NIST Internal Report
NIST IR 8546 ipd

Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile

Initial Public Draft

Jennifer Lynn
Wilko Baks
Daniel Pletea
Rajesh Potturi
Jared Buckley
R. Eugene Craft
Albert Fuchigami
Donato Kava
Brian Korn
Supika Mashiro
Jim Montgomery
Karen Scarfone
Michael Tanori
Michael Thompson
Alex Nelson
Sanjay Rekhi
Nakia Grayson

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8546.ipd

NIST Internal Report
NIST IR 8546 ipd

Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile

Initial Public Draft

Jennifer Lynn
IBM

Wilko Baks
Daniel Pletea
ASML

Rajesh Potturi
Applied Materials Inc.

Jared Buckley
Texas Instruments

R. Eugene Craft
The MITRE Corporation

Albert Fuchigami
PEER Group

Donato Kava
Advanced Energy Industries, Inc.

Brian Korn*
Intel Corporation

Supika Mashiro
Tokyo Electron Limited

Jim Montgomery
TxOne Networks

Karen Scarfone
Scarfone Cybersecurity

Michael Tanori
Intel Corporation

Michael Thompson
The MITRE Corporation

Alex Nelson
Sanjay Rekhi
Computer Security Division
Information Technology Laboratory

Nakia Grayson
Applied Cybersecurity Division
Information Technology Laboratory

**Former Intel employee; most work for this publication was done while at Intel.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8546.ipd

February 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies

How to Cite this NIST Technical Series Publication

Lynn J, Baks W, Pletea D, Potturi R, Buckley J, Craft R, Fuchigami A, Kava D, Mashiro S, Montgomery J, Scarfone K, Tanori M, Thompson M, Nelson A, Rekhi S, Grayson N (2025) Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8546 ipd. https://doi.org/10.6028/NIST.8546.ipd

Author ORCID iDs

R. Eugene Craft: 0009-0009-0164-1241
Nakia Grayson: 0000-0003-1062-4338
Alexander Nelson: 0000-0002-3771-570X
Sanjay Rekhi: 0009-0008-8711-4030
Karen Scarfone: 0000-0001-6334-9486
Michael Thompson: 0000-0002-0836-244X

Public Comment Period

February 27, 2025 – April 14, 2025

Submit Comments

semiconductor-manufacturing-profile@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information

Additional information about this publication is available at the NCCoE's Cybersecurity Framework Profile for Semiconductor Manufacturing project page, including related content and potential updates.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document defines a Cybersecurity Framework (CSF) 2.0 Community Profile with a voluntary, risk-based approach to managing cybersecurity activities and reducing cyber risks for semiconductor development and manufacturing. Collaboratively developed in support of the National Cybersecurity Implementation Plan Version 2, the Semiconductor Manufacturing Profile can be used as a roadmap for reducing cybersecurity risks for semiconductor manufacturers in alignment with sector goals and industry best practices. It is built on top of the Manufacturing Profile documented in NIST IR 8183, Revision 1. The Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Keywords

Cybersecurity; Cybersecurity Framework (CSF); manufacturing; risk management; semiconductor; semiconductor development; semiconductor manufacturing.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Audience

This document covers details that are specific to semiconductor manufacturing systems. Readers of this document should be acquainted with operational technology, general cybersecurity concepts, and communication protocols, such as those used in networking. The intended audience is varied and includes the following:

- Cybersecurity engineers, integrators, and architects who design or implement secure semiconductor manufacturing systems and semiconductor equipment and tooling
- Fab and Enterprise Information Technology (IT) system administrators, engineers, and other IT professionals who administer, patch, or secure semiconductor manufacturing systems
- Managers who are responsible for semiconductor manufacturing systems and semiconductor equipment and tooling

- Senior management who are trying to understand implications and consequences as they justify and implement a semiconductor manufacturing systems cybersecurity program to help mitigate impacts to business functionality
- Researchers, academic institutions, and analysts who are trying to understand the unique security needs of semiconductor manufacturing systems

Note to Reviewers

NIST welcomes requests and suggestions for terms that should be added to this document's Glossary.

The Criticality Tables in Section 4 followed a procedure that prioritized preserving criticality judgements from the Manufacturing Profile. This procedure is suspected to have propagated too many CSF 2.0 Subcategories into "critical" designations in support of some mission objectives. Suggestions on CSF 2.0 Subcategories that might not be critical in support of some mission objectives are welcome. This applies to Subcategories of any criticality judgement status within Section 4.

The Criticality Tables in Section 4 have some criticality judgements that were suggested by the document's working group. These are temporarily bold-weighted for the public comment period and will be resolved to binary criticality judgements after comments are received. Feedback is encouraged from any members of the public, particularly those whose job duties include focus on the mission objective and on whether some particular CSF Subcategory is considered critical to meeting that objective. Absent feedback, any of the Subcategories that currently lack a criticality judgement for a certain mission objective will be considered non-critical due to lack of advocacy.

