




# An Industry Plan for Semiconductor Cybersecurity

Speaker: Mayura Padmanabhan, SEMI

# AGENDA

- 1 SEMI and Cybersecurity
- 2 SMCC Introduction and Organization
- 3 Cybersecurity Supplier Assessment working Group Update
- 4 SEMI E187 Cybersecurity Forum
- 5 Cybersecurity Forum 2025  
Call to Action & Summary

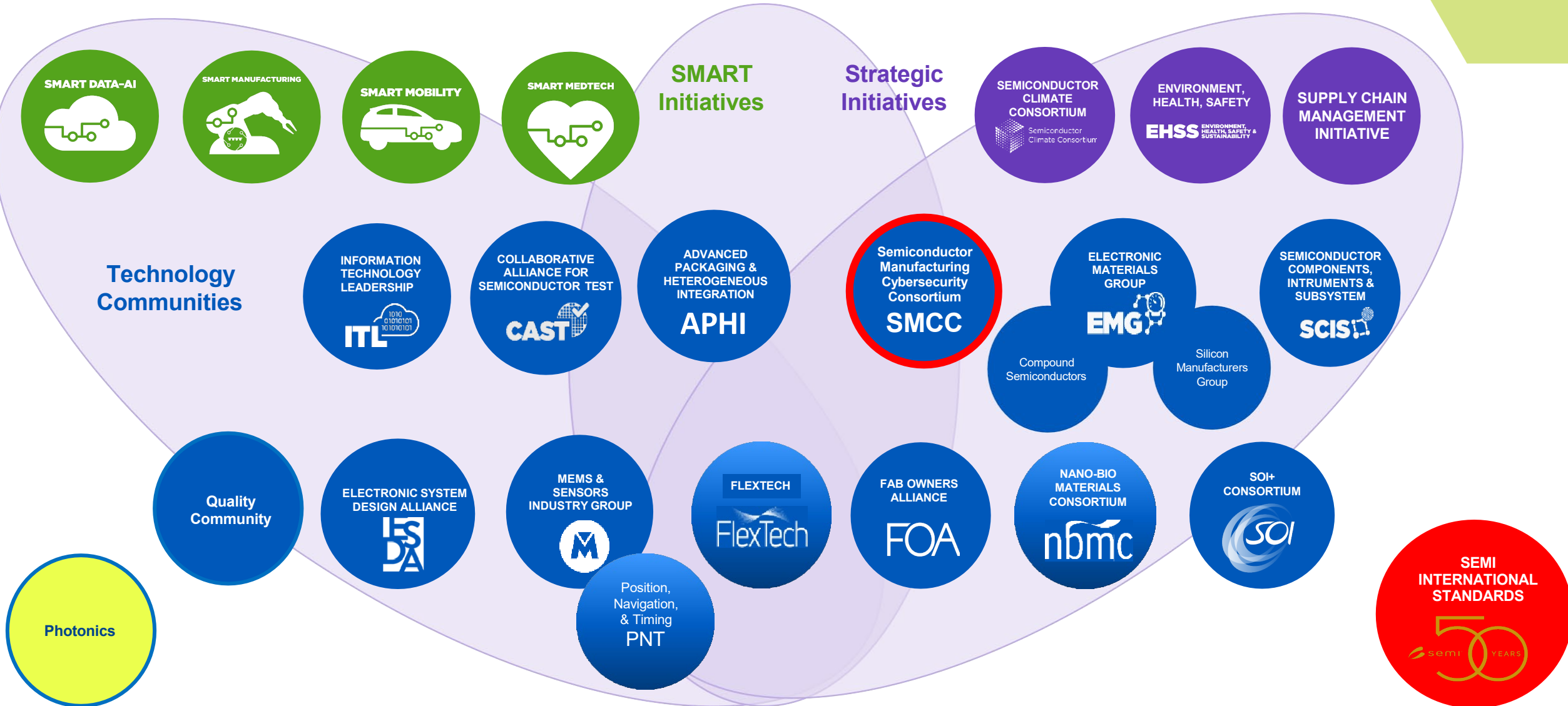
# SEMI is Uniquely Qualified to Address the Industry's Top Challenges that Require Global Collaboration

