

Hardware Asset Management (HWAM) Capability Description

Purpose: The Hardware Asset Management Capability provides an organization visibility into the hardware ([devices](#)) operating on their network(s) so they can manage and defend it in an appropriate manner. It also provides a view of device management responsibility such that prioritized defects can be presented to the responsible party for mitigation actions and risk acceptance decisions.

How does it work: HWAM identifies devices (including virtual machines) actually present on the network and compares them with the '[desired state](#)' [inventory](#) to determine if they are authorized. Some devices are network-addressable, and others are [removable](#) (and presumably connected to addressable devices). The means for identifying the actual devices will vary, depending on the automated capabilities available and which 'type' of device it is.

The CDM process (as adapted for your D/A) will provide insight into what percentage of the actual hardware assets are included in the desired state, and of those, how many of them identify an assigned manager.

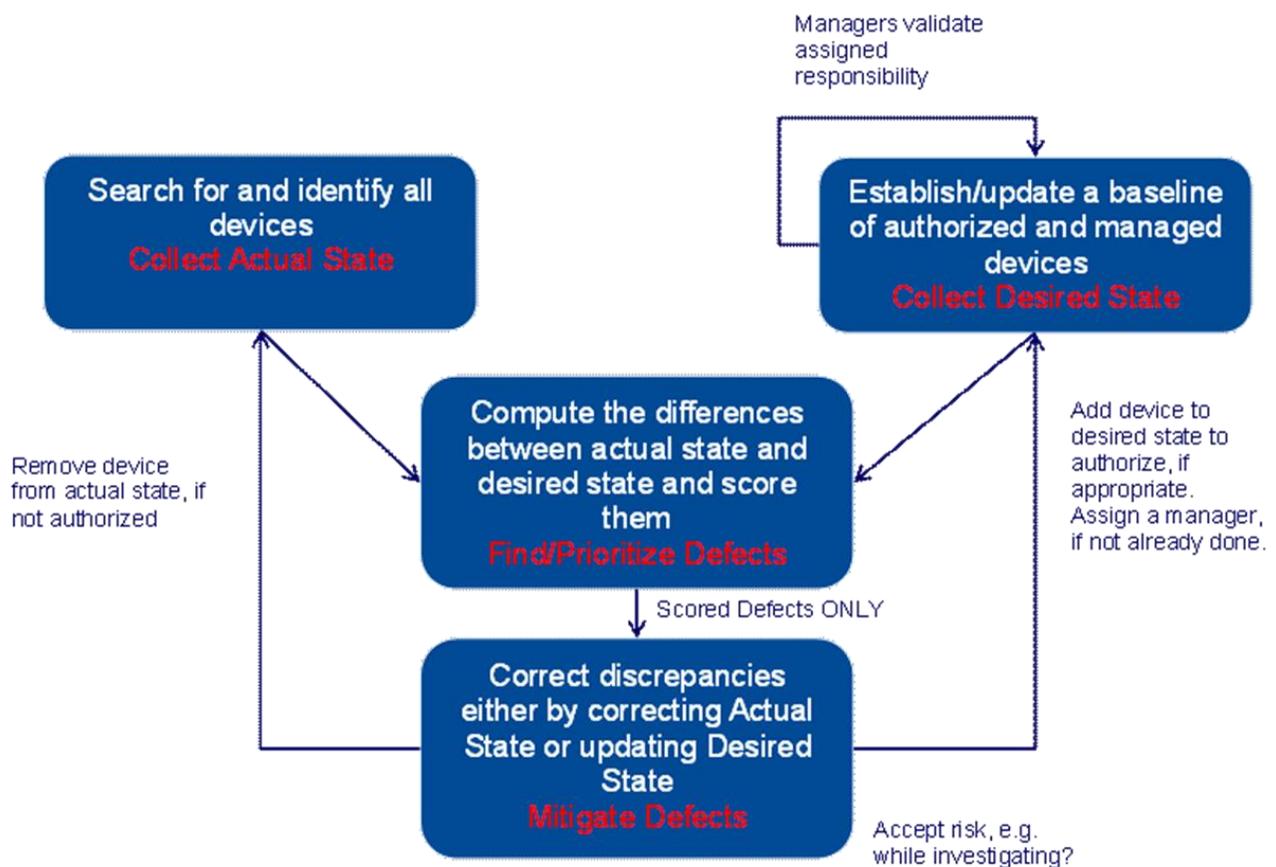


Figure 1 The HWAM Capability Process

How do Unauthorized and Unmanaged Devices Impact the Network: Attackers continually scan for hardware systems that they can exploit to gain control of and use to access other devices and data. Typically, the most exposed devices are those that are unauthorized or unmanaged. Systems or removable media such as Universal Serial Bus (USB) flash drives, are often compromised outside the secured network, and then when attached to the secure network, any installed malware can then potentially infect other hosts. Additionally, missing devices with information contained on them can be used for either the value of the content itself or as leverage/resources to conduct future attacks on the system and network.

