Continuous Diagnostics and Mitigation (CDM) Phase II – Managing People & Access

Jim Quinn

October 28, 2014

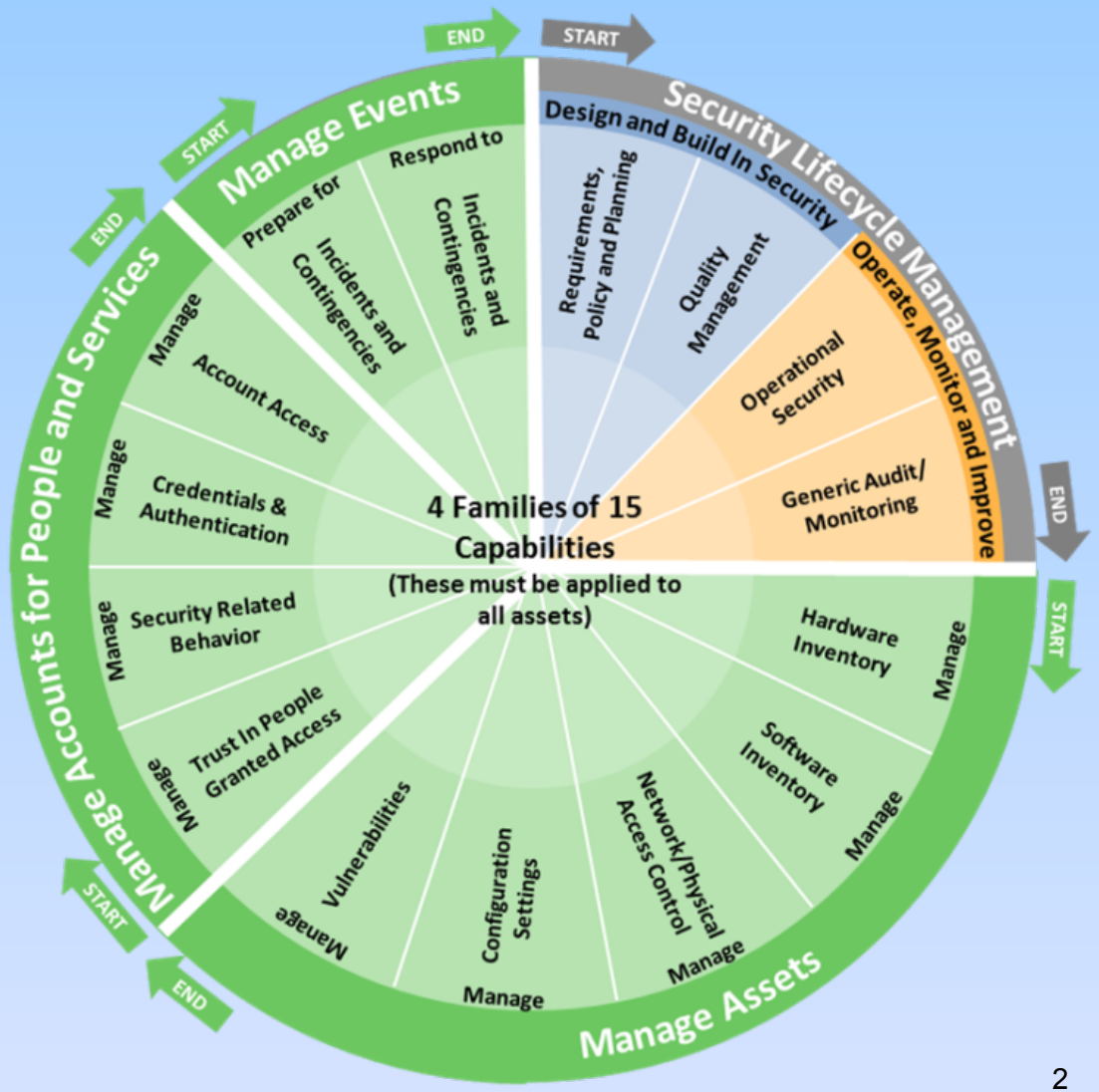
Homeland Security

CDM Capabilities

Capability:

A collection (set) of security controls that work together to achieve an overall security purpose

