Designing and Building a Cybersecurity Program Based on NIST Cybersecurity Framework

Larry Wilson
lwilson@umassp.edu
June, 2019

Learning with Purpose

Cybersecurity Program Roles, Objectives, Deliverables

1. Role: Executive / Senior Management

Objectives: Design, Build, Maintain Secure and Resilient Digital Workspace

Deliverables: Cybersecurity Workforce, Cybersecurity Strategy, Cybersecurity Governance, Cybersecurity Policy

2. Role: Cybersecurity Risk Management

Objectives: Analyze and Manage Cyber Risk to Critical Assets

Deliverables: System Security Plan, Risk Assessment, Plan of Action and Milestones (POA&M), Executive Scorecard

3. Role: Cybersecurity Engineering / Design

Objectives: Engineer and Design Cybersecurity Solutions that protect our Critical Infrastructure from Cyber Threats

Deliverables: What's on the network, Who's on the network, How's the network protected?, What's happening on the network, How's the data protected?

4. Role: Cybersecurity Technology / Operations

Objectives: Build and Operate Cybersecurity Solutions that protect Critical Infrastructure from Cyber Threats

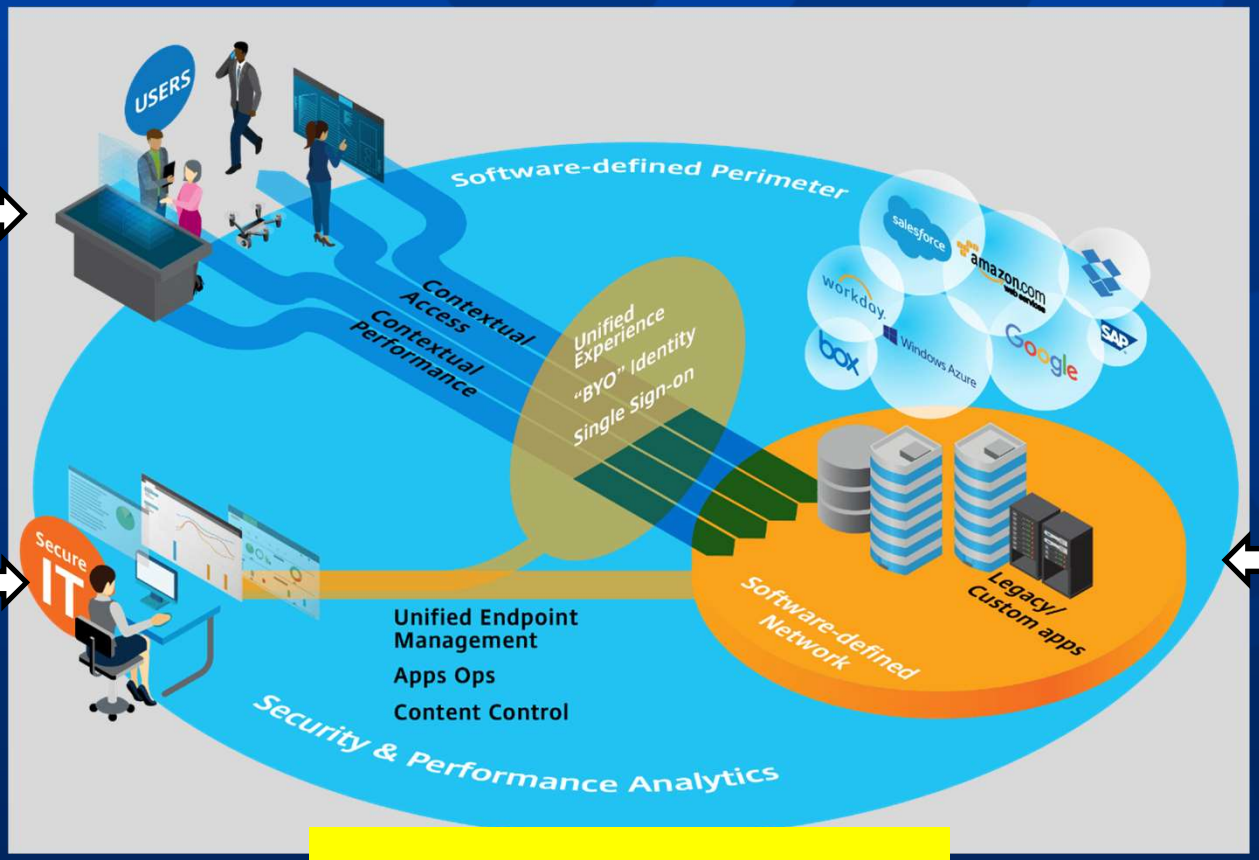
Deliverables: Basic Controls, Foundational Controls, Organizational Controls

Senior Management Roles /Objectives / Deliverables

Digitally Transforming our Aging Critical Infrastructure

Goal: Build a Secure and Resilient Digital Workspace

End User Access
[Devices, Apps, Data]



Digital Operations
[Workforce]

Digital Services
[Workloads]

Cybersecurity Requirements & Deliverables?

The digital workspace is a delivery and enablement approach that provides end users with contextually aware access to devices, applications, and data in a secure manner. It's a framework of technologies that together help unify traditional end user computing tools with the needs of an increasingly mobile workforce.

Key Benefits of a Digital Workspace

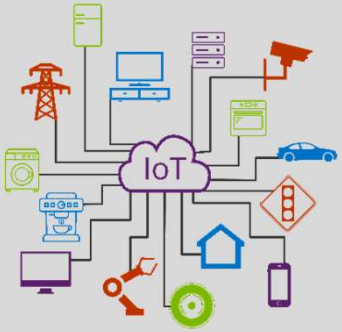
Leveraging digital technologies to create enhanced, customer centric business models

Digital transformation creates unique marketplace challenges and opportunities, as organizations must contend with competitors who take advantage of the low barrier to entry that technology provides

Digital Transformation: Areas of Growth

Growth in Information

Growth in Devices



Growth in Software

Growth in Cloud

Growth in Outsourcing

Growth in Threats

Learning with Purpose

UMASS LOWELL

Digital Transformation: Key Components

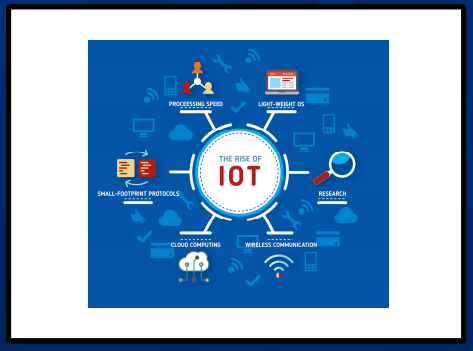
The six core technology trends that make Digital Transformation possible

Social Media: Websites and applications enable users to create and share content.

Mobile Devices: Transform how people interact, consume information, work.

Big Data: Analyze large datasets to reveal patterns, trends, associations.

Cloud Computing: A network of remote servers hosted on the Internet to store, manage, and process data .



Internet of Things: The interconnection via the Internet of computing devices embedded in everyday objects.

Cybersecurity: Technologies & practices that protect networks, computers, data from attack or unauthorized access.

Source: Digital Transformation Strategy Template and Training – ex Deloitte and McKinsey Consultants
https://www.slideshare.net/BySlidebooks/digital-transformation-strategy-template-and-training

Deliverable 1: Cybersecurity Strategy

That enables Digital Transformation

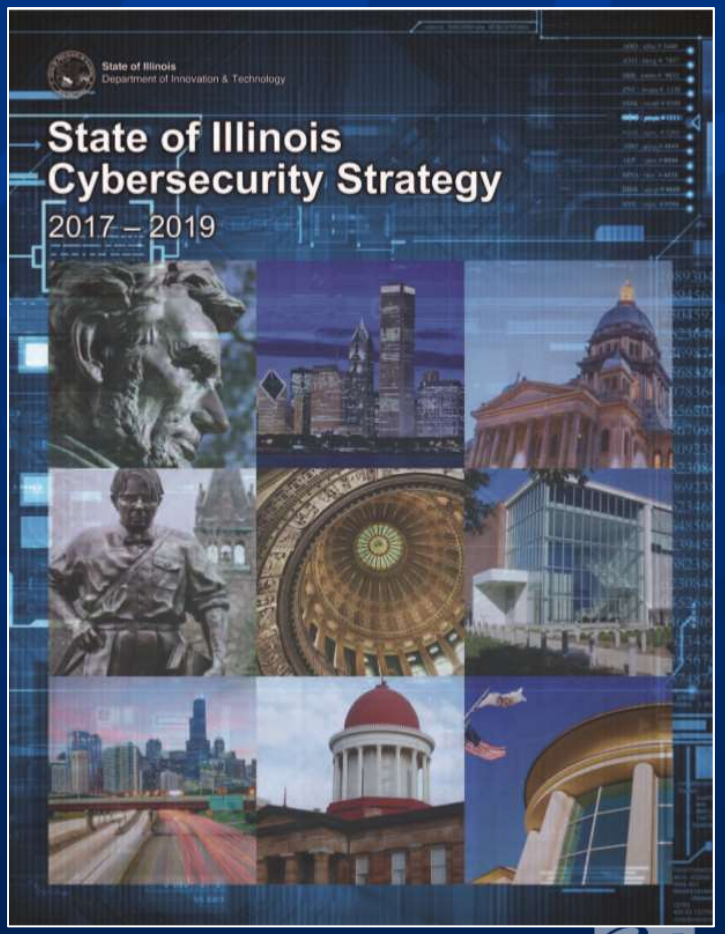
Goal 1: Protect State of Illinois Information & Systems
Focus on protecting the confidentiality, integrity, availability and cyber-resiliency of State of Illinois information and critical information systems.

Goal 2: Reduce Cyber Risk
Create the culture, frameworks and processes required to address cyber-risk, enhance decision making and better protect the state through continual risk awareness.

Goal 3: Best-in-Class Cybersecurity Capabilities
Develop the practices, processes, workforce and overall cybersecurity capabilities required to protect the state from the cyber-threats while ensuring the alignment of security priorities with the business needs and strategies of the state.

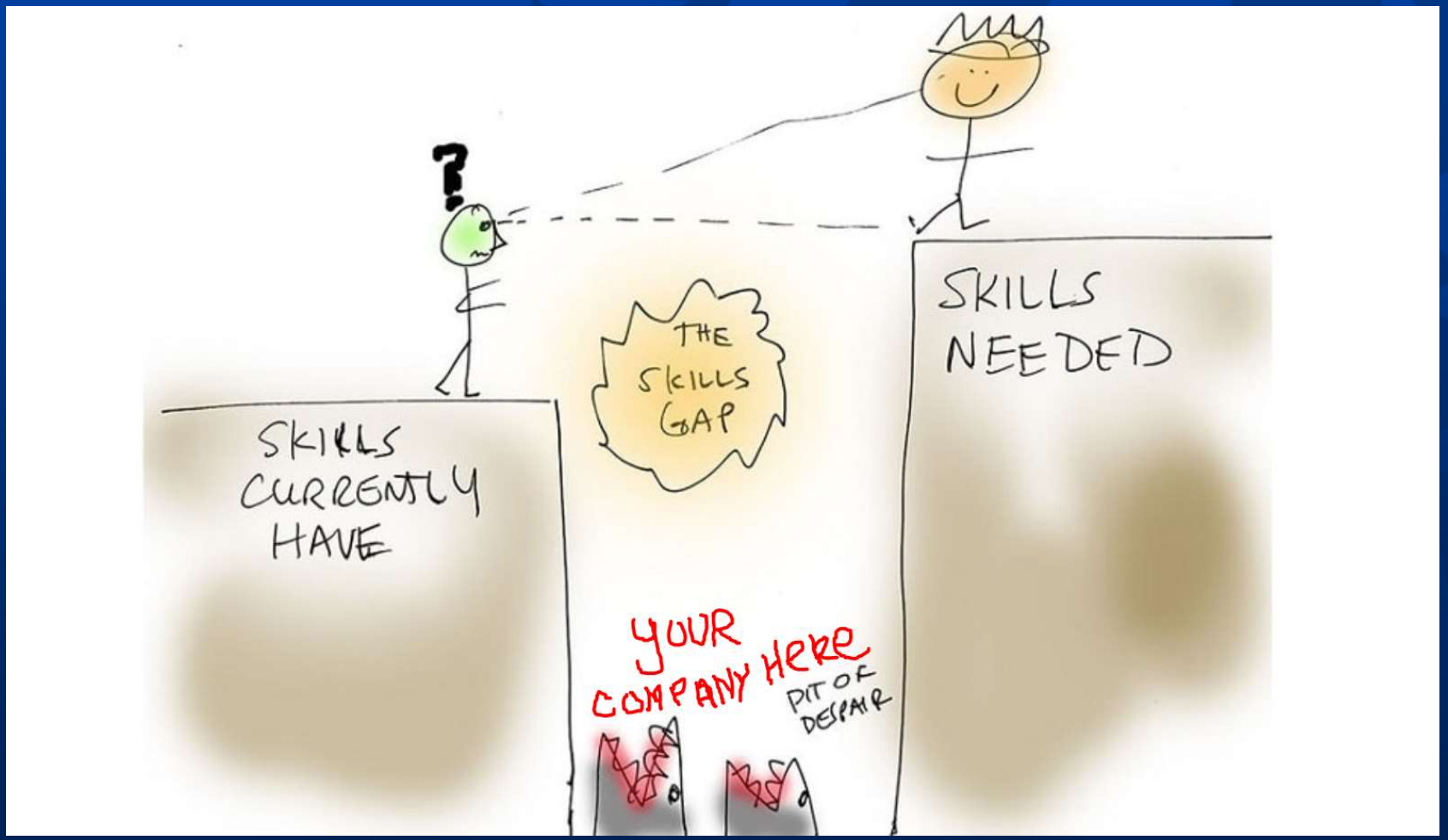
Goal 4: Enterprise Approach to Cybersecurity
Enhance cybersecurity through the establishment of an enterprise-level cybersecurity program, and the adoption of best-practices, common frameworks, and enterprise information security policies.