	Foundational	Expanded Programs and Scope			2025 Top Priorities		
<div>3,000+ members worldwide</div> <div>Spanning the Semiconductor and Electronics Design and Manufacturing Supply Chain</div> <div>Driving Global Programs</div>	Thought Leadership	Worldwide Offices	Market Intelligence Reports	Tech partners: imec, Fraunhofer, CEA-Leti, IEEE, ITRI, AIST	Supply Chain Resilience	Global Advocacy & SIPS Platform	
	Standards	2,300+ Program Hours				Workforce Development	
	SEMICON® Expositions/Conferences	170+ Tech Programs	Smart Initiatives	Strategic Tech Communities: ESDA, IESA, FOA, FlexTech, MSIG, SOIIC		Sustainability	
	EHS	20+ Tech Communities				PFAS	
				Think Tanks			Cybersecurity & AI

# SEMI Technology Communities

PROVIDING TECHNOLOGY STEWARDSHIP & COLLABORATION ACROSS THE ECOSYSTEM

PARTICIPATE | CONNECT | CONTRIBUTE | LEARN | LEAD | ENGAGE | COLLABORATE | TEACH | NETWORK | DISCUSS | CHALLENGE



# SEMI Manufacturing Cybersecurity Standards

## **SEMI E187 - Specification for Cybersecurity of Fab Equipment**

Defines overarching and fundamental cybersecurity requirements as a baseline to secure semiconductor fab equipment by design and support security protection in operation and maintenance.

## **SEMI E188 - Specification for Malware Free Equipment Integration**

Provides a framework for how to mitigate the propagation of malware to manufacturing facilities during capital equipment delivery and support activities.

## **NEW! SEMI E191 - Specification for Computing Device Cybersecurity Status Reporting**

Specifies a framework for reporting cybersecurity status information about a computing device.

# Semiconductor Manufacturing Cybersecurity Consortium (SMCC) – A SEMI Technology Community



**Vision:** **Strengthen cyber resilience and protection** of the global semiconductor supply chain against evolving threats.



**Mission:** Develop and promote a **standards-based, industry-wide** approach to improve cybersecurity and accelerate implementation of actionable solutions.



## **Optimal Member Profile**

- Mix of **DMs & OEMs** representing **large and small** companies
- Active participation in **pre-competitive** environment with focus on **problem-solving**

## Key focus areas

SMCC workgroups are focused on implementing Cybersecurity controls into our industry factories & supply chain

1

Develop a **robust framework** for cybersecurity that incorporates **lessons learned** from the recent transition and embraces open collaboration.

2

Create a **semiconductor industry-specific framework** to assess the strength of cybersecurity across the supply chain and **implement measures** to better protect ecosystem networks.

