCTION

SECTION 2: LINKING ASSESSMENT TO SECURITY RESULTS/OUTCOMES

Areas to cover:

1. Use the NIST “Security Capability” concept introduced in 800-53 rev4.
2. Define/Select CDM Security Capabilities that allow
   a. A security program to be built in meaningful pieces.
   b. Clarify how NIST 800-53 controls work together as parts of systems-of-controls to achieve common security outcomes.

Understanding NIST Security Capabilities

- **Both CDM and NIST 800-53 utilize the idea of a "security capability"**
  - **NIST Security capability (See** NIST 800-53 rev4):
    - The concept of *security capability* is a construct that recognizes that the protection of information being processed, stored, or transmitted by information systems, seldom derives from a single safeguard or countermeasure (i.e., security control). p.21
    - A "security capability" is a set of "mutually reinforcing security controls" p. 24, to achieve a common purpose, such as secure "remote authentication." p.21

NIST leaves the task of defining specific capabilities to "organizations."

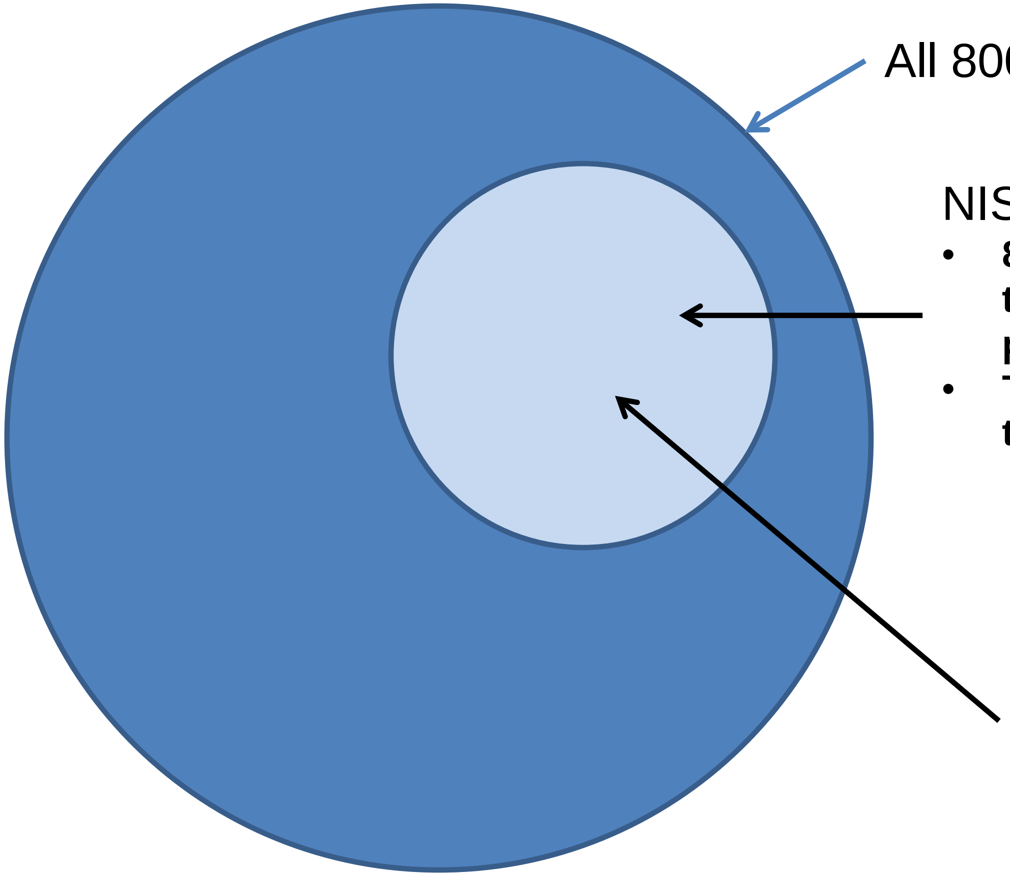
Defining CDM's Security Capabilities

- A CDM security capability is a NIST security capability which has the following additional traits:
  - The purpose of the capability is to address a specific attack scenario or exploit.
  - The capability focuses on attacks towards specific object types (e.g., devices, people, etc.)
  - There is a viable way (capability level concept of operations) to perform ISCM on the security capability.
  - The set of CDM security capabilities is designed to "cover" all current and relevant attack scenarios/exploits, and thus also includes all 800-53 controls in at least one capability.

CDM pre-defines a comprehensive set of 15 high level capabilities.

Security Capabilities and 800-53 Controls

How 800-53 Controls and Capabilities Work Together



All 800-53 Controls

NIST Security Capability:

- **800-53 controls that work together to achieve a purpose.**
- **Totally discretionary on how to define.**

CDM Security Capability:

- Purpose: thwart an exploit/attack type
- Focus: on object types attacked
- Has: way to automate assessment
- Has: way to use respond to improve security
- **Finite pre-defined number**
- Comprehensive set

Understanding Security Capabilities

- Why not use 800-53 Control Families?
  - Control families are ways of semantically grouping controls
    - Control families are **not focused on consequences or outcomes.**
  - Individual controls often support multiple security capabilities
    - the control families were developed with **each control in only one family.**
  - These considerations mean that **control families are not security capabilities.**