Goal 5: A Cyber-Secure Illinois
Enhance the cybersecurity of the state as a whole through partnerships with both the public and private sector.



Deliverable 2: Cybersecurity Workforce

Cyberattacks are growing , but the talent pool of defenders is not keeping pace



Deliverable 3: Cybersecurity Governance

Cybersecurity Roles

1. Executive Management
- Role: 1st Line of Defense
- Understand: Cybersecurity Impact on Digital Transformation
- Responsible for: Cybersecurity Leadership & Approach
- Deliverables: Workforce, Strategy, Policy, Governance

2. Risk Management
- Role: 2nd Line of Defense
- Understand: NIST Risk Management Framework, NIST Cybersecurity Framework
- Responsible for: Cybersecurity Risk Management Program
- Deliverables: System Security Plan, Risk Assessment, POA&M, Executive Report

3. Engineering Management
- Role: 3rd Line of Defense
- Understand: Assets & Identities, Threats & Vulnerabilities, Risks & Controls
- Responsible for: Cybersecurity Engineering and Design
- Deliverables: What's on the Network?, Who's on the Network? How is the Network Protected? What's Happening on the Network?, How is Data Protected?

4. Operations Management
- Role: 4th Line of Defense
- Understand: Engineering, Technical, Business Requirements
- Responsible for: Secure and Resilient Networks and Systems
- Deliverables: Basic Security Controls, Foundational Security Controls, Organizational Security Controls

Cybersecurity Responsibilities

Cybersecurity Leadership

Risk Management Program

Engineering Program

Technology / Operations Program

Deliverable 4: Cybersecurity Policy

Goal 1: Demonstrate Executive Commitment
Security-first mindset starts at the top through the commitment of decision-makers and the attitudes of employees. An information security policy guides the company, it's employees and business partners on how to process and store information securely.

Goal 2: Align Cybersecurity Skills with Organizational Needs
Cybersecurity training is needed across all levels of the organization. Technology alone cannot prevent cyber-attacks, and industry leaders understand the importance of staff skills as part of their broader security operation.

Goal 3: Promote User Best Practices
No matter how strong a company's cyber-security technology, employees still manage to introduce threats by falling prey to phishing scams, giving away passwords and posting sensitive information on social media. To limit potential attacks and mitigate losses, every cyber-security policy should clearly communicate user best practices.

Goal 4: Establish Cybersecurity Program Governance
Establish governance team that will effectively manage cyber risk in concert with your business objectives. Today's CISOs must exhibit security expertise, corporate governance and risk management while maintaining business objectives.

Goal 5: Improve Organizational Awareness
Cybersecurity policies promote awareness among employees, which leads to better preparation for cyber-threats, and decrease the likelihood that an organization will suffer a security breach.

Senior Management Deliverables

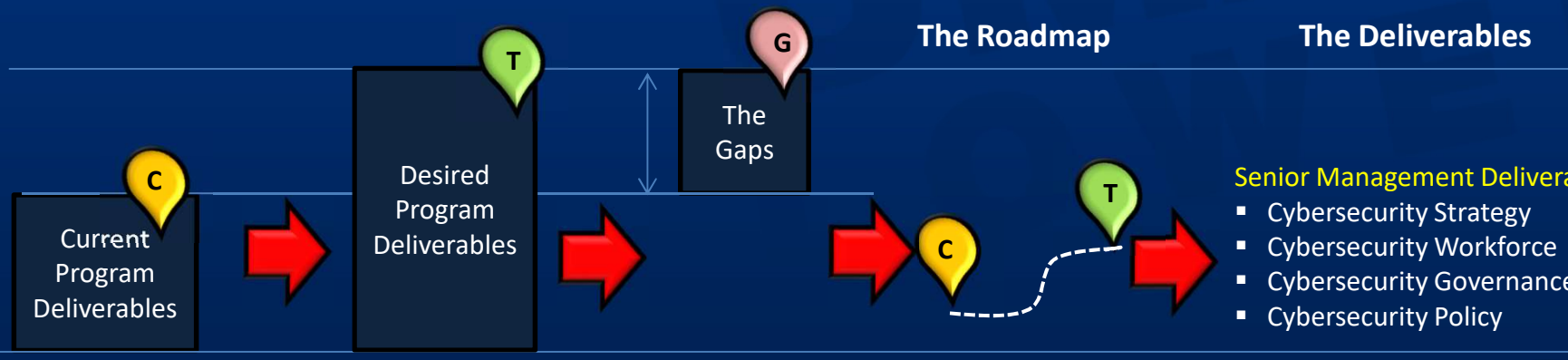
The Assessment → **Where are we now?**

The Strategy → **Where do we want to be?**

The Gap Analysis → **What are our Gaps?**

The Plan of Action → **How do we get there?**

The Results → **How do we know our impact?**



Senior Management Deliverables

Cybersecurity Strategy

1. The Cybersecurity Strategy goal is to identify significant cybersecurity challenges that impact the business and commit to establishing and maintaining a cyber-secure enterprise.

Cybersecurity Workforce

2. For most organizations, talent is the single biggest overhead expense and the biggest competitive advantage, so optimizing talent strategy is critical.

Cybersecurity Governance

3. Without an information security strategy and governance framework to implement it, an organization will continue to implement ad hoc tactical point solutions rather than a meaningful and integrated plan of action.

Cybersecurity Policy

4. The Information Security Policy is designed to protect assets and interests of the organization, increase awareness and ensure a coordinated approach for maintaining a control environment based on industry best practices.

Cybersecurity Program Roles & Deliverables

Cybersecurity Roles & Responsibilities

Senior Management

Cybersecurity Program Deliverables

1. Senior Management Deliverables

- Cybersecurity Strategy
- Cybersecurity Workforce
- Cybersecurity Governance
- Cybersecurity Policy

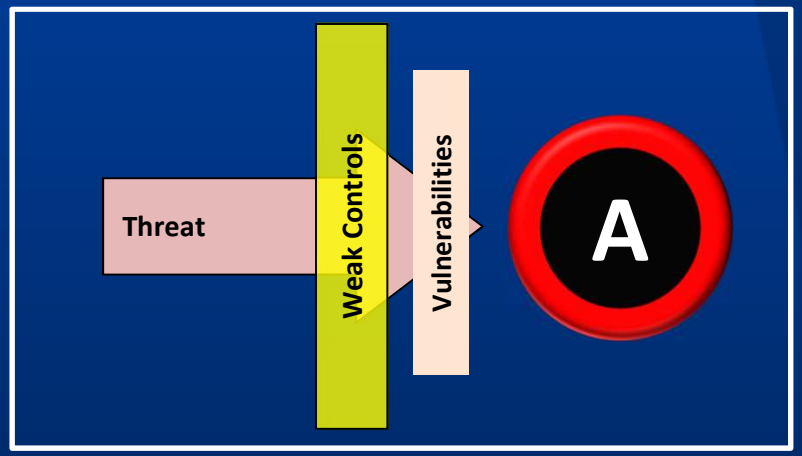
Cybersecurity Program Results

Documents

Cyber Risk Management Objectives / Deliverables

What problem are we trying to solve?

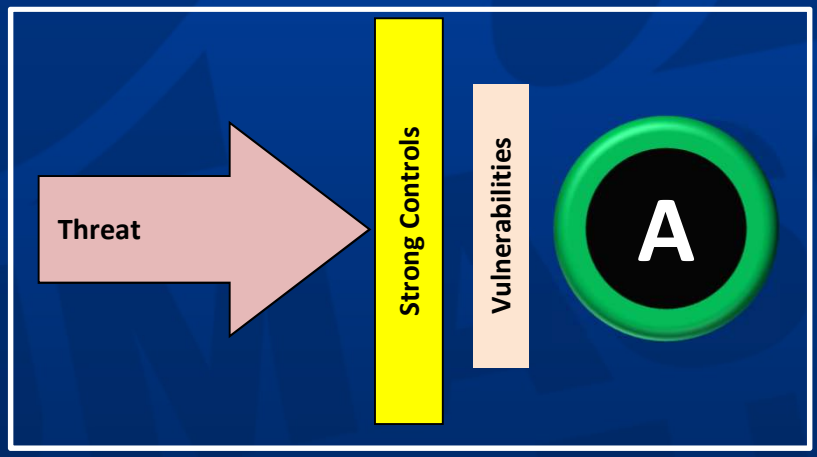
Unmanaged Assets: Weak security controls



Unmanaged Assets = High Risk

This means a higher opportunity or higher likelihood of a compromise or unintended outcome

Managed Assets: Strong security controls



Managed Assets = Low Risk

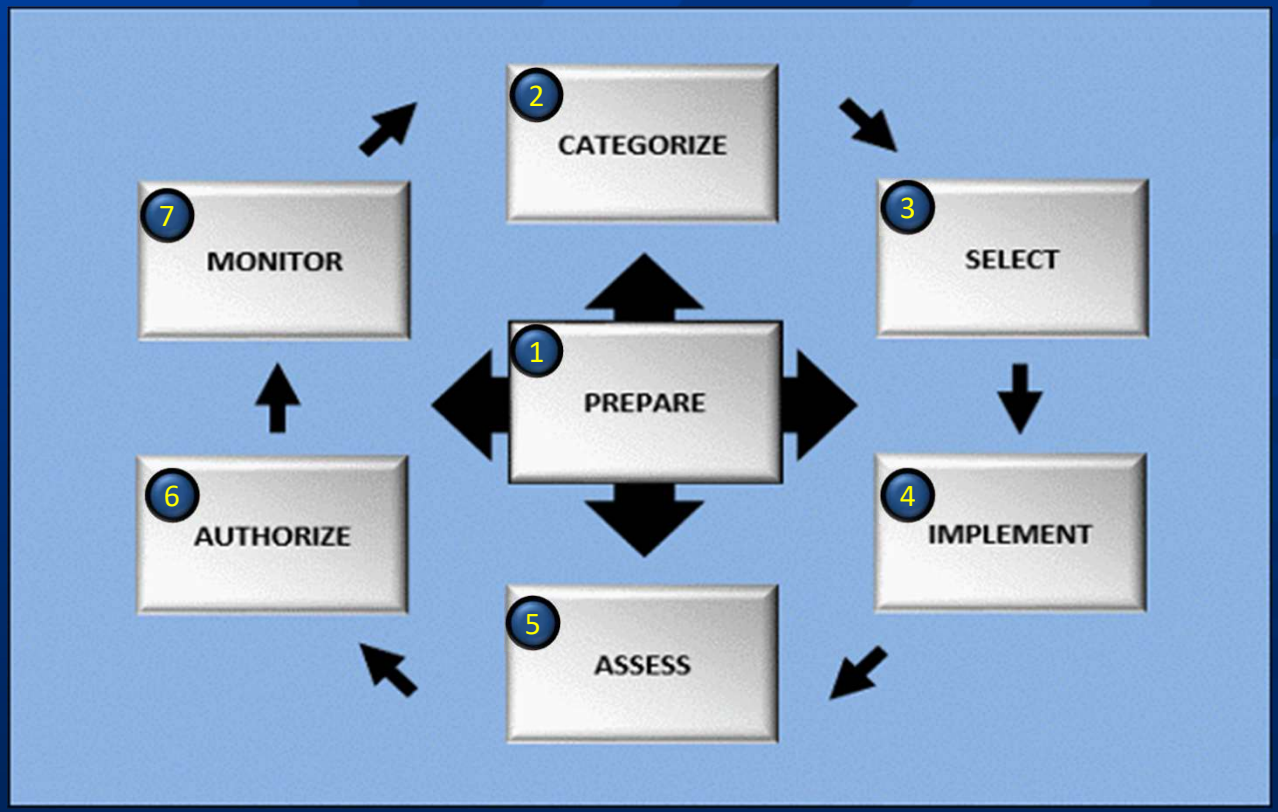
This means a lower opportunity or lower likelihood of a compromise or unintended outcome

Learning with Purpose

UMASS LOWELL

NIST 800-37r2 Risk Management Framework

RMF Steps and Structure



RMF Steps and Structure

All seven steps are essential for the successful execution of the RMF.