Section 5 is known to include some references to documents that are superseded, such as SP 800-53r4 which is superseded by SP 800-53r5. Though the Initial Public Draft contains these references, the next version of this document is planned to update these references to incorporate the latest versions' guidance.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: semiconductor-manufacturing-profile@nist.gov

Table of Contents

Executive Summary 1

1. Introduction 2

1.1. Purpose 2

1.2. Semiconductor Fabrication Ecosystem Functional Domains 3

1.2.1. Development of Secure Equipment and Tooling 5

1.2.2. Fab Environment 5

1.2.3. Enterprise IT Infrastructure in Semiconductor Manufacturing 6

1.3. Security of Semiconductor Manufacturing 7

1.4. Relationship to CSF Core and Manufacturing Profile 8

1.5. Document Organization 10

2. Overview of Semiconductor Manufacturing and Operational Systems 11

2.1. Importance of NIST CSF 2.0 in Semiconductor Manufacturing 11

3. Overview of CSF 2.0 13

3.1. The CSF Core 13

3.2. Community Profiles 15

3.3. Applying the NIST CSF to Semiconductor Manufacturing 15

4. Applying Business and Mission Objectives to Profile Creation 17

4.1. Semiconductor Manufacturing Business and Mission Objectives 17

4.1.1. Objective 1: Maintain Environmental Safety 17

4.1.2. Objective 2: Maintain Human Safety 18

4.1.3. Objective 3: Maintain Production Goals 19

4.1.4. Objective 4: Maintain the Quality of Semiconductors 19

4.1.5. Objective 5: Protect Sensitive Information 20

4.2. Aligning Subcategories to Meet Business and Mission Objectives 21

4.2.1. Govern 21

4.2.2. Identify 23

4.2.3. Protect 23

4.2.4. Detect 24

4.2.5. Respond 25

4.2.6. Recover 25

5. Semiconductor Manufacturing Community Profile Subcategory Guidance 26

5.1. Govern 29

5.2. Identify 47

5.3. Protect 64

5.4. Detect 87

5.5. Respond 97

5.6. Recover 107

References 114

Appendix A. Selected Bibliography 119

Appendix B. List of Symbols, Abbreviations, and Acronyms 120

Appendix C. Glossary 124

Appendix D. Figure Descriptions 125

D.1. Description of Fig. 1 125

D.2. Description of Fig. 2. 125

D.3. Description of Fig. 3. 125

D.4. Description of Fig. 4. 127

List of Tables

Table 1. Criticality determinations for GOVERN Function in business and mission objectives 22

Table 2. Criticality determinations for IDENTIFY Function in business and mission objectives 23

Table 3. Criticality determinations for PROTECT Function in business and mission objectives 23

Table 4. Criticality determinations for DETECT Function in business and mission objectives 24

Table 5. Criticality determinations for RESPOND Function in business and mission objectives 25

Table 6. Criticality determinations for RECOVER Function in business and mission objectives 25

Table 7. CSF 2.0 Functions and Categories 27

Table 8. Subcategory-level guidance for GOVERN Function 29

Table 9. Subcategory-level guidance for IDENTIFY Function 47

Table 10. Subcategory-level guidance for PROTECT Function 64

Table 11. Subcategory-level guidance for DETECT Function 87

Table 12. Subcategory-level guidance for RESPOND Function 97

Table 13. Subcategory-level guidance for RECOVER Function 107

List of Figures

Fig. 1. Semiconductor manufacturing ecosystem. 3

Fig. 2. Functional domains of the semiconductor manufacturing ecosystem. 4

Fig. 3. Elements of semiconductor cybersecurity 7

Fig. 4. Several patterns of CSF subcategory mappings between CSF 1.1 and CSF 2.0. 9

Acknowledgments

The authors gratefully acknowledge and appreciate the efforts of SEMI Semiconductor Manufacturing Cybersecurity Consortium (SMCC) Workgroup 4 (WG4) - International Regulation and Specs, as well as the significant contributions of SEMI SMCC Project Managers, Mayura Padmanabhan and Basak Ulutas Ozturkler, in facilitating and supporting the group's activities and SMCC WG4 Sponsor Kannan Perumal, Applied Materials. A special acknowledgment is also extended to the following members:

- Laurent Chalifoux, Siemens Industry Inc.
- Tom Dodson, Intel Corporation
- Melissa Grupen-Shemansky, SEMI
- Swetha Kalidindi, Applied Materials Inc.
- Hideyuki Kato, Deloitte Tohmatsu Cyber LLC.
- Tim Kokes, Onto Innovation Inc.
- Takayuki Nishimura, SCREEN Semiconductor Solutions
- Taylor Roberts, Intel Corporation
- Paul Trio, SEMI

The authors also thank the NIST Manufacturing CSF Profile team, especially Keith Stouffer, Michael Pease, CheeYee Tang, and Timothy Zimmerman, as well as the NIST Genomics CSF Profile team, and Isabel Van Wyk.