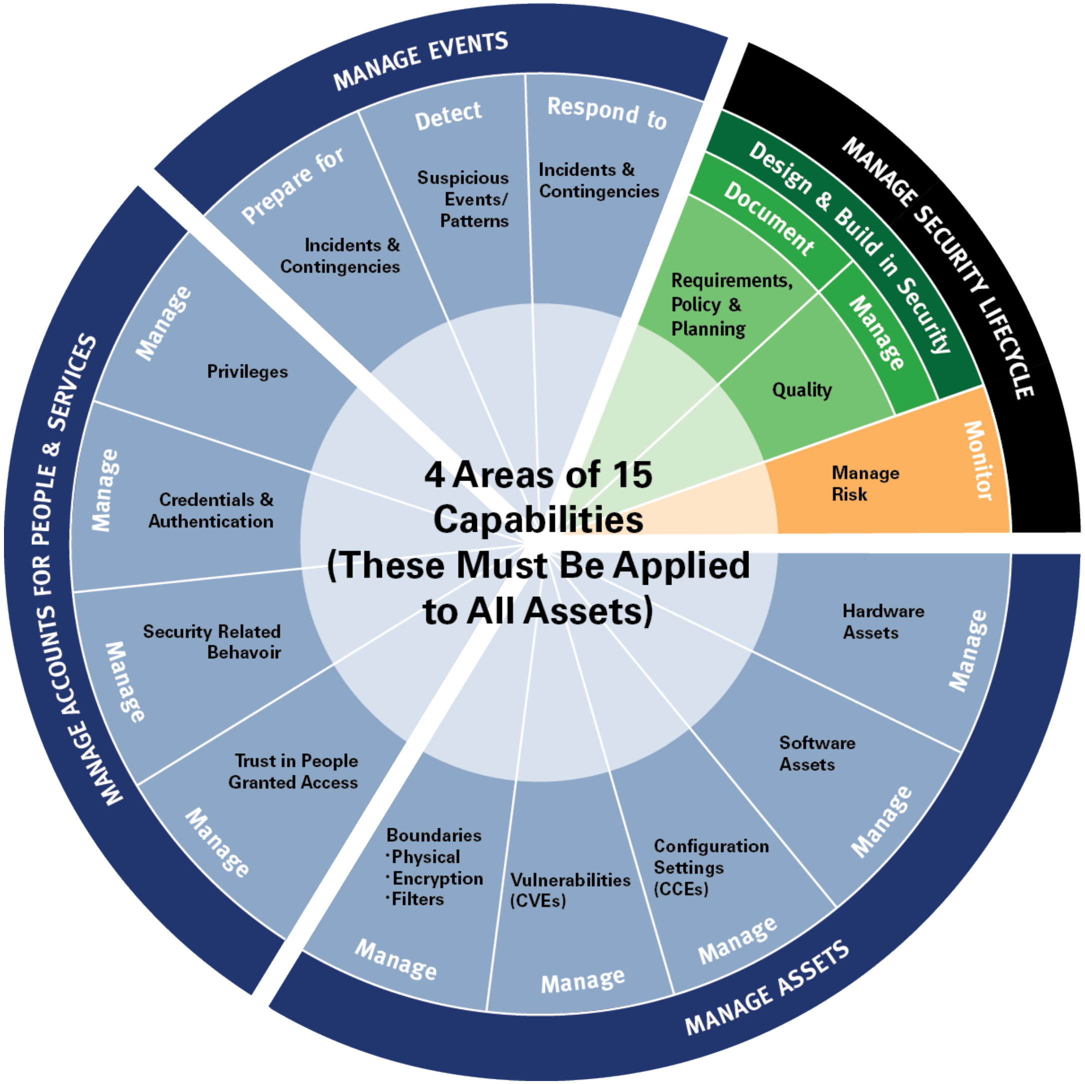
Understanding Security Capabilities

- Why not use 800-137 Continuous Monitoring Automation Domains?
  - An automation domain is defined as:
    - an information security area that includes a grouping of tools, technologies, and data.
  - An automation domain is ***not*** a set of security controls, It is a grouping of tools and/or technologies that produce data that may be useful to ISCM.

These considerations mean that

automation domains are not security capabilities.

CDM’s Security Capabilities


MANAGE EVENTS
Prepare for
Incidents & Contingencies
Detect
Suspicious Events/ Patterns
Respond to
Incidents & Contingencies
MANAGE SECURITY LIFECYCLE
Design & Build in Security
Document
Requirements, Policy & Planning
Manage
Quality
Monitor
Manage Risk
MANAGE ASSETS
Manage
Hardware Assets
Manage
Software Assets
Manage
Configuration Settings (CCEs)
Manage
Vulnerabilities (CVEs)
Manage
Boundaries
·Physical
·Encryption
·Filters
MANAGE ACCOUNTS FOR PEOPLE & SERVICES
Manage
Trust in People Granted Access
Manage
Security Related Behavoir
Manage
Credentials & Authentication
Manage
Privileges
4 Areas of 15 Capabilities
(These Must Be Applied to All Assets)

- Defined by a rigorous process to “linking” 800-53 controls to the desired outcomes to be achieved (thwarted attacks/exploits).

- Validated for completeness (current) by SMEs in various fields.

Understanding Security Capabilities

CDM Capabilities Purposes – Phase 1

Capability Name	Purpose
Hardware Asset Management (HWAM)	Identify unauthorized and unmanaged devices that are likely to be used by attackers as a platform from which to extend compromise of the network to be mitigated.
Software Asset Management (SWAM)	Identify unauthorized software on devices that is likely to be used by attackers as a platform from which to extend compromise of the network to be mitigated.
Configuration Settings (CCE) Management	identify configuration settings (CCEs) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.
Vulnerability (CVE) Management	identify vulnerabilities (CVEs) on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

Understanding Security Capabilities

CDM Capabilities Purposes – Phase 2

Capability Name	Purpose
Trust Management (TRUST)	Ensure that untrustworthy persons are prevented from being trusted with network access to prevent insider attacks.
Behavior Management (BEHAVE)	Ensure that people are aware of expected security related behavior and are able to perform their duties to prevent advertent and inadvertent behavior that compromises information.
Manage Credentials and Authentication (CRED)	Ensure that people have the credentials and authentication methods necessary (and only those necessary) to perform their duties, while limiting access to that which is necessary.
Manage Privileges (PRIV)	Ensure that people have the privileges necessary (and only those necessary) to perform their duties, to limit access to that which is necessary.

Understanding Security Capabilities

CDM Capabilities Purposes – Phase 2/3

Capability Name	Purpose
Manage Boundaries (BOUND)	**Part 1: Filters** -- Ensure that traffic in-to and out-of the network (and thus out of the physical facility protection) does not compromise security. Do the same for enclaves that sub-divide the network. **Part 2: Encryption** -- Ensure that information is encrypted (with adequate strength) when needed to protect confidentiality and integrity, whether in motion, or at rest **Part 3: Physical Boundaries** -- Ensure that movement (of people, media, equipment, etc.) in-to and out-of the physical facility does not compromise security.

Understanding Security Capabilities

CDM Capabilities Purposes – Phase 3

Capability Name	Purpose
Prepare for Events (PREP)	Ensure that procedures and resources are in place to respond to with both routine and unexpected events that can compromise security. • Potential responses include a wide range of possible actions, including, but not limited to, continuity of operations, recovery, and forensics. • The unexpected events include actual attacks and contingencies (acts-of-god) like floods, earthquakes, etc.
Detect Events (DETECT)	Identify routine and unexpected events that can compromise security in a time frame that prevents as much of the impact/consequences of the events as possible.
Respond to Events (RESPOND)	Ensure that both routine and unexpected events that can compromise security that require a response to maintain functionality and security are responded to (once identified) in a time frame that prevents as much of the impact/consequences of the events as possible.

RECAP

SECTION 2: LINKING ASSESSMENT TO SECURITY RESULTS/OUTCOMES

Areas that were covered:

1. Use the NIST “Security Capability” concept introduced in 800-53 rev4.
2. Define/Select CDM Security Capabilities that allow
   a. A security program to be built in meaningful pieces.
   b. Clarify how NIST 800-53 controls work together as parts of systems-of-controls to achieve common security outcomes.

INTRODUCTION

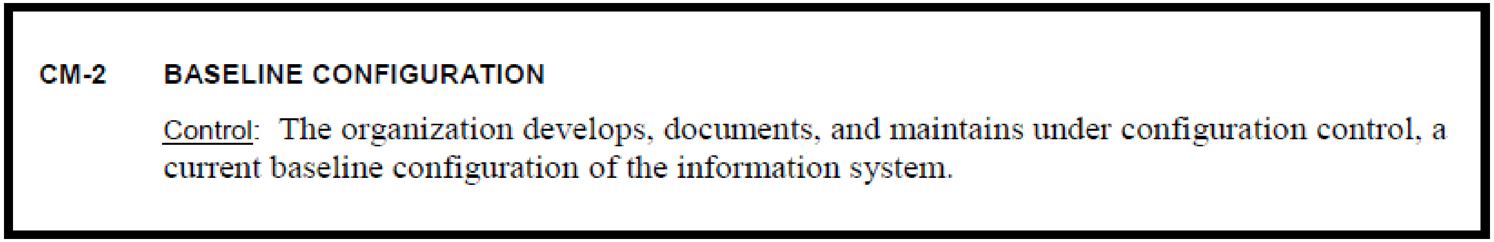
SECTION 3: CHECKING CAPABILITY DEFINITIONS LINKING TO 800-53 CONTROLS

Areas to cover:

1. Criteria for testing the CDM capabilities:
   1. Each control supports at least one capability (otherwise) the capabilities are incomplete.
   2. SME’s agree that no important goals are missing.
   3. The list can be expanded if new attack/exploit types emerge.
2. The controls that work together to thwart the attack/exploit type are identified.

