

Interim IT Committee NDUS IT Security Update

Darin King
NDUS Deputy CIO

NDUS Information Security Strategic Plan



Governance

Program Charter

Mult-Factor Authentication

Endpoint Protection

Training and Awareness

Sensitive Information Discovery

Vulnerability Management

Centralized Logging

Policy

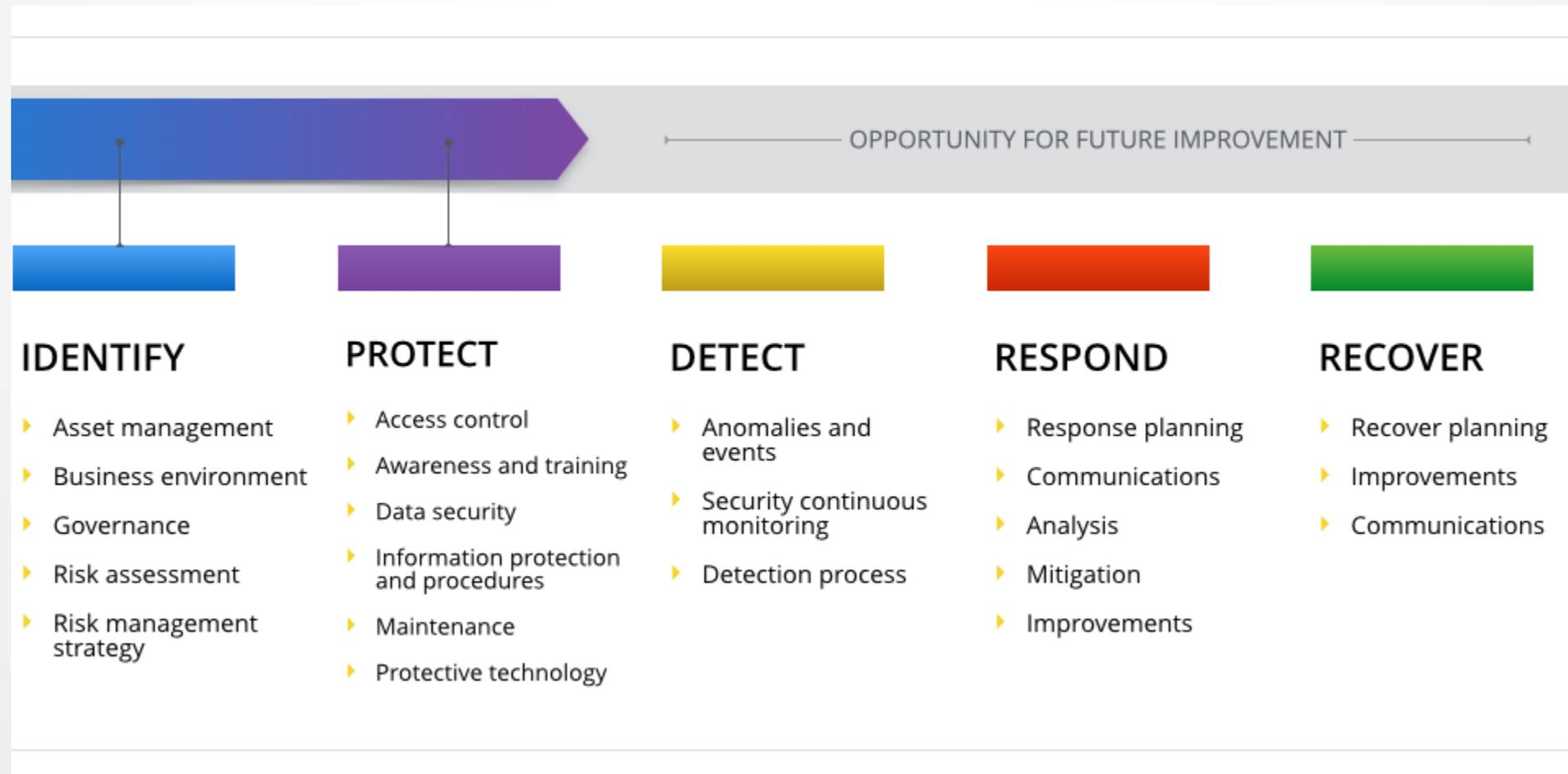
Standards

Procedures

Cybersecurity Frameworks and Standards

Data Classification

Information Security



NIST Cybersecurity Framework Core

Information Security

Governance

- NDUS Information Security Council (ISC)
- CTS Information Security Group (ISG)

