TEXAS RE

CIP-010-4 R4 and CIP-003-8 R2 Section 5 TCA & RM Internal Controls

Kenath Carver
Director, Compliance Assessments

October 6, 2023

TCA & RM Internal Controls

Inventory

Database

Monitoring

Alerting

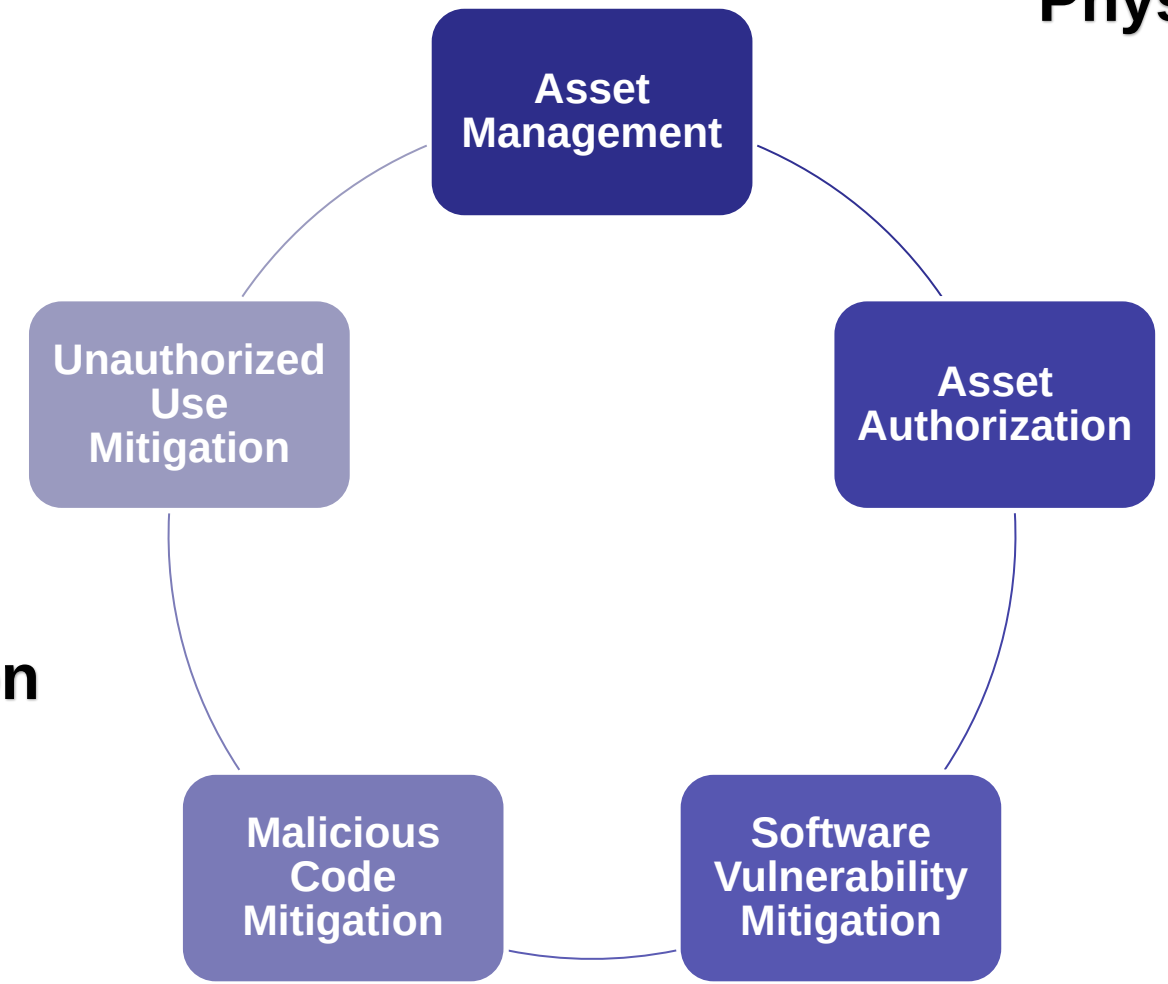