1) **Prepare** to execute the RMF from an organization and a system-level perspective by establishing a context and priorities for managing security and privacy risk.

2) **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.

3) **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

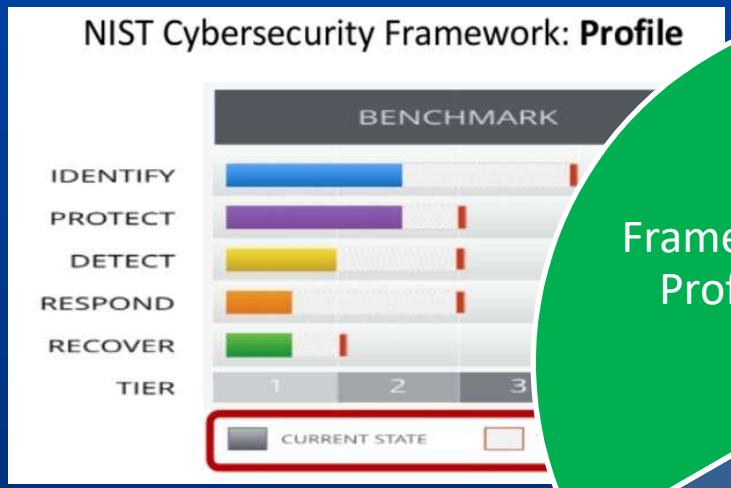
4) **Implement** the controls and describe how the controls are employed within the system and its environment of operation.

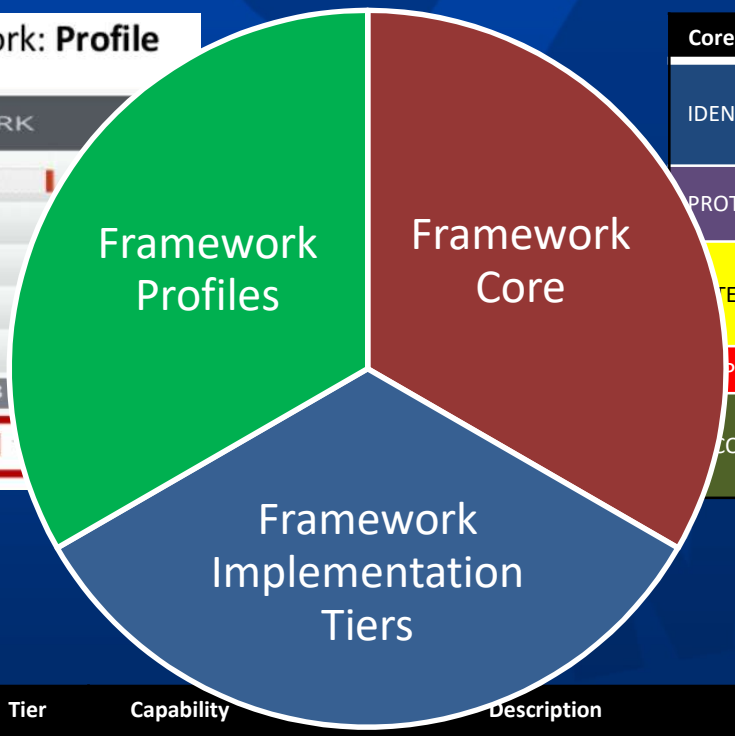
5) **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

6) **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.

7) **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

The NIST Cybersecurity Framework





Core Function	Definitions
IDENTIFY (ID)	An understanding of how to manage cybersecurity risks to systems, assets, data and capabilities
PROTECT (PR)	The controls and safeguards necessary to prevent or defer cybersecurity threats
TECT (DE)	Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events
POND (RS)	Incident response activities
COVER (RC)	Business continuity plans to maintain resilience and recover capabilities after a cyber breach

Tier	Capability	Description
Tier 1	Partial	Risk management is ad-hoc.
Tier 2	Risk Informed	Risk management processes and programs are in place but not integrated enterprise-wide.
Tier 3	Repeatable	Formal policies for risk management processes and programs are in place enterprise-wide.
Tier 4	Adaptive	Risk management processes and programs are based on lessons learned and imbedded in culture.

Learning with Purpose

UMASS LOWELL

The Framework Core Functions / categories

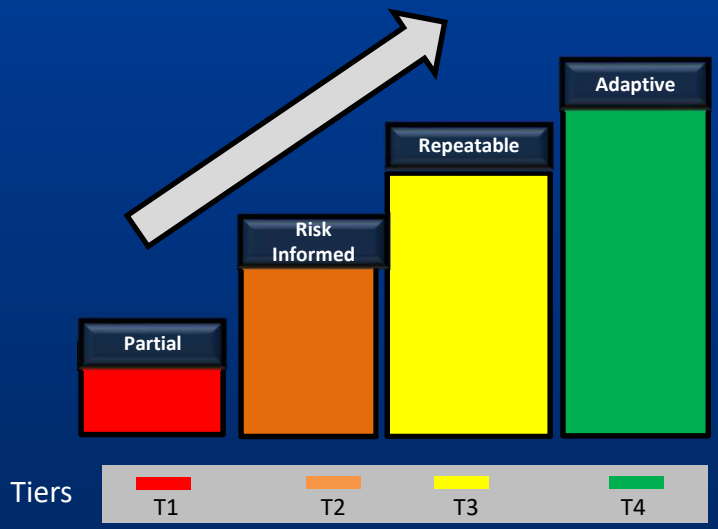
What assets need protection?	What safeguards are available?	What techniques identify incidents?	What techniques contain impact?	What techniques restore capabilities?

NIST Cybersecurity Framework (CSF)

Identify	Protect	Detect	Respond	Recover
Asset Management (ID.AM)	Identity Management and Access Control (PR.AC)	Anomalies and Events (DE.AE)	Response Planning (RS.RP)	Recovery Planning (RC.RP)
Business Environment (ID.BE)	Awareness and Training (PR.AT)	Security Continuous Monitoring (DE.CM)	Communications (RS.CO)	Improvements (RC.IM)
Governance (ID.GV)	Data Security (PR.DS)	Detection Processes (DE.DP)	Analysis (RS.AN)	Communications (RC.CO)
Risk Assessment (ID.RA)	Information Protection Processes and Procedures (PR.IP)		Mitigation (RS.MI)	
Risk Management Strategy (ID.RM)	Maintenance (PR.MA)		Improvements (RS.IM)	
Supply Chain Risk Management (ID.SC)	Protective Technology (PR.PT)			

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

NIST Framework Implementation Tiers



Tier 1 - Partial: Organizations operating at Tier 1 typically swarm to cybersecurity incidents in an ad hoc manner.

Tier 2 - Risk Informed: Management within the organization approves risk management decisions.

Tier 3 - Repeatable: Management within the organizations has formally approved cybersecurity policy and procedures.

Tier 4 - Adaptive: Organizations update their formalized cybersecurity policy and procedures on an ongoing basis based on lessons learned and predictive threat indicators.

Learning with Purpose

UMASS LOWELL

NIST Framework Profiles

Desired state of alignment between core elements and organizational requirements, risk tolerance, & resources

Current state of alignment between core elements, organizational requirements, risk tolerance, & resources

How to Use the Framework

A systematic process for identifying, assessing, and managing cybersecurity risk.

Using the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program.

The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices.

It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The Framework can be applied throughout the life cycle phases of plan, design, build/buy, deploy, operate, and decommission.

Managing Cybersecurity Risk

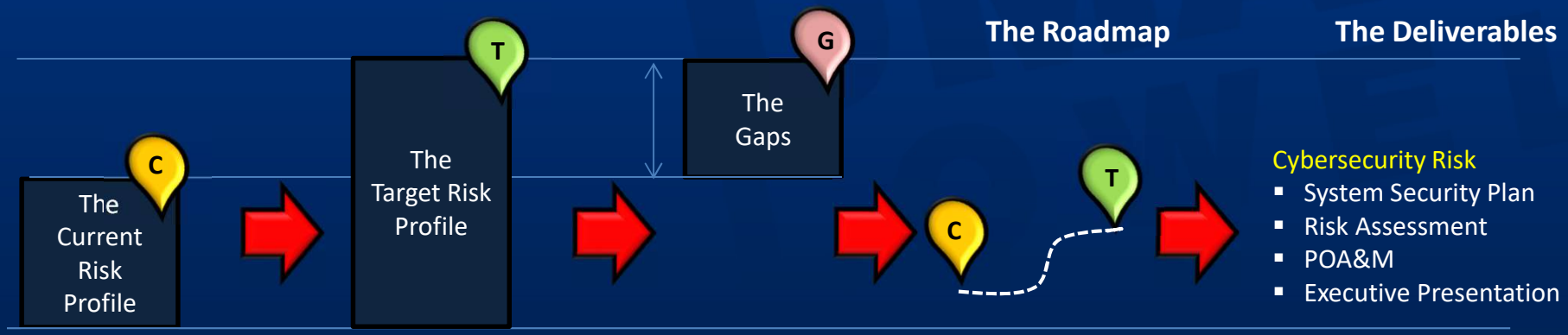
The Assessment — **Where are we now?**

The Strategy — **Where do we want to be?**

The Gap Analysis — **What are our Gaps?**

The Plan of Action — **How do we get there?**

The Results — **How do we know our impact?**



Learning with Purpose

UMASS LOWELL

Risk Management Deliverables

System Security Plan (SSP)

1. The SSP should adequately describe your organization's security requirements.

Cybersecurity Risk Assessment

2. Evaluate the security controls documented in the SSP to determine the extent to which the controls are implemented, operating as intended, and producing desired outcome.

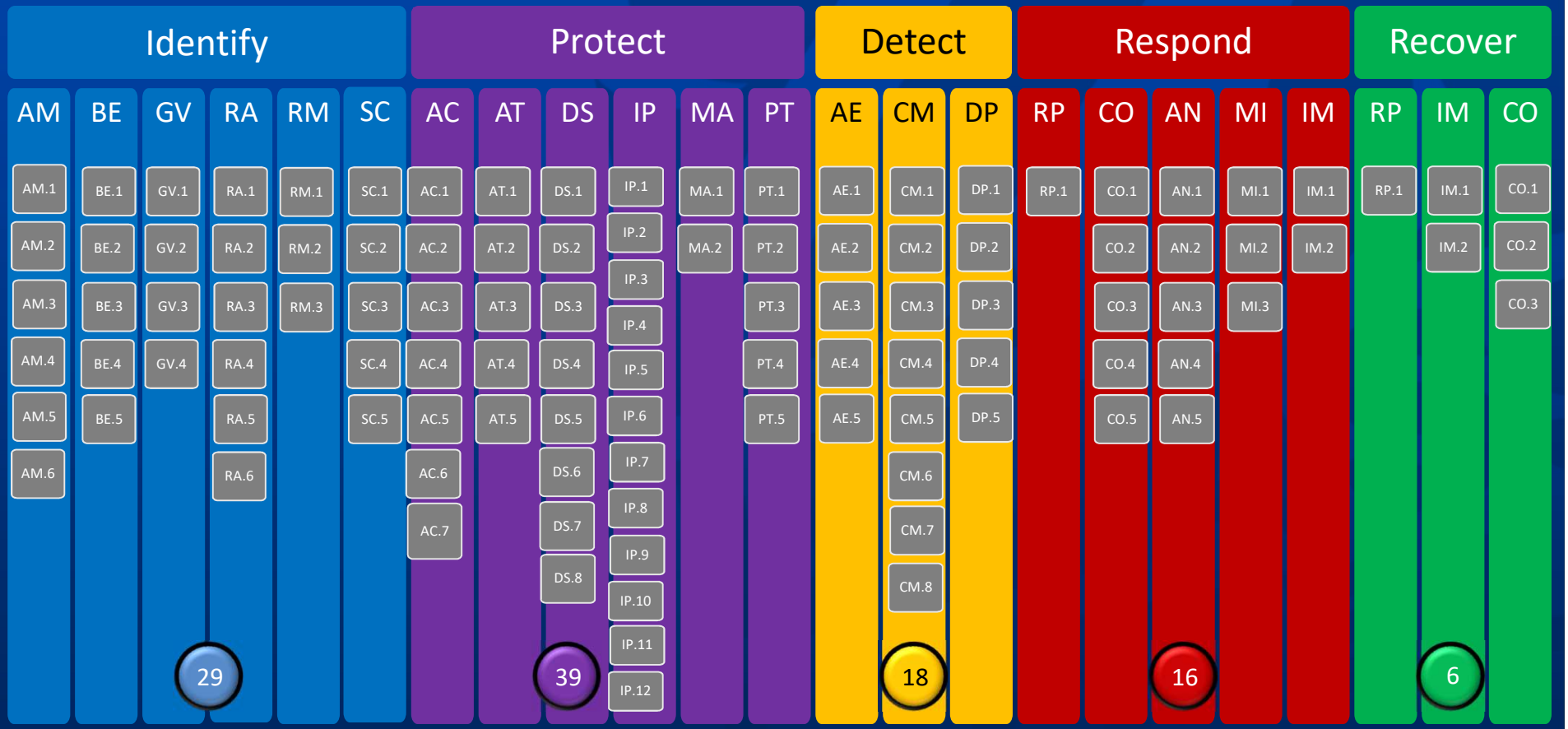
Plan of Action & Milestones (POA&M)

3. A specific, measurable, achievable, relevant, and time-bound plan to mitigate security gaps identified in the Risk Assessment.