Information Security

Policy

Standards

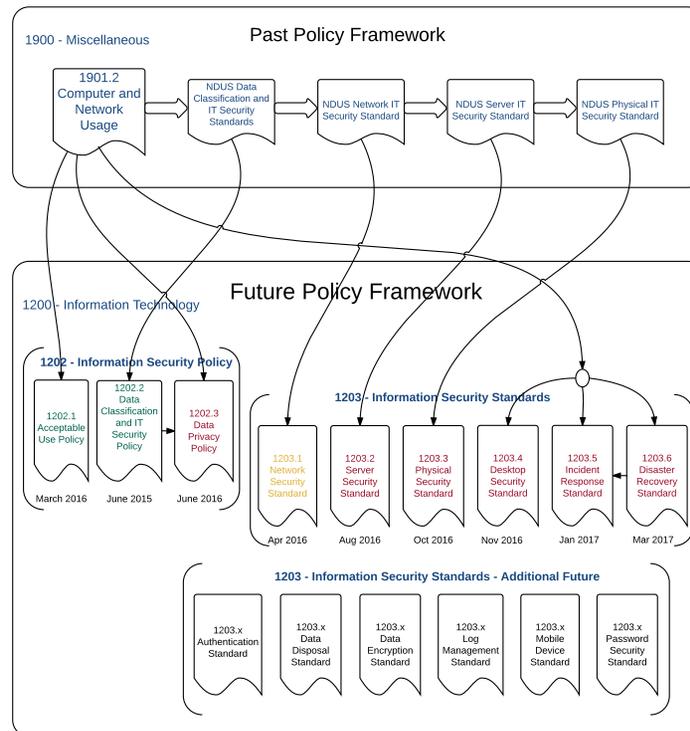
Procedures

Cybersecurity Frameworks and Standards

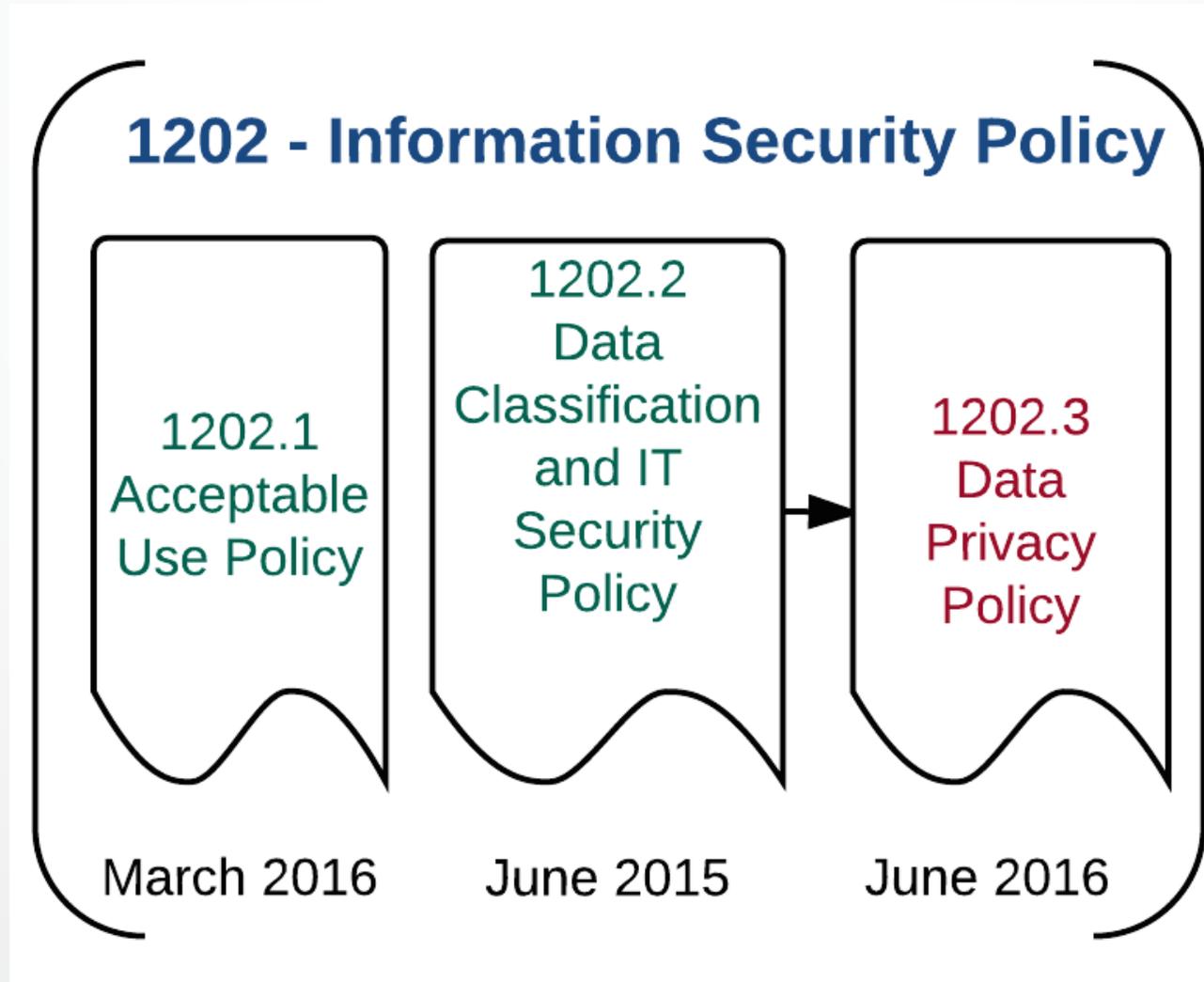
Data Classification

- Problems/Risks
 - Old outdated policy and standards
 - Need a data classification standard as a foundation for protection
 - No consistent understanding, implementation, and enforcement of policies and standards
- Benefits
 - Clear security baselines for all member institutions
 - Standards-based foundation to measure compliance and results
 - Consistent application of security controls based on data classification and system criticality

