



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



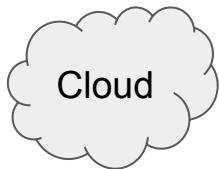
What Makes Up Cybersecurity?

Frameworks



Security

Infrastructure



Network

Organizational

Information

Access

Application

Encryption

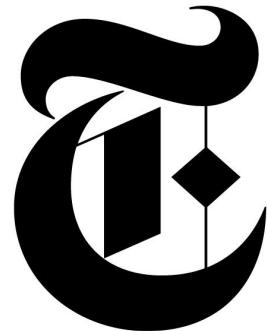
User Behavior

User Education

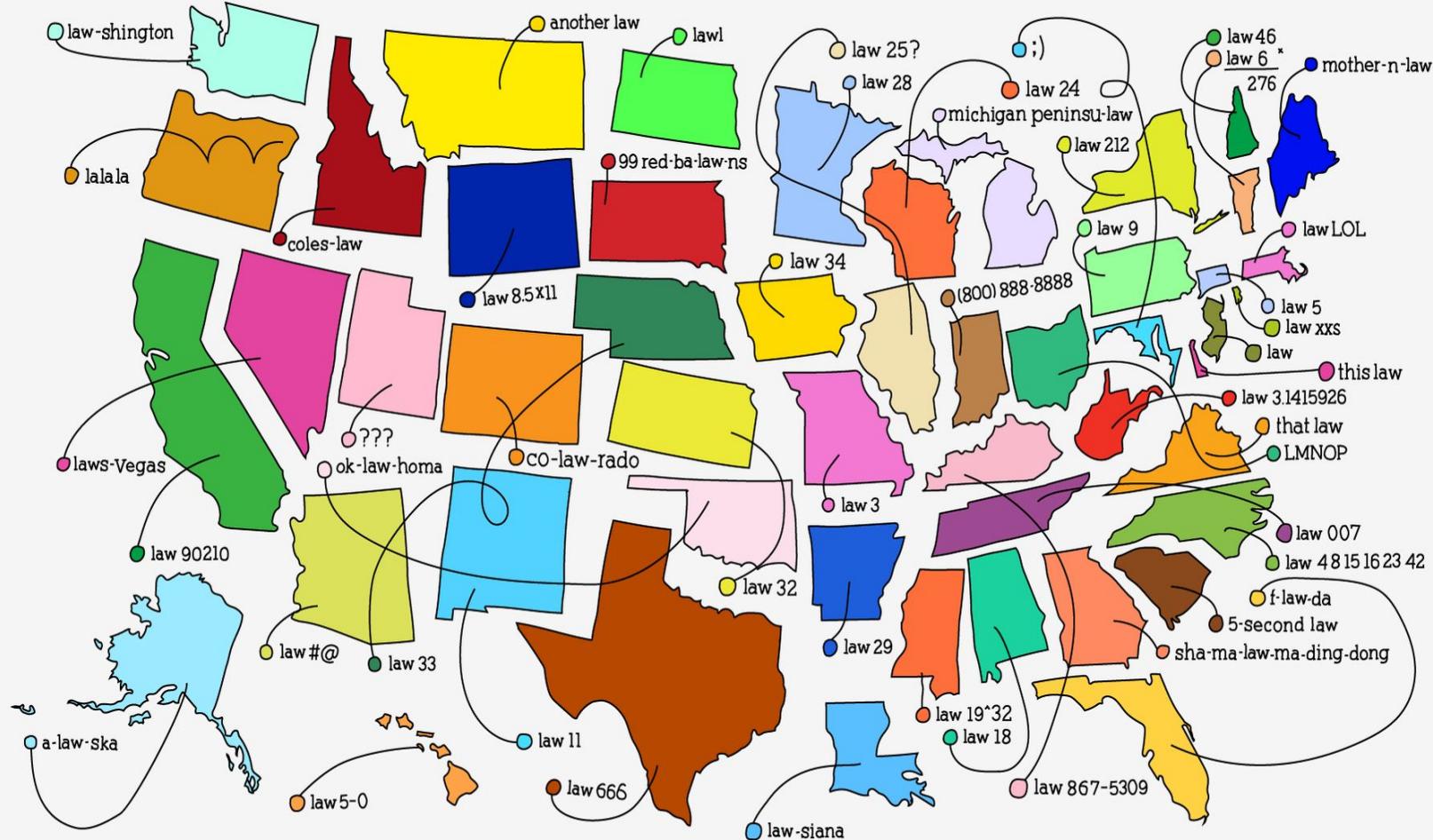
Disaster Recovery

Laws





Our expertise,
your peace of mind



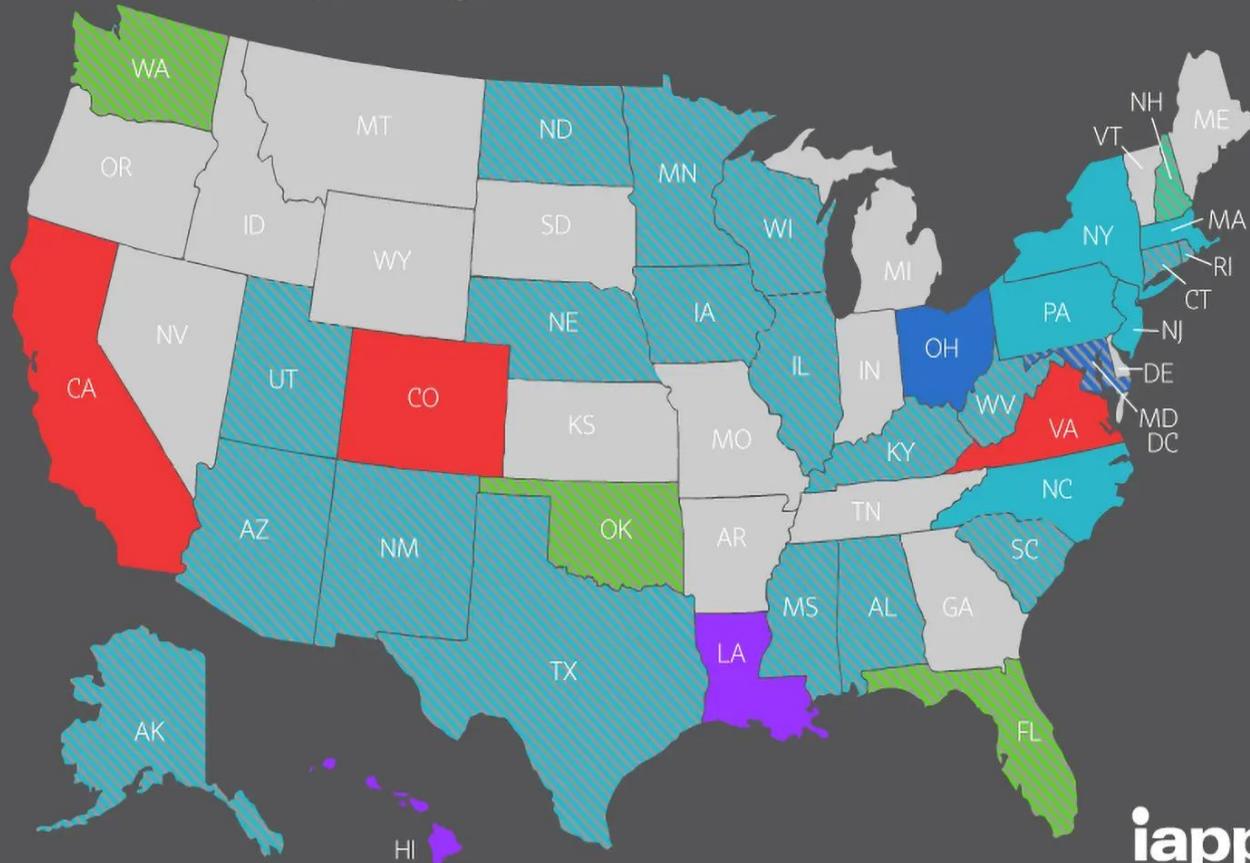
US State Privacy Legislation Tracker



- Task Force Substituted for Comprehensive Bill
- Bill Died in Committee or Postponed
- None

Statute/Bill in Legislative Process:

- Introduced
- In Committee
- Cross Chamber
- Cross Committee
- Passed
- Signed



Last updated: 7/28/2021

iapp

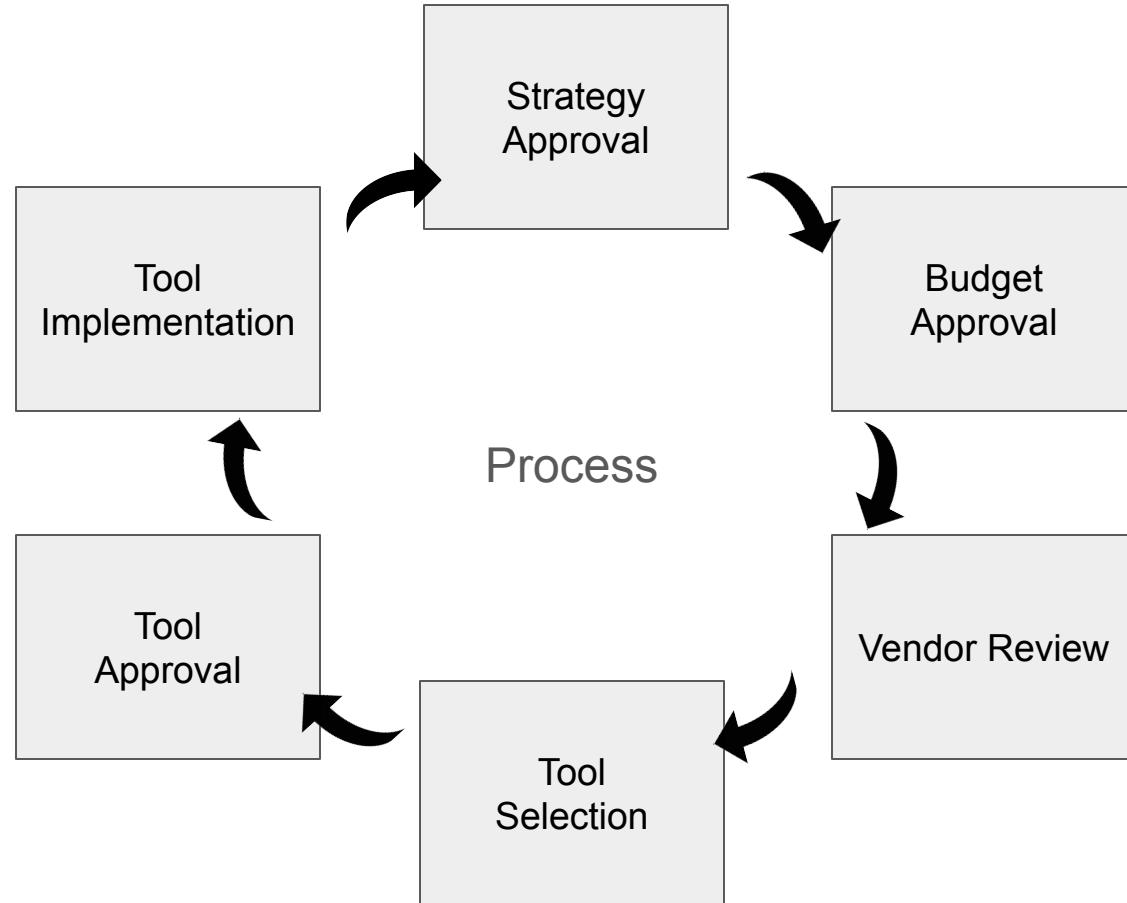




Business Strategies



MONTAGE
MARKETING



Cybersecurity Strategies

Requirements

NIST

800-53



20 Domains
316 Controls