Executive Scorecard

4. Provides a review and action plan that includes the target state profile, the current state profile, gap analysis, POA&M and overall cybersecurity maturity.

NIST Cybersecurity Framework



NIST Cybersecurity Framework (NCSF)

Identify	Protect	Detect	Respond	Recover
AM: Asset Management	AC: Access Control	AE: Anomalies and Events	RP: Response Planning	RP: Recovery Planning
BE: Business Environment	AT: Awareness and Training	CM: Security Continuous Monitoring	CO: Communications	IM: Improvements
GV: Governance	DS: Data Security	DP: Detection Processes	AN: Analysis	CO: Communications
RA: Risk Assessment	IP: Information Protection Procedures		MI: Mitigation	
RM: Risk Management	MA: Maintenance		IM: Improvements	
SC: Supply Chain	PT: Protective Technology			

Cybersecurity Program Roles & Deliverables

Cybersecurity Roles & Responsibilities

Cybersecurity Program Deliverables

Cybersecurity Program Results

Senior Management

Risk Management

1. Senior Management Deliverables

- Cybersecurity Strategy
- Cybersecurity Workforce
- Cybersecurity Governance
- Cybersecurity Policy

2. Risk Management Deliverables

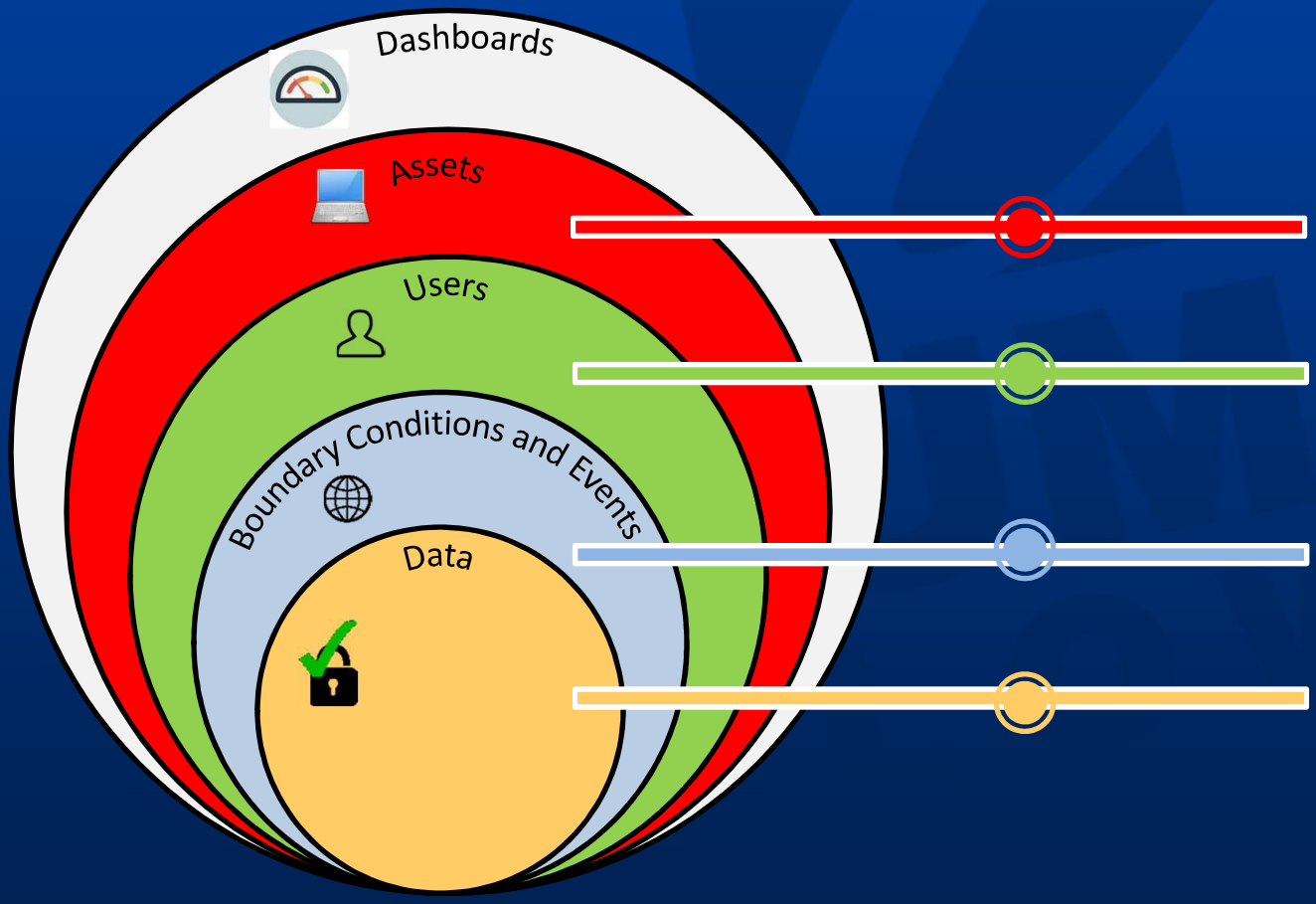
- System Security Plan (SSP)
- Cyber Risk Assessment
- Plan of Action & Milestones (POA&M)
- Executive Report

Documents

Documents

Cyber Engineering Objectives / Deliverables

Continuous Diagnostics & Mitigation (CDM) Program Focus Areas



Phase 1
What's on the Network?

Phase 2
Who's on the Network?

Phase 3
What's happening on the Network?

Phase 4
How is data protected?

CDM Program Areas of Focus

DHS set the CDM program up to be implemented in three distinct phases

1. **Endpoint integrity:** The scope is the local computing environment, with focus on identifying and managing hardware and software assets, listing known vulnerabilities and malware, and device configuration management.

2. **Least privilege and infrastructure integrity:** This is focused on people in the environment, and being able to manage their account and network privileges, managing the configuration of network infrastructure devices and services.

3. **Boundary protection and event management:** This includes event detection and response, encryption, remote access management and access control, and ensures security is built into networks rather than added on as an after-thought.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Phase Details

Phase 1: "What's on the network?"
Managing "what's on the network?" requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).

Phase 2: "Who's on the network?"
Managing "who's on the network?" requires the management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE). These four functions have significant interdependence and are thus managed together as part of Phase 2.

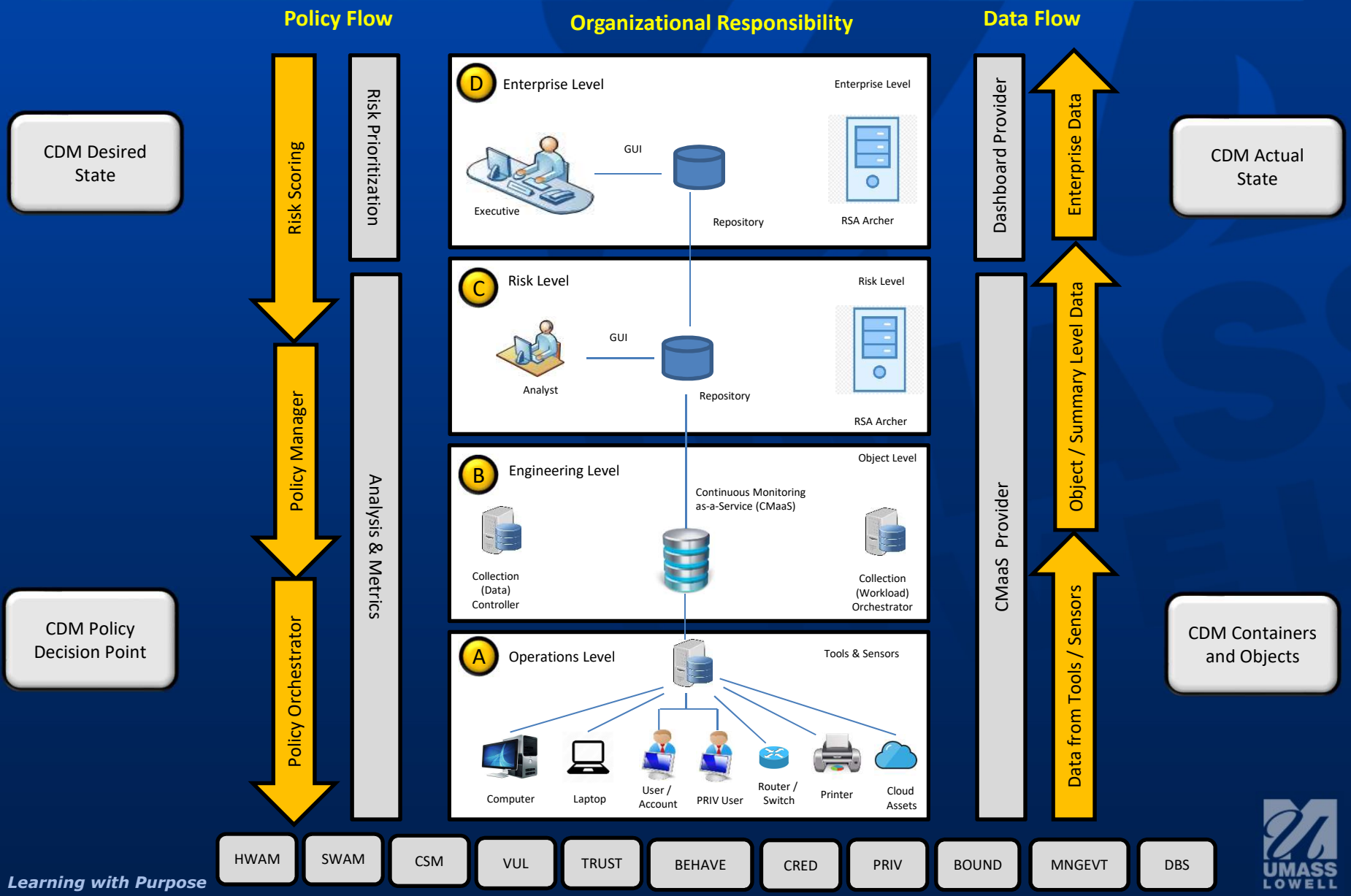
Phase 3: "What's happening on the network?"
Managing "what's happening on the network?" builds on the CDM capabilities provided by "what's on the network?" and "who's on the network?" These CDM capabilities include network and perimeter components, host, and device components, data at rest and in transit, and user behavior and activities. These capabilities move beyond asset management to more extensive and dynamic monitoring of security controls. This includes preparing for and responding to behavior incidents, ensuring that software/system quality is integrated into the network/infrastructure, detecting internal actions and behaviors to determine who is doing what, and finally, mitigating security incidents to prevent propagation throughout the network/infrastructure.

Phase 4: "How is data protected?"
CDM Phase 4 capabilities support the overall CDM Program goal to identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

The 20 CDM Functional Requirements

No.	Program Phase	Focus Area	Functional Requirements
1	Phase 1	What's on the Network?	Hardware Asset Management (HWAM)
2	Phase 1	What's on the Network?	Software Asset Management (SWAM)
3	Phase 1	What's on the Network?	Configuration Settings Management (CSM)
4	Phase 1	What's on the Network?	Vulnerability Management (VUL)
5	Phase 2	Who's on the Network?	Manage Trust in People Granted Access (TRUST)
6	Phase 2	Who's on the Network?	Manage Security Related Behavior (BEHAVE)
7	Phase 2	Who's on the Network?	Manage Credentials and Authentication (CRED)
8	Phase 2	Who's on the Network?	Manage Account Access and Privileges (PRIV)
9	Phase 3	How's the Network Protected?	Manage Network Access Controls (BOUND)
10	Phase 3	What's Happening on the Network?	Prepare for Contingencies and Events (MNGEVT)
11	Phase 3	What's Happening on the Network?	Respond to Contingencies and Events (MNGEVT)
12	Phase 3	What's Happening on the Network?	Design and Build in Requirements Policy and Planning (DBS)
13	Phase 3	What's Happening on the Network?	Design and Build in Quality (DBS)
14	Phase 3	What's Happening on the Network?	Manage Audit Information (OMI)
15	Phase 3	What's Happening on the Network?	Manage Operations Security (OMI)
16	Phase 4	How is Data Protected?	Data Discovery / Classification (DATA_DISCOV)
17	Phase 4	How is Data Protected?	Data Protection Techniques (DATA_PROT)
18	Phase 4	How is Data Protected?	Data Loss Prevention (DATA_DLP)
19	Phase 4	How is Data Protected?	Data Breach / Spillage Mitigation (DATA_SPIL)
20	Phase 4	How is Data Protected?	Information Rights Management (DATA_IRM)