NIST 800-53Rev4 p21



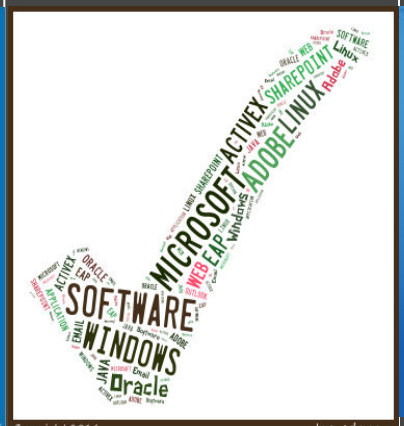
Homeland Security

2

Review of the Phase 1 Capabilities

HWAM	SWAM	CSM	VUL

• Find all addressable Devices
• Determine valid
• Risk Manage Differences
	• What Software?
	• Baseline
	  • O/S
	  • Common
	  • Specific
	• Authorization?
		• Baseline
		• Policy variance
		• Authorization?
		• Risk Manage Differences
			• Detect
			• Score
			• Characteristics

Homeland Security

Phase II Capabilities

- 5: **Manage Network Access Controls (NAC)** is to prevent, and allow the agency to remove and limit, unauthorized network connections/access to prevent attackers from exploiting internal and external network boundaries and then pivoting to gain deeper network access and/or capture network resident data in motion or at rest.

- 6: **Manage Trust in People Granted Access (TRUST)** is to prevent insider attacks by carefully screening new and existing persons granted access for evidence that access might be abused.

- 7: **Manage Security Related Behavior (BEHAVE)** is to prevent general users from taking unnecessary risks and further to prevent attackers from exploiting network and application users via social engineering scams. BEH prevents users with elevated privileges and special security roles from taking unnecessary risks to prevent attackers from exploring poor engineering and/or remediation.

Homeland Security

Phase II Capabilities

- 8: **Manage Credentials and Authentication (MCA) [aka CRED]** is to prevent a) the binding of credentials to or b) the use of credentials by other than the rightful owner (person or service) by careful management of credentials, preventing attackers from using hijacked credentials to gain unauthorized control of resources, especially administrative rights.
- 9: **Manage Account Access (MAA) [aka PRIV]** is to prevent access beyond what is needed to meet business mission by limiting account access and eliminating unneeded accounts to prevent attackers from gaining unauthorized access to sensitive data.

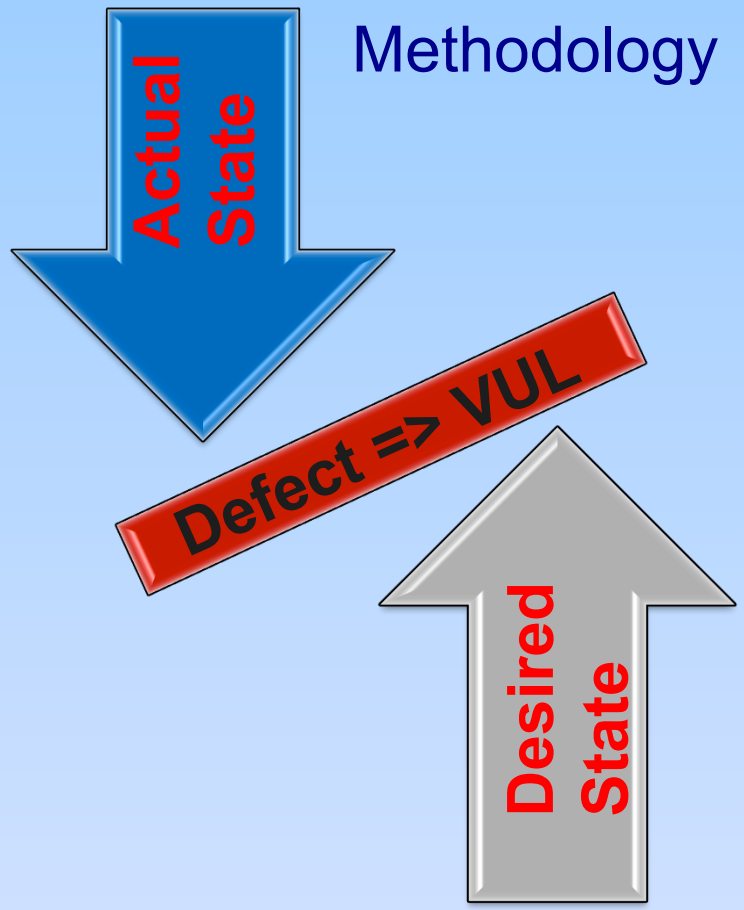
Homeland Security

Measurement + Metrics

"Measurement is the first step that leads to control and eventually to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it." — H. James Harrington

"If a measurement matters at all, it is because it must have some conceivable effect on decisions and behaviour. If we can't identify a decision that could be affected by a proposed measurement and how it could change those decisions, then the measurement simply has no value"
— Douglas W. Hubbard