Port Blocking

Data Loss Prevention

Network Segmentation

Training

Chain of Custody



Physical Access Controls

Access Management

Encryption

MFA

Patch Management

Signature Updates

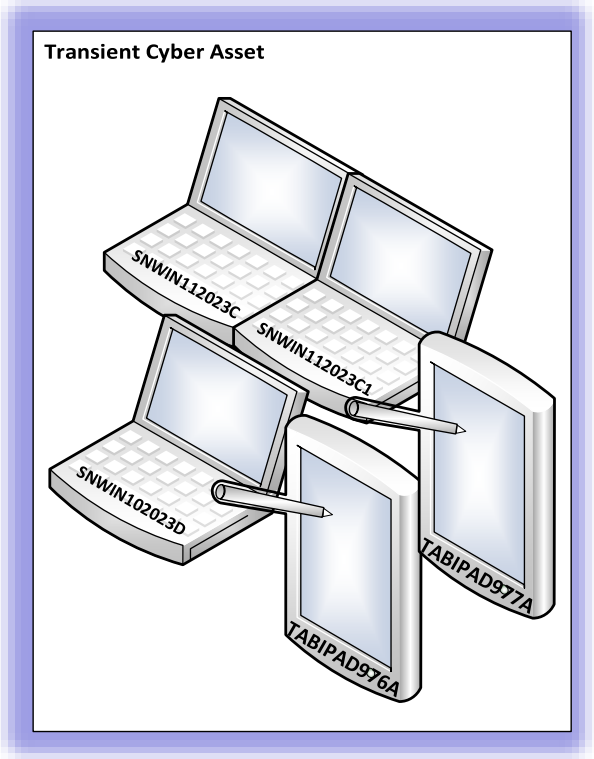
