DOT Traffic Management Centers Cyber Security Assessment Methodology

John Contestabile
Israel Anthony Lopez
December 2023

SKYLINE
TECHNOLOGYSOLUTIONS

Need to assess Cyber at DOT's

- While IT security for the enterprise has developed as the threat has emerged/evolved, the OT security environment has not kept pace.
- In the past, the OT network of field devices was on a separate network….not so anymore
- The OT network[s] are typically operated by the maintenance/operations part of the DOT whereas the enterprise network is operated by the CIO/IT part of the organization.
- The IT staff, while having responsibility for cyber security, may not have the expertise to deal with OT networks which are typically a collection of fiber/wireless/cellular service providers and endpoint equipment which is not familiar

SKYLINE TECHNOLOGYSOLUTIONS

TRAFFIC NETWORKS

- **Operational Technology**
- Networks with field devices serving business functions
- Low rate of change
- Limited Internet Access

TMC

ATMS

BUSINESS NETWORKS

DOT Business/ Enterprise Network

- **Information Technology**
- Network supporting users with office products
- High change
- Extensive Internet access

EXTERNAL NETWORKS

- Traffic data consumers and producers
- Need controlled means for exchanging digital data

Partners
Jurisdictions
Media
Public Safety

Internet
Public

SKYLINE TECHNOLOGYSOLUTIONS

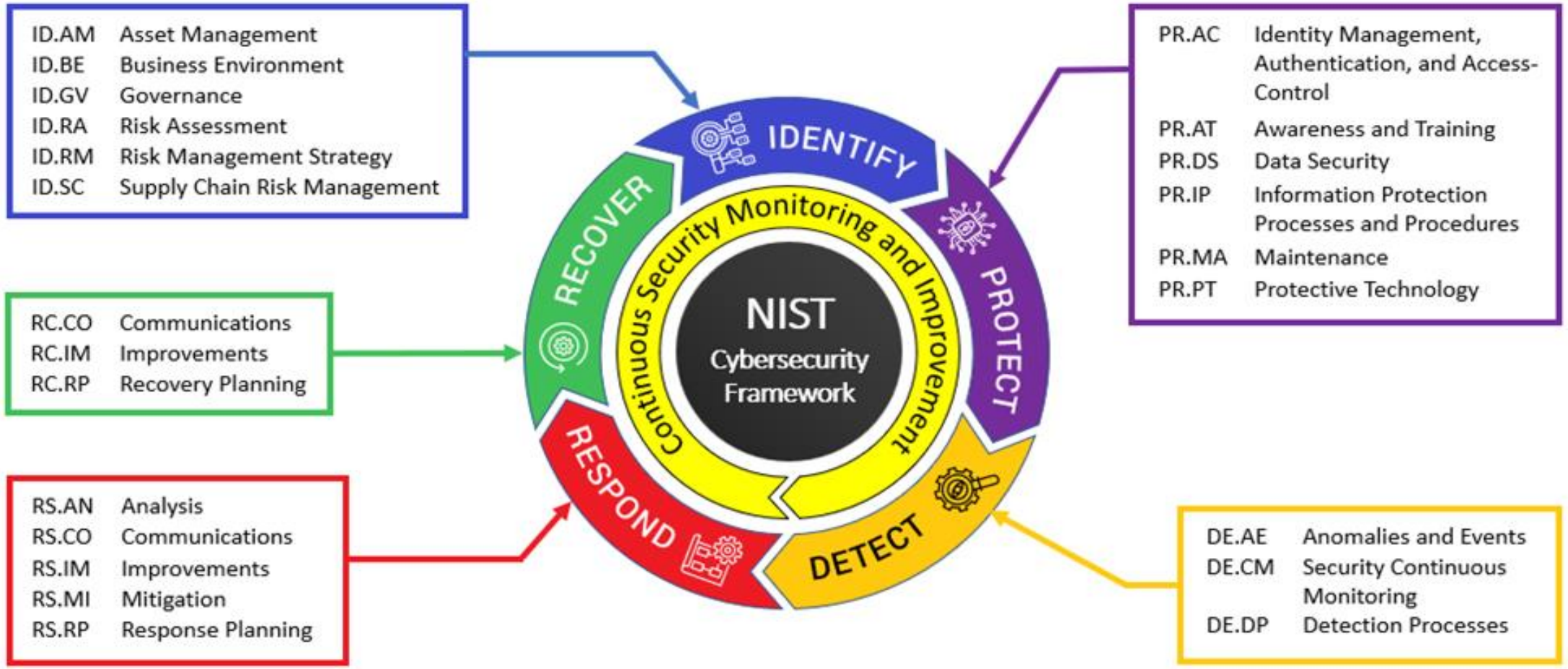
Methodology

Skyline utilizes the National Institutes of Technology (NIST) Cybersecurity Framework (CSF) v 1.1 as the guiding framework for conducting the assessments. The assessment incorporated several other source documents in developing an IT and OT questionnaire for the initial evaluation. Those sources include:

- The National Cooperative Highway Research Program (NCHRP) Project 03-127 "Cybersecurity of Traffic Management Systems"
- NIST Security and Privacy Controls for Information Systems and Organizations, Special Publication (SP) 800-53 Revision 5 (Special Publication (SP) 800-53r5)
- The Federal Highway Administration's Technical Report on "Transportation Management Center IT Security"

SKYLINE TECHNOLOGYSOLUTIONS

Methodology – NIST CSF



See: Cybersecurity Framework | NIST

Methodology – DHS CISA

Department of Homeland Security – Cyber Infrastructure Security Agency [DHS-CISA] – March 2023 update

"CISA's Cybersecurity Performance Goals (CPGs) are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. These voluntary CPGs strive to help small- and medium-sized organizations kickstart their cybersecurity efforts by prioritizing investment in a limited number of essential actions with high-impact security outcomes."

See: Cross-Sector Cybersecurity Performance Goals | CISA

SKYLINE TECHNOLOGY SOLUTIONS

Skyline DOT TMC Cyber Assessment Approach

Privva Questionnaire
Each Region completed the questionnaire / survey and was interviewed.

NIST CSF Codes
Each question is associated with a NIST CSF category.

Finding
A series of issues are identified, and finding are developed based on the survey.

CISA CPG Codes
The NIST CSF Codes are mapped to the CISA CPGs.

Themes
A group of findings that are similar, both as a finding and as steps to resolution.

SKYLINE TECHNOLOGYSOLUTIONS

Methodology

Results in the identification of various issues and findings for both IT and OT systems as well as recommendations.

Key IT Issues - Executive Summary – A Systemwide Perspective							
Threat	**NIST CSF Domain**	**Vulnerability**	**Asset**	**Impact**	**Likelihood**	**Risk**	**Control Recommendations and Assessment**
1. Lack of Lifecycle Management.	Identify	High	Critical	Critical	High	High	Critical
	The ability to identify is reduced due to the lack of life cycle management planning for devices and software.	Inadequate life cycle planning for IT operations and cybersecurity.	All - This applies to devices, software, and infrastructure.	All devices and services (ATMS, FMS, ATIS, and others) may be affected for an unknown period.	The likelihood that the TMC does not have a fully vetted replacement lifecycle plan which will affect recovery is high.	Potential loss from $10,000 to $10,000,000	Lifecycle management should involve developing a plan to identify replacement needs, plan for replacement, and to budget the replacement of equipment, hardware, software, and licensing.

Example of an IT Issues/Executive Summary

SKYLINE TECHNOLOGYSOLUTIONS

Methodology

Key OT Issues - Executive Summary – A Systemwide Perspective							
Threat	**NIST CSF Domain**	**Vulnerability**	**Asset**	**Impact**	**Likelihood**	**Risk**	**Control Recommendations and Assessment**
1. Lack of Vulnerability Management.	Detect	High	Critical	Critical	High	High	**Critical**
	The ability to Detect is limited due to the lack of vulnerability management for devices and software.	Inadequate vulnerability management.	All - This applies to devices, software, and infrastructure.	All services (ATMS, FMS, ATIS, field network, and other services) may be affected for an unknown period.	The likelihood that most vulnerabilities are not tracked is high.	Potential loss from $10,000 to $10,000,000	Configure a vulnerability scanner to scan a test environment to confirm settings that incorporates device types sensitive to scanning and test the various firmware versions. Begin scanning the network for vulnerabilities.

Example of an OT Issues/Executive Summary

SKYLINE TECHNOLOGYSOLUTIONS

Methodology

The Questionnaire was followed by an in-person field visit to review the answers and observe equipment installations/configurations.

The assessment yields a rating that identified areas of concern warranting a greater focus.

Table 1 – IT and OT Results Table

Environment Area	Rating	Issues	Critical	High	Medium	Low
IT	58%	39	7	11	14	7
OT	56%	33	12	7	6	8

Example of the IT/OT Results

11 Typical Transportation Themes across both IT/OT

1. IT and OT Boundary Standard
2. Security Hygiene
3. Network Documentation
4. Network Services Architecture
5. Identity Management, Passwords, and MFA
6. Log Management, SIEM, and Time Servers
7. Governance: Policies and Procedures
8. Asset Inventory and Management
9. Personnel Training
10. Vulnerability Management
11. Email Security

SKYLINE TECHNOLOGYSOLUTIONS

Looking Ahead

Practice due care and diligence in building **a layered defense** focused on a *people-process-and technology driven program with the right governance, services and tools.*