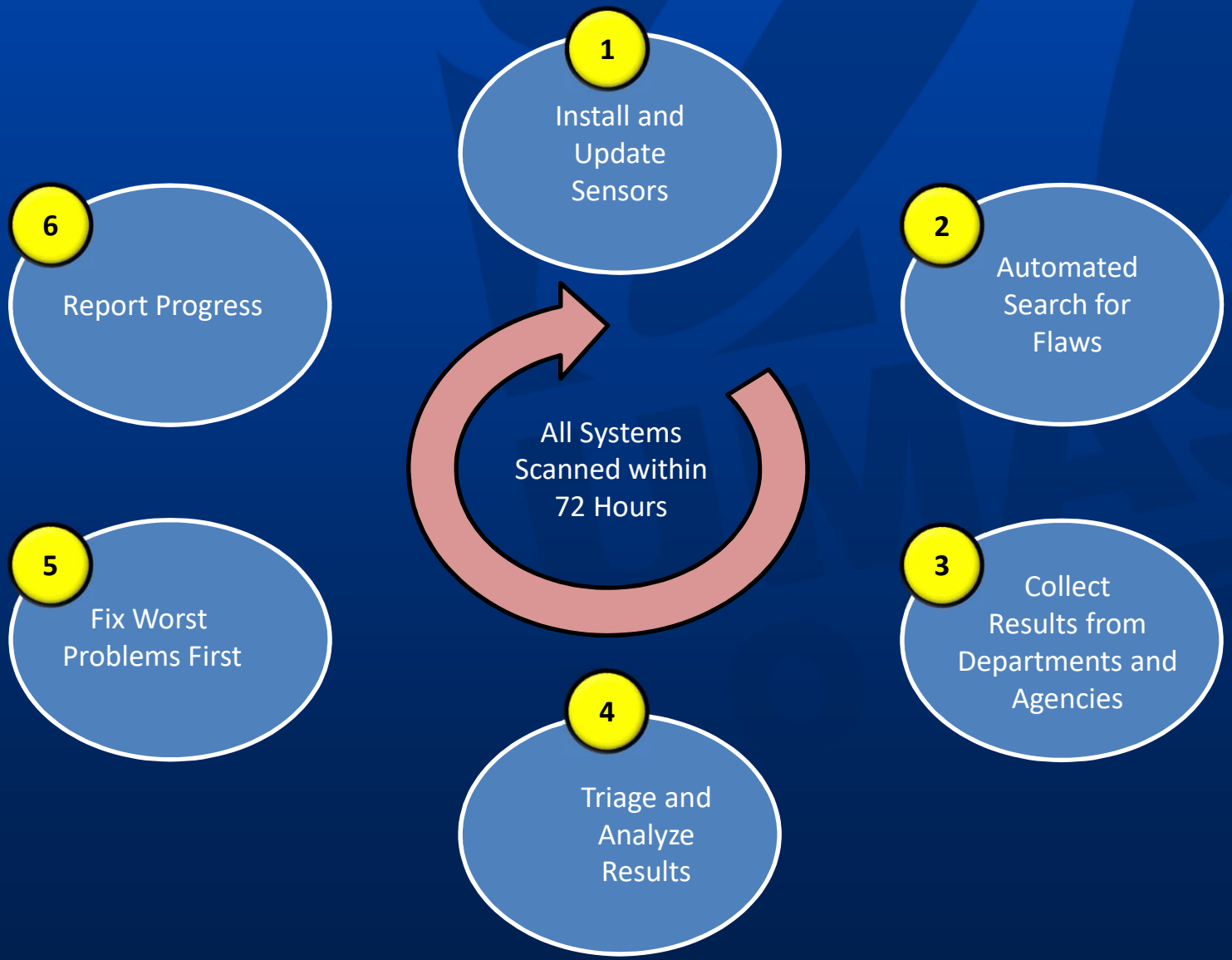
CDM Conceptual Architecture



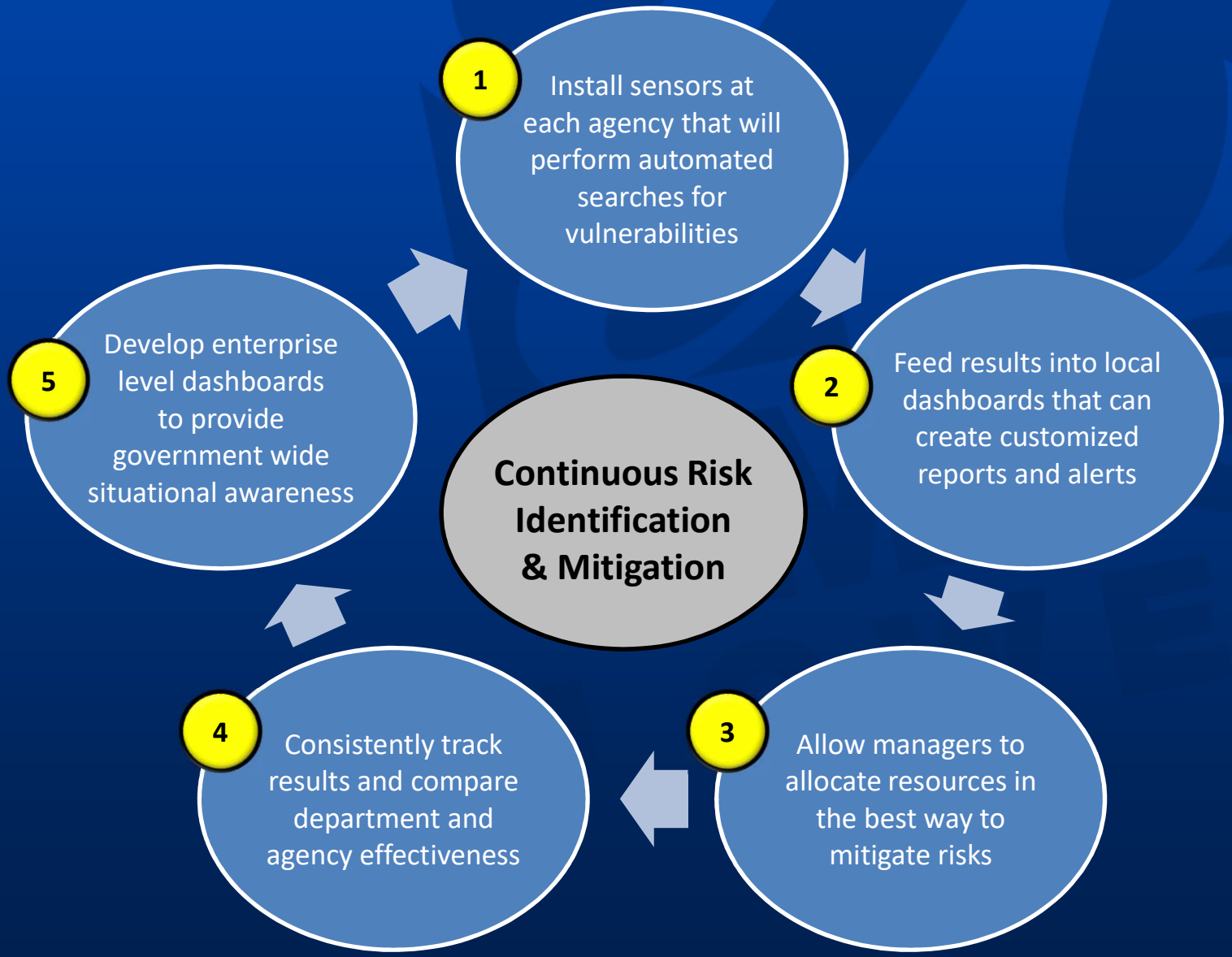
Learning with Purpose

UMASS LOWELL

The CDM Six Step Process

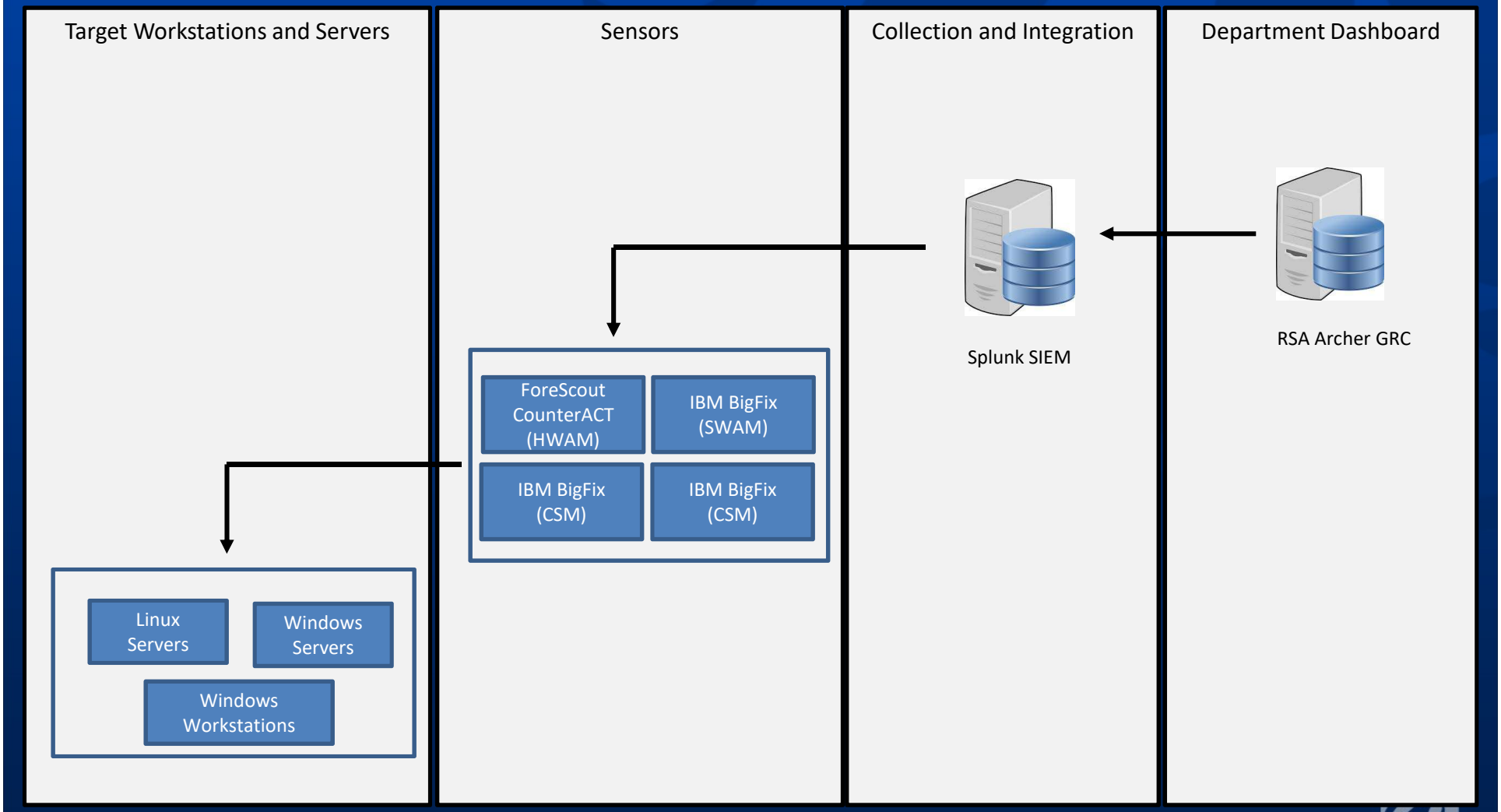


The CDM End Goal



CDM Sample Implementation

Tools and Data Flow



CDM Functional Areas

What's on the Network?

1. HARDWARE ASSET MANAGEMENT (HWAM)

The Hardware Asset Management (HWAM) Function is to discover unauthorized or unmanaged hardware on a network. Once unauthorized or unmanaged hardware is discovered, the organization will take action to remove this hardware. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.

2. SOFTWARE ASSET MANAGEMENT (SWAM)

The Software Asset Management (SWAM) Function is to discover unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network. Once unauthorized or unmanaged SWCI are discovered, the organization will take action to remove these SWCI. Because unauthorized software is unmanaged, it is probably vulnerable to being exploited as a pivot to other IT assets if not removed or managed.

In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings; malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate itself throughout the enterprise.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

What's on the Network?

3. CONFIGURATION SETTINGS MANAGEMENT (CSM)

The Configuration Management (CSM) Function is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual, and operating system) and software. Once a misconfiguration of hardware devices is discovered, the organization will be responsible to take any needed action to resolve the problem or accept the risk.

Over 80% of known vulnerabilities are attributed to misconfiguration and missing patches. Cyber adversaries often use automated computer attack programs to search for and exploit IT assets with misconfigurations, especially for assets supporting Federal agencies, and then pivot to attack other assets.

4. VULNERABILITY MANAGEMENT (VUL)

The Vulnerability Management (VUL) Function is to discover and support remediation of vulnerabilities in IT assets on a network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified. Once these mistakes and deficiencies are identified, the organization will take action to remove or remediate these from operational systems so that they can no longer be exploited. (An information security vulnerability is a deficiency in software that can be directly used by a hacker to gain access to a system or network).