Executive Summary

This document introduces the NIST Cybersecurity Framework (CSF) 2.0 Semiconductor Community Profile, which provides guidance for mitigating cybersecurity risks and aligning with the unique goals and best practices of the semiconductor sector.

The Semiconductor Community Profile offers the following benefits:

- **Enhanced Cybersecurity Posture:** Provides a structured method for identifying and addressing areas to improve the current cybersecurity practices within semiconductor manufacturing systems
- **Risk Management:** Facilitates an evaluation of risk levels to ensure that control environments operate within acceptable parameters to minimize cybersecurity threats
- **Standardized Approach:** Establishes a consistent methodology for developing and maintaining robust cybersecurity plans for ongoing security assurance across the semiconductor manufacturing life cycle

The Profile is structured around the six primary Functions of the Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond, and Recover. These functional areas serve as the foundation for creating a semiconductor manufacturing-specific profile. Further expansion of the core functional areas leads to the flexibility and adaptability of the framework in various subdomains of the semiconductor ecosystem, namely fabrication, enterprise IT, and equipment and tooling. This expansion provides insights into the separation of duties between these domains and also shows the synergies that will enable the entire semiconductor ecosystem to be more secure.

The Semiconductor Community Profile focuses on achieving key cybersecurity outcomes and offers guidance for identifying and prioritizing opportunities for improvement. It aligns security activities with specific business and mission objectives to ensure that relevant and actionable security practices are implemented effectively.

This Profile also provides a voluntary, risk-based approach to managing cybersecurity activities and reducing cyber risks in the semiconductor sector. It is designed to supplement — not replace — existing cybersecurity standards and industry guidelines, thereby enhancing the overall security framework within the industry.

By adopting CSF 2.0, semiconductor manufacturers can improve their cybersecurity resilience, assist with regulatory compliance, and protect their critical assets from evolving cyber threats. This comprehensive framework supports the industry’s commitment to maintaining robust cybersecurity measures and safeguarding both operational integrity and sensitive data.

1. Introduction

The NIST Cybersecurity Framework (CSF) [CSF v2] describes desired cybersecurity outcomes that are sector-, country-, and technology-neutral. Each outcome is mapped to potential security controls for immediate consideration to mitigate cybersecurity risks. The CSF is voluntary and provides each organization with the flexibility needed to address its unique risks, technologies, and mission considerations. Created through collaboration between government and the private sector, the CSF provides a common language for addressing and managing cybersecurity risks in a cost-effective way based on business needs without imposing additional regulatory requirements.

A CSF Community Profile is a baseline of CSF outcomes that addresses shared interests and goals among a number of organizations. NIST's existing Manufacturing Community Profile [IR 8183r1] defines specific cybersecurity activities and outcomes for the protection of manufacturing systems and their components, facilities, and environments. Using the Manufacturing Profile, manufacturers can align cybersecurity activities with business requirements, risk tolerances, and resources.

The National Cybersecurity Implementation Plan Version 2 [NCSIP] directed several organizations, including NIST, to collaboratively develop cybersecurity guidance for semiconductor development and manufacturing. The semiconductor manufacturing environment is a complex ecosystem of device makers, equipment OEMs, suppliers, and solution providers. The Semiconductor Manufacturing Community Profile — further referenced in this document as "the Profile" — builds on the Manufacturing Community Profile, maps its guidance from CSF 1.1 to CSF 2.0, and refines its guidance to semiconductor-specific development and manufacturing.

The Profile considers threats and risks that are specific to the semiconductor manufacturing industry. As an initial draft, this Profile is still in development. Topics are expected to be added to future drafts (e.g., provenance with immutable records for validation purposes).