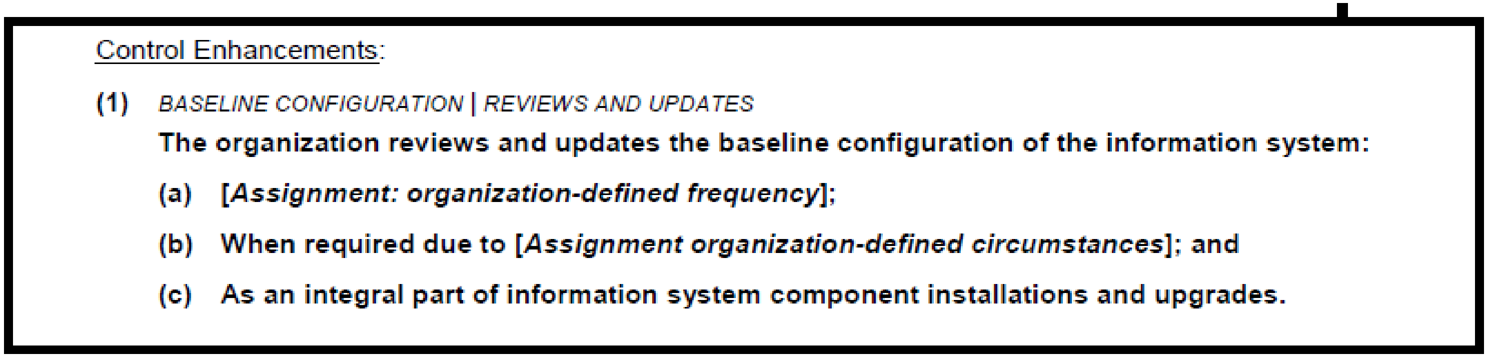
800-53 Control Parts

- NIST Controls are most often made up of many parts
  - Base control (1-8 parts).
  - Control enhancements (often a dozen, often with parts).
  - A “Control” is like a compound, consisting of many individual ingredients. So a control may have many purposes.
  - NIST encourages testing the parts, rather than the “whole” control.



CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.



Control Enhancements:

(1) *BASELINE CONFIGURATION | REVIEWS AND UPDATES*

The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

CDM and Base Controls

- CDM focuses on testing control items
  - A control item is statement of a single testable desired state as part of a control.
    - Each **base control** is a separate control item (apart from its enhancements), or if it has sub-parts designated by a), b) c), etc, each subpart is a control item.

Base Control	Corresponding Control Items
AC-5 SEPARATION OF DUTIES **Control: The organization:** **a. Separates [Assignment: organization-defined duties of individuals];** **b. Documents separation of duties of individuals; and** **c. Defines information system access authorizations to support separation of duties.**	AC-5 SEPARATION OF DUTIES Control: The organization: a. Separates [Assignment: organization-defined duties of individuals];
	AC-5 SEPARATION OF DUTIES Control: The organization: b. Documents separation of duties of individuals; and
	AC-5 SEPARATION OF DUTIES Control: The organization: c. Defines information system access authorizations to support separation of duties.
AC-6 LEAST PRIVILEGE **Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.**	AC-6 LEAST PRIVILEGE Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

CDM and Control Enhancements

- CDM focuses on testing control items
  - A control item is statement of a single testable desired state as part of a control.
    - Each **enhancement** is a separate control item (apart from other enhancements and base controls), or if it has sub-parts designated by a), b) c), etc, each subpart is a control item.

Control Enhancement	Corresponding Control Items
AC-2 **(7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES** **The organization:** **(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;** **(b) Monitors privileged role assignments; and** **(c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.**	AC-2 (7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
	AC-2 (7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES The organization: (b) Monitors privileged role assignments; and
	AC-2 (7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES The organization: (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.
AC-2 **(8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION** **The information system creates [Assignment: organization-defined information system accounts] dynamically.**	AC-2 (8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION The information system creates [Assignment: organization-defined information system accounts] dynamically.

Why focus on Control Items?

- They are individually testable.
- Each control item supports fewer capabilities than the “whole control” would, simplifying the testing process.
- The control item supports each capability more directly, because it doesn’t carry as much baggage that may not relate to the capability.

Understanding Control Items

- NIST emphasizes that a single control item may Support Multiple Capabilities
  - Many controls are very generic in nature.
    - Configuration management controls are a good example. CM controls can be used to Diagnose/Mitigate:
      - unauthorized hardware.
      - unauthorized software.
      - unacceptable software settings.
      - vulnerable software (CVEs).
  - Such generic controls will typically map to multiple vulnerabilities.

Mapping 800-53 Control Items to CDM Security Capabilities

- How CDM takes 800-53 **control items** and links them to **CDM Security Capabilities**
  - In finding the control items in 800-53 rev4, “regular expressions” were developed and used to do the mapping through automation.
    - This process allowed validation of the rules, testing for missed control items, and estimation of false positive and false negative rates.
    - Focus to completely avoid false negatives (and remove false positives manually).

Examples of the regular expressions:

A control item maps to HWAM if one or more of the following are true:
It contains **“inventory”.**
It contains “supply chain”, and NOT “monitoring”.
……And about 12 other conditions…….

Mapping 800-53 Control Items to CDM Security Capabilities

- Results:
  - NIST SP 800-53 rev4 has about 1,300 control items
    - About half of these are in the high baseline.
    - Another large group are “not selected”.
  - Regular expressions found about 2,900 control item to capability mappings, or an average of < 3 capabilities supported by each control item.
  - As NIST and DHS write testing guidance, we are reducing the number by removing false positives.
  - The number can be further reduced for routine systems because roughly half the control items are “not selected” even for the “high” baseline.

Good News:
D/As do not have to repeat this analysis!!

RECAP

SECTION 3: CHECKING CAPABILITY DEFINITIONS LINKING TO 800-53 CONTROLS

Areas that were covered:

1. Criteria for testing the CDM capabilities:
   a. Each control supports at least one capability (otherwise) the capabilities are incomplete.
   b. SME's agree that no important goals are missing.
   c. The list can be expanded if new attack/exploit types emerge.
2. The controls that work together to thwart the attack/exploit type are identified.

INTRODUCTION

SECTION 4: DEFINING TESTS (DEFECT CHECKS) THAT ASSESS CONTROL ITEM EFFECTIVENESS

Areas to be covered:

1. If the [actual state] <> [desired state] equals a “security defect.”
2. A defect check is a statement of which desired state attributes need to be tested to find significant security risks (and also control effectiveness).

This section illustrates how defect checks are defined in CDM.

What to Assess: Defect Checks

- In reviewing control Items CDM focuses on testing for defect checks
  - A Defect Check is:
    - A statement about a particular attribute or behavior of an object type/role that can have security defects, flaws, weaknesses, and/or vulnerabilities; expressed in data.
    - A way to implement the determination statement (from SP 800-53A), which has the following additional properties:
      - It is stated as a test (wherever appropriate).
      - Can be automated (wherever possible).
      - It explicitly says what desired state will be compared to what actual state to determine the test result.
  - A key function of the defect check is to restate the determination statement in a way that can be tested, and can measure degree of risk, not just a pass/fail measure.