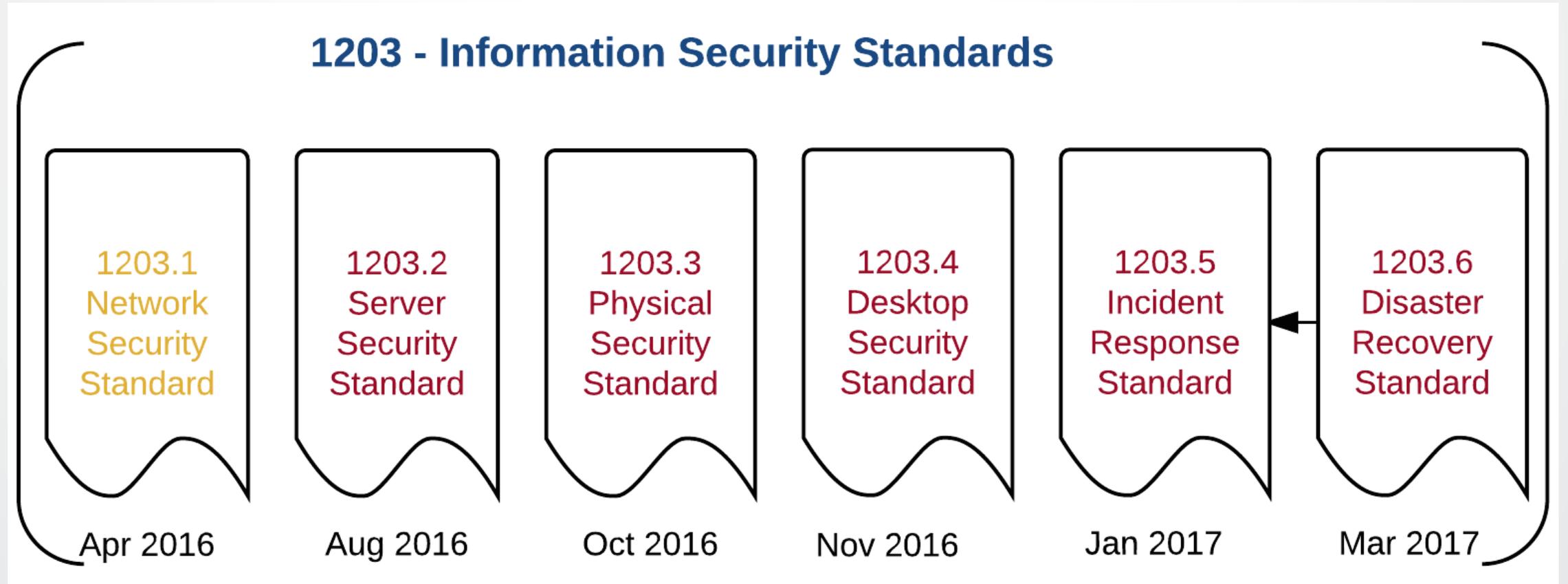
Information Security



Information Security



Information Security



Information Security

Multi-Factor Authentication

- Problems/Risks
 - 95% of breaches involve the exploitation of stolen credentials (2015 Verizon DBIR)
- Solution
 - NDUS is implementing a system-wide Multi-factor authentication solution
 - Already protecting over 10 services and expanding to campuses and Campus Solutions (PeopleSoft)
- Benefits
 - Reduces the risk of compromised NDUS credentials being used to gain unauthorized access to critical systems and data
 - Provides a notification mechanism for compromised credentials

Information Security

Endpoint Protection

Problems/Risks

- Many of the threats we face involve our endpoints (computers, laptops, servers) – phishing, malware, web browsing attacks, malicious email

Solution

- Need to implement advanced endpoint protection capabilities
- An Endpoint Protection RFP and Procurement process is underway

Benefits

- Reduces the risk of compromised NDUS credentials being used to gain unauthorized access to critical systems and data
- Provides a notification mechanism for compromised credentials

Information Security

Training
and
Awareness

Problems/Risks

- Protection of systems is not just a technical challenge – it relies on knowledge and action of the people within our organization.
- Without proper training and awareness, faculty and staff become targets and not part of the solution.

Solution

- Create a security training and awareness program
- A security awareness training program was procured and is currently being used in CTS and three campuses

Benefits

- Make individuals aware that the data on their computers is valuable and vulnerable
- Empower individuals with the knowledge to be the first, and last, line of defense against security threats for protecting their systems and data

Information Security

A blue square containing the text "Vulnerability Management" in white, serif font.

Vulnerability Management

Problems/Risks

- All systems and applications are affected by vulnerabilities that are used by attackers to breach our environment

Solution

- Currently have deployed a system-wide vulnerability management system

Benefits

- Allows for the quick remediation of vulnerabilities on critical systems, network devices, and applications

Information Security

A blue square box containing the text "Centralized Logging" in white, centered within the box.

Centralized
Logging

Problems/Risks

- Systems generate a large amount of log data that can be collected and analyzed to help identify, prevent, detect and recover from an attack.

Solution

- Currently deploying a log management system to centrally collect logs within the NDUS data center

Benefits

- Protects critical system logs from unauthorized access and modification
- Provides a mechanism for log and event correlation to prevent, detect, and respond to a security incident

Information Security

- Ongoing Process
 - Policy/Standards/Procedures
- Annual Strategic Planning Summit
 - July 2017