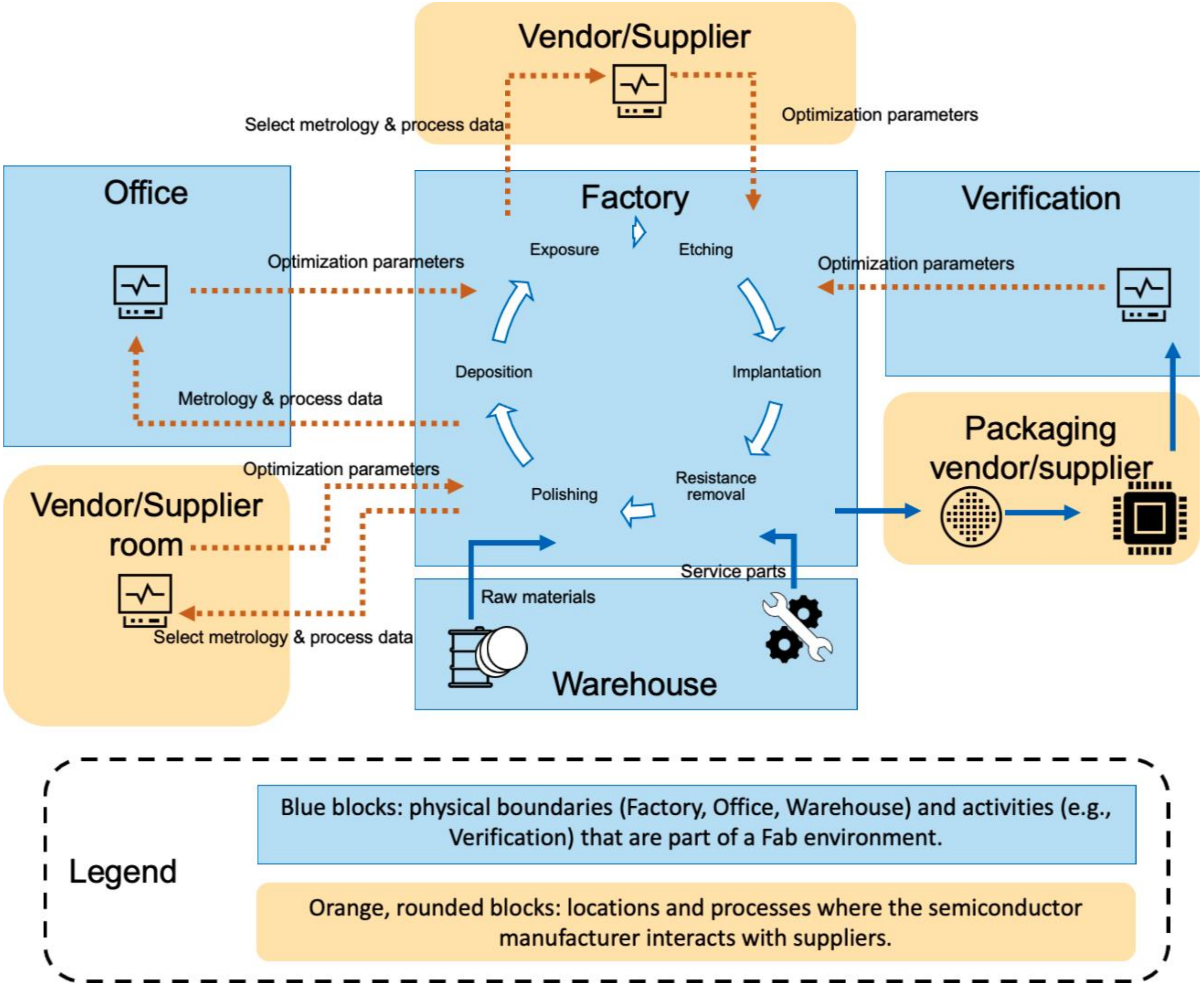
1.1. Purpose

This document defines the Semiconductor Manufacturing Community Profile, which provides a voluntary, risk-based approach for managing cybersecurity activities, reducing cyber risks, and improving the cybersecurity posture of semiconductor manufacturing systems.

The Profile suggests prioritizations of security activities to meet specific business and mission objectives and identifies relevant and actionable security practices that can be implemented in support of those objectives. The semiconductor manufacturing sector could establish a baseline that can be used among its constituents as a sector-specific starting point from which to build organization-specific profiles.

1.2. Semiconductor Fabrication Ecosystem Functional Domains

Figure 1 shows the semiconductor fabrication ecosystem and data and material flows. The ecosystem consists of multiple units that may be physically separated and are denoted with building blocks. The steps needed to create a semiconductor design are carried out in the factory region and normally performed on thin slices of highly purified, defect-free crystalline material called *wafers*. The most used material is single silicon crystal.



Blue blocks: physical boundaries (Factory, Office, Warehouse) and activities (e.g., Verification) that are part of a Fab environment.

Orange, rounded blocks: locations and processes where the semiconductor manufacturer interacts with suppliers.

Fig. 1. Semiconductor manufacturing ecosystem

The factory is also sometimes referred to as the “clean room.” Even a minute amount of dust can disrupt the manufacturing process. The International Organization for Standardization (ISO) provides classifications for clean rooms, with an ISO1 being the highest classification of cleanliness.

A semiconductor design consists of tens or hundreds of layers of various materials — some conducting, some insulating — that need to be perfectly aligned to implement the complex circuitry of a modern-day semiconductor microchip. These layers are created on the wafer using photomasks (“masks”), and material is either deposited or etched. Manufacturing a modern-day microchip may require more than 75 masks. All of these steps are performed in the factory and repeated for different masks to create the different layers. They are broadly classified as exposure, etching, implantation, removal of photo-resistance, surface polishing, deposition, and others.

The materials and minerals required to process the layers are stored in the warehouse. Strict inventory controls ensure adequate quantities of appropriate quality materials and minerals, many of which may only be obtained from other regions of the world.

Due to the precise control necessary to ensure that layers are aligned and formed correctly, metrology is fundamental to ensuring the successful construction of each layer. Various parameters are measured from the layers or special structures, which helps optimize the parameters for the various equipment needed to accomplish the steps described in the factory. Verification helps ensure the successful construction of a layer and helps further optimize the parameters.

The factory utilizes automated material handling systems (AMHS), which are robotic and other transportation systems that convey materials in the facility or between buildings. IT automation is necessary for various pieces of equipment to perform the factory's steps.