Anti-Virus Software

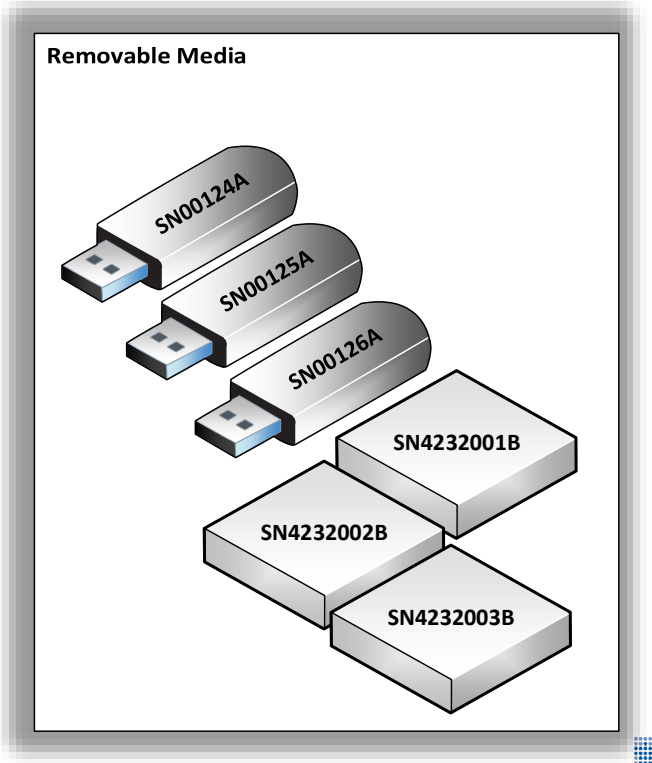
Whitelisting

Contracts/SLA

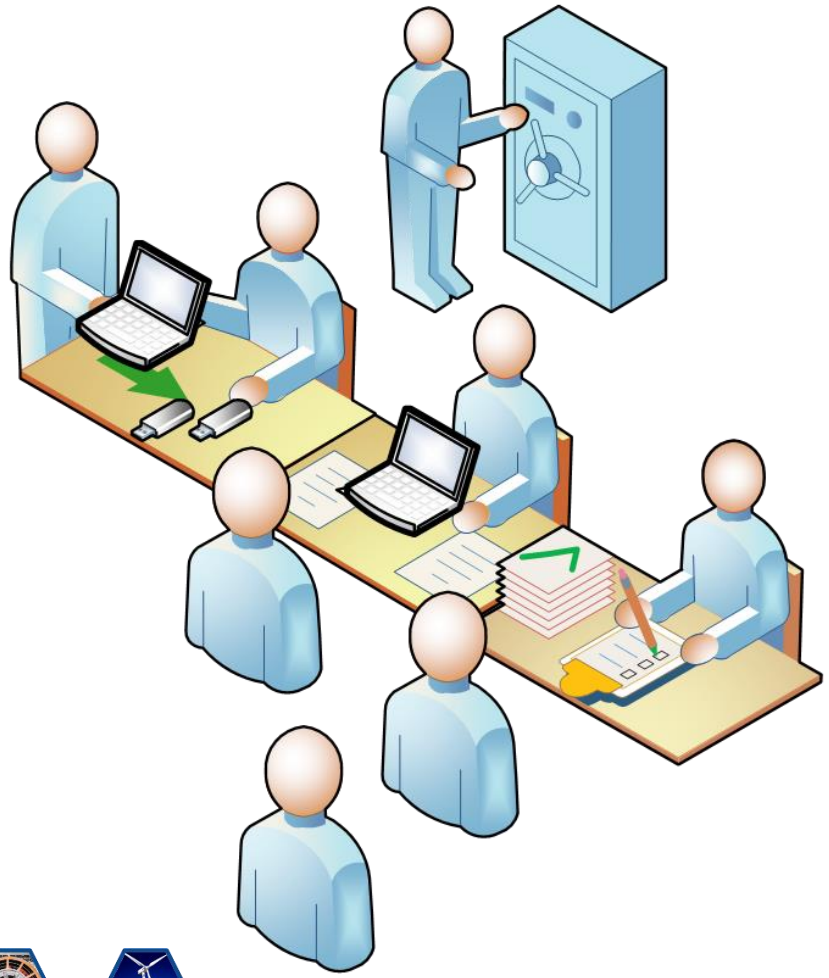
Procedures/Plans

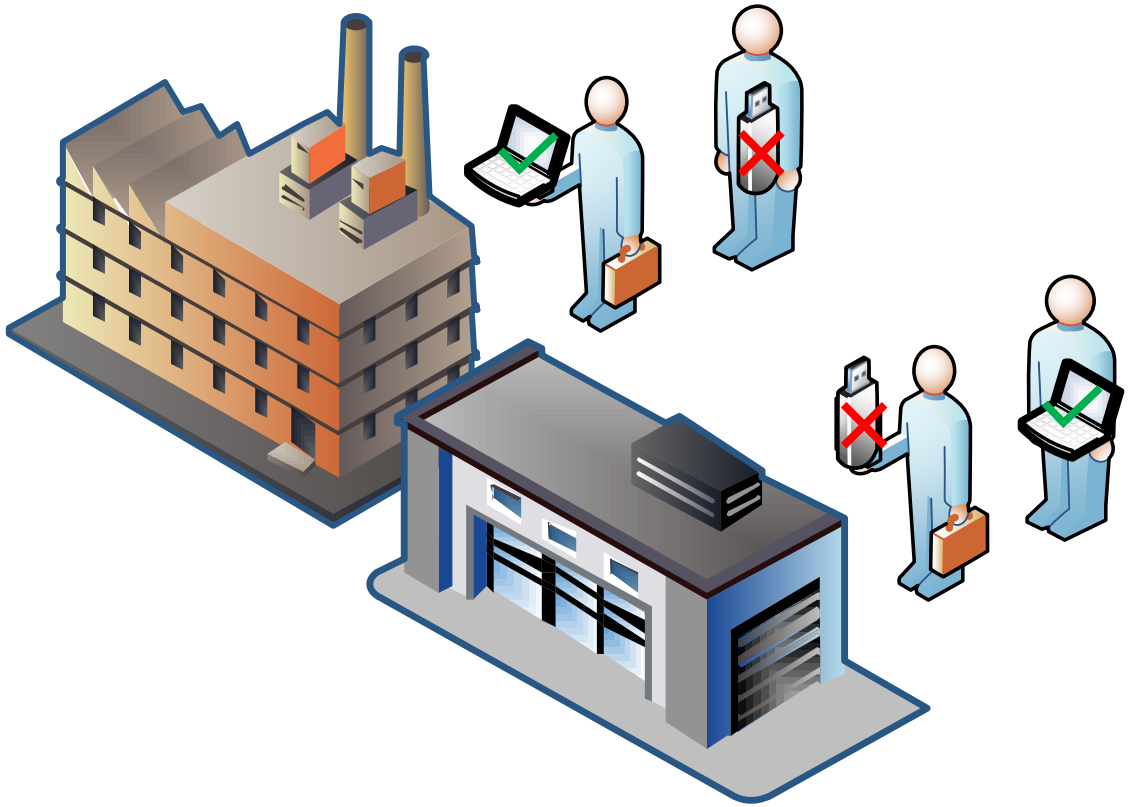
TCA & RM Internal Controls – Asset Management



