Information Security Business Unit

Community Oversight Panel

Alex Di Giacomo, C|CISO, CISA,CISM, CRISC, CISSP, CDPSE, HISP

8/13/25

SOUNDTRANSIT

Agenda

1. **Information Security at ST**: Function Overview and Background
2. **Situational Awareness**: Risks, Current Posture and Recent Attacks
3. **Ongoing Efforts and Current Focus**
4. **Panel Q&A**

About your Presenter

- Sound Transit's Chief Information Security Officer
- BS in Electronic Engineering, specialization in Control Systems
- Master of Engineering and Technology Management, *Summa Cum Laude*
- Over 26 years of experience across industries such as Energy, Consulting, Managed Services, IT and Transit
- Member of the Washington State Technology Services Board Security Subcommittee
- Relevant security designations: C|CISO, CISA, CISM, CRISC, CISSP, CDPSE, HISP

Information Security: Broader than IT Security

Function Overview

Designed for…

Enterprise Oversight | Governance | Assurance Services

To…

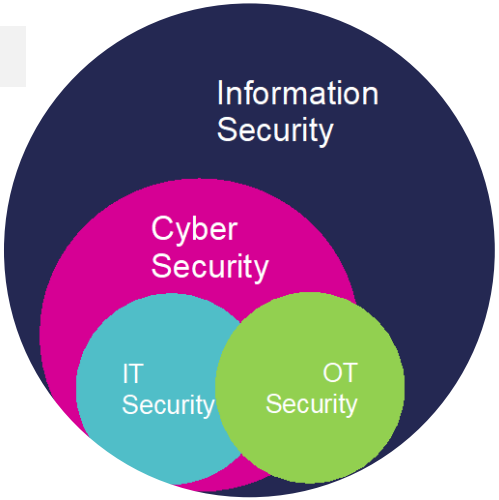
Preserve the Confidentiality, Integrity and Availability of information assets

With…

Agency-wide purview and scope

Based on…

The framework provided by the ISO 27001 international standard for Information Security



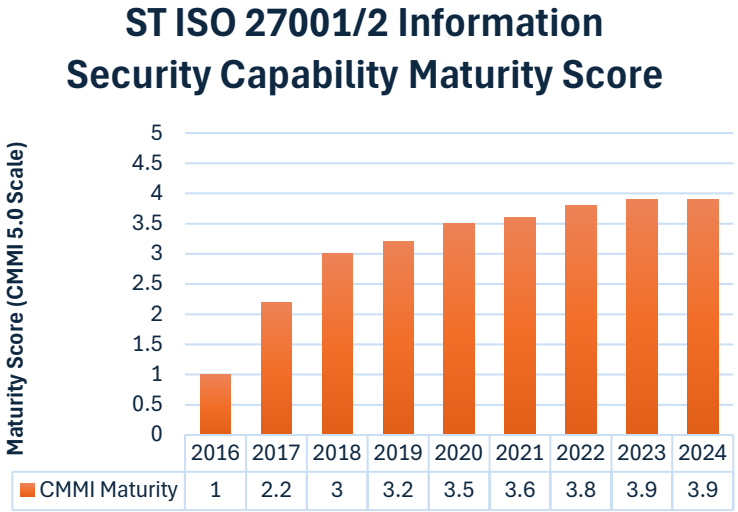
*The Information Security function is enabled by **Agency Policy 1100** which establishes its core component – the agency's Information Security Management System (**ISMS**)*

Background

Pre '16 Cybersecurity not explicitly addressed prior to 2016, leading to significant gaps across the board

