Jon Brown

Information Systems Security Officer
@ Montage Marketing Group

LinkedIn: @jonbrown2

MacAdmins Slack: @Jon Brown

Cybersecurity is the **convergence of people, processes and technology that come together to protect organizations**

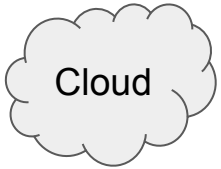

Integrity
Confidentiality
Availability

What Makes Up Cybersecurity?

Frameworks

Security

Infrastructure



Network

Organizational

Information

Access

Application

Encryption

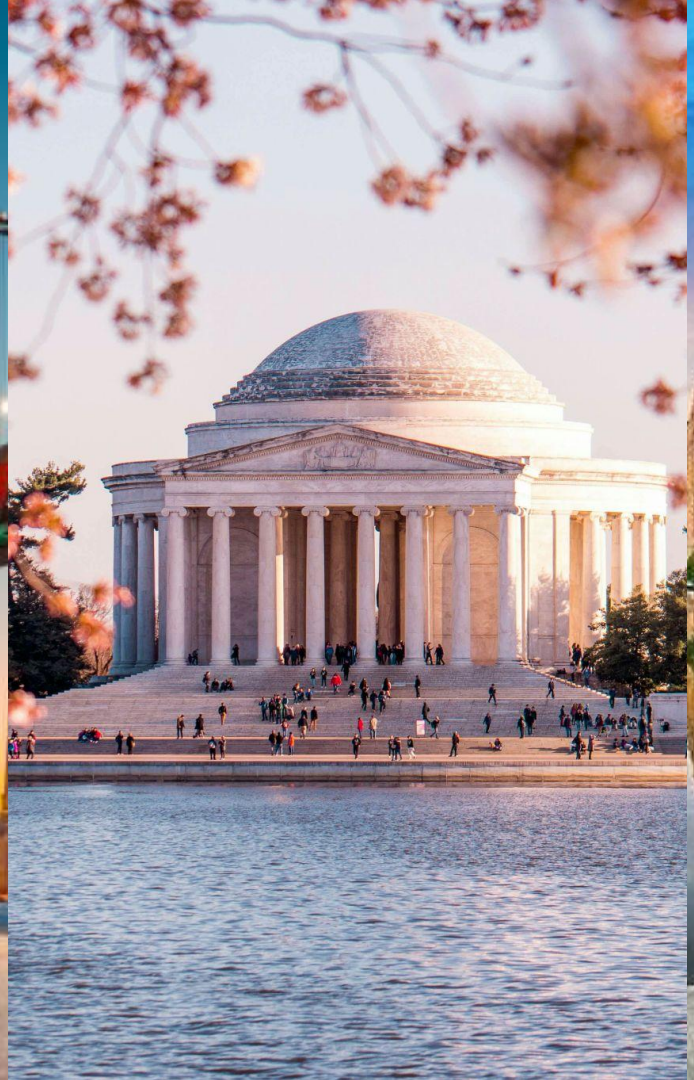
User Behavior

User Education

Disaster Recovery

Laws

Our expertise,
your peace of mind

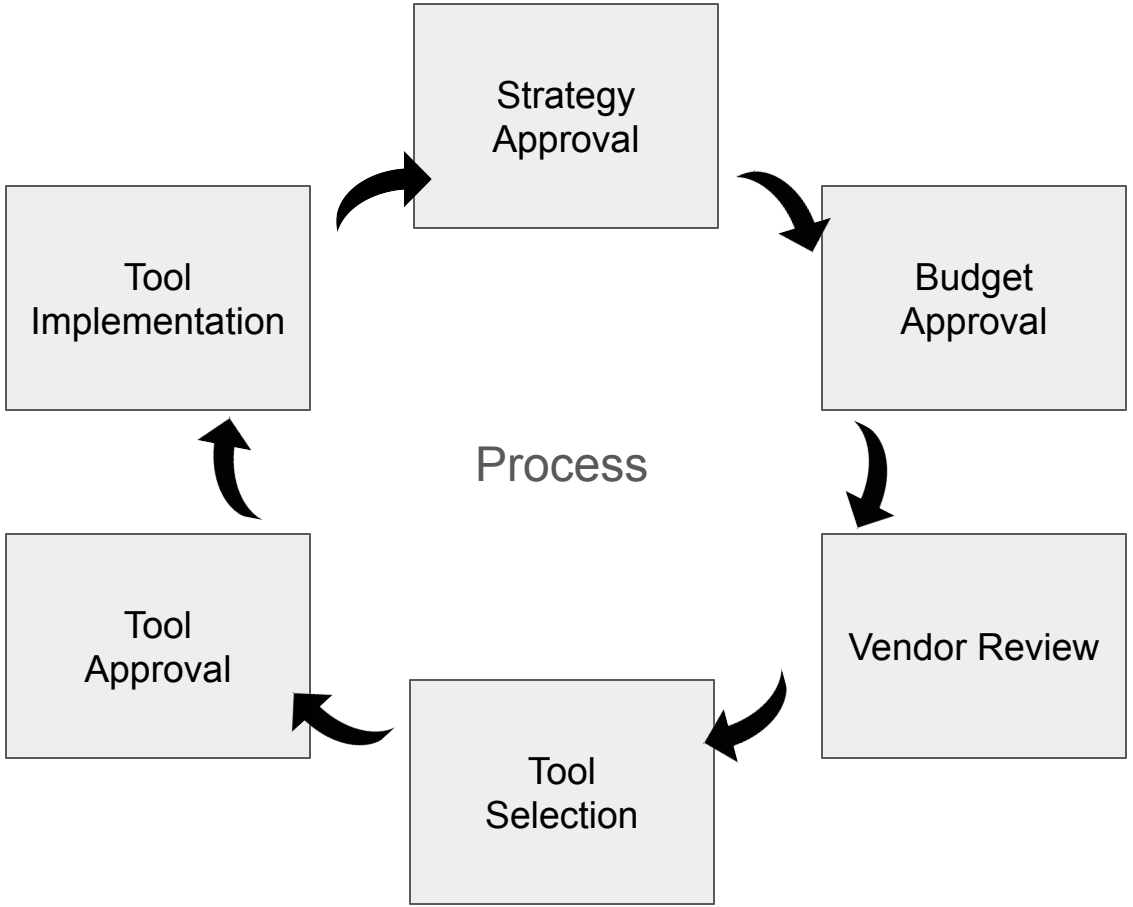





filewave
mosyle
BlackGlove
AUTOMOX
avast
CROWDSTRIKE
kandji
eset
Vanta
KnowBe4
RAPID7
NordLayer
intruder
SuperOps.ai
druva
intego
splashtop
ARCTIC WOLF
SentinelOne
CISCO
Cisco Umbrella
Microsoft Defender
Kaseya
paloalto NETWORKS
Meraki
secureframe
jumpcloud
LIBRAESVA
LetsDMARC
HOOK SECURITY
Addigy
Malwarebytes
THREATLOCKER
redcanary
SYXSENSE
CYBERARK
halcyon
ninjaOne
Apptega
Cybersecurity Management Software
Judy Security
jamf PRO
kaspersky
Trellix
DARK READING