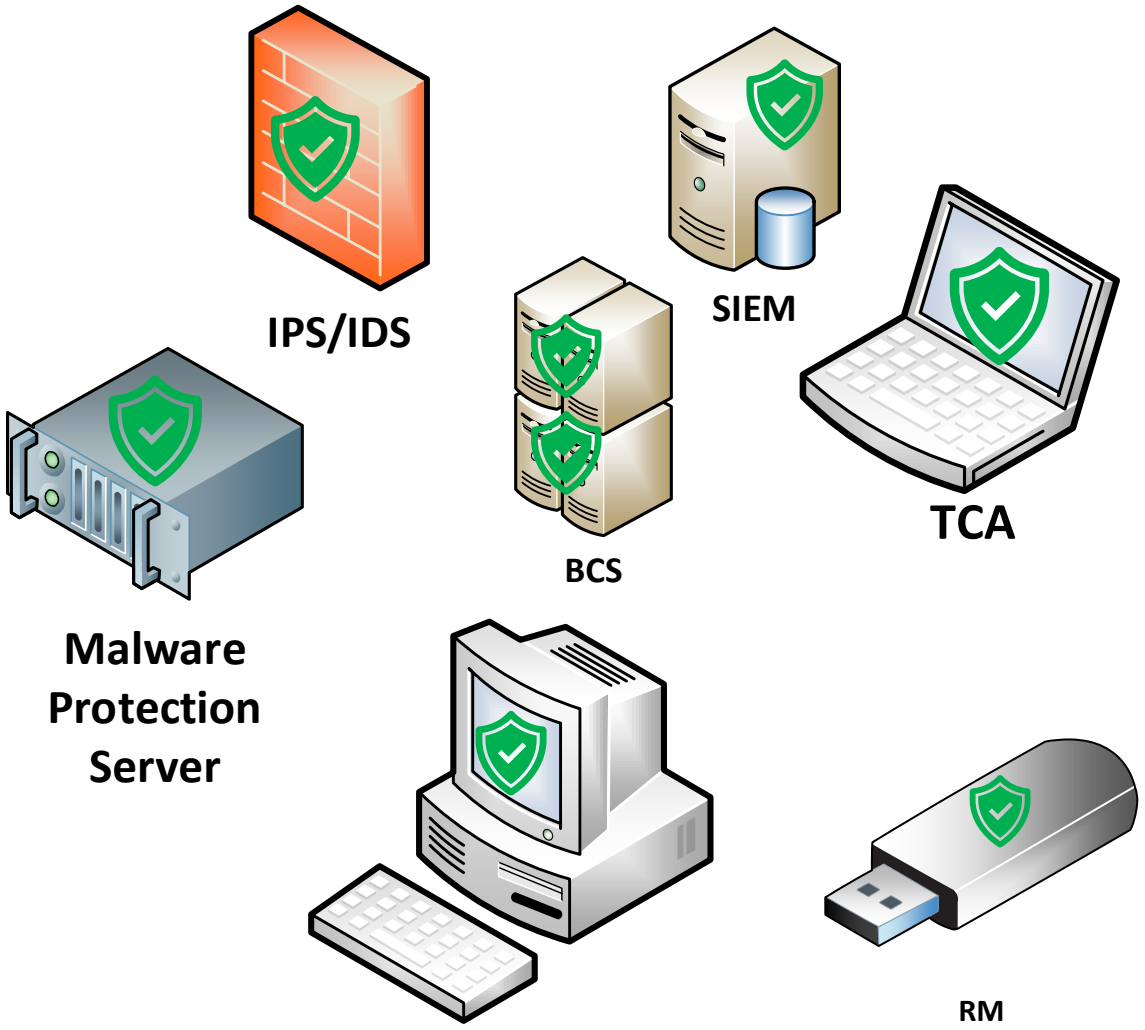


TCA & RM Internal Controls – Asset Authorization





TCA & RM Internal Controls – Malicious Code Mitigation



- Frequency of Scans
- Thoroughness of Scans
- Signature Update Frequency
- Anti-virus/Whitelisting/Etc.
- Quarantine
- Port Blocking
- Monitoring/Alerting
- Logs

NSA/CISA - Top Ten Cybersecurity Misconfigurations

- Default configurations of software and applications
- Improper separation of user/administrator privilege
- Insufficient internal network monitoring
- Lack of network segmentation
- Poor patch management
- Bypass of system access controls
- Weak or misconfigured multifactor authentication (MFA) methods
- Insufficient access control lists (ACLs) on network shares and services
- Poor credential hygiene
- Unrestricted code execution

TEXAS RE
Ensuring electric reliability for Texans

Upcoming Events