NIST Control Items and 800-53A "Determination Statements"

AC-2 (2).1 ACCOUNT MANAGEMENT	
The Control Statement (800-53 rev 3)	**Determination Statement (800-53A)**
The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a time period for each type of account after which the information system terminates temporary and emergency accounts; and* *(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.*

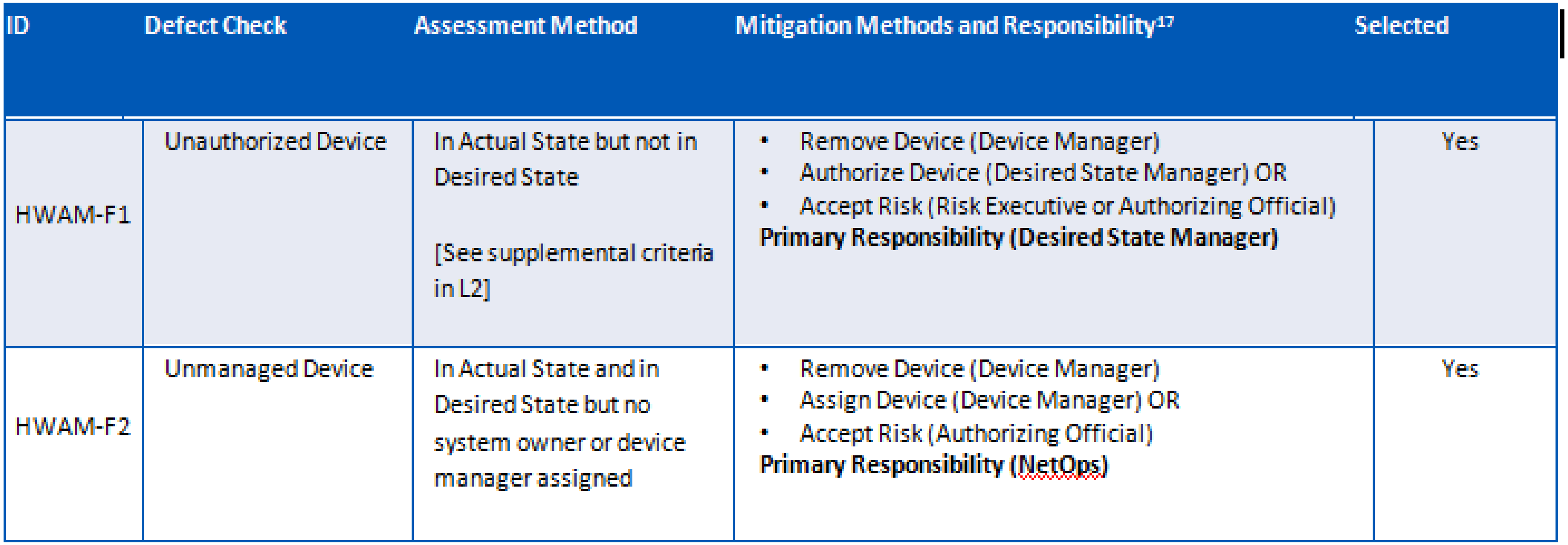
We need one or more defect checks that will "fail" if each control item is not effective.

The defect checks then assess or test the control item.

A defect check might test more than one control item.

Defect Check Tables

- Defect Check Tables document the testing that CDM performs. It defines the following for each test
  - Defect Check
  - Assessment Method
  - Mitigation Methods and Responsibility



ID	Defect Check	Assessment Method	Mitigation Methods and Responsibility[17]	Selected
HWAM-F1	Unauthorized Device	In Actual State but not in Desired State [See supplemental criteria in L2]	• Remove Device (Device Manager) • Authorize Device (Desired State Manager) OR • Accept Risk (Risk Executive or Authorizing Official) **Primary Responsibility (Desired State Manager)**	Yes
HWAM-F2	Unmanaged Device	In Actual State and in Desired State but no system owner or device manager assigned	• Remove Device (Device Manager) • Assign Device (Device Manager) OR • Accept Risk (Authorizing Official) **Primary Responsibility (NetOps)**	Yes

What to Assess: Defect Checks

- CDM Federal and Local Defect Checks
  - Federal defect checks are those essential to the purpose of the capability and the quality of the data being reported. These Federal defect checks need to be implemented by all federal organizations, as they are part of CyberScope reporting.
    - Federal defect check results are reported to the federal dashboard.
    - The CDM Scoring and Metrics WG will help determine what defect checks are considered “Federal.”
  - Local defect checks are those defect checks which may be optional for federal organizations to implement.
    - Local defect check results stay local to a given Department or Agency.
    - If the local defect check applies to an implemented control from an applicable SP 800-53 baseline, the organization is responsible for either selecting the CDM local defect check OR assessing the control/control item on their own.

Example / Notional – HWAM Federal Defect Checks

ID	Defect Check	Determination Statement	Mitigation Methods and Responsibility	Selected
HWAM-F1	Unauthorized Devices	In Actual State but not in Desired State [See supplemental criteria in L2]	• Remove Device (Device Manager) • Authorize Device (Desired State Manager) OR • Accept Risk (Risk Executive)	Yes
HWAM-F2	Unmanaged Devices	In Actual State and in Desired State but no “appropriate” manager assigned	• Remove Device (Device Manager) • Assign Device (Device Manager) OR • Accept Risk (Risk Executive)	Yes
HWAM-F3	Non-Reporting Devices	In Desired State but not in Actual State	• Restore Device Reporting (CDM Operator) • Declare Device Missing (Device Manager) OR • Accept Risk (Risk Executive)	Yes
HWAM-F4	Non-Reporting Defect Checks	Defect Checks are selected, but the HWAM Actual State Collection Manager does not report testing on all devices	• Restore Defect Check Reporting (CDM Operator) • De-Select Defect Check (Risk Executive) • Accept Risk (Risk Executive)	Yes
HWAM-F5	Completeness-Metric	Completeness of the actual inventory collection is below an [organization-defined-threshold].	• Restore Completeness (CDM Operator) • Accept Risk (Risk Executive)	Yes
HWAM-F6	Timeliness-Metric	Frequency of update (timeliness) of the actual inventory collection is not as frequent as an [organization-defined-threshold].	• Restore Frequency (CDM Operator) • Accept Risk (Risk Executive)	Yes

Example / Notional – HWAM Local Defect Checks

ID	Defect Check	Assessment Method	Mitigation Methods and Responsibility	Selected
HWAM-L1	Device for Travel	Desired State says Device is approved for Travel. Device type or subcomponents do not meet D/A defined rules (for before or after travel).	• Remove Authorization to use for travel (Device Manager) • Correct hardware configuration (Device Manager) • Accept Risk (Risk Executive)	
HWAM-L2	Unauthorized Device	Device must be in the desired state and subsequently approved by a separate authorized person from the person who added it and manages it.	• Remove Device (Device Manager) • Authorize Device (Desired State Manager) OR • Accept Risk (Risk Executive)	
HWAM-L3	Required device not installed	Device in desired state, authorized, and has not appeared in the actual state after [an organization-defined] number of collections.	• Install device (Device Manager) • Remove requirement (Risk Executive) • Accept Risk (Risk Executive)	
HWAM-L4	Unapproved device owner	The device owner is other than a value in an approved list. (Could also apply to sub-components.)	• Remove Device (Device Manager) • Correct Ownership (Desired State Manager) • Accept Risk (Risk Executive)	

Example / Notional – HWAM Local Defect Checks

HWAM-L5	Unapproved Supplier or Manufacturer	The device supplier or manufacturer is not in an approved list	• Remove Device (Device Manager) • Correct Supplier Data (Desired State Manager) • Correct Manufacturer Data (CDM Operator) • Accept Risk (Risk Executive)
HWAM-L6	Subcomponents not Authorized. All controls on hardware configuration.	Subcomponents added to the actual and desired state, and system verifies that [organization-defined sub-component types] are authorized or creates a defect	• Remove Sub-Component (Device Manager) • Correct Configuration (Risk Executive) • Accept Risk (Risk Executive)
HWAM-L7	Authorization reached Sunset	Track an authorization sunset date, which can be expired by trigger events. Score all devices past their sunset date as unapproved.	• Re-authorize (Device Manager) • Remove Device (Device Manager) • Accept Risk (Risk Executive)
HWAM-L8	Required Device Data	Track additional device data and score devices that don't have that data	• Add Data (Desired State Manager) • Remove Device (Device Manager) • Accept Risk (Risk Executive)
HWAM-L9	Proposed Changes too old	Proposed changes not approved after [organization-defined timeframe]. Assumes L2 is selected.	• Withdraw proposed change (Desired State Manager) • Approve proposed change (Desired State Manager) • Accept Risk (Risk Executive)

Control Assessment Narratives

- Each CDM security capability provides control assessment narratives which provides and documents an assessment plan for the controls on a system.

