Standards Based Supplier Cybersecurity Assessments for the Semiconductor Industry

May 2025 NIST Software and Supply Chain Assurance Forum
Cybersecurity Supply Chain Risk Management

Andrew Seward – Tokyo Electron America
Lori Kessler – Applied Materials

AGENDA

1. SEMI and Cybersecurity
2. SMCC Introduction and Organization
3. Cybersecurity Supplier Assessment working Group Update
4. Cybersecurity Forum 2025 – Call for Abstracts
5. Call to Action & Summary

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

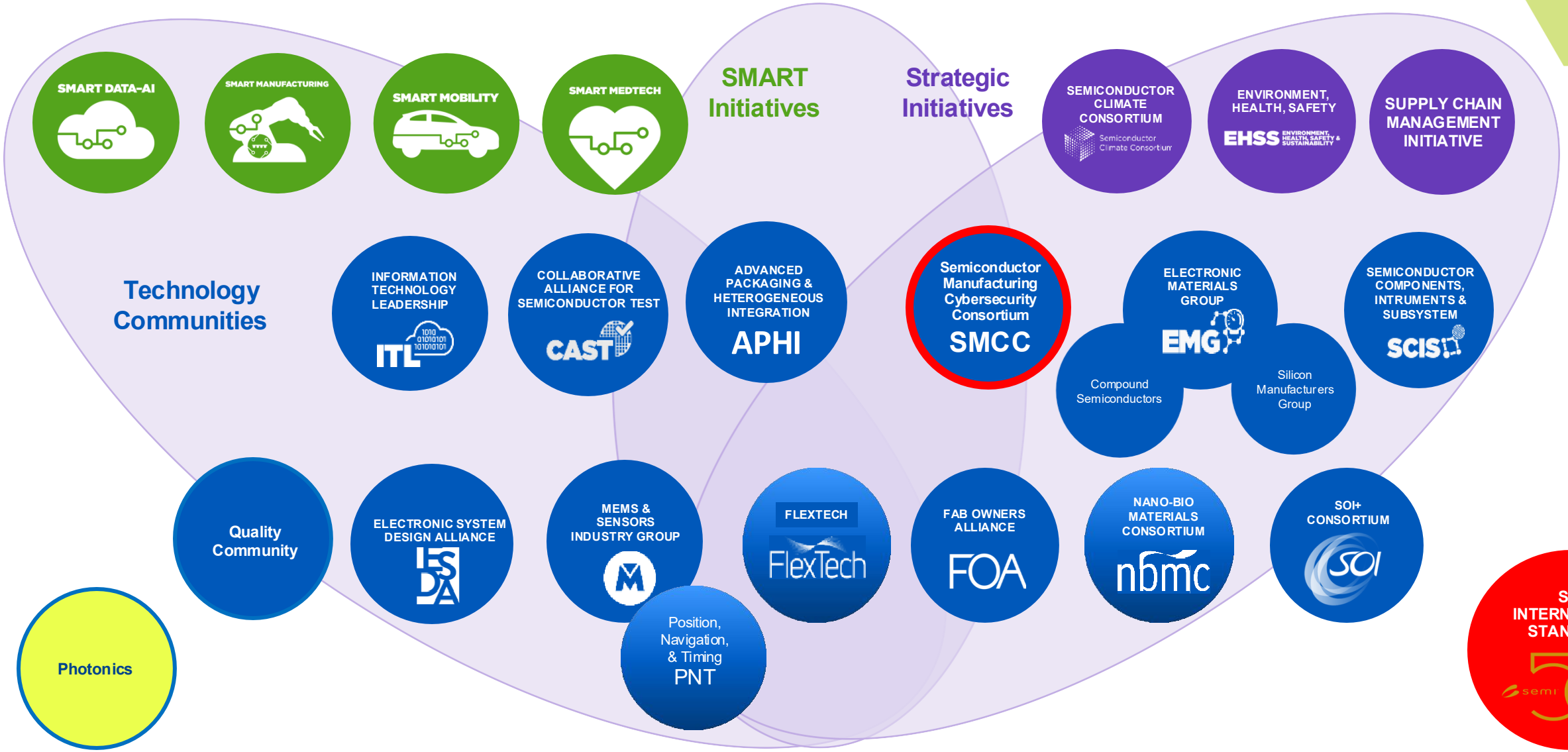
semi	Foundational		Expanded Programs and Scope			2025 Top Priorities
3,000+ members worldwide **Spanning the Semiconductor and Electronics Design and Manufacturing Supply Chain** **Driving Global Programs**	Thought Leadership	Worldwide Offices	Market Intelligence Reports	Tech partners: imec, Fraunhofer, 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 Think Tanks	Strategic Tech Communities: ESDA, IESA, FOA, FlexTech, MSIG, SOIIC		**Sustainability**
	EHS	20+ Tech Communities				**PFAS**
						Cybersecurity & AI