CDM Metrics Methodology

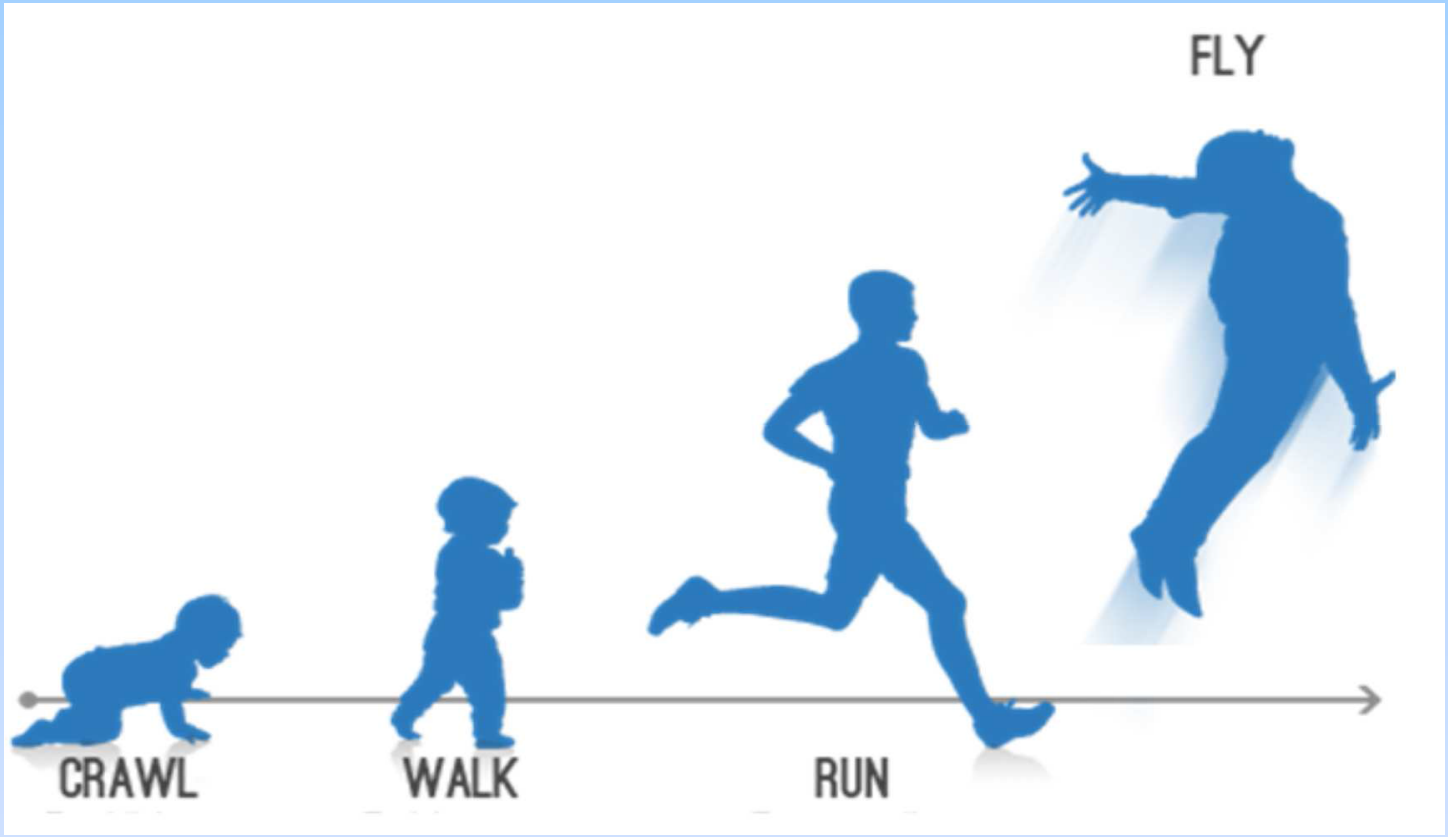


Homeland Security

6

Maturity Model Approach

- The objective of a Maturity Model is to allow any organization to show the extent of progress regardless of where they start



Homeland Security

Maturity Model Approach - CDM

1. Recognizes four “Levels” of maturity
2. Applied selectively, not “one size fits all” security, so organizations can implement CDM capabilities progressively over time and organizational structure
3. Measures within each maturity level show how much progress has been made

- For Phase II (capabilities 6-9 that focus on managing people and access) an association has been created with ICAM and their Lifecycle Maturity model

Homeland Security

CDM Maturity Levels

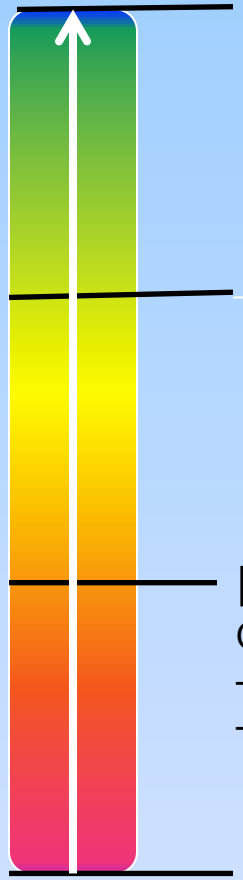
The norm is sufficiency; not perfection!
Why? The last few % improvement doubles the cost.