Notional Control Narrative

Control CM-03b: CONFIGURATION CHANGE CONTROL. (HWAM)

Determine if:

The organization reviews proposed configuration-controlled changes to the information system {devices and device components} and approves or disapproves such changes with explicit consideration for security impact analyses;

- ***Control Item Implemented by:*** The devices' system: Desired State Manager(s)
- ***Inheritance by:*** CDM Assessed Systems using that device
- ***Assessment Boundary:*** A CDM Target Network
- ***Assessment and Diagnosis Responsibility:*** CDM Checks
- ***Assessment Methods:***
- Test 1: HWAM-C1-Unauthorized Devices will show a defect if the Actual State and Desired States are not equal. This would include when devices are added without authorization.
- Test 2: HWAM-NC2-Unauthorized Devices will show a defect if the device approval was not verified by a separate person from the one who added the device to authorized inventory and connected it to the CMD-TN. This ensures authorizations are reviewed.
- ***Required Maturity:*** Level 2 – Capability
- ***Mitigation Methods and Responsibility:*** See the Defect Check Table.

These narratives provide a template for a completed system assessment plan.
The D/A may adopt them as-is, modify them, or start from scratch.

Control Assessment Narratives

- Control Assessment Narratives do the following:
  - Describes default operational roles for things like assessment and mitigation.
  - Documents assessment boundaries and inheritance availability.
  - Documents required determination statements and assessment methods.
  - Lists defect checks which may support assessment of the control.
  - States the required level of maturity that is considered essential in CDM for that capability to justify use of the automated testing.

Control Allocation Tables

- The Control Allocation Tables provide a summary of the Assessment Plan Narratives.
- Concept developed by the DHS/CIO’s Office.
- Summarizes test plans for high, moderate, and low impact baselines.
- Complements the defect check tables and assessment narratives to document the assessment plan.

Notional Control Allocation Tables

Control Item	Implemented by	Inherited by	Assessment Boundary	Diagnostic Responsibility	Defect Metrics	Selected	Risk Acceptance	Frequency	Impact
AC-19 (5)	Dev-System	CDM-ASys	CDM-TN	CDM Checks	F1 & L4			<4 days	
CM-03 (1a)	Dev-System	CDM-ASys	CDM-TN	CDM Checks	F1 & L2			<4 days	
CM-03 (1b)	Dev-System	CDM-ASys	CDM-TN	CDM Checks	F1 & L2			<4 days	
CM-03 (1c)	Dev-System	CDM-ASys	CDM-TN	CDM Checks	L9 & F1			<4 days	
CM-03 (1d)	CDM Dash	CDM-ASys	CDM-TN	CDM Checks	F1 & L2			<4 days	
CM-03 (1e)	Dev-System	CDM-ASys	CDM-TN	CDM Checks	F1, F3, L2 & L7			<4 days	
CM-03 (1f)	CDM-Dash	CDM-ASys	CDM-TN	CDM Checks	F1 & L2			<4 days	
CM-08 (2)	Dev-System	CDM-ASys	CDM-TN	CDM Checks	F1, F3 & L6			<4 days	
CM-08 (4)	Dev-System & CDM-TN	CDM-ASys	CDM-TN	CDM Checks	F2			< 4 days	
SA-12	Dev-System	CDM-ASys	CDM-TN	CDM Checks	L5			< 4 days	

RECAP

SECTION 4: DEFINING TESTS (DEFECT CHECKS) THAT ASSESS CONTROL ITEM EFFECTIVENESS

Areas that were covered:

1. If the [actual state] <> [desired state] equals a “security defect.”
2. A defect check is a statement of which desired state attributes need to be tested to find significant security risks (and also control effectiveness).

This section illustrates how defect checks are defined in CDM.

INTRODUCTION

SECTION 5: REPORTING DISCOVERED RISK

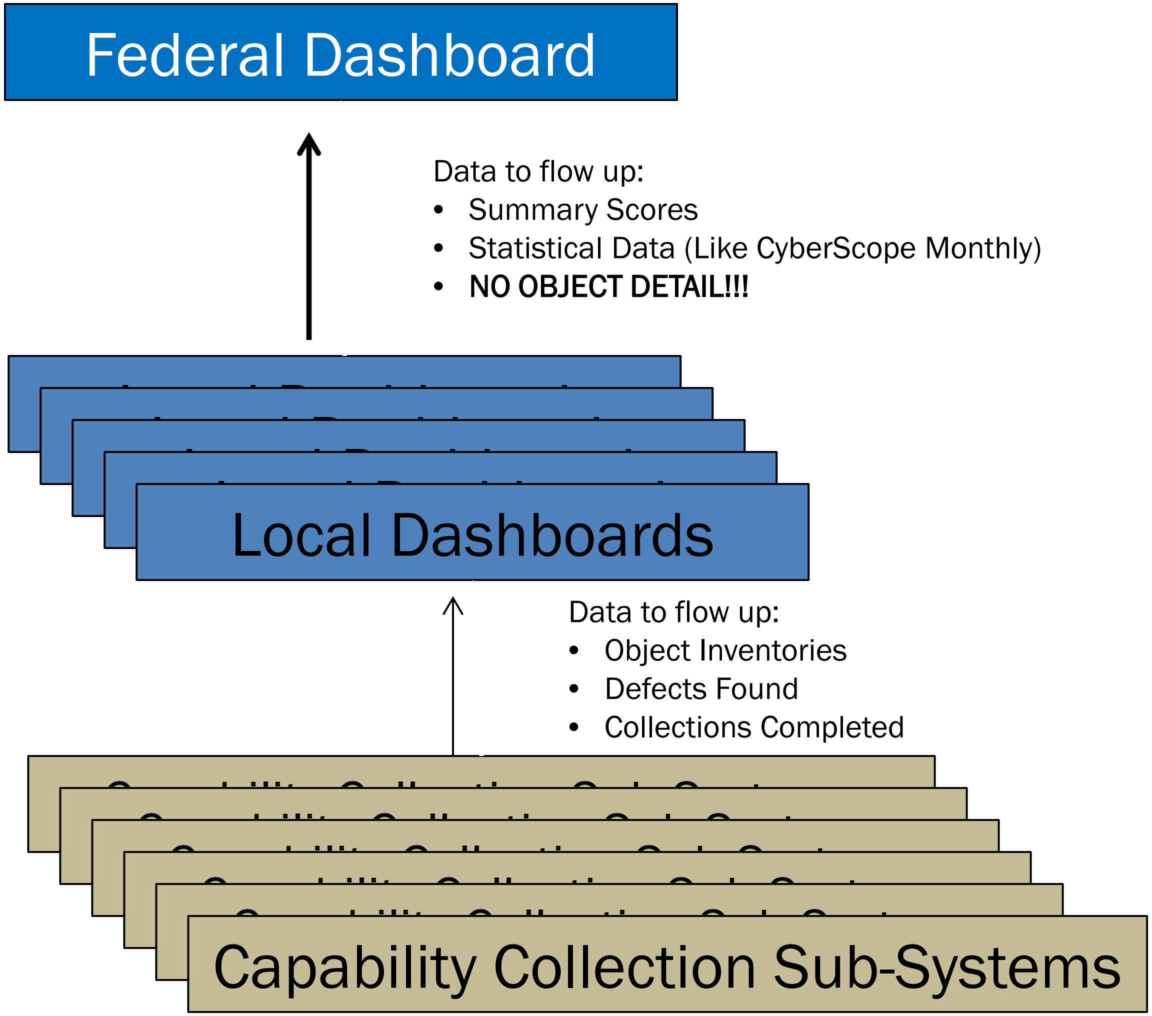
Areas to be covered:

1. The role of the dashboard.
2. Conducting root cause analysis.
3. Identifying the roles and responsibilities.
4. Understanding the role of assessment and authorization boundaries.
5. Learn about how CDM display defects.