NIST

800-171



14 Domains
110 Controls

Security

Disaster Recovery

Access Control

Information

Organizational

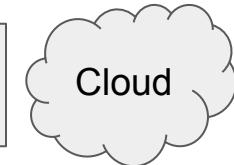
Infrastructure

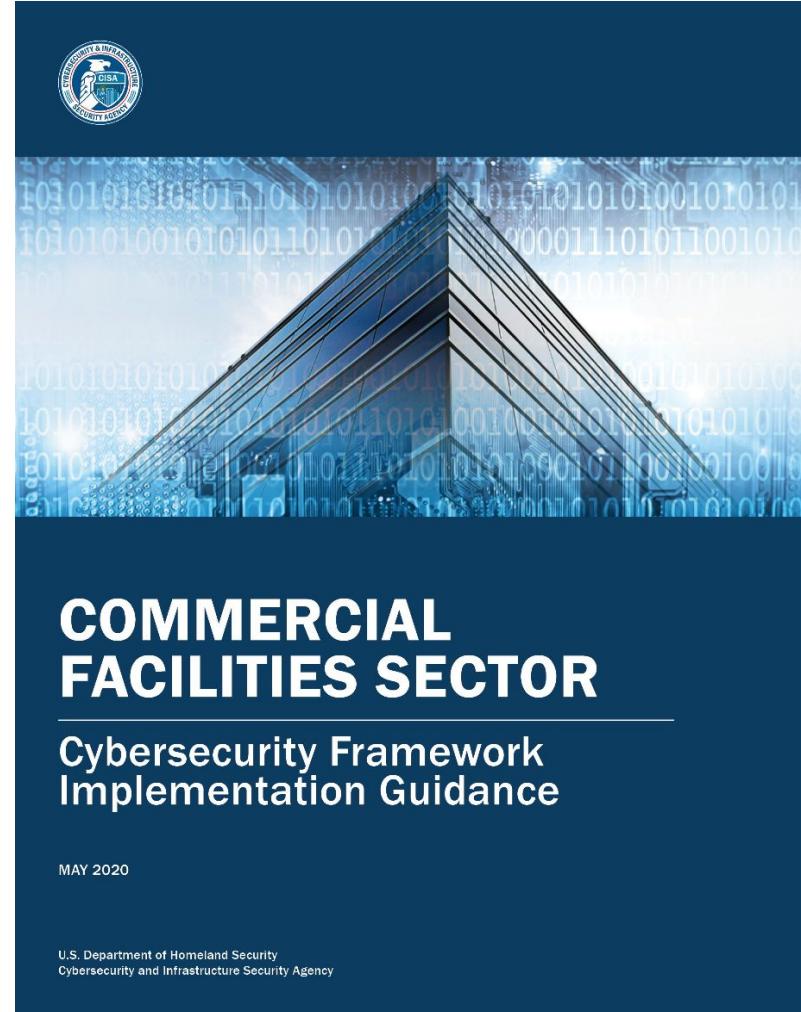
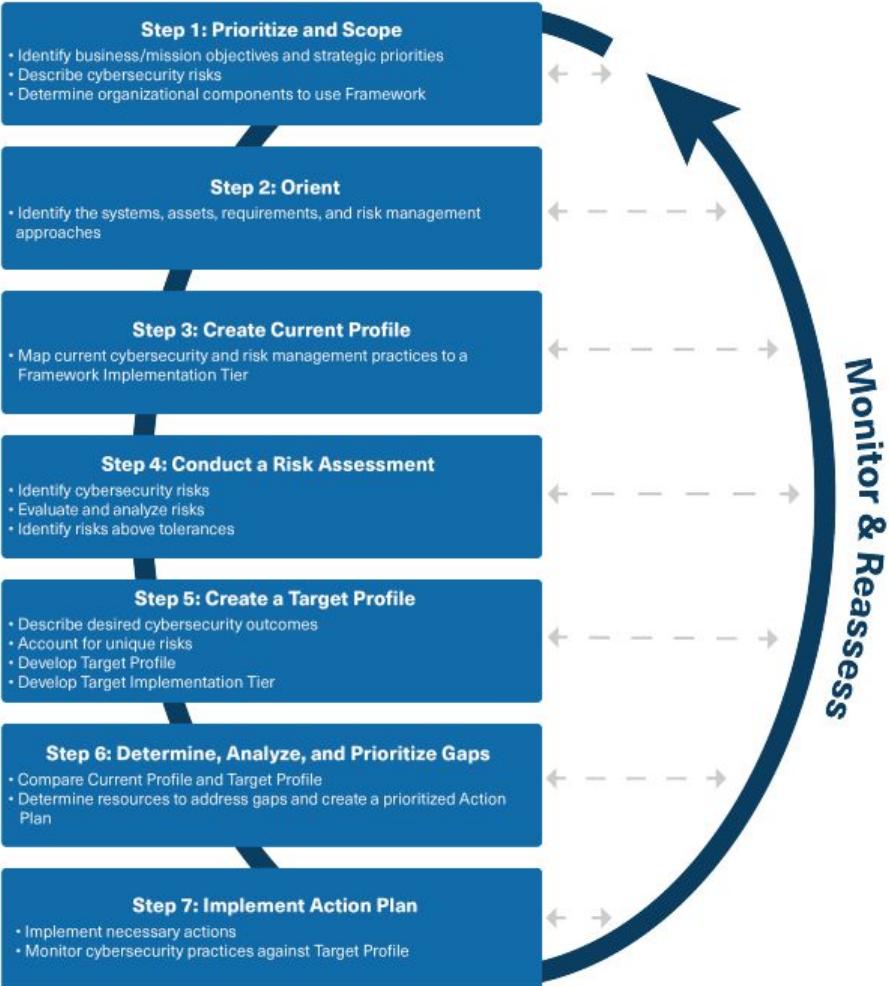
User Education