Risk : function of

Threat
[Probability (exploit)]

Impact
[Measure of criticality of resource]

Vulnerability
[Measure of defect intrinsic/base risk e.g. CVSS]



Risk Management (3)
Better balance of cost to impact reduction
- Acceptable impact defined by management
- Actual Impact estimated and in acceptable range

Capability (2)
Reduced Chance of Missing a Defect
- Increased coverage
- Increased Timeliness

Foundational (1)
Growing ability to perform all necessary tasks
- Cost/Effectiveness metrics
- Generally semi-automated

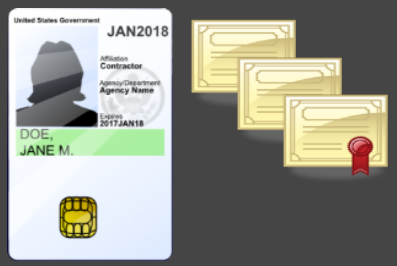
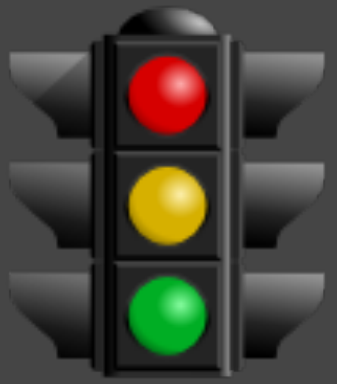
Base (0)