CONNECT - COLLABORATE - INNOVATE

SEMI Technology Communities

PROVIDING TECHNOLOGY STEWARDSHIP & COLLABORATION ACROSS THE ECOSYSTEM

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



AGENDA

1. SEMI and Cybersecurity
2. **SMCC Introduction and Organization**
3. Cybersecurity Supplier Assessment working Group Update
4. Cybersecurity Forum 2025 – Call for Abstracts
5. Call to Action & Summary

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**

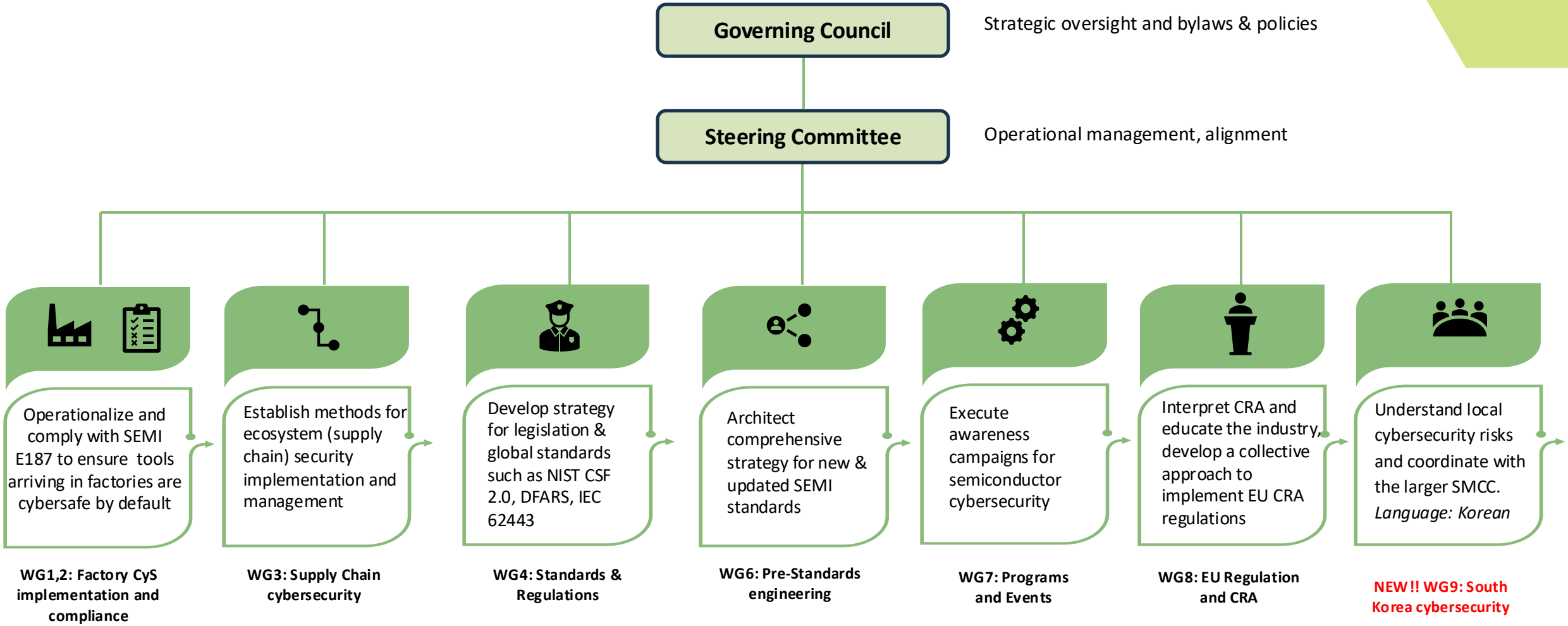
Key focus areas

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

Organizational Structure



Celebrating success of NIST SMCC Collaboration

Examples of Industry & Government Collaborations

SMCC presentation at NIST NCCoE "Enhancing Security of Devices and Components Across the Supply Chain" workshop