Numerous vendors and suppliers with expertise in equipment or the handling of materials are crucial to overall operations. There may be different types of vendors with varying degrees of access to the factory, such as within a vendor/supplier room that has a supplier network for monitoring and optimizing certain parameters.

Figure 2 shows three functional domains for managing cybersecurity across the factory ecosystem: equipment and tooling, the fab environment, and Enterprise IT infrastructure.

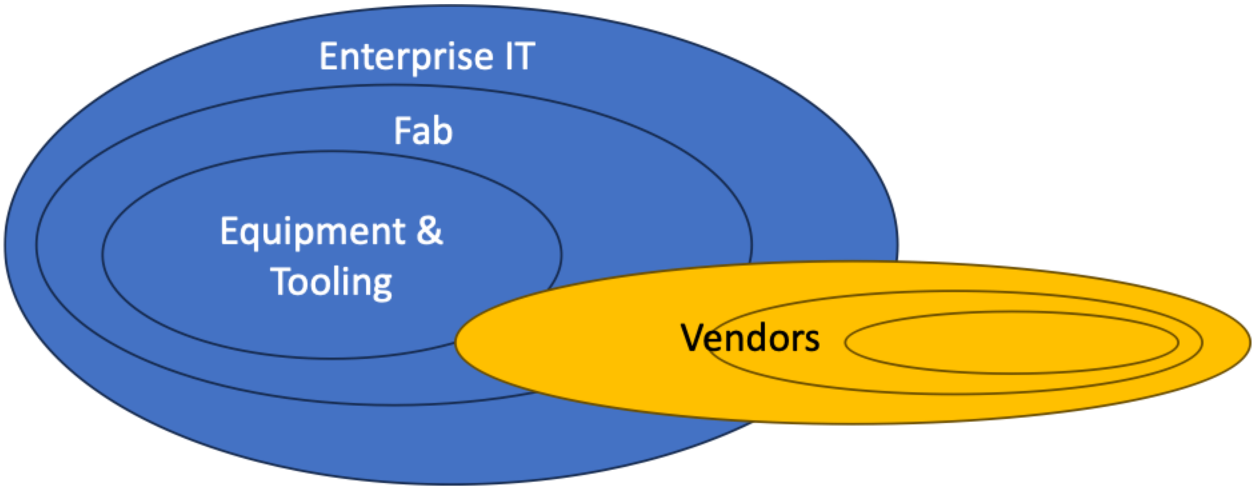


Fig. 2. Functional domains of the semiconductor manufacturing ecosystem

The equipment and tooling domain is necessary to perform the various steps and necessary metrology for manufacturing microchips. The equipment is in the factory ecosystem, or "fab" domain, which interacts with Enterprise IT to receive accurate monitoring data (e.g., environmental, user activity) and controls. The Enterprise IT domain also provides critical support to both the fab and equipment and tooling domains by managing monitoring and control data.

1.2.1. Development of Secure Equipment and Tooling

The scope of equipment and tooling within this Community Profile encompasses the equipment, tooling, and networks required to develop and manufacture semiconductors, including their underlying software and hardware components that may be vulnerable to cyber threats. This initial document emphasizes risk management, the availability of the manufacturing process, and the intellectual property of the semiconductor design rather than the resulting device or provenance. It does not delve into the specific security measures, practices, or protocols related to the physical or digital protection of the actual semiconductor designs themselves. The semiconductor industry develops advanced tools and machinery that are vital to:

- Ensuring continuity in the advanced manufacturing process and
- Providing the next generation of tools and machinery required to drive innovation and meet technological challenges, such as generative AI, quantum computing, and cloud computing.

Semiconductor manufacturing relies on a variety of sophisticated tooling and equipment, including firmware, software, hardware, and supporting services. Examples include but are not limited to:

1. **Photolithography machines:** For transferring circuit patterns onto wafers
2. **Vapor deposition systems:** For depositing thin films on wafers
3. **Etching systems:** For selectively removing material to create circuit patterns
4. **Material modification systems:** For modifying the properties of semiconductor materials
5. **Metrology equipment:** For measuring and inspecting wafers to ensure quality control
6. **Automated material handling systems (AMHSs)**: Robotic or other transportation systems for conveying materials in the facility or between buildings

These tools are often provided by original equipment manufacturers (OEMs) and are integrated with the fab's IT networks for real-time monitoring and control.

1.2.2. Fab Environment

The fab is the core of semiconductor manufacturing. It is a controlled environment in which silicon wafers are processed to create integrated circuits (ICs). Operational technology (OT) is one of the primary cybersecurity differentiators in the fab.