Reporting Discovered Risk

- Provisional risk will be reported by the CDM Dashboard
  - Two levels
    - Federal level
    - Local Department / Agency level
  - Audience
    - System Owners
    - ISSOs
    - DAA
  - Helps make operational decisions

Reporting Discovered Risk



Data to flow up:

- Summary Scores
- Statistical Data (Like CyberScope Monthly)
- NO OBJECT DETAIL!!!

Data to flow up:

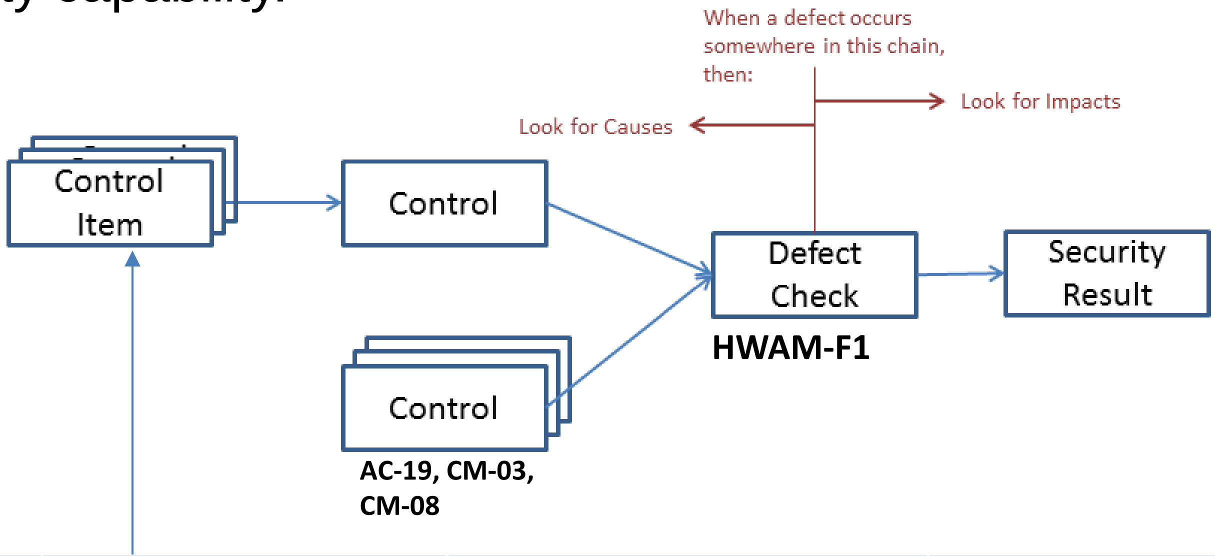
- Object Inventories
- Defects Found
- Collections Completed

Reporting Discovered Risk

- Operational decisions
  - What needs to be fixed first (highest risk).
  - Should the system continue to be authorized to operate.
  - What systemic problems need investment and/or engineering.
  - Which operational teams are doing well (or not) at managing risk.
    - This includes teams managing controls implemented
      - Directly by the system.
      - Inherited as common controls, but implemented by others.
    - This includes helping those teams know which are currently the highest risk problems so those can be addressed first.

Root Cause Analysis

- Root cause analysis is often needed when a control fails.
- Root cause analysis operates on the logical flow of cause to effect from control items to the security result which is the objective of a security capability.



Defect Check	Low Baseline	Moderate Baseline	High Baseline
HWAM-F1	CM-08-a	CM-03b, CM-03c, CM-03 (2), CM-08 (1), CM-08 (3a),	AC-19 (5), CM-03 (1a), CM-03 (1b), CM-03 (1c), CM-03 (1d), CM-03 (1e), CM-03 (1f), CM-08 (2)

Root Cause Analysis

- Root cause analysis includes:
  - Looking back toward the control items to see which failures may have caused the defect.
  - Looking forward to see the impact on the desired security result.

Roles and Responsibilities

- NIST Roles
  - Information Owner/Steward
  - Senior Information Security Officer
  - Authorizing Official
  - Authorizing Official Designated Representative
  - Common Control Provider
  - Information System Owner
  - Information System Security Officer
  - Information Security Architect
  - Information System Security Engineer
  - Security Control Assessor

Roles and Responsibilities

- CDM NOTIONAL Roles
  - CDM operational roles and responsibilities are illustrative operational roles that those with managerial roles would typically delegate to others.
  - Depending on the size and complexity of the system, these operational roles may be full time positions or they may be performed along with other duties. While each organization might define these operational roles in different ways, the goal is to ensure that operational duties are assigned to roles and then to individuals or teams with enough capacity to perform the role. Thus, the roles defined here are examples to help implement ongoing assessment and response and to maintain the desired system security posture.
    - Examples – System Owner, ISSO, System Administrator

CDM Notional Roles

CDM Non-normative Operational Roles	Responsibilities
CDM Checks	Indicates that the role is fulfilled by implementation of the specified CDM Defect Check(s) within the HWAM data collection sub-system, and sending appropriate defect data to the CDM dashboard covering the relevant system(s). CDM Checks are responsible for the assessment of most HWAM NIST SP 800-53 security controls.
CDM Dashboard	Indicates that the role is fulfilled by the CDM dashboard which uses basic data collected to display important data for security actors and decision makers (including HWAM). The CDM Dashboard is responsible for implementing selected security controls, mostly related to reporting to management.
CDM Operations (CDM Ops)	Indicates that the role is fulfilled by the operator of the CDM collection subsystems, especially the actual state collection system, but also supporting desired state specifications. CDM Ops is responsible for implementing selected security controls, mostly related to keeping actual state data current, complete, and accurate. This role might be filled by the CDM program ConMon as a Service contractor or by the department or agency.
Device Manager (DM)	Assigned to a device-system, device managers are (for HWAM) responsible to add/remove devices from the network, and for the hardware configuration of each device (adding and removing hardware components). The device managers are to be specified in the desired state inventory specification. The device manager may be a person or a group. If a group, there is a group manager in charge.
Desired State Manager (DSM)	Desired State Managers are needed for both the CDM Target Network and each device-system. The desired state managers ensures that data specifying the desired state of the relevant capability (in this case HWAM) is entered into the CDM system's desired state data, and is available to guide the actual state collection sub-system. The DSM for the CDM Target Network has a special role to resolve any ambiguity about which device system (if any) has each unallocated device in its boundary.
Manual Check	Assessment is not automated by the CDM system and is done by traditional A&A assessors using manual methods.