SMCC presentation at NIST NCCoE "CHIPS R&D Semiconductor Supply Chain Trust and Assurance Data Standards" workshop

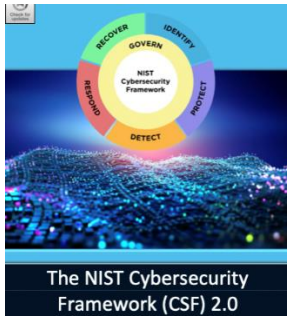
WG4 Workshop 1
SEMI ASMC Albany, NY

WG4 Workshop 3
NIST HQ Gaithersburg, MD

SMCC SEMICONDUCTOR MANUFACTURING CYBERSECURITY CONSORTIUM

Jan 2024 → Feb 26th → Feb 27th → Mar 12th → Apr 2nd → May 7th → May 16th → … → Jul 9th → … → Oct 30th → … → Jan 2025

Communicated to NIST of the SMCC WG4 intention to own the creation of the NIST CSF Semiconductor Community Profile



The NIST Cybersecurity Framework (CSF) 2.0

In-Person Visit to White House Office of the National Cybersecurity Directorate to showcase the SMCC and our NIST CSF efforts

Section 5.5.5…create a "Cybersecurity Framework Profile tailored to the semiconductor manufacturing industry"

WG4 Workshop 2
SEMICON West 2024

Submitted CSF 2.0 Semiconductor Manufacturing Profile to NIST

Public Comment open through May 30, 2025

SMCC SEMICONDUCTOR MANUFACTURING CYBERSECURITY CONSORTIUM

SMCC Leadership

Governing Council

Aernout Reijmer
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 Director

Roberto Berigan
Systems Engineer
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

Rajesh Potturi
Sr. Director, AMAT

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

Standards Based Supplier Cybersecurity Assessments for the Semiconductor Industry

May 2025 NIST Software and Supply Chain Assurance Forum
Cybersecurity Supply Chain Risk Management

Supply Chain Cyber Risk Management | Semi Industry

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

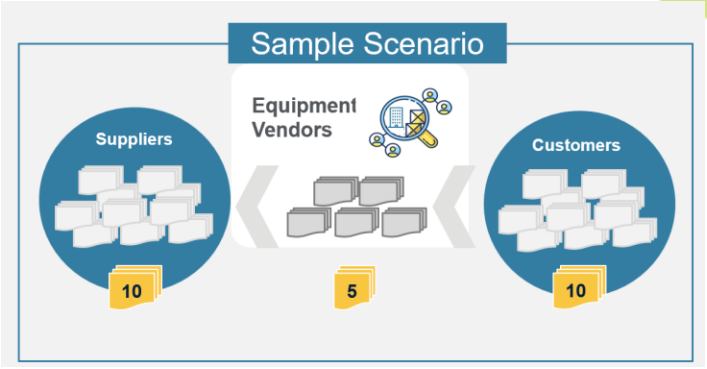
Sample Assessment Program

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	✓	✓	✓
3rd-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

Supply Chain Cyber Risk Management | Semi vs. Auto Industry

Semi Industry	Area	Auto Industry
Each company	Security Requirements	Industry Standard
Each Company Conducted by customers Suppliers complete many self-evaluation	Security Assessments	Industry Standard Conducted by 3rd parties Suppliers complete one 3rd party evaluation
Inconsistent & Incomplete	Assessment Criteria	Standards-based; Recovery & Resiliency
Negotiable and ineffective	Effectiveness	Formally tracked and audited



SEMI Approach	100 Unique Assessments Results shared 1:1
Auto Approach	15 Unique Assessments Results shared 1:many

By reducing the number of audits and using a common question bank, automotive industry has improved the efficiency & quality of the audit, and save cost

SMCC Standard Framework:

- Semi **standard questionnaire** can be used by DMs, OEMs, and other important companies in semiconductor supply chain
- Standard questionnaire represents key areas **important to semiconductor** industry such as Product Security
- Respondent **shares results with other clients** in semiconductor space
- Identified **core set of auditors** removes assessment burden

WG 3: Supply Chain Cybersecurity

Chair: Hagio-san (TEL) **Vice-chairs:** Lori Kessler (Applied Materials); Bill Higgs (ASML)
Governing Council Sponsor: Kannan Perumal (Applied Materials)

OBJECTIVE:

- Significantly reduce supply chain cybersecurity risks and speed adoption of best practices industry wide through a standardized industry framework
- Achieve a common understanding for how corporate cybersecurity readiness will be assessed for each supplier and specific products

WHY?

- Vast majority of cybersecurity impacts in industry begin in our supply chain with specific concerns for suppliers below Cybersecurity poverty line
- Lack of a standardized framework results in key suppliers utilizing limited resources to answer multiple questionnaires instead of continuous control improvement

APPROACH:

- Utilize a phased approach to define ecosystem security implementation & measures

WHAT SUCCESS LOOKS LIKE / INCLUDE CRITERIA:

- Define core cybersecurity controls for each supplier tier
- Develop a question bank to continually maintain categorized questions as risk evolves based on negative outcomes
- Adopt a TISAX-style method for supplier assessment

PROGRESS SO FAR:

- Question Bank final draft in review. Early adoption in progress.
- High Level framework drafted. Detailed process in development.

HIGHEST PRIORITY DELIVERABLES:

- Aligned supplier & sub-supplier assessment questionnaire
- 10 companies to adopt by Semicon West (Oct 2025)

OPTIMAL MEMBER PROFILE:

- Members with working knowledge of frameworks, involved in their own company's supplier tiering, assessment processes
- Commit to 2-4 hrs/wk (vary based on deliverables working on)

Meeting time GEO alignment: Mondays 4:00pm North America Pacific during Summer / 9:00am Japan Standard Time

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.

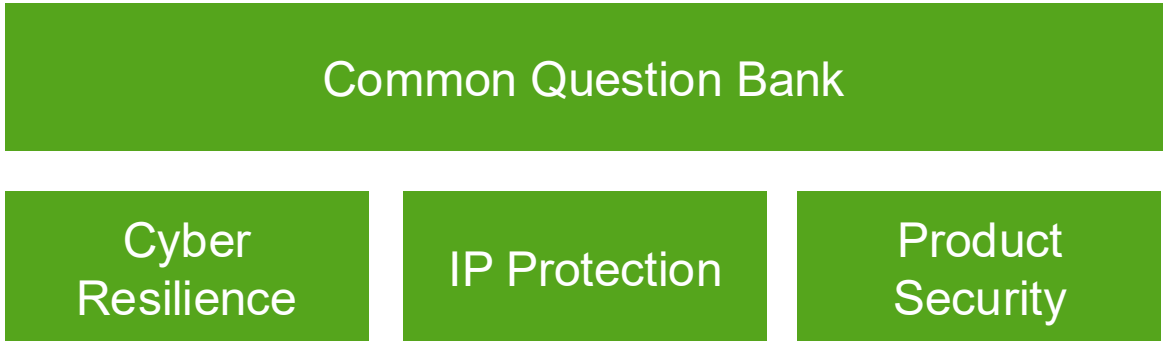
Semi Standard Supplier Assessment | Common Question Bank

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



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

Maturity multiple choice or Yes/No choice

Question & Level of definition of a mature organization

Choices along maturity level

NIST Categori-zation

NIST Category	NIST Sub-Domain	Objective	Question Type	Question	CheckBox (Multiple Choice)	A fully mature organization will exhibit	Response 0	Response 1	Response 2	Respons
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 susbequent 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.	Compre control docume consiste across r applicat IAM pro with for and reg Access includes comple segrega and disa for term employe contract review applicat physica privileg

... IT OT Asset Mgmt | Metrics and KPIs | Cloud Security | Protect Phys Sec | Aware Train | Access Control | Network Security | Protect Email | Internet Access | Endpt Pr ...