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

Who's on the Network?

5. MANAGE TRUST IN PEOPLE GRANTED ACCESS (TRUST)

The Manage Trust in People Granted Access (TRUST) Function is to prevent insider attacks by carefully screening new and existing persons granted access for evidence that access might be abused. The Manage Trust in People Granted Access capability provides background information and potential risk or compromise factors. These factors are used to determine if someone should be granted access to certain resources (e.g., sensitive data).

6. MANAGE SECURITY RELATED BEHAVIOR (BEHAVE)

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

The Manage Security Related Behavior capability addresses the behavior of someone who has been granted access to information technology devices and systems.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

Who's on the Network?

7. MANAGE CREDENTIALS AND AUTHENTICATION (CRED)

The Manage Credentials and Authentication Function 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. The CRED capability ensures that account credentials are assigned to, and used by, authorized people. This capability ensures that only trusted people receive credentials, including credentials for physical and logical access.

8. MANAGE ACCOUNT ACCESS / PRIVILEGES (PRIV)

The Manage Account Access / Privileges Function 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. The Manage Account Access capability will assign access to computing resources based, in part, on their level of trustworthiness.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

How's the Network Protected?

9. MANAGE NETWORK ACCESS CONTROLS (BOUND)

The Manage Network Access Controls Function is to prevent, and allow the organization 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.

Boundaries include firewalls as well as encryption (virtual private networks).

Additionally, the function will prevent, remove, and limit unauthorized physical access.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

What's Happening on the Network?

10. PREPARE FOR CONTINGENCIES AND INCIDENTS (MNGEVT)

The Prepare for Contingencies and Incidents Function is to prevent loss of confidentiality, integrity, and/or availability by being prepared for unanticipated events and/or attacks that might require recovery and/or special responses, preventing attacker's compromises from being effective by adequate recovery as needed, and natural events from causing permanent loss by adequate preparation as needed.

11. RESPOND TO CONTINGENCIES AND INCIDENTS (MNGEVT)

The Respond to Contingencies and Incidents Function is to prevent repeat of previous attacks and limit the impact of ongoing attacks by using forensic analysis, audit information, etc. to a) appropriately respond to end ongoing attacks and to b) identify ways to prevent recurrence to prevent attackers from maintaining ongoing attacks and exploiting weaknesses already targeted by others.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

What's Happening on the Network?

12. DESIGN AND BUILD IN SECURITY POLICY AND PLANNING (DBS)

The Design and Build in Security Policy and Planning Function is to prevent exploitation of the system by consciously designing the system to minimize weaknesses and building the system to meet that standard in order to reduce the attack surface and increase the effort required to reach the parts of the system that remain vulnerable.

The Design and Built in Requirements, Policy, and Planning capability includes software assurance best practices to ensure that security is built into the System Development Lifecycle. This capability addresses how to avoid or remove weaknesses and vulnerabilities before the system is released into production caused by poor design and insecure coding practices.

13. DESIGN AND BUILD IN QUALITY (DBS)

The Design and Build in Quality Function is to prevent attackers from exploiting weaknesses by finding and prioritizing weaknesses and fixing the most important weaknesses first. This capability addresses software before it is installed and operational.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

What's Happening on the Network?

14. MANAGE AUDIT INFORMATION (OMI)

The Manage Audit Information Function is to prevent persistent attacks and weaknesses by using audit information to identify them and initiate an appropriate response. The function addresses efforts to monitor the behavior of employees (for example, downloading pornography, unusual times/volumes of access, etc.). The results of these audits help determine an individual's suitability for continued access based, in part, on their behavior.

15. MANAGE OPERATION SECURITY (OMI)

The Manage Operation Security Function is to prevent attackers from exploiting weaknesses by using functional and operational control limits to help senior managers determine when to authorize operation of systems, and when to devote extra attention to reducing risks to prevent attackers from exploiting preventable weaknesses and analyze prior failures to identify and resolve system weaknesses. This activity supports leadership decisions to enable improvement of security. It covers information about all operational capabilities and does not apply to the creation of a system.

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Functional Areas

How's the Data Protected?

"How's data protected?" Focuses on protection of sensitive data, which is covered by the following capabilities:

1. Data Discovery / Classification describes techniques for the identification, discovery, and classification of data.
2. Data Protection describes data protection techniques.
3. Data Loss Prevention describes techniques to minimize data loss.
4. Data Breach / Spillage Mitigation describes techniques for response and recover activities for data breach / spillage.
5. Information Rights Management describes data protection functions specific to information rights management.

Sensitive data requires security and privacy protections at rest, in use, and in transit, to ensure confidentiality, integrity, and availability of data assets, and to ensure information is subject to authorized access and use only.

"How is data protected?" covers establishment of policies and management of data protection processes for:

- Identify sensitive data assets
- Know where the data asset resides and the associated data flows
- Classify the data assets based on severity and impact
- Identify roles, users, uses, processing, disclosures, data retention
- Establish access controls and protection safeguards
- Monitor the efficacy of the data asset controls and safeguards
- Collect and report on data asset compromise
- Timely response to notify stakeholders of data breach or spillage
- Effective recovery to support operational and mission success

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

CDM Program Benefits

Top 10 Benefits of CDM

CDM helps organizations procure a set of tools that will:

1) Provide cyber professionals with real-time analysis of their networks
2) Assess risks and threats
3) Mitigate and identify flaws at near network speed
4) Create a smaller attack surface and decrease risk for operational networks
5) Find weaknesses and vulnerabilities
6) Improve hardware asset management for organizations
7) Improve software asset management for organizations
8) Improve vulnerability management for organizations
9) Create CDM dashboards to show network security
10) Improve the management and trust of people granted access to a network

Source: Homeland Security Continuous Diagnostics and Mitigation Technical Capabilities Volume 2 Requirements Catalog, May, 2018

Managing Cybersecurity Engineering

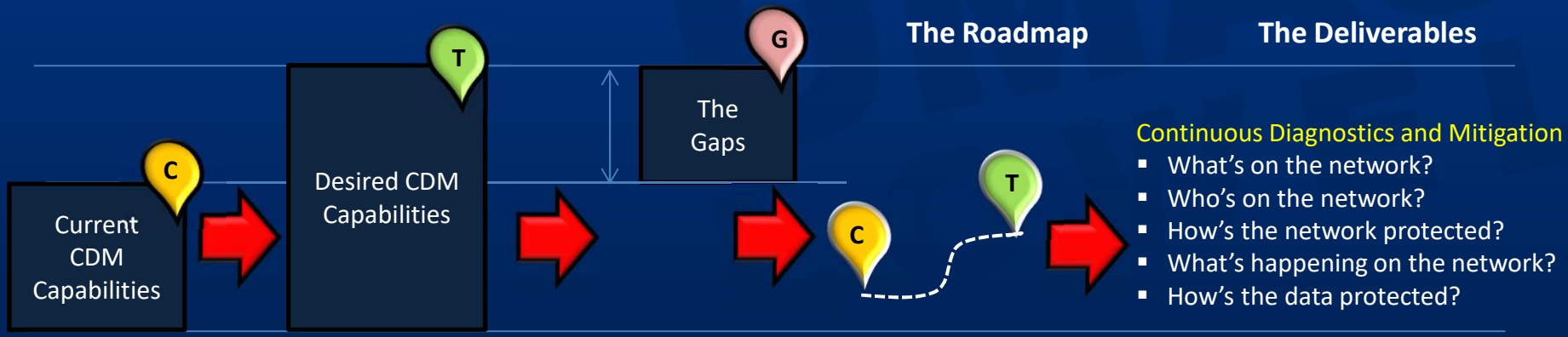
The Assessment — Where are we now?

The Strategy — Where do we want to be?

The Gap Analysis — What are our Gaps?

The Plan of Action — How do we get there?

The Results — How do we know our impact?



Continuous Diagnostics and Mitigation

- What's on the network?
- Who's on the network?
- How's the network protected?
- What's happening on the network?
- How's the data protected?

Learning with Purpose

UMASS LOWELL

Cybersecurity Engineering Deliverables

What's on the Network?

1. Requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).

Who's on the Network?

2. Requires the management and control of managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE).

How's the Network Protected?

3. Requires capabilities that limit, prevent, and/or allow the removal of unauthorized network connections/access that allow attackers to cross internal and external network boundaries and pivot to gain deeper network access.

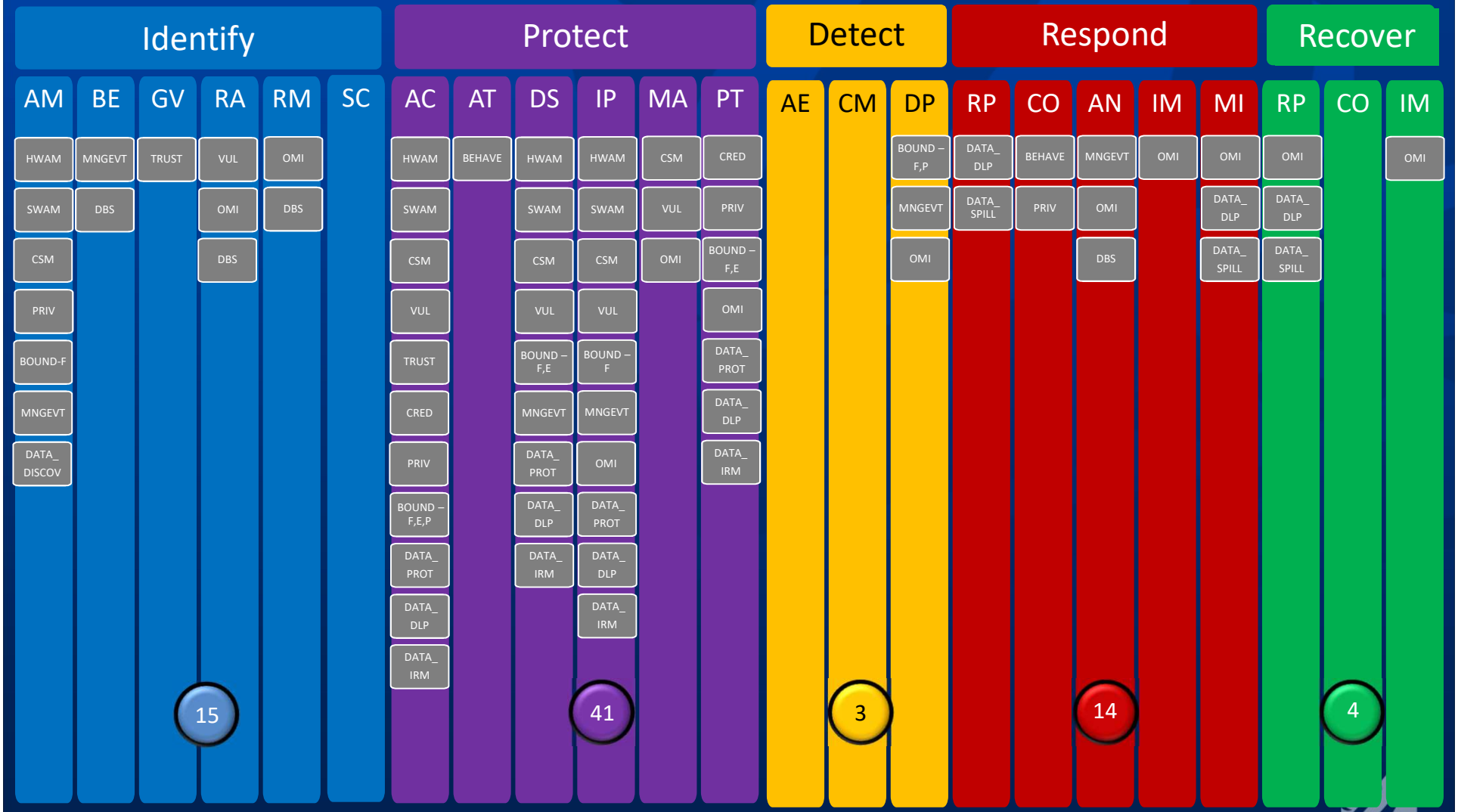
What's Happening on the Network?

4. Managing "What is happening on the network?" builds on "What is on the network?" and "Who is on the network?" These capabilities move beyond asset management to a more extensive and dynamic monitoring of security controls.

How's the Data Protected?

5. Data protection management focuses on "how data is protected" with capabilities including identification of cybersecurity risks on an ongoing basis, prioritizing risks based on potential impacts, and enabling cybersecurity personnel to mitigate the most significant problems first.

The CDM Program mapped to NIST Framework



Cybersecurity Program Roles & Deliverables

Cybersecurity Program Deliverables

Cybersecurity Program Results

Senior Management

1. Senior Management Deliverables
- Cybersecurity Strategy
- Cybersecurity Workforce
- Cybersecurity Governance
- Cybersecurity Policy

Documents

Risk Management

2. Risk Management Deliverables
- System Security Plan (SSP)
- Cyber Risk Assessment
- Plan of Action & Milestones (POA&M)
- Executive Report

Documents

Cybersecurity Engineering

3. Cybersecurity Engineering Deliverables
- What's on the network?
- Who's on the network?
- How's the network protected?
- What's happening on the network?
- How's the data protected?