Business **Strategies**

MONTAGE MARKETING



Cybersecurity **Strategies**

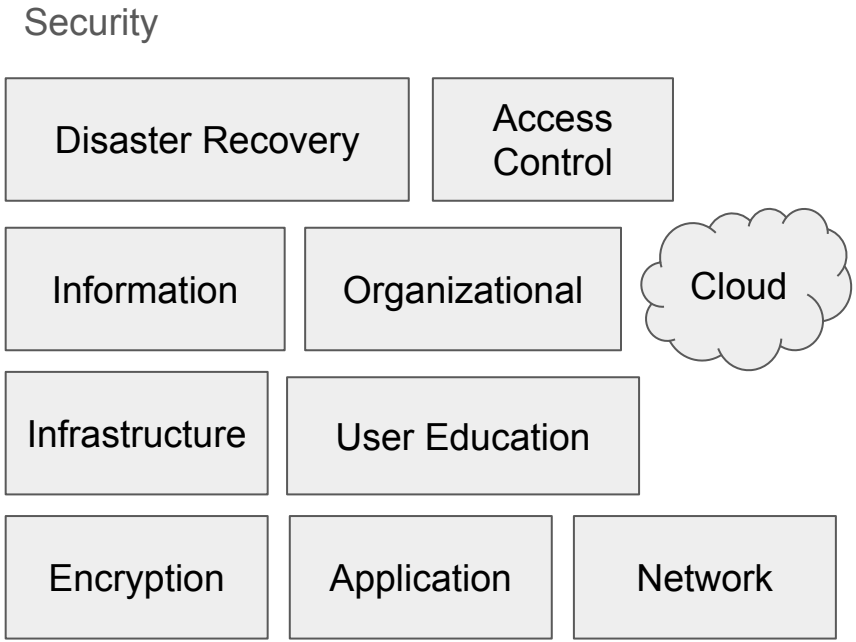
Requirements

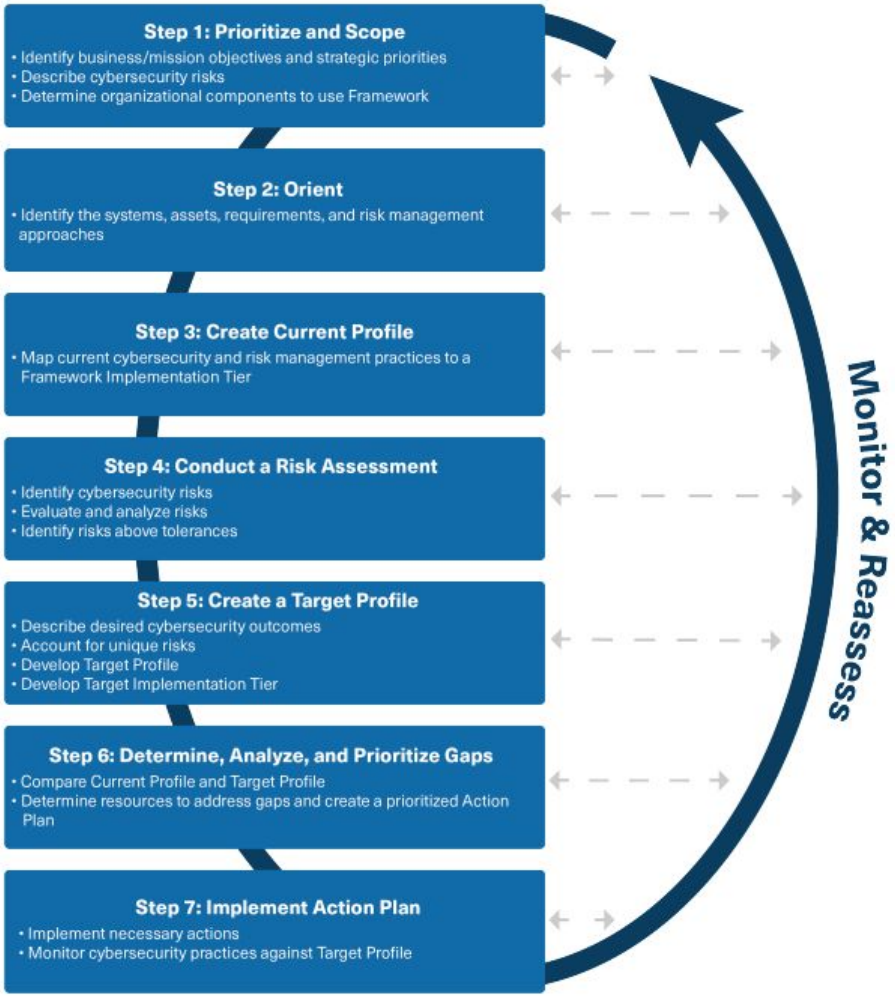
NIST 800-53

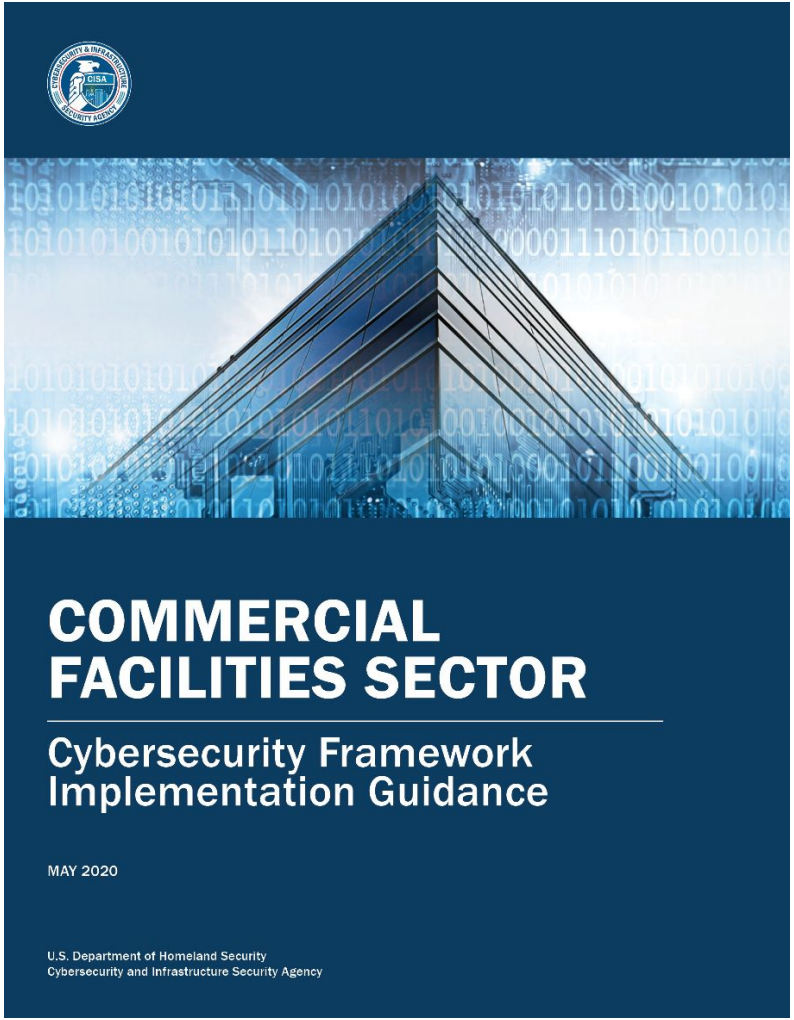
20 Domains
316 Controls

NIST 800-171

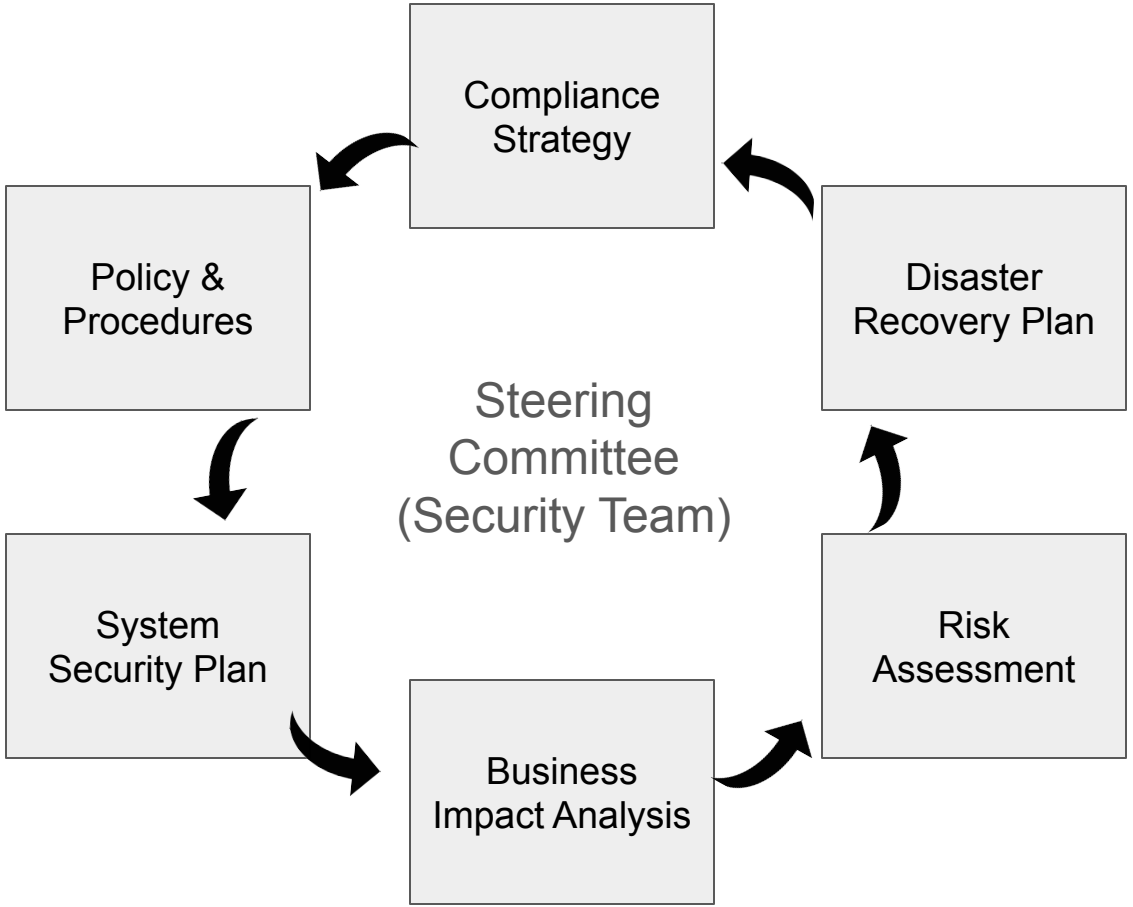
14 Domains
110 Controls




Step 1: Prioritize and Scope
• Identify business/mission objectives and strategic priorities
• Describe cybersecurity risks
• Determine organizational components to use Framework
Step 2: Orient
• Identify the systems, assets, requirements, and risk management approaches
Step 3: Create Current Profile
• Map current cybersecurity and risk management practices to a Framework Implementation Tier