Encryption

Application

Network





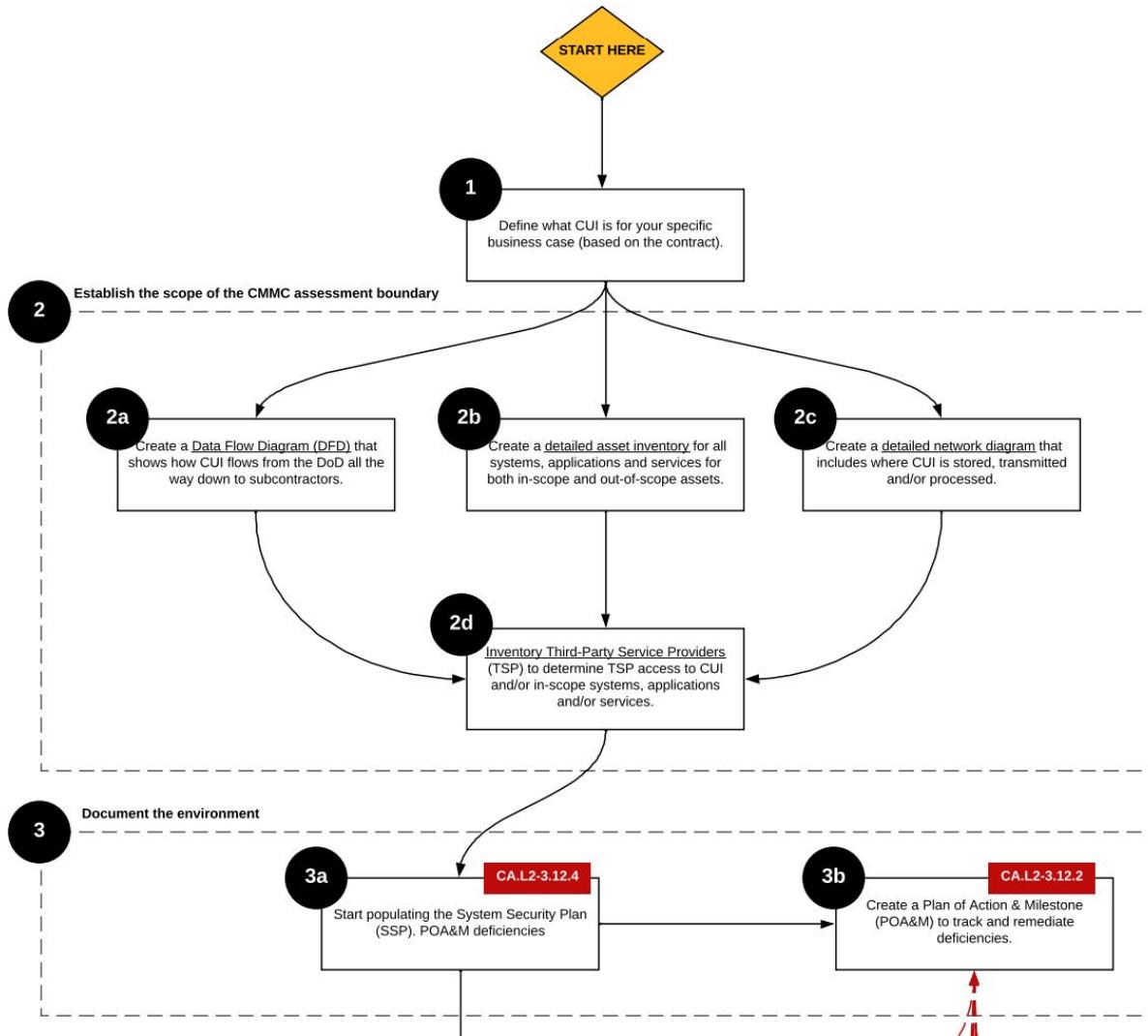


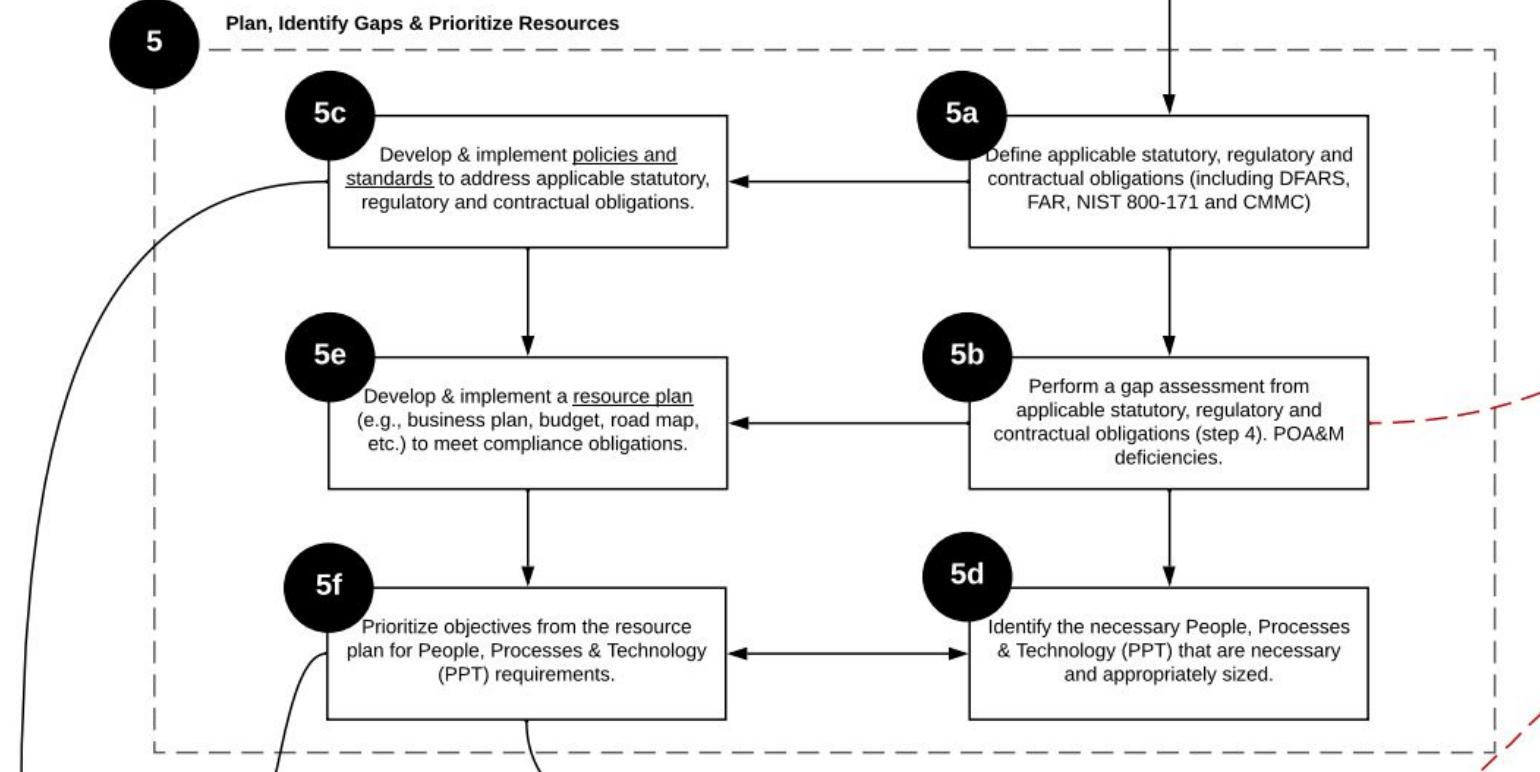
MONTAGE
MARKETING

Compliance

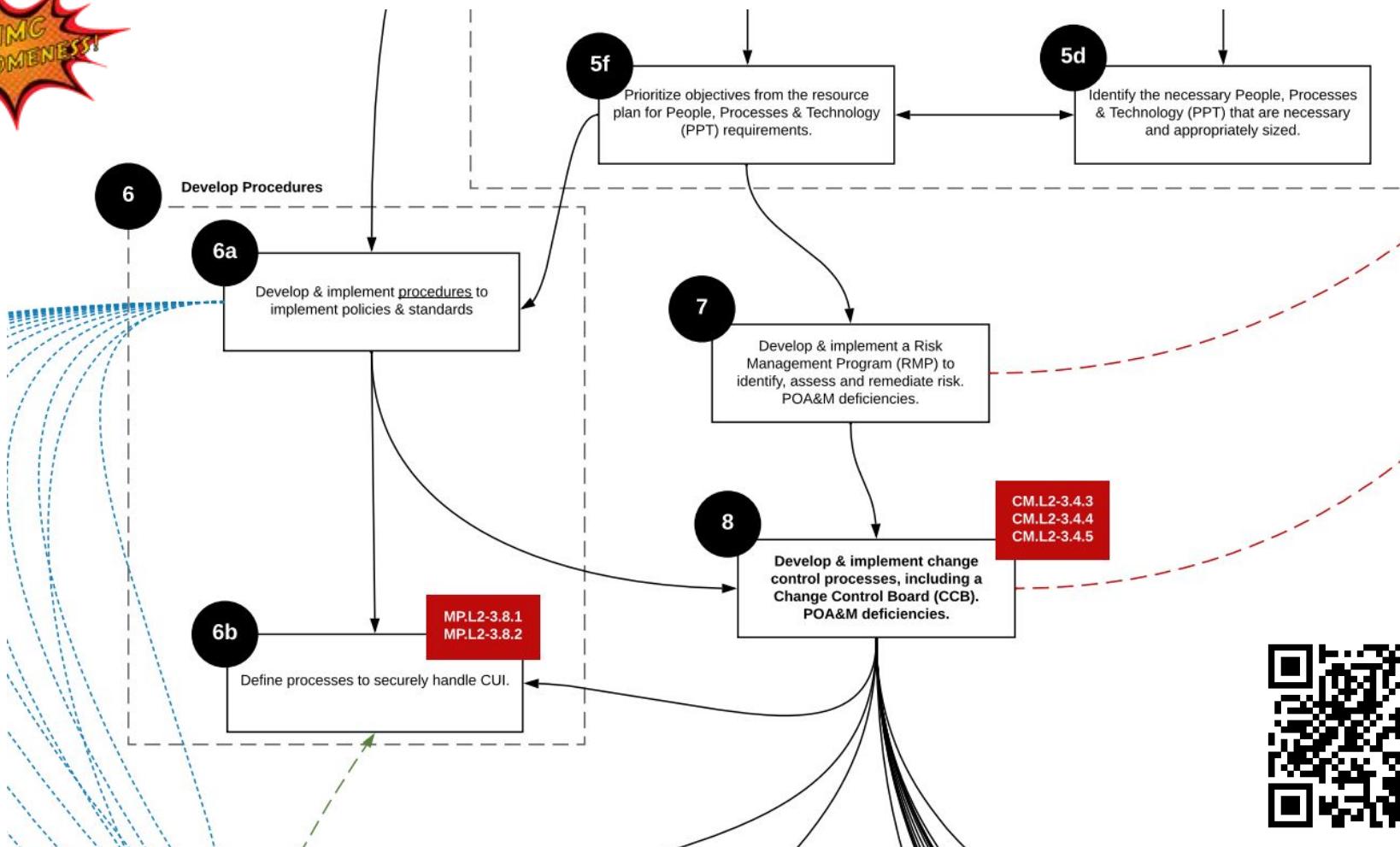


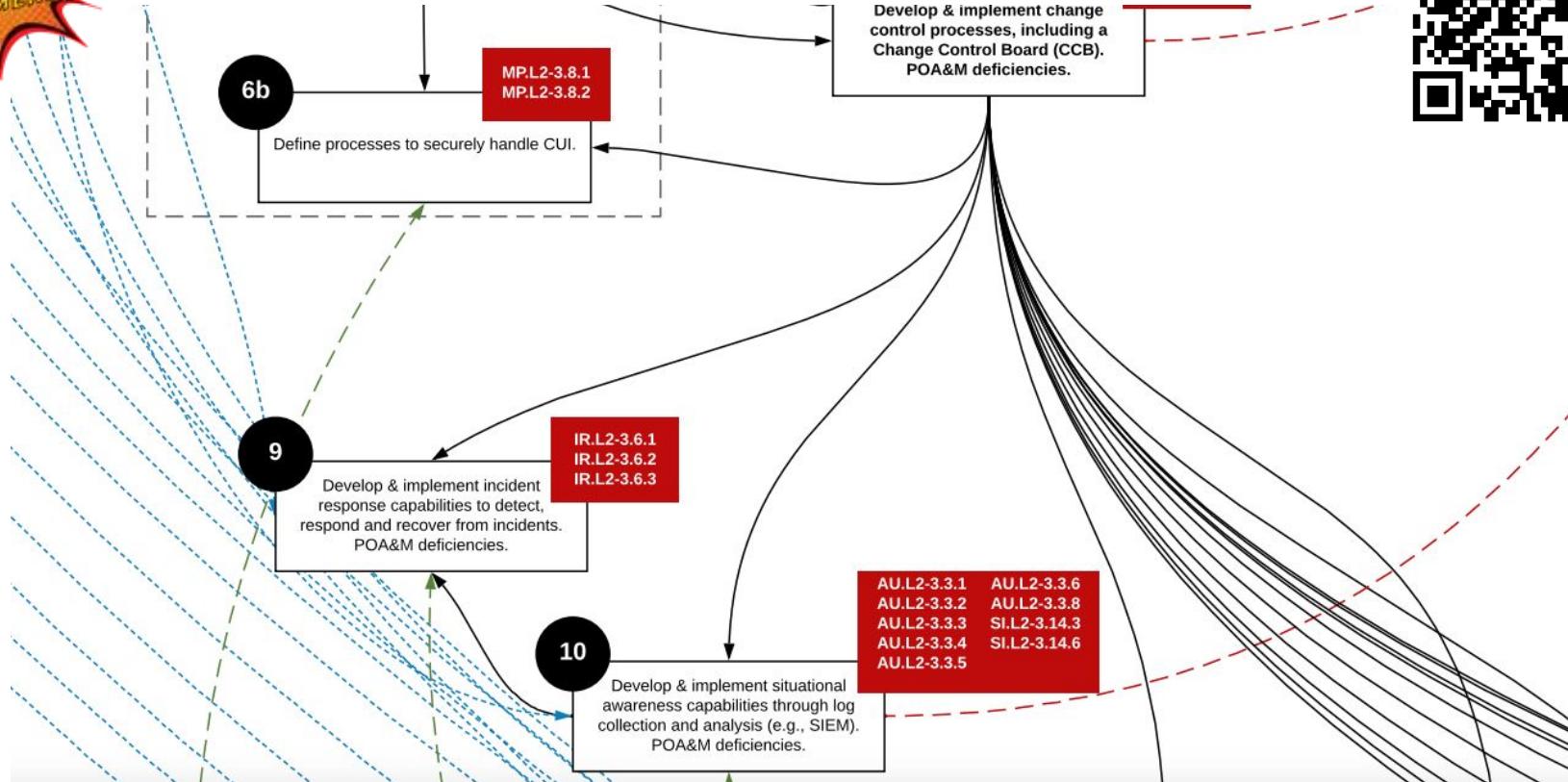
Multiple Strategies