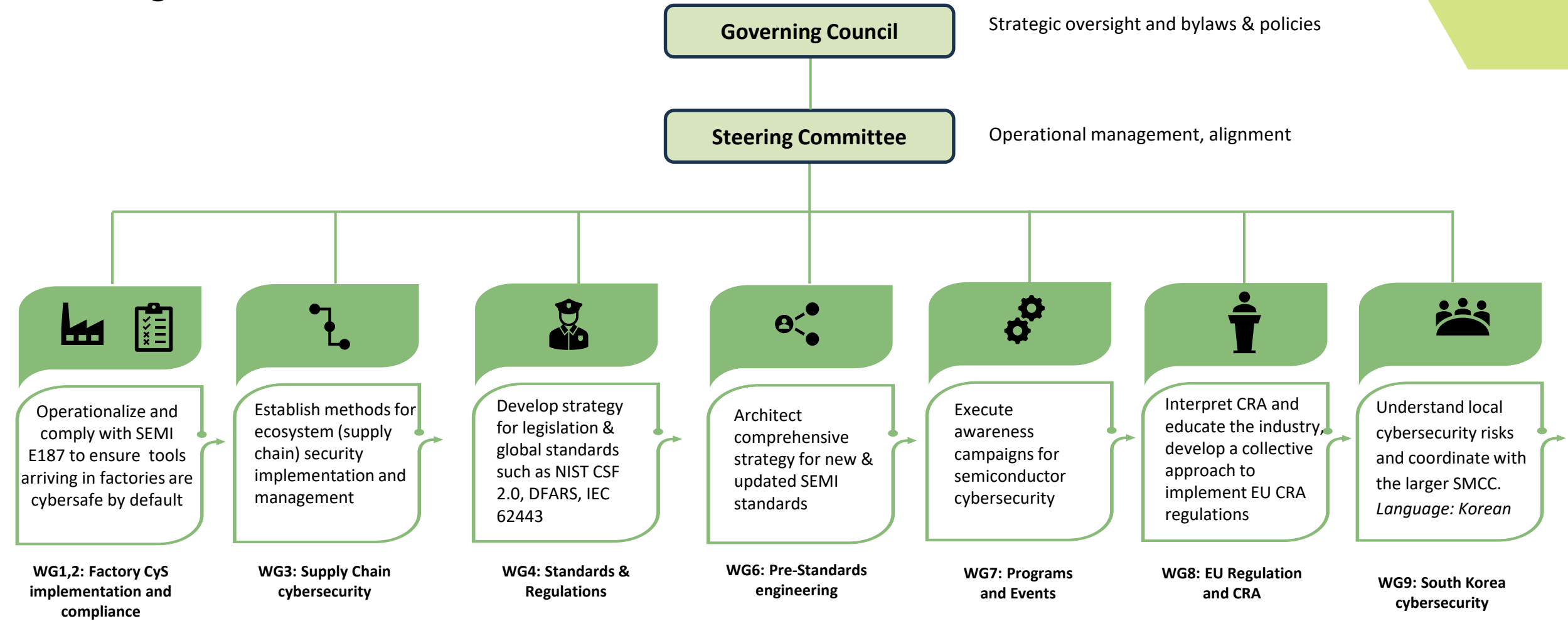
3

Incorporate **best practices from other industries** such as **automotive and medical** with the aim to modernize security protocols and facilitate greater collaborative information sharing through SEMI.



For more information or to join, contact [cybersecurity@semi.org](mailto:cybersecurity@semi.org)