Step 4: Conduct a Risk Assessment
• Identify cybersecurity risks
• Evaluate and analyze risks
• Identify risks above tolerances
Step 5: Create a Target Profile
• Describe desired cybersecurity outcomes
• Account for unique risks
• Develop Target Profile
• Develop Target Implementation Tier
Step 6: Determine, Analyze, and Prioritize Gaps
• Compare Current Profile and Target Profile
• Determine resources to address gaps and create a prioritized Action Plan
Step 7: Implement Action Plan
• Implement necessary actions
• Monitor cybersecurity practices against Target Profile
Monitor & Reassess


COMMERCIAL FACILITIES SECTOR
Cybersecurity Framework Implementation Guidance
MAY 2020
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

MONTAGE MARKETING



Multiple **Strategies**

START HERE

1

Define what CUI is for your specific business case (based on the contract).

2 **Establish the scope of the CMMC assessment boundary**

2a

Create a Data Flow Diagram (DFD) that shows how CUI flows from the DoD all the way down to subcontractors.

2b

Create a detailed asset inventory for all systems, applications and services for both in-scope and out-of-scope assets.

2c

Create a detailed network diagram that includes where CUI is stored, transmitted and/or processed.

2d

Inventory Third-Party Service Providers (TSP) to determine TSP access to CUI and/or in-scope systems, applications and/or services.