Key processes within a fab include:

1. **Photolithography:** Using light to transfer a pattern onto the wafer
2. **Etching:** Removing material from the wafer to create the circuit design
3. **Doping:** Adding impurities to alter electrical properties
4. **Deposition:** Applying layers of materials onto the wafer surface
5. **Packaging facility:**
    a. **Assembly:** Attaching the die to a substrate or lead frame and connecting it to the package leads
    b. **Testing:** Performing comprehensive testing to ensure that the device meets all specifications and is free of defects
    c. **Wafer-level assembly (WLA):** Stacking multiple dies together without a package substrate

The fab environment includes supporting materials, communications, security, safety systems, and sophisticated software and hardware infrastructure. It uses a multi-step detailed process that includes design, materials, interconnected transport processes, intricate wafer engineering, data analysis, automation software and hardware, assembly, packaging, and testing technologies to fabricate and manufacture semiconductor devices. The environment is also characterized by stringent control over contamination, temperature, and humidity to ensure the high quality and yield of semiconductor devices, as well as human and environmental safety.

1.2.3. Enterprise IT Infrastructure in Semiconductor Manufacturing

The IT infrastructure in semiconductor manufacturing has a specialized application stack that supports a wide range of functions, including:

1. **Manufacturing execution systems (MESs):** Managing and monitoring production processes and ensuring that manufacturing operations run smoothly
2. **Data management systems:** Collecting and analyzing data from various stages of the manufacturing process to optimize performance and yield
3. **Supply chain management:** Coordinating with suppliers and logistics to ensure the timely delivery of materials and components
4. **Enterprise resource planning (ERP):** Integrating core business processes (e.g., finance, HR, and procurement) with manufacturing operations
5. **Material control systems (MCSs) and AMHSs:** Optimizing production by managing AMHS hardware, interfacing with key automation systems, tracking real-time data, and serving as the plan of record for lot locations, physical movements, and routing to improve yield, efficiency, and quality

The interconnected nature of these IT systems makes them crucial for the efficient functioning of semiconductor fabs but also exposes them to cybersecurity risks.

1.3. Security of Semiconductor Manufacturing

Securing semiconductors involves protecting the design and related intellectual property (IP), tracking the history of components to build trust, and ensuring a secure manufacturing process. Securing the microchip also includes measures like tamperproof packaging and strong encryption to protect data. Secure boot processes ensure that only verified software runs on the device, and verifying and auditing the supply chain help prevent counterfeit parts. Managing the entire life cycle involves secure setup, updates, and end-of-life handling supported by thorough security tests and compliance with regulations. Educating users on security practices and continuously improving security measures help defend against new threats and ensure that semiconductor devices stay secure throughout their use.

Figure 3 illustrates various elements for securing semiconductors and establishing trust and provenance. It also highlights a crucial foundational activity that is necessary before other mechanisms to establish security can be discussed. The illustrated regions represent the stages of the semiconductor lifecycle and its broader ecosystem where the Manufacturing Profile plays a role. The figure also highlights example threats that the Semiconductor Manufacturing Profile aims to mitigate.

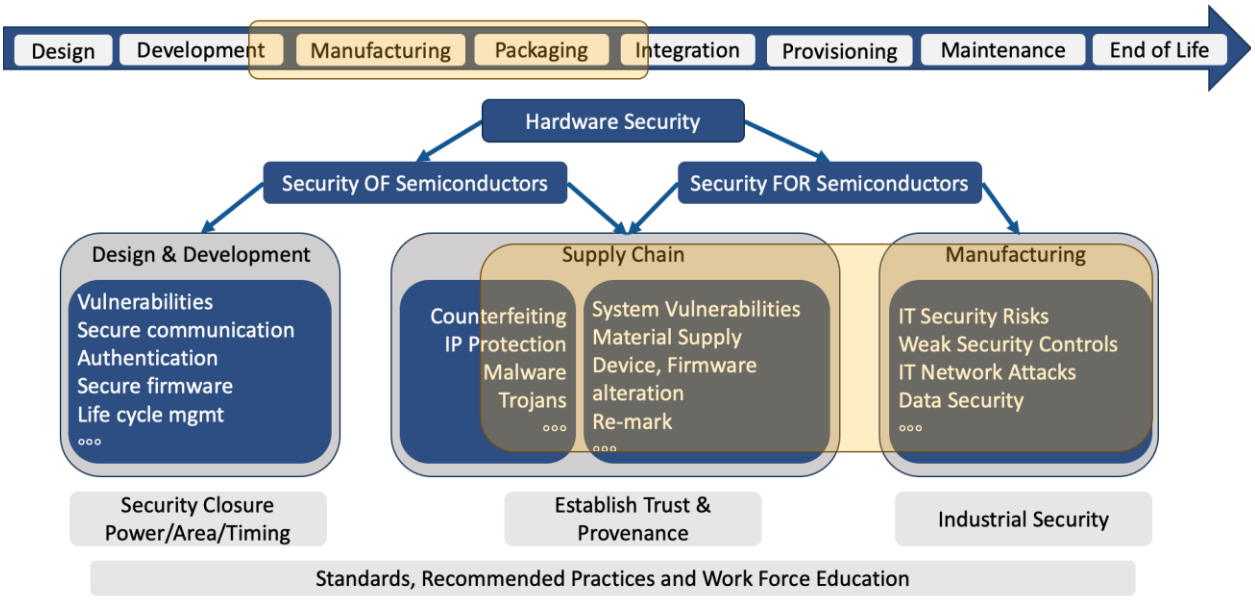


Fig. 3. Elements of semiconductor cybersecurity

Securing the manufacturing ecosystem is fundamental to securing a microchip. Microchips are manufactured in a highly sophisticated clean room environment called a semiconductor fabrication plant or “fab.” A modern-day fab costs many billions of dollars. Securing the high-cost investment is one of the key components of the overall security of semiconductors. There are several reasons to ensure security of the fab:

- Fab facilities are highly automated and rely on complex digital systems that are vulnerable to cyber attacks. Such attacks could disrupt production, alter manufacturing processes, or steal proprietary design data. Securing these facilities helps prevent data breaches, IP theft, and sabotage, ensuring that the chips made are safe, reliable, and free from tampering.
- The semiconductor industry invests heavily in research and development, leading to unique and proprietary designs and processes. A breach at a fabrication plant could result in the theft or exposure of this valuable IP, giving competitors an advantage. Keeping fabs secure is vital for preventing IP theft and maintaining a lead in chip technology.
- The manufacturing process in a fab is delicate; even small disruptions or tampering can cause defects and poor-quality products. Ensuring the security of the fab environment helps maintain smooth production without interruptions that could impact product performance. This is especially crucial for high-performance and mission-critical applications where chip quality and reliability are particularly important.
- Fabs are a key part of a global supply chain that produces advanced chips for various products and industries. Any disruption in a fab's operations — whether from cyber attacks, sabotage, or natural disasters — can cause major supply chain issues that lead to shortages and economic consequences across different sectors. A secure manufacturing environment ensures that the facility operates without interruptions, supports a reliable supply of chips, and meets regulatory and compliance standards as well as economic and revenue goals.

The Cybersecurity Framework Profile developed for this document supports Initiative 5.5.5 in the National Cybersecurity Strategy Implementation Plan [NCSIP], which asks NIST and other government agencies to "develop guidance for secure development and manufacturing of semiconductors."

1.4. Relationship to CSF Core and Manufacturing Profile

This document should be referenced in conjunction with NIST Internal Report (IR) 8183r1 (Revision 1), *Cybersecurity Framework Version 1.1 Manufacturing Profile*, which provides a foundation for the new Community Profile that focuses on semiconductor manufacturing using CSF 2.0. Readers should have a copy of IR 8183r1 available in order to understand some of the later sections of this document.

The Semiconductor Manufacturing Community Profile is structured much like the Manufacturing Profile: several sections of introductory and expository text precede tables of specific guidance on Subcategory-level CSF goals. The sections before the tables are meant to be read alone, except for two specific references on prioritizations in the Manufacturing Profile. However, the Subcategory-level tables in Sec. 5 heavily reference guidance from the Manufacturing Profile.

There are several motivations for this reading style:

1. The early timeline of this document's production coincided with NIST's release of CSF 2.0 [CSF_v2].

2. The Manufacturing Profile, written based on CSF 1.1, had not yet transitioned to CSF 2.0 when the Semiconductor Manufacturing Community Profile was specified to have its initial version completed [NCSIP].

3. Guidance in the Manufacturing Profile was found by the participating semiconductor manufacturing community to be widely applicable. However, the Manufacturing Profile's guidance was acknowledged as a potential challenge for reuse in a CSF 2.0 document. Much of the guidance is copied from the Manufacturing Profile, often split with more specificity than in the general Subcategory mappings that are available between CSF 1.1 and 2.0. Readers are still encouraged to review IR 81831r1 for the original guidance points' risk levels, which were not chosen to be refined or much noted within this document (see Sec. 5). The participants found it most pragmatic to incorporate some of the Manufacturing Profile's Subcategory guidance, carefully track reference sources, and enhance the guidance with rationales and considerations that are specific to semiconductor manufacturing.

This document mitigates some of the challenges in converting the CSF 1.1-structured content in the Manufacturing Profile to use the CSF 2.0 structure in the new Community Profile. NIST has provided two resources to map CSF Subcategories between version 1.1 and 2.0. One resource [CSF_2to1] takes a CSF 2.0 Function, Category, or Subcategory and lists its corresponding CSF 1.1 counterparts. The other resource [CSF_1to2] starts from CSF 1.1 and maps similarly to CSF 2.0. Some of these mappings align, as with DE.AE-2 in CSF 1.1 mapping to DE.AE-02 in CSF 2.0. However, some mappings are asymmetric, such as CSF 1.1 subcategory ID.AM-3, which maps to CSF 2.0 Subcategories ID.AM-03 and ID.AM-07, though ID.AM-03 maps from 2.0 to ID.AM-3 and DE.AE-1 in 1.1. These mapping patterns and others are illustrated in Fig. 4. The Semiconductor Manufacturing Community Profile handles these mappings in specifically described manners for Subcategory-suggested prioritizations (Sec. 4) and enumerated Subcategory references in the guidance tables (Sec. 5).