Collect Actual State: Use tools to collect information about what IP-addressable devices, virtual machines and removable media are actually present on the network. The network and connected devices are continuously observed to detect and learn about IP-addressable devices and removable media. Methods to detect devices (when it was first seen, and when/where it was last seen) include (but are not limited to):

- passive listening to identify devices talking
- active IP range scanning, to detect devices (e.g., respond to a “ping”)
- active mining of DHCP logs and/or switch tables
- Network Access Control (if present)

Methods to learn about discovered devices include (but are not limited to):

- Passive listening to types of traffic to/from devices
- active methods (e.g., trace route) to collect data about the device’s location
- active agents on the device to detect sub-components and other details

The CDM process will identify the assets actually on the network that are addressable and can provide the information required to compare them with the authorized inventory. Also, you will need to identify how much of the network is being monitored to discover the actual hardware operating on it.

Collect Desired State: Create an [Authorized Hardware Inventory](#) ([white list](#) and possibly a [black list](#)) using policies, procedures, and processes suggested by the CDM program and/or defined in the organization. Output is a HW Inventory that contains identifying information for a device (to include physical location), when it was authorized, when the authorization expires, and who manages the device. Only authorized removable media are allowed to connect to IP-addressable devices on a network (e.g. plugged into a USB port), and which removable media are authorized for each device will be listed on an inventory.

Diagnose (By Finding and Prioritizing [Defects](#)): Comparing the list of devices discovered on the network with the authorized hardware inventory list, some devices might exist on one list and not on the other. This will identify unauthorized devices that need to be dealt with, as well as missing authorized devices that may indicate an additional security risk. Additional defects related to hardware management may

be defined by the D/A. After devices are detected, they will be automatically [scored](#) and prioritized (using federal and D/A defined criteria) so that the worst problems can be addressed first¹.

Mitigate Defects: The CDM dashboard will generally be organized to show worst problems first. Worst problems should be mitigated first. The following table shows the most important defect types and mitigation options. The full set of Defects and mitigations are documented in the *Hardware Asset Management Datasheet*.

| Defect Type | Detection Rule | Mitigation Options |
|-----------------------|--|--|
| Unauthorized Devices | In Actual State but not in Desired State | <ul style="list-style-type: none"> Remove Device Authorize Device OR Accept Risk |
| Unmanaged Devices | In Actual State and in Desired State but no “appropriate” manager assigned | <ul style="list-style-type: none"> Remove Device Assign Device OR Accept Risk |
| Non-Reporting Devices | In Desired State but not in Actual State | <ul style="list-style-type: none"> Restore Device Reporting Declare Device Missing OR Accept Risk |
| Missing Devices | Non-Reporting and declared lost, stolen or missing in Desired State after search | <ul style="list-style-type: none"> Accept Risk while waiting for the Device to be Found Reauthorize a Found Device OR Remove Device (i.e., accept loss of device) |

¹ Many defects will have a “grace period” built into the scoring function. For CDM, these grace periods are calculated from the time the defect is first identified, not when the desired state specification or actual state changed.

Appendix A - Definitions

| <u>Term</u> | <u>Definition</u> |
|---|--|
| Authorized Hardware Inventory | List of authorized hardware assets for an organization or subnet. |
| Black List | Banned list of assets for an organization or subnet. |
| Defect | A condition where the Desired State specification and the Actual State do not match in a manner that incurs risk to the organization. |
| Device | IP-addressable asset on the network or a non-addressable component (e.g. removable media) able to interact with the organization's data and resources. |
| Device Role | An enterprise-wide label for a class of devices that perform a like function in the environment. Examples are file servers, external web server, or workstation. The device role is intended to simplify assigning asset values or scoring weights by allowing D/As to define them for groups of devices and having individual devices inherit the values. |
| Hardware Asset Management (HWAM) Capability | The Continuous Diagnostic and Mitigation (CDM) capability that ensure unauthorized and/or unmanaged hardware is removed from the organization's network, or authorized and assigned for management, before it is exploited, compromising confidentiality, integrity, and/or availability. |
| Removable media | Removable storage devices that can be attached to a hardware asset on a network, typically by USB ports. |
| Scoring | The process of calculating the risk points for a defect. Identified defects will be "scored" based on the amount of perceived risk they create. The CDM program will be providing a scoring system that is generic across D/As. Each D/A may adapt this with additional D/A specific information to better prioritize defects for action. |
| White List | Approved list of assets for an organization or subnet. |