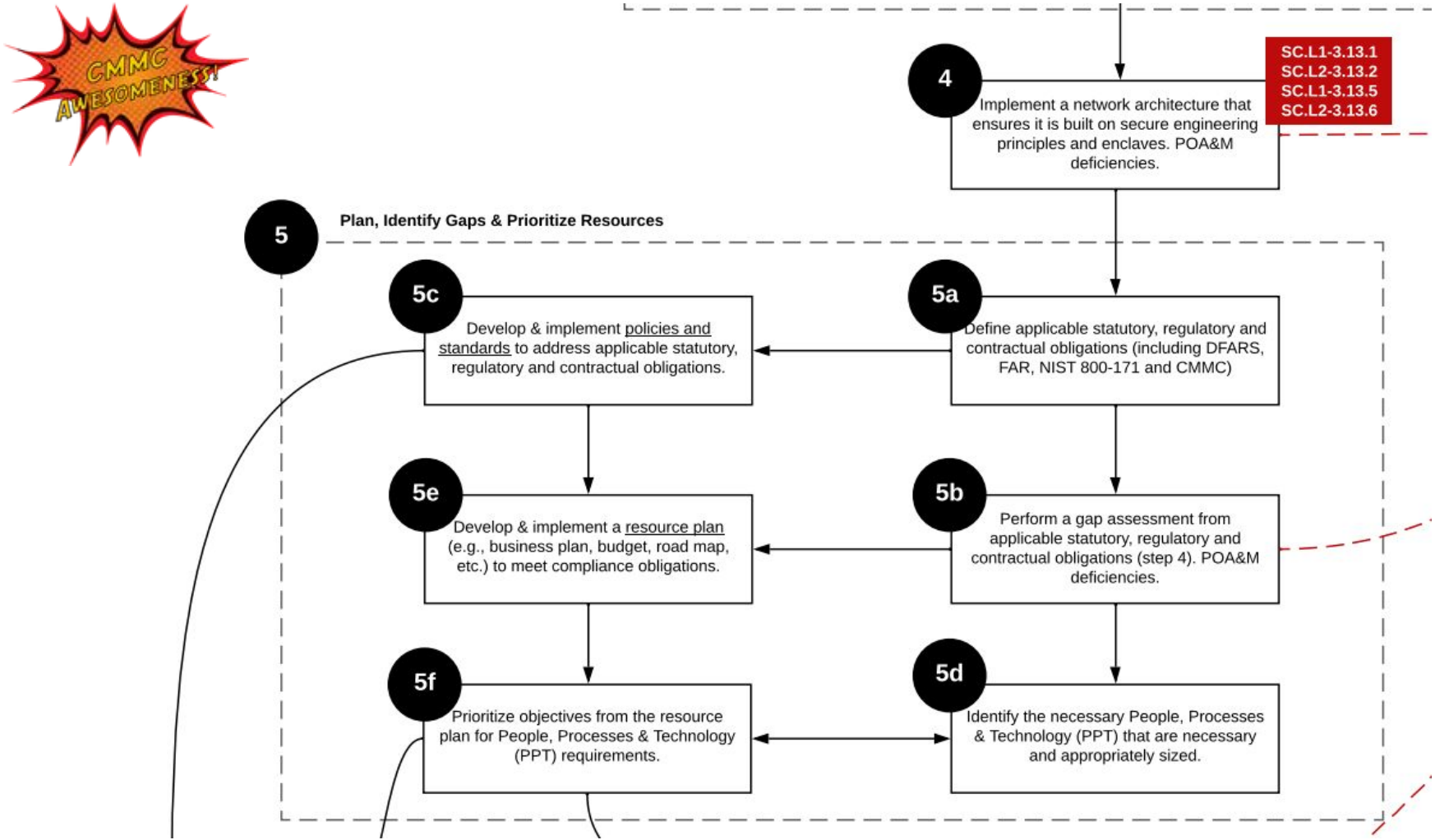
3 **Document the environment**

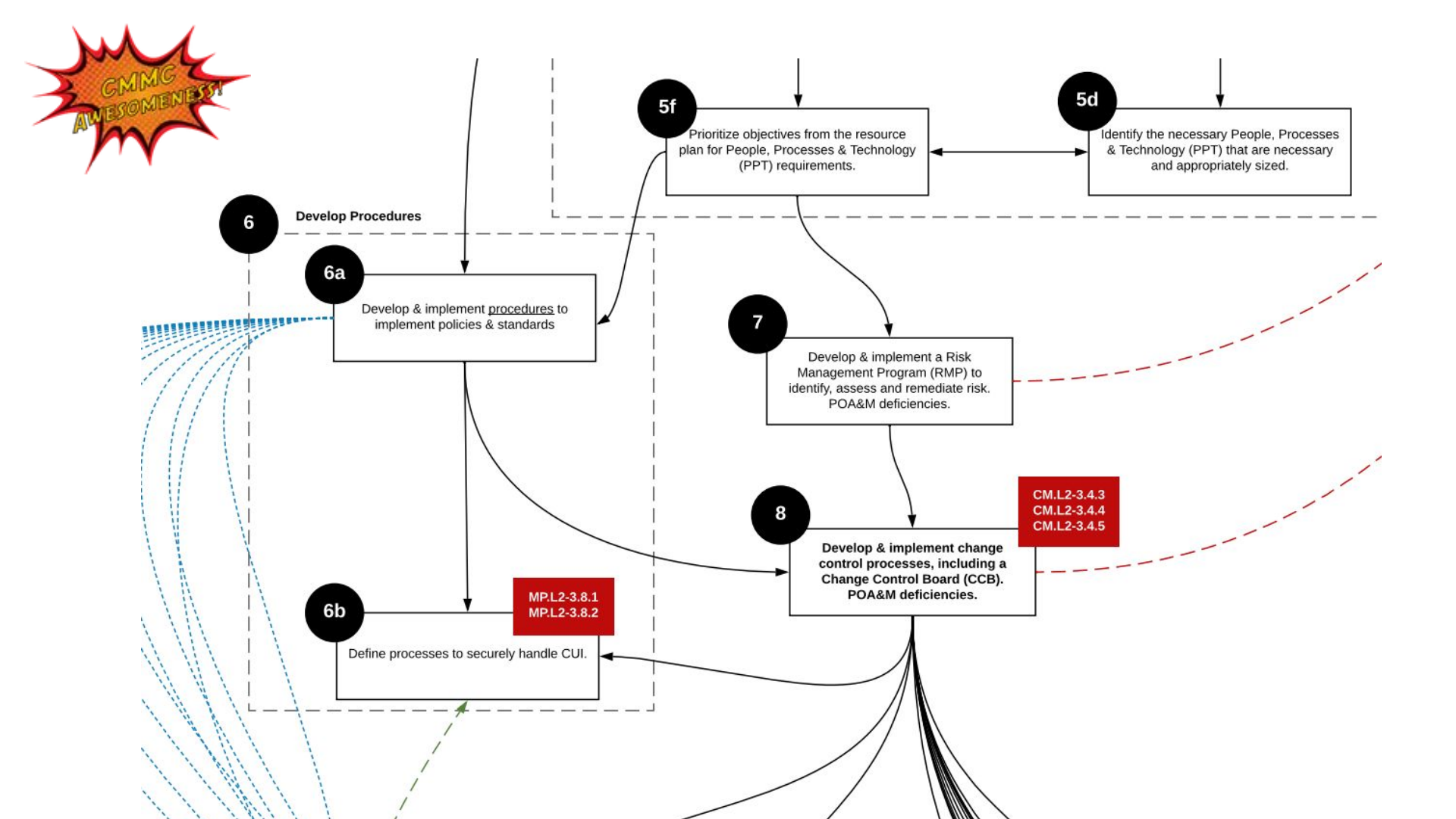