Homeland Security

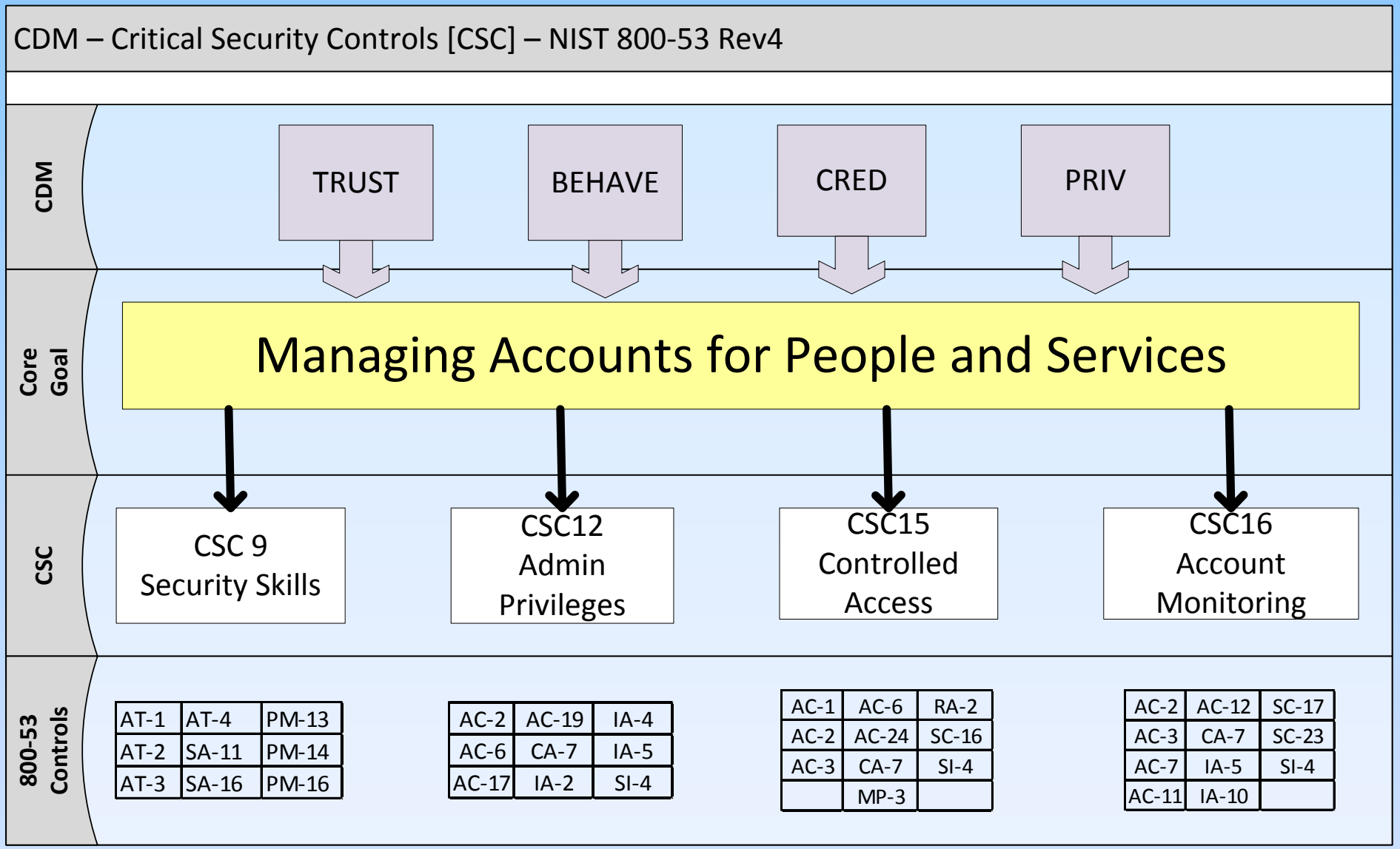
Maturity Model for ICAM Metrics

Homeland Security

Review of the Phase 2 Capabilities

TRUST	BEHAVE	CRED	PRIV
• People • Suitability • Clearance • Entry on Duty	• Training • Monitoring • Reporting	• Credential Type • Assurance Level • Account Linking	• Roles • Security Groups • Attributes
			