SC.L1-
SC.L2-
SC.L1-
SC.L2-



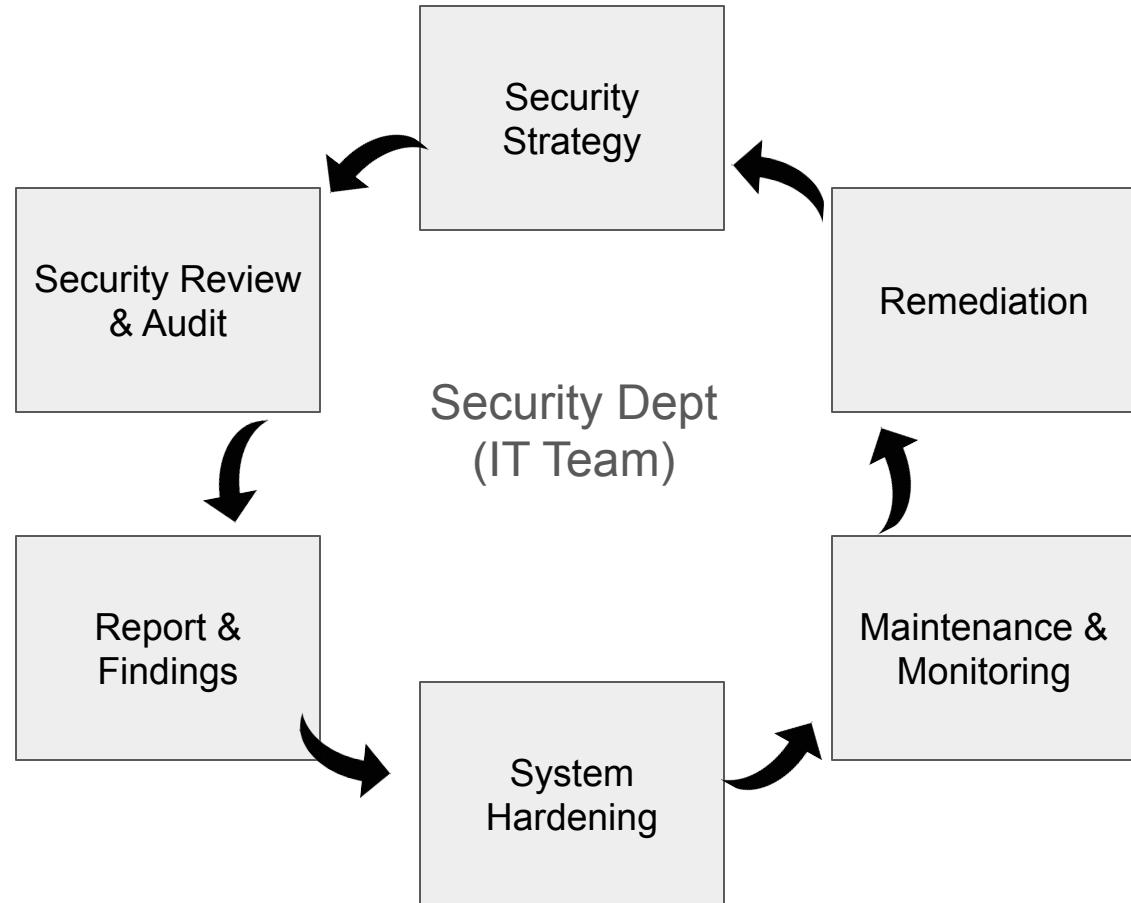


Security Strategies

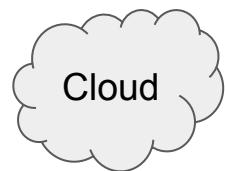


MONTAGE
MARKETING

Security



Infrastructure



Before

Microsoft Intune



Microsoft
Defender