3a CA.L2-3.12.4

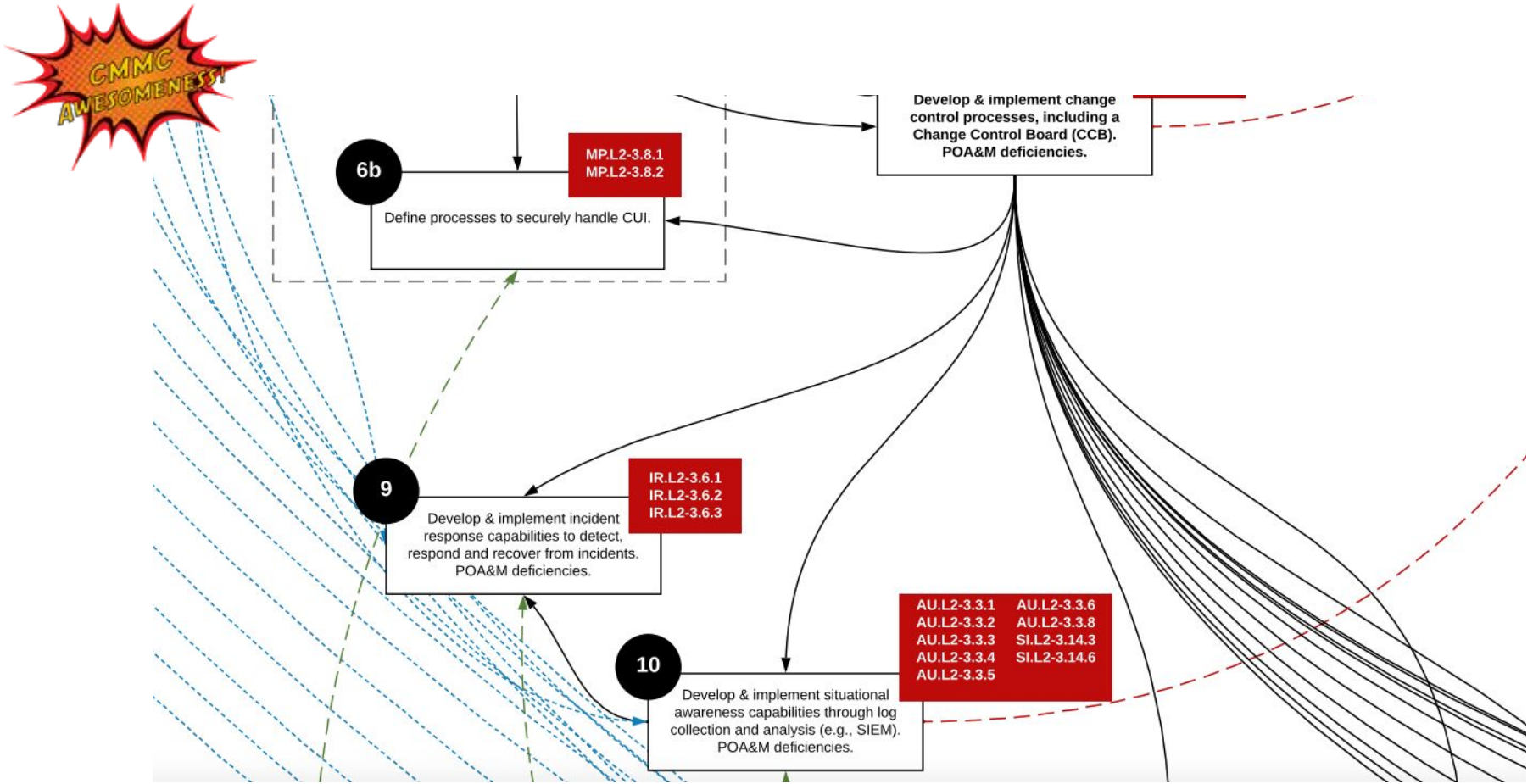
Start populating the System Security Plan (SSP). POA&M deficiencies