Semi Standard Supplier Assessment | Process - Multiple Assessment Levels

Having multiple assurance levels will help perform the “right” level of assessment

Assessment method	Assessment Level 1	Assessment Level 2	Assessment Level 3
Self-assessment	Yes	Yes	Yes
Evidence	No	Plausibility Check	Thorough verification
Interviews	No	Via web conference	In person, on site
On-site inspection	No	At your request	Yes

Customers can choose 1) Focus area, and 2) Assurance level to meet their risk-based expectations

Customer	Supplier	Areas of focus	Assessment Level
Customer 1	Supplier 1	Cyber Resilience	3
		IP Protection	3
		Product Security	3
Customer 1	Supplier 2	Cyber Resilience	2
		IP Protection	2
		Product Security	n/a
Customer 2	Supplier 2	Cyber Resilience	1
		IP Protection	1
		Product Security	3

Having common audit report template and results sharing process will enable sharing results with more than one customer

Section	Details
A	Assessment Related Information
B	Summarized Results
C	Assessment result summary
D	Maturity Levels of VDA ISA (Result Tab)
E	Detailed Assessment Results

Key Benefits: 1. Improves efficiency and audit quality and 2. Saves cost

Semi Standard Supplier Assessment | Process - Choice of the auditor

Need for the Auditor

- Assurance Level 1 is self disclosure only – Do not require any auditor
- Assurance Level 2 and Level 3 requires auditor

Who will be performing the audit?

Auditor	Pros	Cons
Customer	No new cost for auditors	Supplier need to work with multiple customer auditors (inefficiency and increased cost)
Mutually agreed 3rd-party auditor	• Improved quality of the audit • One audit results can be shared with multiple customers	Someone has to pay for the auditor fees
Choose an auditor from a pre-approved list	• Improved quality of the audit • One audit results can be shared with multiple customers • Improved consistency	Someone has to pay for the auditor fees

Options for sharing assessment results

1. Supplier chooses to share the results via email
2. Suppliers and customers can share the results and feedback through a TPRM solution or through a secure exchange

What's Next?

- Further refinement:
  - SMCC member companies finalizing language and eliciting additional expert advise
  - WG4 will provide input based on NIST Semi Industry Profile in the coming weeks

- Adoption:
  - One DM has adopted draft version
  - One Equipment Supplier will use current version with some edits, with additional questions, and send out to ~25 suppliers the week of May 12

- Post WG4 feedback updates, will draft standards information (timing TBD)

- Unveiling in Semicon West (October)

Cybersecurity Forum
Semicon West October 2025
Phoenix Az

Call for Papers

SMCC SEMICONDUCTOR MANUFACTURING CYBERSECURITY CONSORTIUM

Cybersecurity Forum @ SEMICON West 2025

Call for Abstracts

- Wednesday, October 8, 1:00 PM to 3:00 PM
- Session Theme - *"Secure Together: Building Cybersecurity Resilience Through Industry Alliances"*
  - 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.
- Call for Abstract Topics (deadline: May 23)
  - Cybersecurity in Legacy Semiconductor Tools
  - Emerging and Existing Cybersecurity Legislation and Compliance
  - Cybersecurity Maintenance in Manufacturing
  - Impact of Cybersecurity Events on Semiconductor Mfg Operations
  - AI and Digital Twin Security in Semiconductor Manufacturing
  - Supply Chain Security
  - Threat Landscape in Semiconductor Manufacturing
  - IoT and Industry 4.0 Security
- SEMICON West 2025 → October 7-9 in Phoenix Convention Center, Arizona

Scan to submit an abstract

Call to Action

Bridging Industry & Government towards a Secure Future

Call to Action to Secure our Semiconductor Manufacturing Industry's Future

- ***Adopt*** SMCC artifacts and integrate into your company's business processes
- ***Engage*** in SEMI SMCC Development Efforts
  - Review and provide feedback on our draft supply chain assessment questionnaire and certification methodology
- ***Influence*** the direction of the NIST CSF 2.0 Semiconductor Manufacturing Community Profile
  - Provide feedback on the CSF 2.0 Semiconductor Manufacturing Profile to NIST
- ***Share*** your perspectives at the Cybersecurity Forum at SEMICON West 2025
  - Participate in the Call for Abstracts, submit a paper by May 23, 2025

For more information
Contact: cybersecurity@semi.org

Stay Connected!