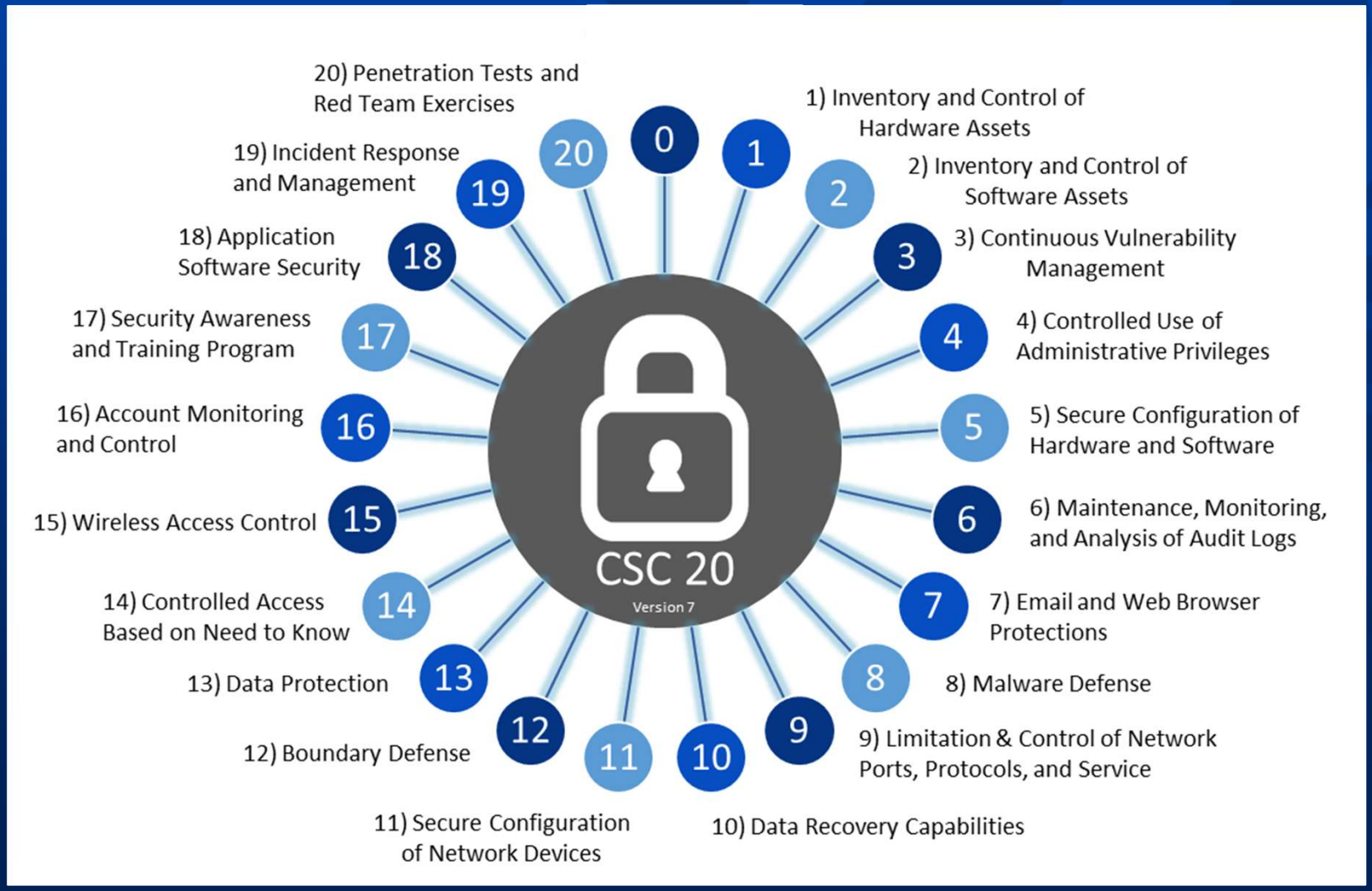
Dashboards

Cybersecurity Operations Objectives / Deliverables

Securing the Digital Assets that run our Critical Infrastructure

The 20 Critical Controls

The CIS Controls (Version 7.1)



The CIS Controls

Background and Introduction

What are the CIS Controls: The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

The CIS Controls have been matured by an international community of individuals and institutions that:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;
- Document stories of adoption and share tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- Map the CIS Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- Share tools, working aids, and translations; and Identify common problems (like initial assessment and implementation roadmaps) and solve them as a community.

These activities ensure that the CIS Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements

CIS Controls Overview

Who created the CIS Controls and when were they developed?

The CIS Controls were developed starting in 2008 by an international, grass-roots consortium bringing together companies, government agencies, institutions, and individuals from every part of the ecosystem (cyber analysts, vulnerability-finders, solution providers, users, consultants, policy-makers, executives, academia, auditors, etc.) who banded together to create, adopt, and support the CIS Controls. The expert volunteers who develop the Controls apply their first-hand experience to develop the most effective actions for cyber defense.

How are they updated?

The CIS Controls are updated and reviewed through an informal community process. Practitioners from government, industry, and academia each bring deep technical understanding from across multiple viewpoints (e.g., vulnerability, threat, defensive technology, tool vendors, enterprise management) and pool their knowledge to identify the most effective technical security controls needed to stop the attacks they are observing.

What is the benefit of the CIS Controls?

Prioritization is a key benefit to the CIS Controls. They were designed to help organizations rapidly define the starting point for their defenses, direct their scarce resources on actions with immediate and high-value payoff, and then focus their attention and resources on additional risk issues that are unique to their business or mission.

CIS Control Categories

CIS Controls V7 breaks down the 20 controls into three distinct categories

Category 1: Basic Security Controls (CSC 1-6): Key controls which should be implemented in every organization for essential cyber defense readiness. The basic controls are a must for every organization, regardless of the size or the industry in question. CIS refers to these Controls as "Cyber Hygiene"—the basic things that you must do to create a strong foundation for your defense." By implementing CIS Controls 1–6 as continuous and evolving processes, organizations can reduce risk while adapting to both changing threats and changing business demands.

Category 2: Foundational Security Controls (CSC 7-16): The next step up from basic – these technical best practices provide clear security benefits and are a smart move for any organization to implement. These areas can help enterprises shore up their security after they have mastered the basic controls. A phased implementation approach also helps ensure that organizations receive the most significant benefits by implementing the highest priority controls first.

Category 3: Organizational Security Controls (CSC 17-20): These controls are different in character from 1-16; while they have many technical elements, are more focused on people and processes involved in cybersecurity. They address the potential skills gap in the workforce and help identify behavior that might leave systems vulnerable.

The Basic Security Controls (1)

CIS Control 1: Inventory and Control of Hardware Assets
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Make Sure You Know What Devices You Have - This control makes perfect sense to any executive, because inventory is foundational concept in all of business, especially finance. The control differentiates between authorized and unauthorized devices in the inventory, and executives should resonate with the importance of this distinction.

CIS Control 2: Inventory and Control of Software Assets
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

Make Sure You Know What Software You Have - Understanding software inventory sounds easier than it is in actual practice. License agreements can be complex, and the ease with which software can be downloaded from the Internet makes a software inventory potentially tough. Controls 1 and 2 are recommended to be worked together.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Basic Security Controls (2)

CIS Control 3: Continuous Vulnerability Management
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Check for and Fix Vulnerabilities Continually - Every cybersecurity professional agrees that a major challenge in the industry involves keeping up with all the vulnerabilities identified in real time across the globe. Sadly, no shortcut exists to constantly maintaining vigilance around such vulnerabilities, and taking steps to mitigate relevant ones quickly.

CIS Control 4: Controlled Use of Administrative Privileges
The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Manage Administrative Privileges Carefully - The control of administrative privileges should be obvious in its importance to enterprise security. Hackers will always target accounts with high privilege, so these privileges need to be inventoried and controlled using tools that monitor and manage all types of activity from these powerful system vantage points.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Basic Security Controls (3)

CIS Control 5: Secure Configuration for Mobile Devices, Laptops, Workstations and Servers
Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings

Configure Your Systems Properly - The systems in scope with this control include mobile devices, laptops, workstations, servers and other devices. The reference to proper configuration focuses on security properties such as making certain that good decisions are made to turn off unnecessary services and properly change defaults.

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Pay Attention to Your Audit Logs - Most systems in the enterprise generate useful log output that contains useful information about potential security attack indicators. Security teams must pay attention to these logs and use them in conjunction with tools that are designed to analyze log information and generate actionable management guidance.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Foundational Security Controls (1)

CIS Control 7: Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Email and Web are common points of entry - Web browsers and email clients are points of attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering.

CIS Control 8: Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Identify, prevent and log attempts to implement malicious software - Organizations should validate that anti-malware is deployed, running and correctly configured. Being able to block malicious applications is only part of this control, there is also a big focus on collecting the logs to help organizations understand what happened within their environment, and this includes ensuring that there is logging enabled.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Foundational Security Controls (2)

CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services
Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attacker

Limit What's Allowed on Your Network - The establishment of security policy rules that prohibit unnecessary services is one of the oldest concepts in information security. Such minimization of services at the network level makes it harder for hackers with scanners to find open ports and listening services through which to gain entry to the enterprise.

CIS Control 10: Data Recovery Capabilities
The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Make Sure You Can Recover Lost Data - Increasingly, hackers understand that data theft is only one dimension of the cyber offensive equation. In addition, they have come to recognize the potential to tamper with the integrity of data and systems. Ransomware is an example. As a result, organizations must have a strong plan for dealing with recovery of lost data should preventive controls fail.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Foundational Security Controls (3)

CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Secure Your Network Devices - Network devices can be viewed as the gateways to your enterprise, whether physical or virtual. As such, proper administration and secure configuration of routers, switches, firewalls and other network devices is essential to managing ingress and egress filtering rules for enterprise policy-based protection.

CIS Control 12: Boundary Defense
Detect/prevent/correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data.

Build a Multi-Layered Boundary Defense - Defense in depth is the preferred architectural paradigm for security engineers, especially with the evolution of the enterprise to hybrid cloud services. The old perimeter model has been supplanted by the view that boundary defenses can be created closer to both data and computing resources, such as in cloud environments.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Foundational Security Controls (4)

CIS Control 13: Data Protection
The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Focus on Protecting Your Data - Modern tools exist that can prevent or detect the leakage or loss of proprietary data. These tools include encryption-based technologies to maintain proper access to sensitive data. In addition, advanced data loss prevention tools examine behaviors to help determine if perhaps a disgruntled or malicious insider is leaking data.

CIS Control 14: Controlled Access Based on the Need to Know
The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Use Need-to-Know for Access - The concept of need-to-know is well established in government. Industry should introduce similar concepts in access management, focusing on minimizing the number of authorized individuals who have been granted access to information or resources. This approach is also known as “least privilege.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Foundational Security Controls (5)

CIS Control 15: Wireless Access Control
The processes and tools used to track/control/prevent/correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.

Control Your Wireless Devices - The explosion of wireless and mobile devices in business is staggering, and executives should recognize that wireless access control, device authentication, inventory and access management are not only sensible, but are absolutely required to keep malicious actors from wreaking havoc on an enterprise.

CIS Control 16: Account Monitoring and Control
Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

Monitor and Control Your Accounts - The "account" is the most basic unit of control in all enterprise computing and networking environments. Despite this, too many security teams have weak or non-control of the accounts in the company. By monitoring and controlling accounts, security teams make it much harder for malicious actors to attack a company and steal or damage assets.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Organizational Security Controls (1)

CIS Control 17: Implement a Security Awareness and Training Program
For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs

Optimize the Security Skills of Your Staff - The security capability of staff in an enterprise is one of the most neglected aspects of cybersecurity. Executives often take for granted how hard it is for experts to keep up with the latest issues in technology and threat. Employees must also maintain high levels of current awareness of best practices in cyber hygiene.

CIS Control 18: Application Software Security
Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses

Implement an Application Security Program - The most popular target for hackers is your application base, so it's essential to implement a comprehensive program of application security controls. This should include scanning, testing, and software development lifecycle (SDLC) controls to reduce the risk of malicious insertion of Trojans and other malware into code.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

The Organizational Security Controls (2)

CIS Control 19: Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Have a Plan for Dealing with Incidents - Even if proper cybersecurity controls are deployed across a company, incidents will certainly occur. To deal with such cases, companies must have well-defined incident response plans that can help recover assets, restore integrity and reconstitute resources that might have been hacked during the incident.

CIS Control 20: Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Test Your Network by Breaking In - While testing is not a great method to demonstrate the complete absence of flaws, it is an excellent way to demonstrate the presence of bugs, flaws and security problems. It's prudent therefore to maintain an ongoing program of security and penetration testing to highlight progress in security across the company.