# Organizational Structure







# SMCC Leadership

Governing Council



**Dirk van der Horst**  
Chief Security Officer  
ASML



**Doug Suerich**  
Director  
PEER Group



**James Tu**  
Head of Global  
Security Management  
TSMC



**Kannan Perumal**  
VP & CISO  
Applied Materials



**Wes Sparks**  
Director  
Intel

SMCC Advisor



**Andrew Seward**  
Manager, TEL

Steering Committee



**Mike Tanori**  
CyS Architect  
Intel Foundry



**Eiji Hagio**  
Vice President  
Info Security, TEL



**Jennifer Lynn**  
CISO Cyber  
Defense, IBM



**Bill Higgs**  
Senior Security  
Officer, ASML



**Leon Chang**  
Deputy Director  
TSMC



**Mayura Padmanabhan**  
Technical Project Mgr  
SEMI



**Wilko Baks**  
Manager Product  
Security, ASML



**Leon Chang**  
Deputy Director  
TSMC



**Lori Kessler**  
Sr. Program  
Director, AMAT



**Jared Buckley**  
IT Security  
Admin, TI



**Jennifer Lynn**  
CISO Cyber  
Defense, IBM



**Ryan Bond**  
Software App  
Architect, Intel



**Quentin Ellis**  
Marketing Manager,  
PEER Group



**Konstantinos  
Papapanagiotou**  
Director, Census Labs



**Dave Dunne**  
Product Security  
Manager, AMAT



**Bill Higgs**  
Senior Security  
Officer, ASML



**Daniel Pletea**  
Product security  
Architect, ASML



**Chet Borg**  
Director of IT,  
Polar Semi



**Albert Fuchigami**  
Sr Std Specialist,  
PEER Group



**Kimberly Daich**  
Director of Marketing  
PDF Solutions

**WG1,2: Factory CyS  
implementation and  
compliance**

**WG3: Supply Chain  
cybersecurity**

**WG4: Standards &  
Regulations**

**WG5: Threat  
Sharing**

**WG6: Pre-Standards  
engineering**

**WG7: Programs  
and Events**

**WG8: EU Regulation  
and CRA**



# What is SEMI E187-0122

- Ransomware, data breaches and cybercrime intrusions are growing at rapid rates
- The global efforts to secure the semiconductor supply chain and industry are of great importance
- SEMI E187-0122 specifications were released in 2022
- SEMI E187 was created specifically for the semiconductor industry
- E187 is intended to reduce risk, secure and protect semiconductor equipment and device manufacturer environments.
- The twelve E187 cybersecurity requirements were built as foundational baselines for securing semiconductor equipment. The industry is currently working to fully understand the requirements as written and how compliance would be interpreted by Device Manufacturer's (DM's) individually.

# E187 Scope

- This document is intended for individuals responsible for the development, manufacturing, operation, management and security of semiconductor tool equipment and device manufacturing.
  - This document will focus solely on E187-0122 requirements for new to Fab supplier equipment.
  - This document applies to any new to fab equipment
- New equipment should be defined as tools that are new in Development or Evaluation and have not already been procured and installed at the DM factory or fab previously.

# The 12 Requirements

#	Requirement Area
1	OS Support
2	Patch Process
3	Use Secure Network Protocols
4	Network Config Documentation
5	Vulnerability Scanning
6	Malware Scanning

#	Requirement Area
7	Anti-Malware Compatibility
8	Device Hardening
9	Authentication
10	Authorization & Access Ctrl
11	Event Log Capability
12	Log Details Specification

# WG1,2 White paper on E187 guidance

## Download Form

### Semiconductor Manufacturing Cybersecurity Consortium (SMCC)

SEMI E187 Supplemental Compliance Guide

[DOWNLOAD NOW](#)



This document was created through the collaborative efforts in the SEMI Semiconductor Manufacturing Cybersecurity Consortium (SMCC) Working Groups 1 and 2. This document is intended to be used as an additional SEMI E187-0122 compliance guidance for small, medium, and large semiconductor original equipment manufacturers (Supplier) and provides guidance to Device Manufacturers (DM) building their own specific requirements specifications using elements of SEMI E187-0122.





# Standards Based Supplier Cybersecurity Assessments for the Semiconductor Industry



# Supply Chain Cyber Risk Management | Semi Industry

## Sample Assessment Program



**Companies are trying their best** on their own with varying levels of success



One supplier often needs to respond to **multiple customer's security** audit questionnaires



**No correlation between** assessment efforts and risk reduction



### No semi-industry standard

- No consistent requirements
- Every company has their own questionnaire
- Assessments are performed by the customer's security team -> Resource intensive
- Assessments are not focusing on all-things-that-matter

Security Coverage	All Suppliers	High-Impact suppliers	Very high touch suppliers
Level of Coverage	Foundational	Advanced	High Touch
Awareness Newsletters	✓	✓	✓
Incident Handling	✓	✓	✓
Dark web intel search	✓	✓	✓
3 <sup>rd</sup> -party cyber risk monitoring services (e.g., Security Scorecard)		✓	✓
Questionnaire-based assessment & Follow up		✓	✓
Collaboration to improve business continuity			✓
Onsite assessment, verification, and follow up			✓

**We are all connected and only as strong as our weakest link**

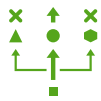


# The Standard Assessment Framework Journey



## 1. Define the Approach

April 2024 Face-to-Face Meeting – question bank approach & TISAX-style processes



## 2. First Draft Questionnaire

November 2024

First draft shared, additional sections identified



## 3. Feedback & Refinement

Target May 2025.

Expert reviews to refine language and questions



## 4. Begin Adoption & Finalize Process

Start now!