Assessments and Authorization Boundaries

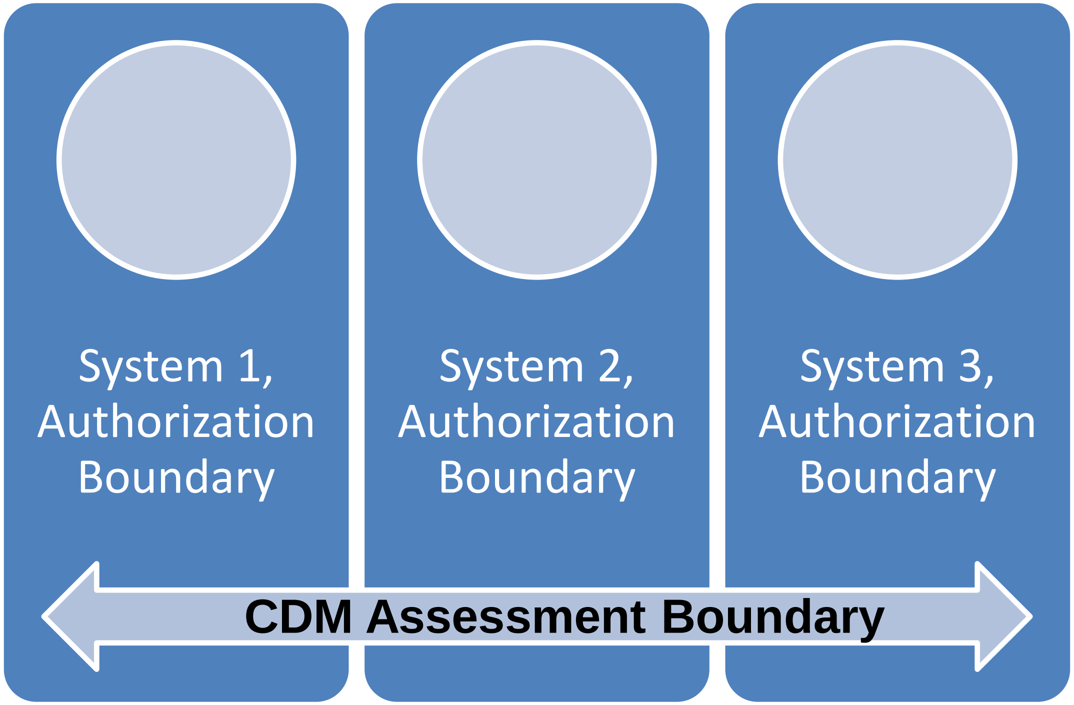
- System boundaries and CDM boundaries are not necessarily the same thing
  - CDM uses a concept known as an “assessment boundary”
    - under CDM, the most cost-effective assessment boundary consisting of all devices in a “network” bounded by traffic filters (firewalls) and other “boundary” protections.
  - NIST guidance uses the concept of a “system authorization boundary”
    - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

These are complementary concepts

- **Assessment boundary is what will be assessed together.**
- **Authorization boundary is what will be managed and authorized together.**

Assessments and Authorization Boundaries

- CDM assessment boundaries are typical larger
  - Multiple system authorization boundaries may be inside of a CDM assessment boundary.


System 1, Authorization Boundary
System 2, Authorization Boundary
System 3, Authorization Boundary
CDM Assessment Boundary

Assessments and Authorization Boundaries

- Benefits of a large CDM Assessment Boundary
  - The fixed cost of setting up the CDM dashboard and sensors, is only paid once.
  - The data can be used to look at risk from all systems across the organization (within the assessment boundary).
  - In large networks, there are typically components that fail to be assigned to any authorization (i.e., information system) boundary. These devices can be assigned to the CDM Assessment Boundary.

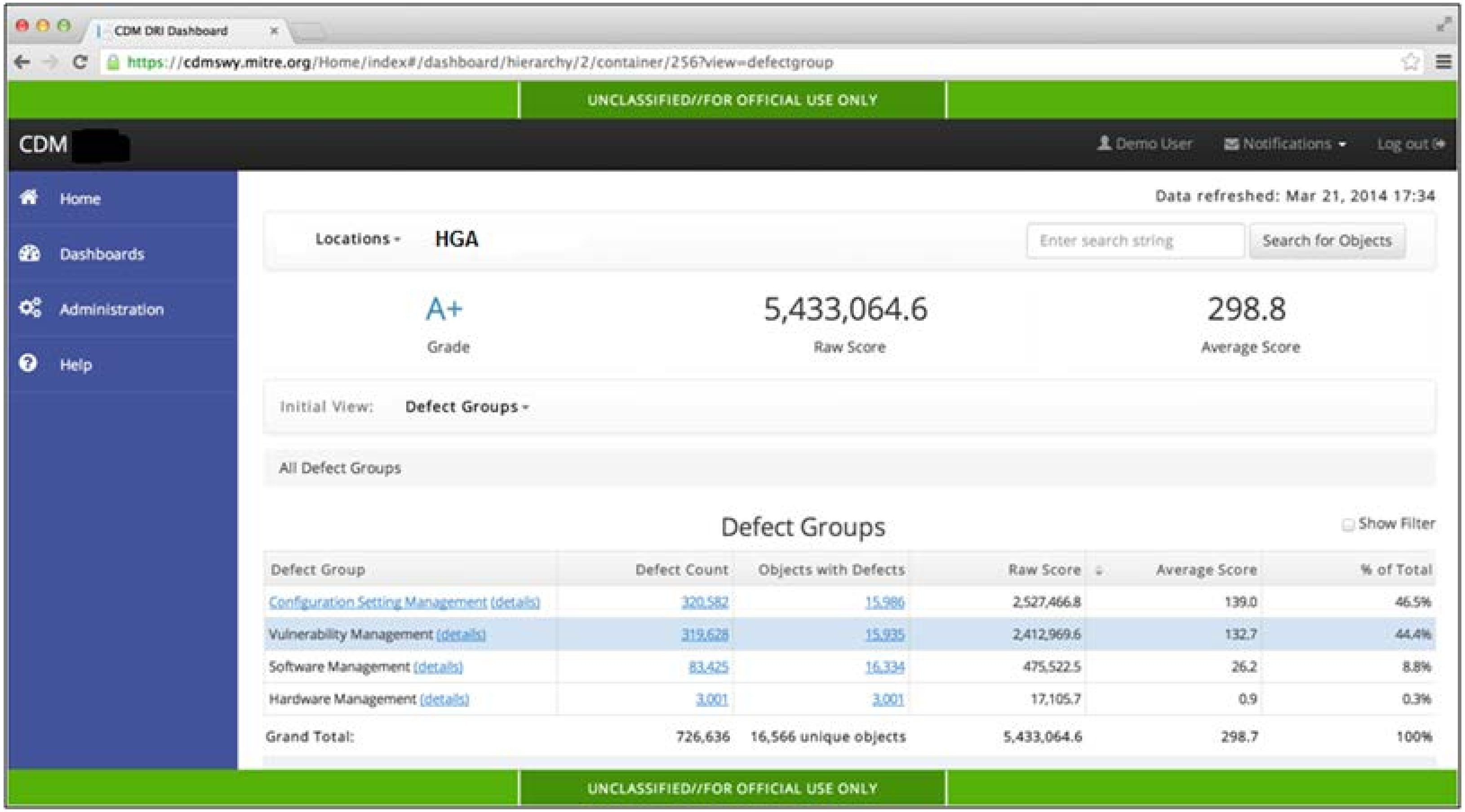
Assessments and Authorization Boundaries

- Tracing the risk to a system to its sources
  - In order for an ISCM implementation (like CDM) to accurately track the risks associated with each authorization boundary (information system) it must be able to do the following:
    - Identify components (objects and their controls) managed as part of the system.
    - Identify components (of other systems) which provide controls formally inherited by the system.
    - Identify components that are on potential attack paths to the system, thereby imposing (hopefully unintended) risk on the system.