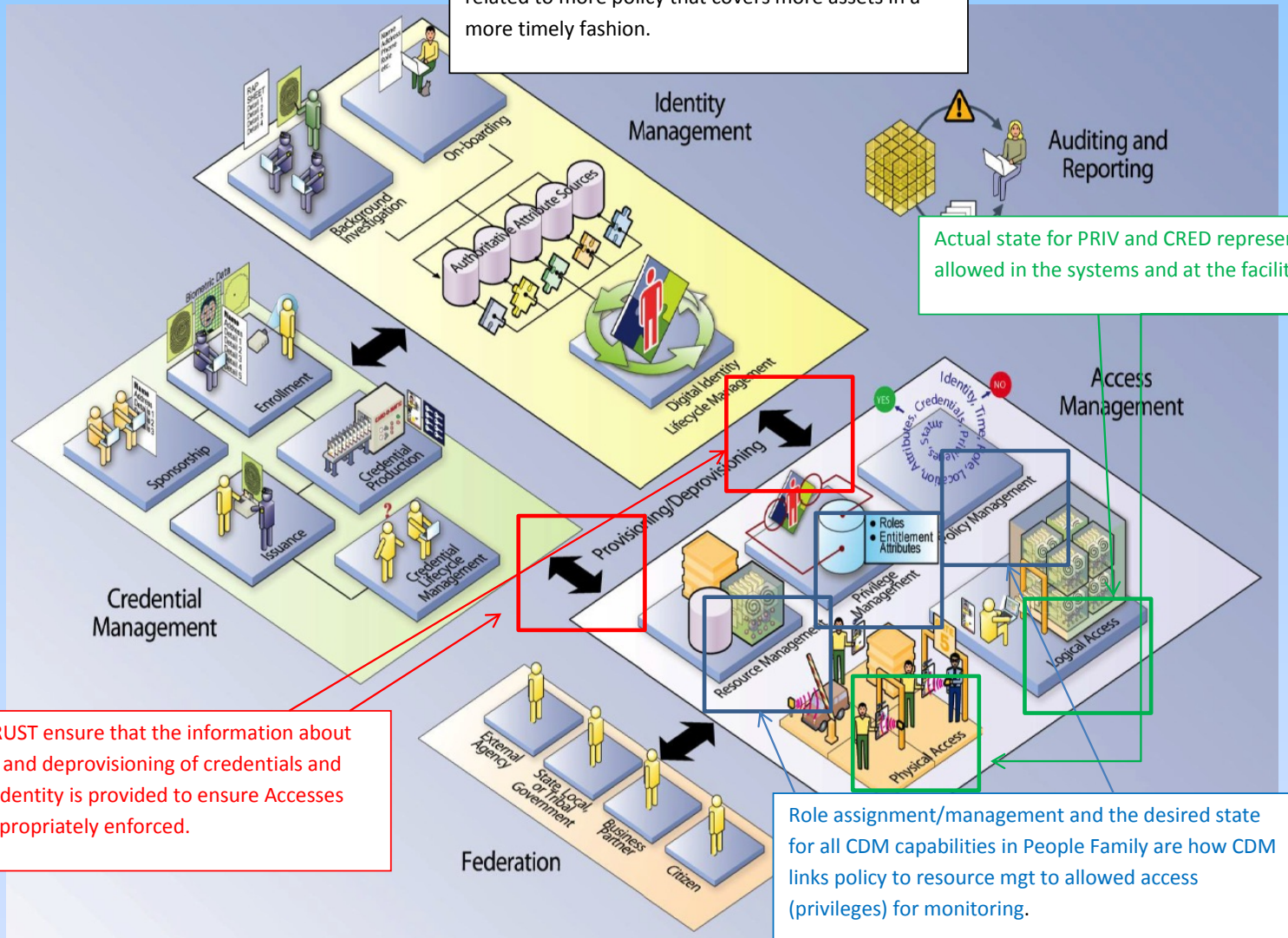
Homeland Security



Homeland Security

CDM OVERLAY

CDM provides a level of consistent auditing and reporting on FICAM implementation as compared to the policy. It also can show incremental improvement related to more policy that covers more assets in a more timely fashion.



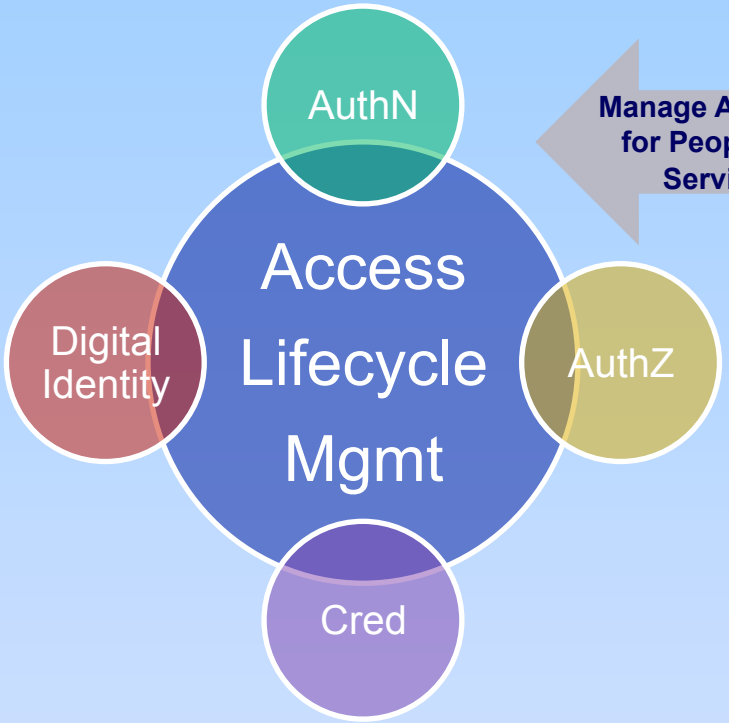
Actual state for PRIV and CRED represent the access allowed in the systems and at the facilities.

CRED and TRUST ensure that the information about provisioning and deprovisioning of credentials and vetting and identity is provided to ensure Accesses are being appropriately enforced.

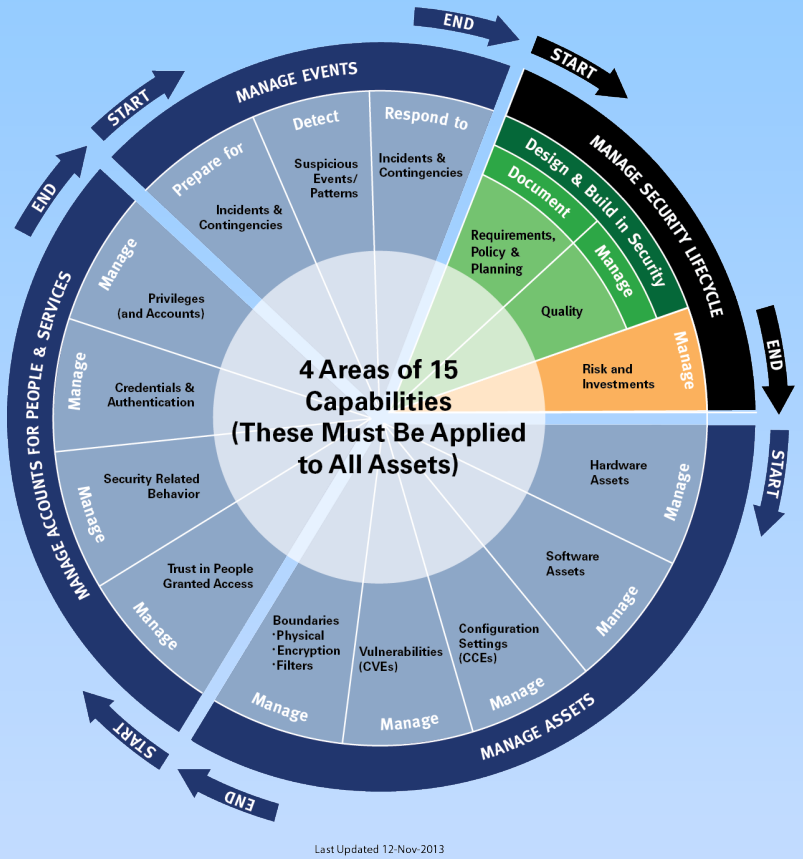
Role assignment/management and the desired state for all CDM capabilities in People Family are how CDM links policy to resource mgt to allowed access (privileges) for monitoring.