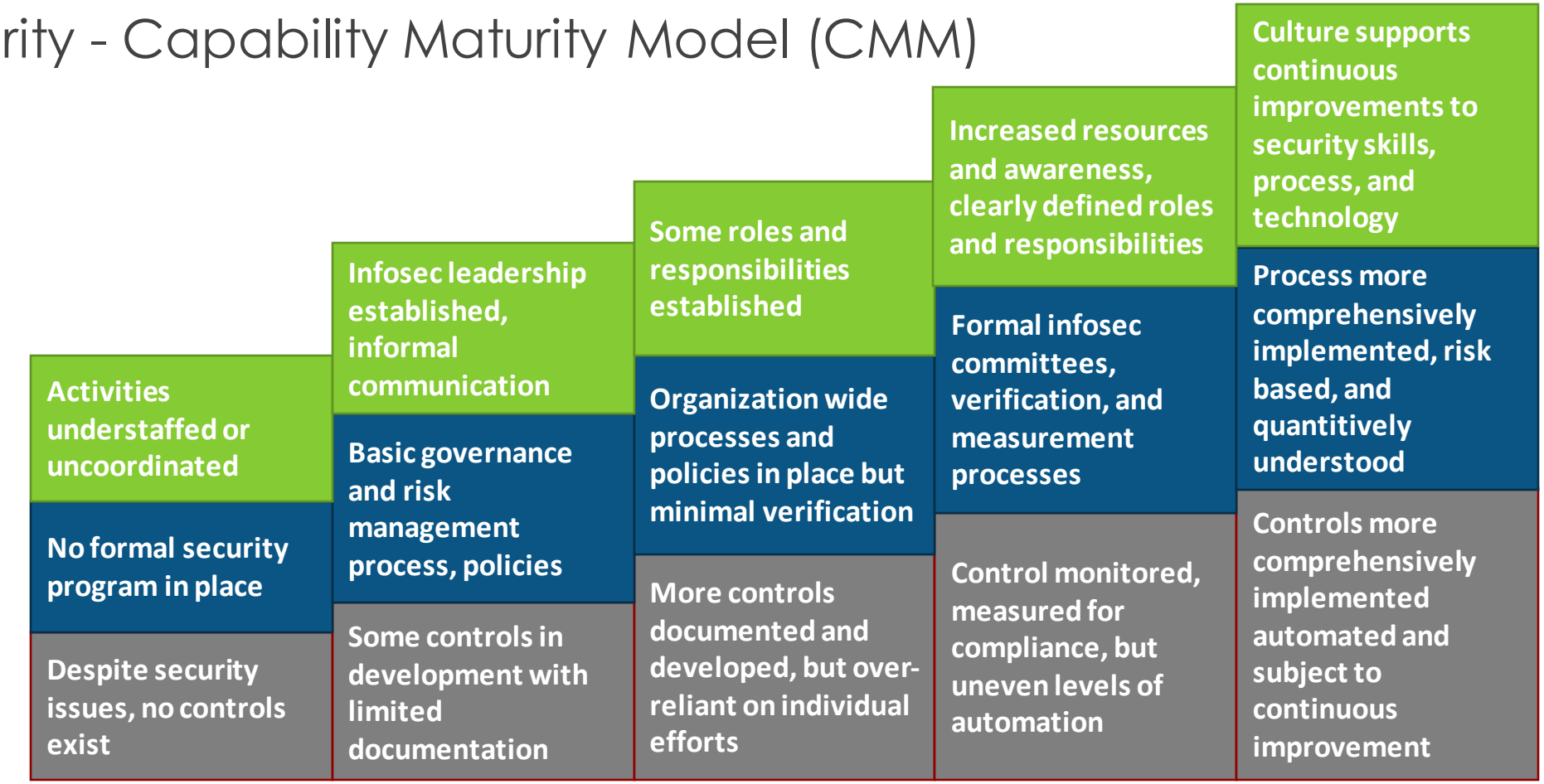
- Examine the **People** issues….Adequate staffing? Sufficient training of employees and key staff? Use of consultants?
- Examine the **Process** issues….Adequate process and procedures? Well documented? Good communications?
- Examine the **Tech** issues….Adequate tools for monitoring? Integrated dashboard that give near real time status?

The above will likely take **Funding**....Is there a cyber program that has budgetary standing and projections over time for staffing/training/tech refresh and new tools?

SKYLINE TECHNOLOGY SOLUTIONS

Cyber Maturity → Cyber Resiliency

Cybersecurity - Capability Maturity Model (CMM)



IT/OT Works Together with Cybersecurity Operations

IT/OT Operations:

- Conduct disaster recovery and testing
- Follow compliance / governance policies
- Install and configure apps
- Manage computers, servers, and other devices
- Maintain hardware inventory
- Monitor and troubleshoot systems
- Perform backups
- Plan and implement technology upgrades
- Provide technical support

Cybersecurity Operations:

- Conduct risk audits and vulnerability assessments
- Ensure compliance with industry regulations
- Hunt for and identify potential threats
- Implement security policies
- Manage identity and access controls systems
- Mitigate threats and malicious activities
- Perform cyber defense testing
- Perform penetration testing

Both Work Together To: Defend Endpoints, Migrate Systems, Manage Systems, and Sustain Digital Operations

SKYLINE TECHNOLOGY SOLUTIONS

Thank You

SKYLINE
TECHNOLOGYSOLUTIONS