3b CA.L2-3.12.2

Create a Plan of Action & Milestone (POA&M) to track and remediate deficiencies.

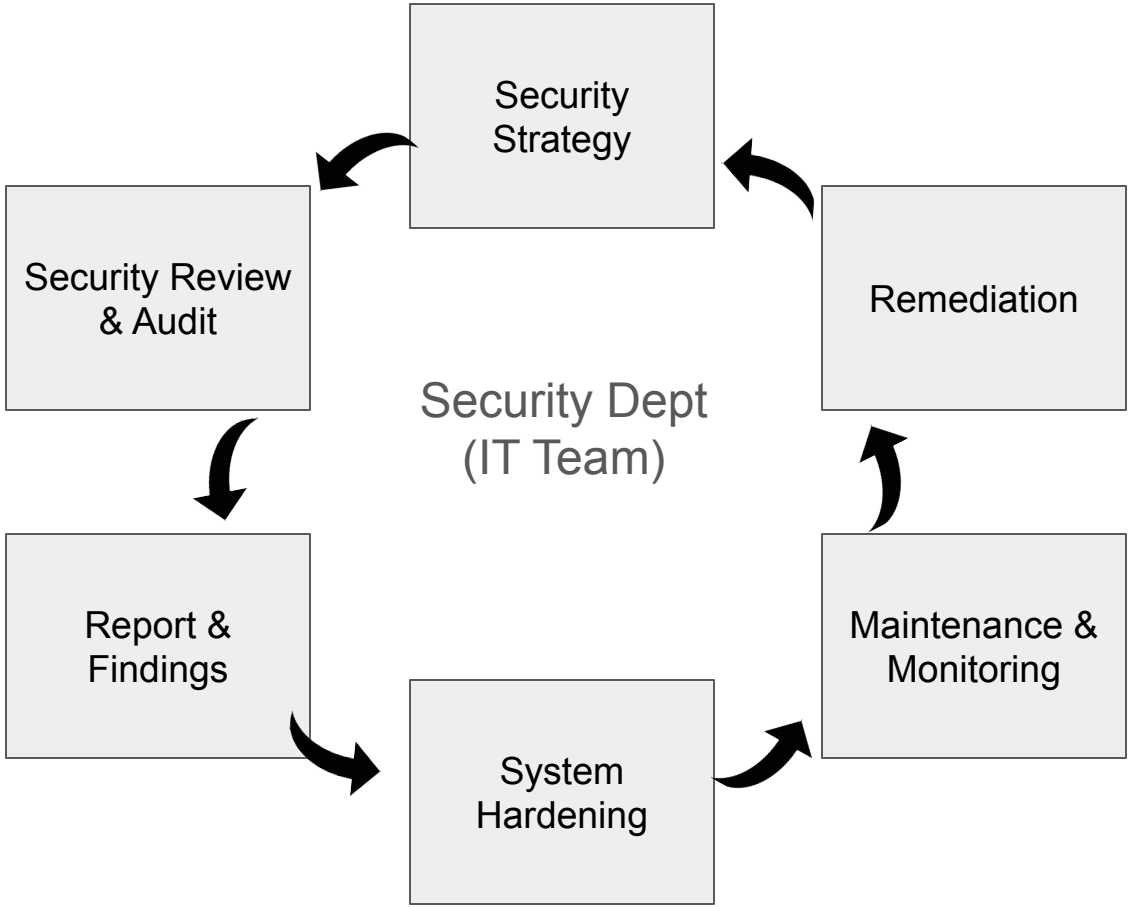

CMMC AWESOMENESS!
4
Implement a network architecture that ensures it is built on secure engineering principles and enclaves. POA&M deficiencies.
SC.L1-3.13.1
SC.L2-3.13.2
SC.L1-3.13.5
SC.L2-3.13.6
5
Plan, Identify Gaps & Prioritize Resources
5a
Define applicable statutory, regulatory and contractual obligations (including DFARS, FAR, NIST 800-171 and CMMC)
5b
Perform a gap assessment from applicable statutory, regulatory and contractual obligations (step 4). POA&M deficiencies.
5c
Develop & implement policies and standards to address applicable statutory, regulatory and contractual obligations.
5d
Identify the necessary People, Processes & Technology (PPT) that are necessary and appropriately sized.
5e
Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to meet compliance obligations.
5f
Prioritize objectives from the resource plan for People, Processes & Technology (PPT) requirements.