Homeland Security

Simplified ICAM Services Meets CDM Capabilities



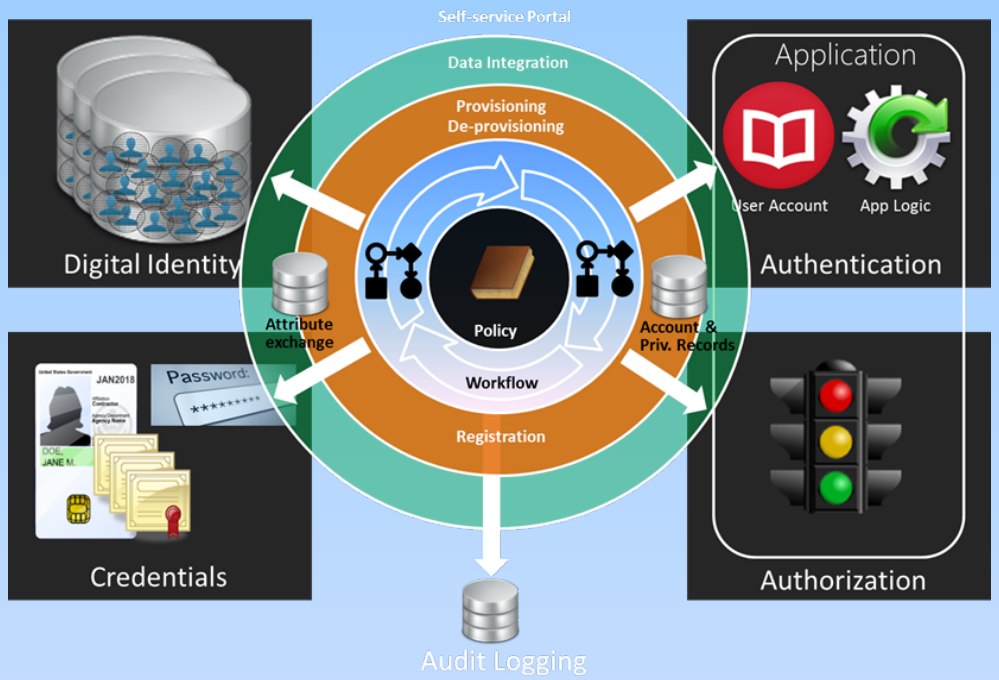
Manage Accounts for People and Services

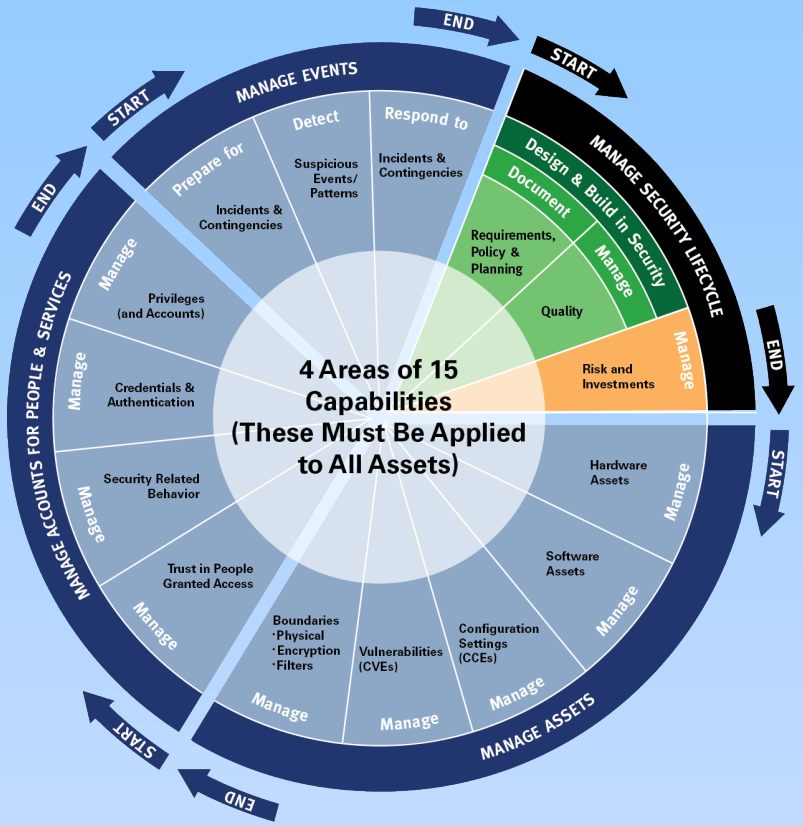


Last Updated 12-Nov-2013

Homeland Security

Simplified ICAM Services Meets CDM Capabilities