Sources: Center for Internet Security: CIS Controls Version 7.1, Tripwire Executive Guide for the CIS Controls

Managing Cybersecurity Operations

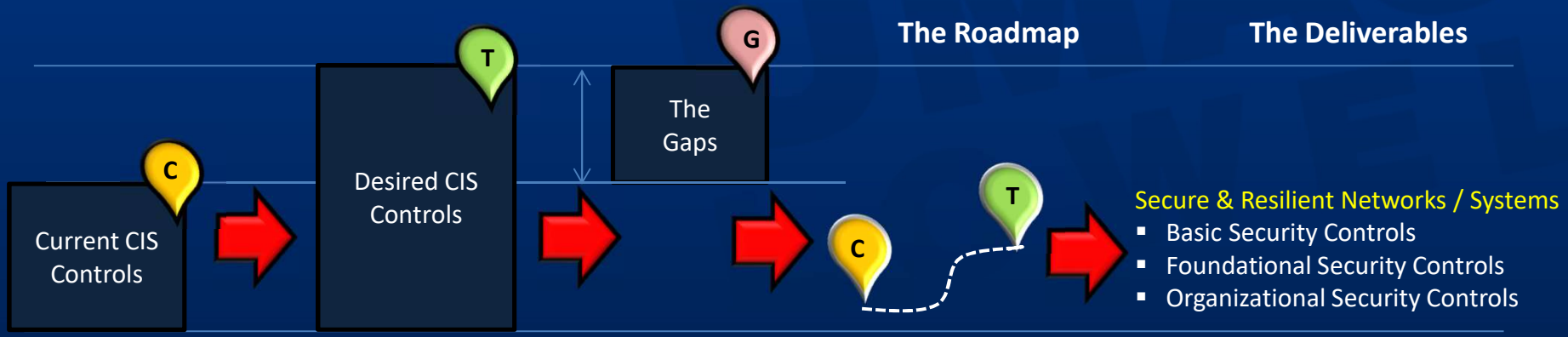
The Assessment — Where are we now?

The Strategy — Where do we want to be?

The Gap Analysis — What are our Gaps?

The Plan of Action — How do we get there?

The Results — How do we know our impact?



Learning with Purpose

Cybersecurity Operations Deliverables

Basic Security Controls

1. Key controls which should be implemented in every organization for essential cyber defense readiness. The basic controls are a must for every organization, regardless of the size or the industry in question.

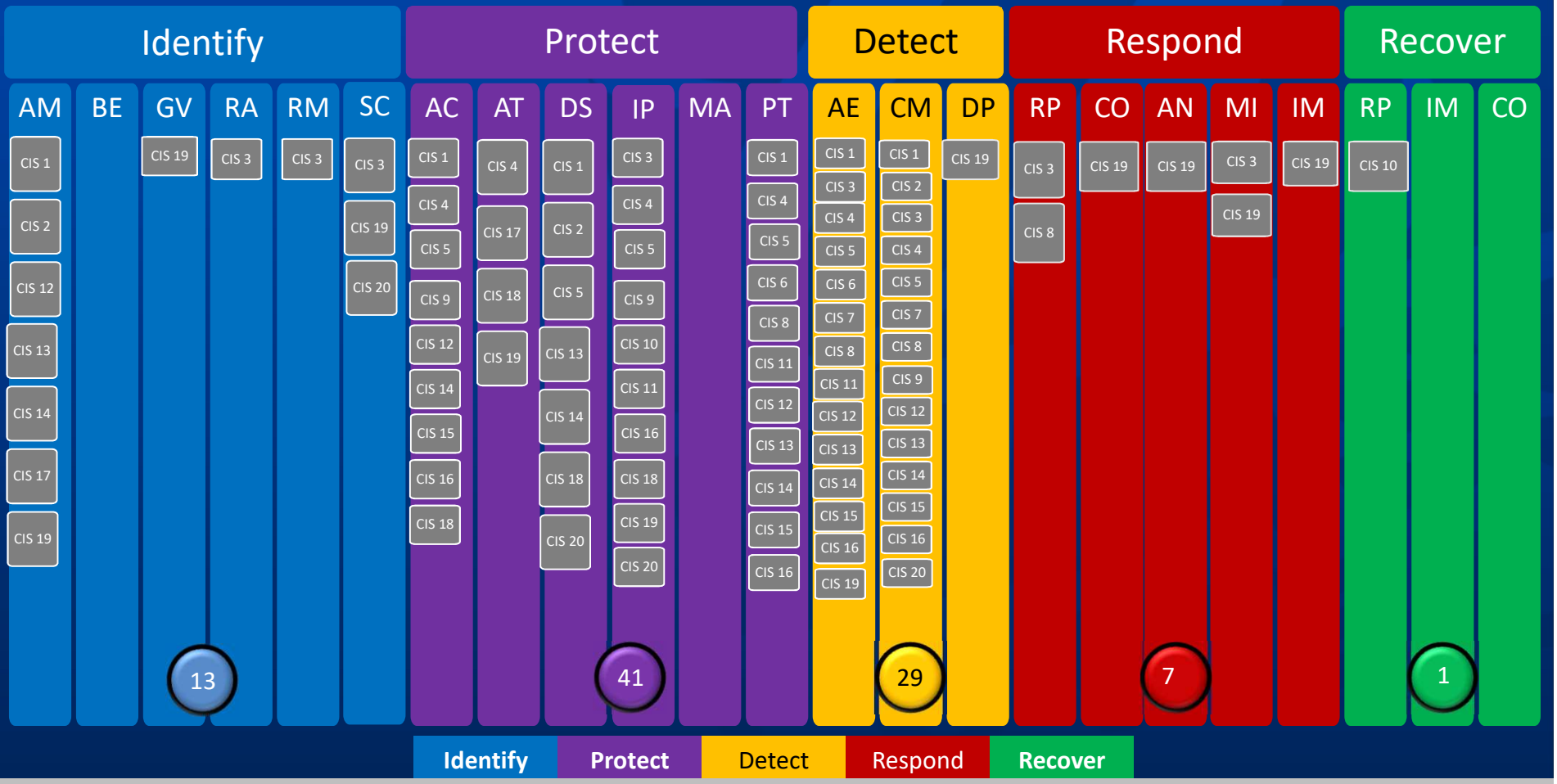
Foundational Security Controls

2. The next step up from basic – these technical best practices provide clear security benefits and are a smart move for any organization to implement. These areas can help enterprises shore up their security after they have mastered the basic controls

Organizational Security Controls

3. These controls are different in character from 1-16; while they have many technical elements, are more focused on people and processes involved in cybersecurity. They address the potential skills gap in the workforce and help identify behavior that might leave systems vulnerable.

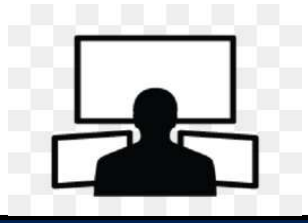
CIS Controls Mapped to NIST Framework



CIS Critical Security Controls (v7.0)

CIS-1) Inventory and Control of Hardware Assets
CIS-2) Inventory and Control of Software Assets
CIS-3) Continuous Vulnerability Management
CIS-4) Controlled Use of Administrative Privileges
CIS-5) Secure Configuration of Hardware & Software
CIS-6) Maintenance, Monitoring, Analysis of Audit Logs
CIS-7) Email and Web Browser Protections
CIS-8) Malware Defenses
CIS-9) Limitation & Control of Network Ports, Protocols & Services
CIS-10) Data Recovery Capabilities
CIS-11) Secure Configuration of Network Devices, Firewalls, Routers
CIS-12) Boundary Defense
CIS-13) Data Protection
CIS-14) Controlled Access Based on Need to Know
CIS-15) Wireless Access Control
CIS-16) Account Monitoring and Control
CIS-17) Security Awareness and Training Program
CIS-18) Application Software Security
CIS-19) Incident Response and Management
CIS-20) Penetration Tests and Red Team Exercises

Cybersecurity Program Roles & Deliverables

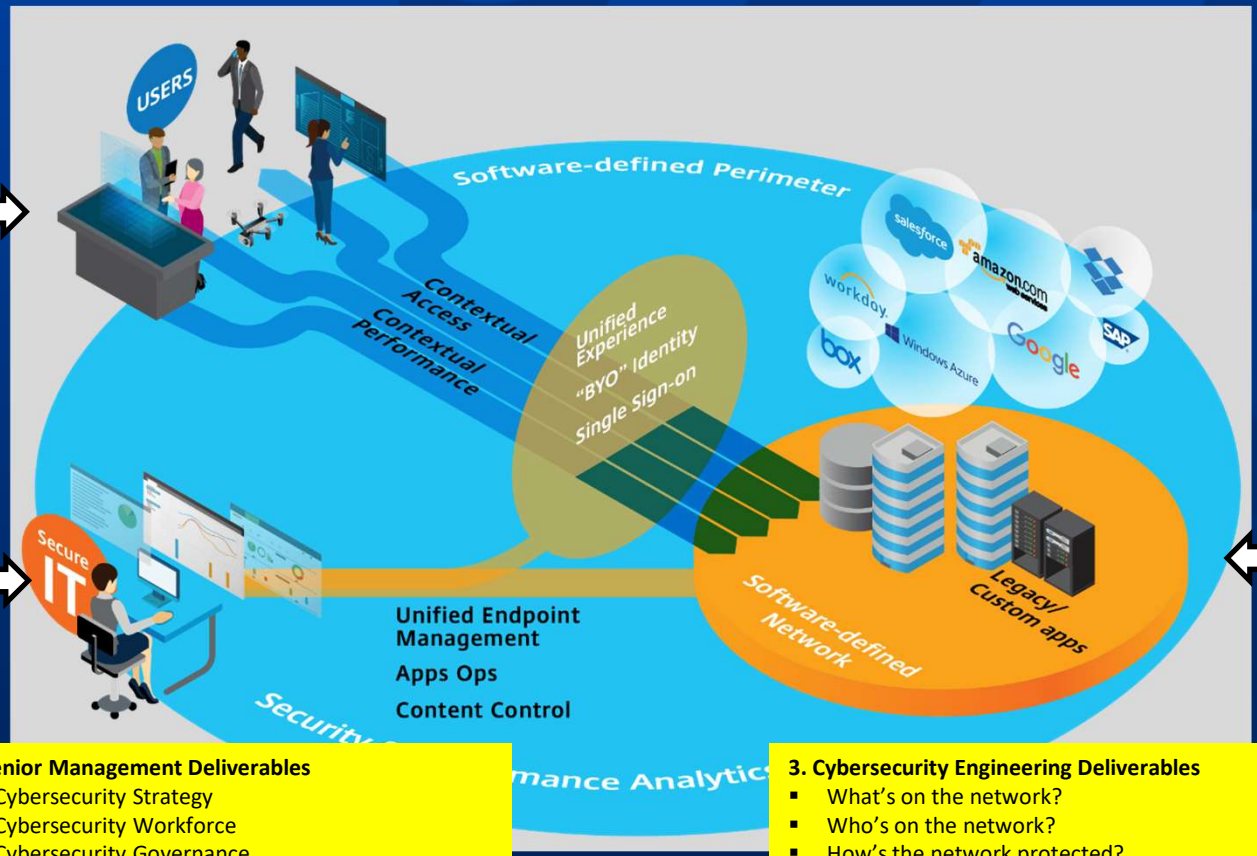
Cybersecurity Roles & Responsibilities	Cybersecurity Program Deliverables	Cybersecurity Program Results
Senior Management 	**1. Senior Management Deliverables** ▪ Cybersecurity Strategy ▪ Cybersecurity Workforce ▪ Cybersecurity Governance ▪ Cybersecurity Policy	Documents 
Risk Management 	**2. Risk Program Deliverables** ▪ System Security Plan (SSP) ▪ Cyber Risk Assessment ▪ Plan of Action & Milestones (POA&M) ▪ Executive Report	Documents 
Cybersecurity Engineering 	**3. Cybersecurity Engineering Deliverables** ▪ What's on the network? ▪ Who's on the network? ▪ How's the network protected? ▪ What's happening on the network? ▪ How's the data protected?	Dashboards 
Technology / Operations 	**4. Technology / Operations Deliverables** ▪ Basic Security Controls ▪ Foundational Security Controls ▪ Organizational Security Controls	Dashboards 

Cybersecurity Program Deliverables Summary

Cybersecurity Best Practices enable Digital Transformation

Digital Services
[Devices, Apps, Data]

Digital Operations
[Workforce]



Digital Platforms
[Workloads]

1. Senior Management Deliverables
- Cybersecurity Strategy
- Cybersecurity Workforce
- Cybersecurity Governance
- Cybersecurity Policy

2. Risk Management Deliverables
- System Security Plan (SSP)
- Cyber Risk Assessment
- Plan of Action & Milestones (POA&M)
- Executive Report

3. Cybersecurity Engineering Deliverables
- What's on the network?
- Who's on the network?
- How's the network protected?
- What's happening on the network?
- How's the data protected?

4. Technology / Operations Deliverables
- Basic Security Controls
- Foundational Security Controls
- Organizational Security Controls

UMASS LOWELL

Questions?