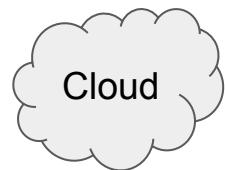
Admin By Request

Addigy

NIST
800-53



Infrastructure



After



Microsoft Intune



Admin By Request

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



jamf CONNECT

jamf PRO



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. Organizational 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



RAPID7



CISCO
Meraki

CISCO.
Cisco
Umbrella

/LIBRAESVA
LetsDMARC

Compliance



DRATA



druva



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

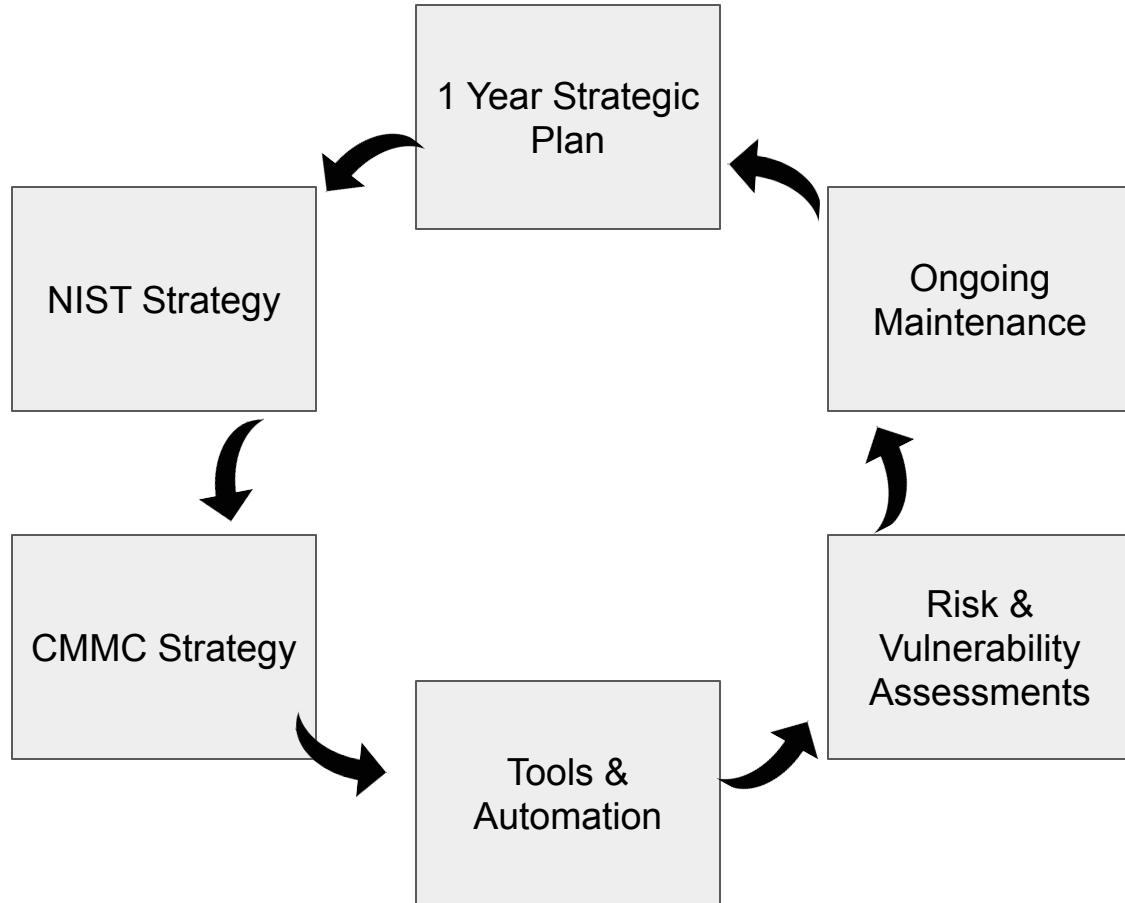
Policies from SANS Institute

- 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

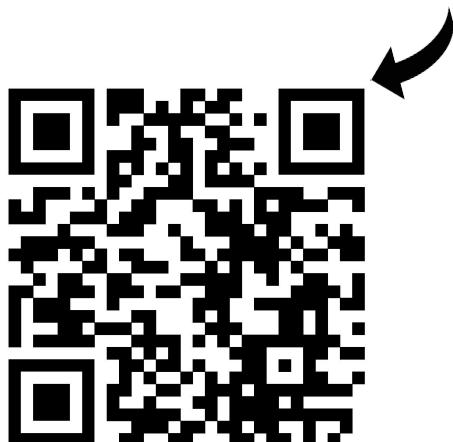
Security



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

Questions?

Download



Review