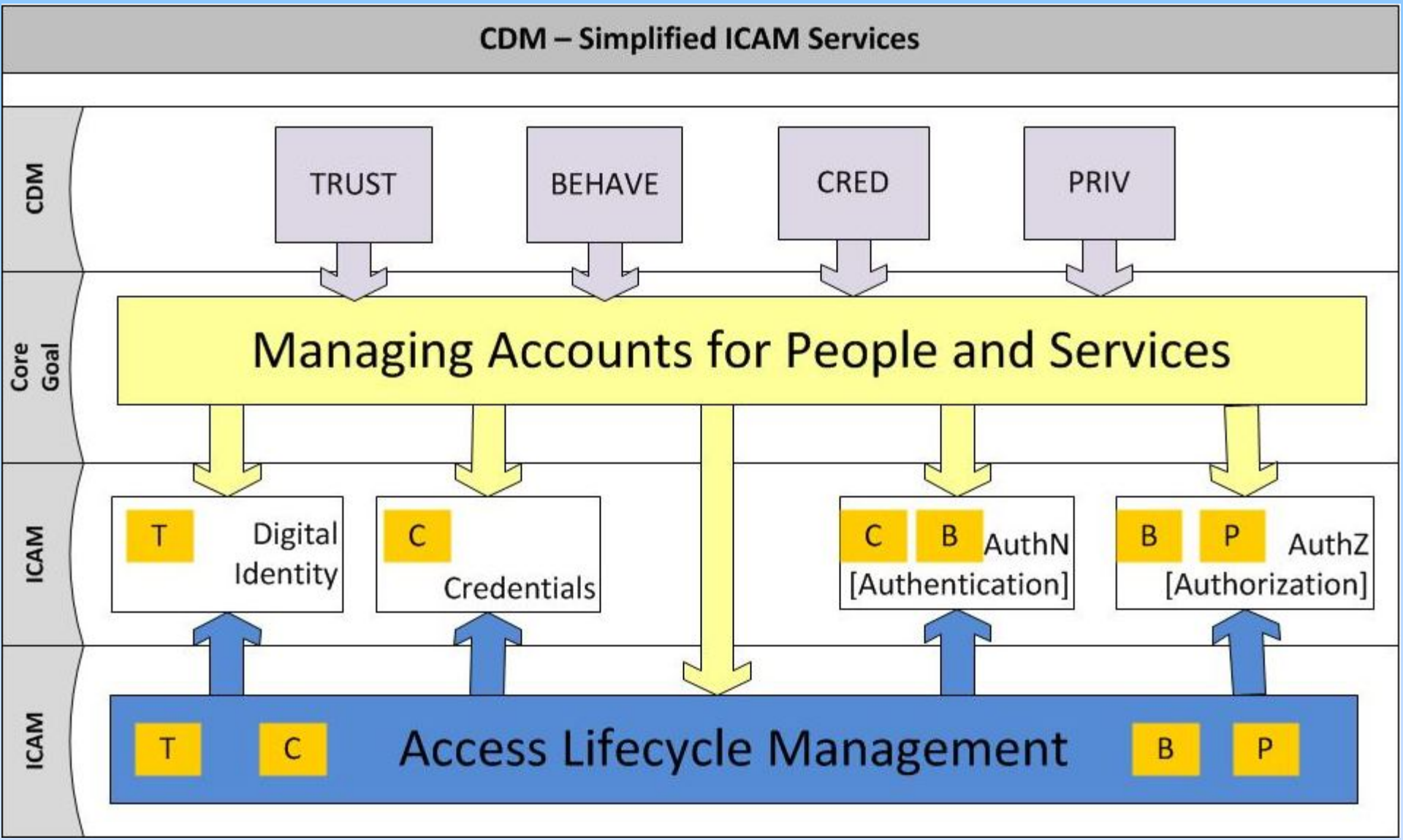




Last Updated 12-Nov-2013

Manage Accounts for People and Services

Homeland Security



Homeland Security

Homeland Security

Information on CMaaS BPA :	CDM@GSA.GOV
Queries on CDM Program:	CDM.FNR@HQ.DHS.GOV
My Contact:	Jim.Quinn@HQ.DHS.GOV