2016 Information Security function formally established under IT, per CIO sponsorship

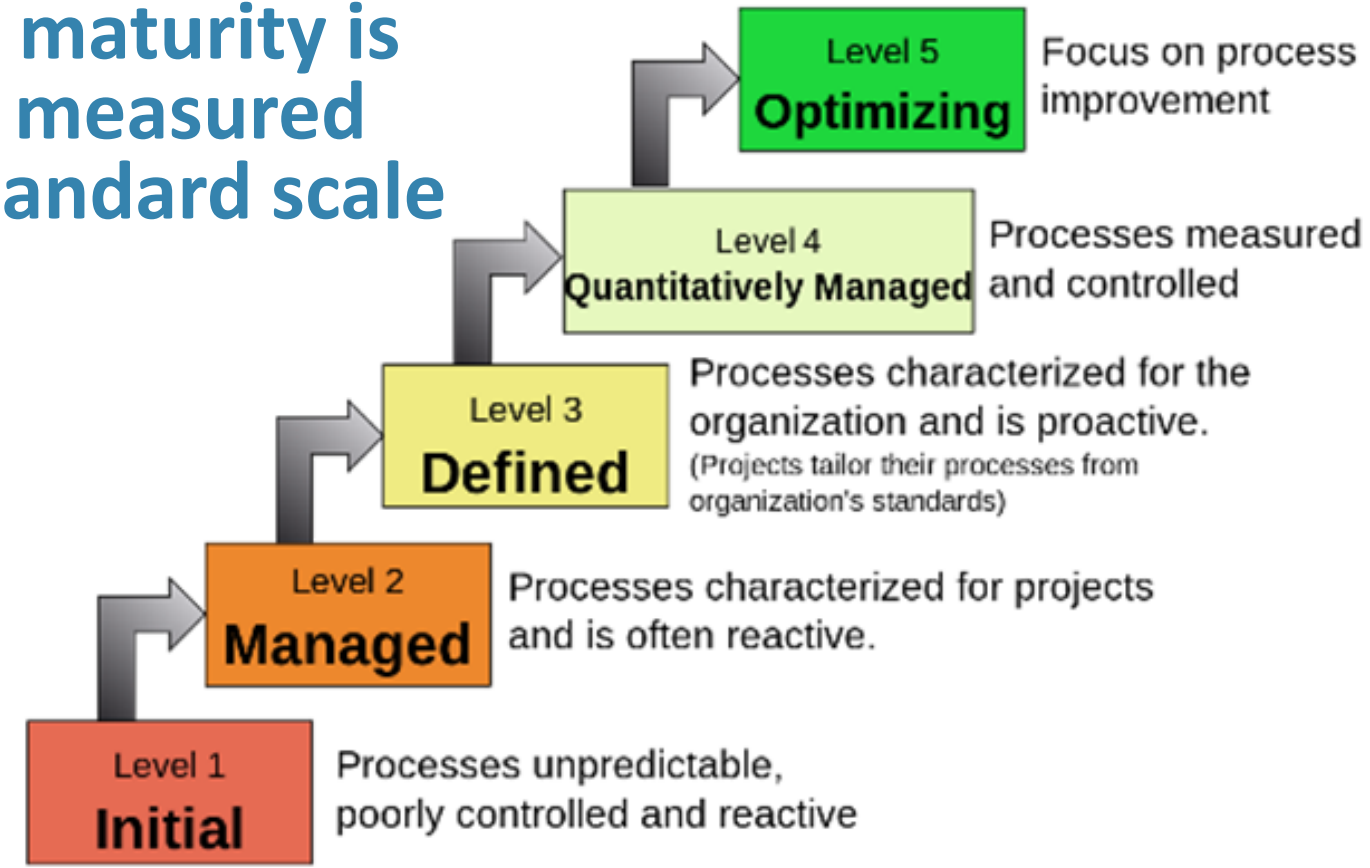
2024 CEO Sparrman sponsors Cybersecurity Activation Plan to address issues and target "best in class" posture



Achievements Externally-audited maturity level of the business function of **3.9** (5-point Gartner scale)

Challenges Funding, large technical debt, limited resource capacity, evolving threats