Displaying Defects

- Defects are displayed by the local and Federal dashboards
  - The dashboard displays defects that get fixed first
  - Dashboards display the following types of attributes
    - Defect Groups
    - Defect Counts
    - Raw Score
    - Average Score
  - Defect Groups are based upon a number of different possible relationships
    - Security Capabilities
    - CDM Assessment Boundary
    - System Authorization Boundary

Displaying Defects



UNCLASSIFIED//FOR OFFICIAL USE ONLY

CDM [redacted]

Data refreshed: Mar 21, 2014 17:34

Locations HGA

A+ Grade

5,433,064.6 Raw Score

298.8 Average Score

Initial View: Defect Groups

All Defect Groups

Defect Groups

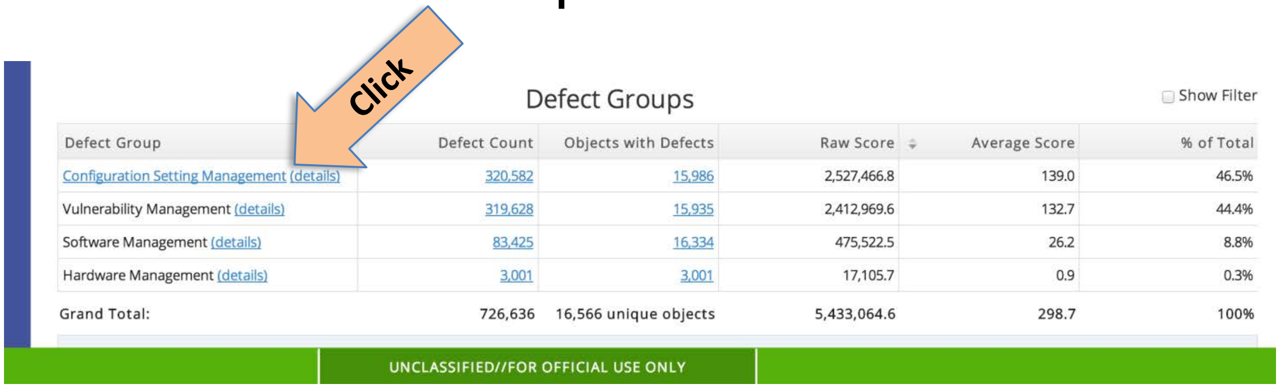
Defect Group	Defect Count	Objects with Defects	Raw Score	Average Score	% of Total
Configuration Setting Management (details)	320,582	15,986	2,527,466.8	139.0	46.5%
Vulnerability Management (details)	319,628	15,935	2,412,969.6	132.7	44.4%
Software Management (details)	83,425	16,334	475,522.5	26.2	8.8%
Hardware Management (details)	3,001	3,001	17,105.7	0.9	0.3%
Grand Total:	726,636	16,566 unique objects	5,433,064.6	298.7	100%

UNCLASSIFIED//FOR OFFICIAL USE ONLY

NOTIONAL CDM DASHBOARD

Displaying Defects

Drilling Down on a Defect Group



Click

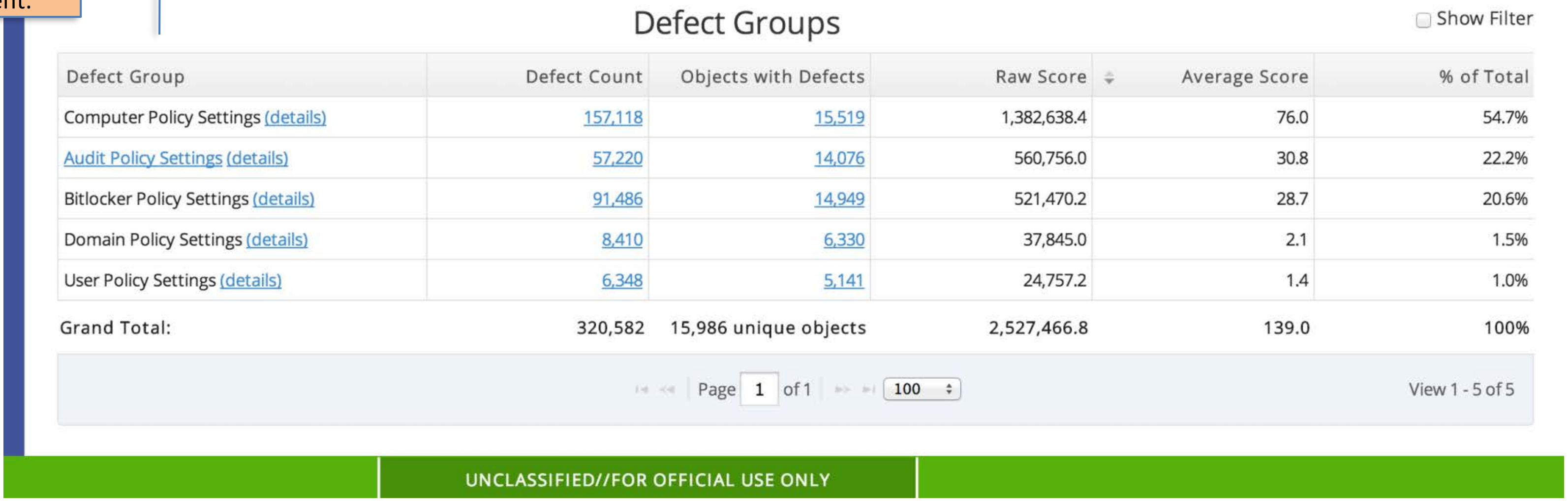
Defect Groups

□ Show Filter

Defect Group	Defect Count	Objects with Defects	Raw Score	Average Score	% of Total
Configuration Setting Management (details)	320,582	15,986	2,527,466.8	139.0	46.5%
Vulnerability Management (details)	319,628	15,935	2,412,969.6	132.7	44.4%
Software Management (details)	83,425	16,334	475,522.5	26.2	8.8%
Hardware Management (details)	3,001	3,001	17,105.7	0.9	0.3%
Grand Total:	726,636	16,566 unique objects	5,433,064.6	298.7	100%

UNCLASSIFIED//FOR OFFICIAL USE ONLY

List of Defect Groups under Configuration Setting Management.



Defect Groups

□ Show Filter

Defect Group	Defect Count	Objects with Defects	Raw Score	Average Score	% of Total
Computer Policy Settings (details)	157,118	15,519	1,382,638.4	76.0	54.7%
Audit Policy Settings (details)	57,220	14,076	560,756.0	30.8	22.2%
Bitlocker Policy Settings (details)	91,486	14,949	521,470.2	28.7	20.6%
Domain Policy Settings (details)	8,410	6,330	37,845.0	2.1	1.5%
User Policy Settings (details)	6,348	5,141	24,757.2	1.4	1.0%
Grand Total:	320,582	15,986 unique objects	2,527,466.8	139.0	100%

Page 1 of 1 100 View 1 - 5 of 5

UNCLASSIFIED//FOR OFFICIAL USE ONLY

RECAP

SECTION 5: REPORTING DISCOVERED RISK

Areas that were covered:

1. The role of the dashboard
2. Conducting root cause analysis
3. Identifying the roles and responsibilities
4. Understanding the role of assessment and authorization boundaries
5. Learn about how CDM display defects

Recap

- ❑ Learning Objectives
- ❑ Section 1: Prerequisites to AUTOMATION of Assessment
- ❑ Section 2: Linking Assessment to Security Results/Outcomes
- ❑ Section 3: Checking Capability Definitions Linking to 800-53 Controls
- ❑ Section 4: Defining Tests (DEFECT CHECKS) that Assess Control Item Effectiveness
- ❑ Section 5: Reporting Discovered Risk