CMMC AWESOMENESS!
5f
Prioritize objectives from the resource plan for People, Processes & Technology (PPT) requirements.
5d
Identify the necessary People, Processes & Technology (PPT) that are necessary and appropriately sized.
6
Develop Procedures
6a
Develop & implement procedures to implement policies & standards
7
Develop & implement a Risk Management Program (RMP) to identify, assess and remediate risk. POA&M deficiencies.
8
CM.L2-3.4.3
CM.L2-3.4.4
CM.L2-3.4.5
Develop & implement change control processes, including a Change Control Board (CCB). POA&M deficiencies.
6b
MP.L2-3.8.1
MP.L2-3.8.2
Define processes to securely handle CUI.


CMMC AWESOMENESS!
Develop & implement change control processes, including a Change Control Board (CCB). POA&M deficiencies.
6b
MP.L2-3.8.1
MP.L2-3.8.2
Define processes to securely handle CUI.
9
IR.L2-3.6.1
IR.L2-3.6.2
IR.L2-3.6.3
Develop & implement incident response capabilities to detect, respond and recover from incidents. POA&M deficiencies.
10
AU.L2-3.3.1
AU.L2-3.3.2
AU.L2-3.3.3
AU.L2-3.3.4
AU.L2-3.3.5
AU.L2-3.3.6
AU.L2-3.3.8
SI.L2-3.14.3
SI.L2-3.14.6
Develop & implement situational awareness capabilities through log collection and analysis (e.g., SIEM). POA&M deficiencies.

Security **Strategies**

MONTAGE MARKETING



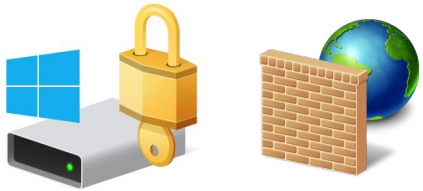
Infrastructure

Cloud

Before

Microsoft Intune

Microsoft Defender



Admin By Request

Addigy

NIST

800-53

Infrastructure

Cloud

After

jamf | CONNECT

Microsoft Intune

jamf | PRO

Microsoft Defender

ARCTIC WOLF

Admin By Request

NIST 800-171

Microsoft Defender

ARCTIC WOLF

NIST 800-171

scipag/
HardeningKitty

HardeningKitty - Checks and hardens your Windows configuration

R33Dfield/
WindowsHardening

Intune configuration files for Windows 10 and 11 hardening

macOS Security Compliance

Bob Gendler

Mac Specialist @ NIST

LinkedIn: @boberito

MacAdmins Slack: @boberito

Organizational

User Education

1. Disaster Recovery Planning
2. Security Awareness Training
3. SOP for Security Incident (Incident Response) for staff and leadership
4. Incident Response Planning (And Incident Response Plan Document)
5. Acceptable Use Policy
6. Organizationational Handbook Review
7. Code of Conduct Review
8. BYOD Policy (Not yet written but we are starting the conversations)
9. Documentation on how to use critical systems.
    a. Naming conventions and how to organize data
    b. How to find information.
    c. How to archive information.

Disaster Recovery | Access Control | Information

1. Access Control Policy
2. Business Impact Analysis
3. Inventory Management best practices implemented
4. Business Impact Assessment
5. Disaster Recovery Plan
6. System Security Plan
7. Implementation of Arctic Wolf
    a. Implementation of Sensors and log integration with all SaaS tooling into their SEIM tooling into their 24X7 SOC for Monitoring.
8. Implemented Drata for Compliance & Supply Chain Management
9. Implementation of Druva for Backups (TBD)
10. Implementation of Box.com for protection of CUI (Retention)

Encryption | Application | Network

1. Implementation of Bitlocker & Filevault
    a. Macadmins / escrow-buddy
2. Hardening of O365 using
    a. Harden365/Harden365
    b. soteria-security/Soteria Inspect
3. Hardening of Meraki (Meraki Security Baseline)
    a. iramku/Meraki-Security-Baseline
4. Cisco Umbrella
5. Arctic Wolf
    a. SaaS Integration
    b. AWS / Azure / Defender Integration

EscrowBuddy

Soteria Inspect

Security

Compliance

Processes & Controls

- REV 4 FedRAMP SSP Moderate Baseline Template
- 800-53ar5 Assessment Procedures
- 800-53 Control Baselines
- 800-53 Controls
- 800-53 Crosswalk
- CMMC Self Assessment Guide
- CMMC Center of Awesomeness (2022.3)
- Microsoft Product Placemat for CMMC

Policies from SANS Institute

- Acceptable Encryption Policy
- Acceptable Use Policy
- Acquisition Assessment Policy
- Antivirus Guidelines
- Artificial Intelligence Policy
- Automatically Forwarded Email Policy
- Bluetooth Baseline Requirements Policy
- CFIHF Incident Response Identification Policy
- + 25 More

MONTAGE MARKETING

At the end of the day **we picked the right processes, technology, and tools, that came together to protect our organization.**

Questions?