Program maturity is typically measured with a standard scale



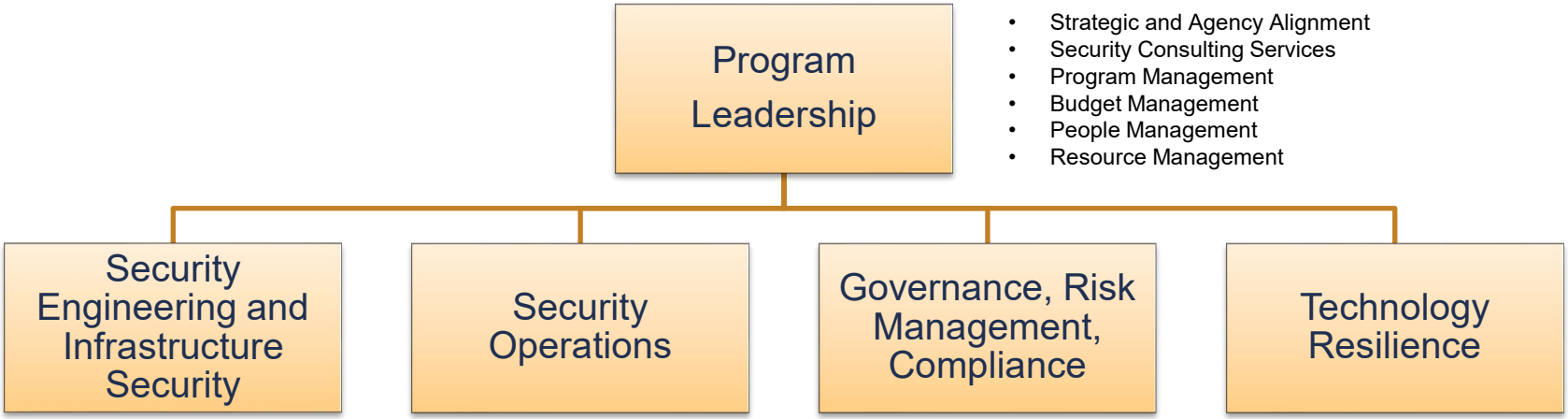
Data Classification: Unrestricted

An effective program also encompasses elements from many functions and areas

Governance, Risk and Compliance	Data Security	Change Management	Identity and Access Management	Application Security	Vendor Risk Management
User Education and Awareness	Vulnerability Management	Endpoint Security	Network Security	Cloud Security	HR Security
Back End Security	Physical Security	Disaster Recovery	Assurance Activities	Secure Development	Security Operations
Incident Response	Lifecycle Maintenance	Asset Management	Configuration Management	Threat Management	Continuous Improvement

InfoSec Program – Main Objectives

InfoSec BU Functional Organization



Situational Awareness

Government is actively being targeted	Federal Regulation is looming – DHS CISA	Attacks consistently exploit the fundamentals
Financial losses resulting from attacks are increasing	Attackers are better resourced	Threat landscape continuously evolves
Geopolitical conditions drive attack increases	Extortion and Ransomware are still profitable	Attackers are nimbler, adopt new tech faster

Challenges

- Legacy technology infrastructure
- Generally low maturity of industry vendors
- Limited resources
- Competing priorities
- Incompatible maintenance horizons
- Uncertainty in regulatory space

Ongoing Efforts and Current Focus

- CEO Constantine maintains Sound Transit focus and executive support of cybersecurity investments for high priority areas, supporting the agency's Information Security Strategic Plan

Enhance **prevention** & **detection**	Reduce **technical debt**	Introduce / enhance robust cyber **access control** practices	Address **technical issues**	Introduce mature **data protection** capabilities	Deploy security systems in the **cloud**

Key Success Factors

Key Enablers for Continued Progress

Continued investment in Information Security space

Recognition of Information Security objectives as a key strategic enabler

Integration of security controls as essential requirements for capital projects

Panel Q&A

Thank you.

SOUNDTRANSIT

soundtransit.org