Applied Materials and one DM are early adopters.

Summer – finalize the assessment process



## 5. SEMI Standard

Target September to publish questionnaire and process as a SEMI Standard.



# Semi Standard Supplier Assessment | Common Question Bank

## Why do we create a new questionnaire?

- While standards like ISO 27001 are very good, they have too many questions that are not necessary to check cyber resilience
- These standards often lack right questions that are relevant to semiconductor industry
- We believe this is why automotive industry created their own questionnaire as part of the TISAX process

## One Common Question Bank

- Our DRAFT questionnaire is created based on the work done in SEMI Taiwan and in few SMCC member companies
- Inspired by TISAX and modified to meet semiconductor industry's unique needs
- 3 Question domains: Cyber Resilience, IP Protection, and Product Security

### Common Question Bank

Cyber  
Resilience

IP Protection

Product  
Security

### Key Benefits

1. Helps communicate the security requirements better
2. Suppliers don't have to answer multiple questionnaires
3. Improves efficiency and saves cost

# Semi Standard Supplier Assessment | Sample Question

NIST Categorization

Maturity multiple choice or Yes/No choice

Question & Level of definition of a mature organization

Choices along maturity level

NIST Category	NIST Sub-Domain	Objective	Question Type	Question	CheckBox (Multiple Choice)	A fully mature organization will exhibit	Response 0	Response 1	Response 2	Response 3
Protect	Access Control	Ensure that access to systems, applications, and data is managed and controlled to protect sensitive information and maintain the integrity and confidentiality of resources, including effective identity management for joiners, movers, and leavers.	CMMI Maturity Multiple Choice (Choose One)	Describe your organization's access control processes, including how they are consistently applied across all applications. Additionally, explain if and how your identity access management program addresses the specific needs of joiners, movers, and leavers for employees and contractors.		Continually improve the management of user access to the organization's applications and systems by automating the identity and access management lifecycle, through implementation of role-based access control, increased privileged access management, and greater integration of physical controls. Examples - they will have an inventory of privileged accounts that are mandatory to support business systems and applications and perform automated (preferably) access review and perform subsequent actions like handling and removing the accounts if not required. Ensure passwords align to industry accepted standards for password complexity NIST-800-63-3. There	-No documented access control policies or awareness of the need for one. No IAM program for joiners, movers and leavers.	Awareness of the need for access control exists, but no formal policies or processes. Access control is applied inconsistently across applications. No structured IAM program.	Basic access control policy exist and are applied to some key applications, but there are gaps in consistency. IAM process is in place but not formalized or consistently followed. Access control policy includes password complexities and basic segregation of duties. Regular review of user access for some critical applications but the process is mostly manual.	Comprehensive control documents exist across all applications with formalized IAM process and regulatory requirements. Access control includes segregation and disconnection for temporary employees and contractors. Review of access control physical and privilege

IT OT Asset Mgmt

Metrics and KPIs

Cloud Security

Protect Phys Sec

Aware Train

Access Control

Network Security

Protect Email

Internet Access

Endpt Prt ...

# Cybersecurity Forum @ SEMICON West 2025

Session Theme - *“Secure Together: Building Cybersecurity Resilience Through Industry Alliances”*

- **Wednesday, October 8, 12:30 PM to 6:30 PM**

- The semiconductor industry has long grappled with the critical issue of supply chain security. With the trends of globalization and digitization, semiconductor supply chains have become increasingly complex and susceptible to cybersecurity threats. In recent years, the development of emerging technologies such as the Internet of Things, AI, and big data has further heightened the cybersecurity challenges facing semiconductor supply chains.

- **Speakers:**

- Keynotes: McKinsey, FBI
- 6 oral presenters: Moxa, TxOne, imec, ISA, Accenture, NY Creates
- Invited Speakers: Qualcomm, AMD, Applied Materials, Renesas, IBM
- Panel: NIST, NSTC, American Bureau of Shipping
- Networking and Reception

SEMICON West 2025 → October 7-9 in Phoenix Convention Center, Arizona

**Scan to view agenda**