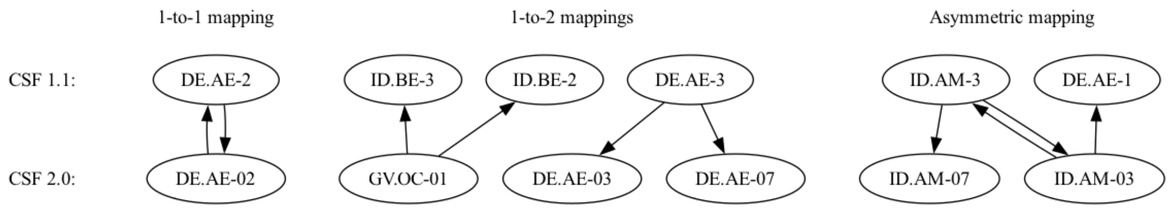


Fig. 4. Several patterns of CSF subcategory mappings between CSF 1.1 and CSF 2.0

The Semiconductor Manufacturing Community Profile is structured to be accessible, regardless of prior familiarity with the CSF. Some mapping challenges are present from building on a CSF 1.1 Community Profile. This document addresses much of the mapping challenges between CSF 1.1 and 2.0 by pre-applying existing NIST mapping guidance, as described in this section. In summary, this document specializes previous guidance on the cybersecurity posture of manufacturers for the semiconductor manufacturing ecosystem.

1.5. Document Organization

The remainder of this document is organized as follows:

- Section 2 provides an overview of semiconductor manufacturing systems.
- Section 3 provides an overview of CSF 2.0.
- Section 4 provides the rationale for integrating cybersecurity into semiconductor manufacturing business and mission objectives.
- Section 5 describes the semiconductor manufacturing implementation of the CSF subcategories.
- The References section provides a list of sources and citations used in this document.
- Appendix A provides a list of other resources used in the development of this document.
- Appendix B provides a list of acronyms and abbreviations used in this document.
- Appendix C provides a glossary of terms used in this document.
- Appendix D provides detailed descriptions of the figures in this document.

2. Overview of Semiconductor Manufacturing and Operational Systems

The semiconductor manufacturing industry has unique characteristics that can make it challenging to implement cybersecurity mitigations. For example:

- Intellectual property (IP) protection mechanisms should be suited to scenarios in which protected IP is shared between the local organization, suppliers, and customers.
- Legacy systems often cannot be patched and are generally difficult to adapt or modify to meet current cybersecurity standards.
- Environmental control requirements can be especially sensitive, as operations produce devices measured in nanometers.
- The threat landscape for the industry is growing due to increased connectivity within fabs and between fabs and other external resources, analytics and required internal and external data flows, and rapidly expanding global workforces and supply networks.
- Standard outages in the IT world have a highly restricted corresponding window in fab operations, which limits the ability to test disaster recovery protocols or implement additional controls.

2.1. Importance of NIST CSF 2.0 in Semiconductor Manufacturing

The NIST CSF is crucial for managing cybersecurity risks in semiconductor manufacturing by addressing:

1. **Risk Management:** It provides a structured approach to identifying, assessing, and managing cybersecurity risks, which is vital in the highly sensitive and interconnected semiconductor fab environment.
2. **Resilience:** It emphasizes the importance of resilience to enable fabs to quickly detect, respond to, and recover from cybersecurity incidents, thus minimizing downtime and economic loss.
3. **Supply Chain Security:** It addresses the security of the entire supply chain to ensure that all components are secure, including those from third-party suppliers. This is particularly important given the reliance on OEM tools and equipment.
4. **Operational Efficiency:** Implementing the CSF can improve operational efficiency by ensuring that IT systems and manufacturing processes are secure and reliable.

To maximize the impact of the CSF, the semiconductor industry emphasizes four key strategies:

1. **Fostering collaboration** among semiconductor manufacturers, OEM equipment suppliers, and supply chain partners to develop a comprehensive and unified CSF Community Profile that is tailored to the unique needs and challenges of the semiconductor industry.
2. **Identifying, standardizing, and disseminating best practices** for cybersecurity across the semiconductor industry, including guidelines and protocols that address specific

risks and vulnerabilities inherent to semiconductor fabs, OEM equipment, and the supply chain.

3. **Promoting cybersecurity awareness and providing specialized training** for personnel at all levels within the semiconductor industry to build a culture of security and ensure that all stakeholders understand their roles and responsibilities in maintaining cybersecurity.
4. **Implementing mechanisms for continuous feedback and improvement of the CSF Community Profile** within the semiconductor community, including regular reviews, updates, and the integration of new technologies and threat information to keep the framework relevant and effective.

By creating a dedicated NIST CSF community within the semiconductor industry, stakeholders can collaborate, standardize practices, and adapt to emerging threats. This collective effort not only mitigates cybersecurity risks but also ensures a secure, resilient, and efficient manufacturing ecosystem that benefits the entire sector.

3. Overview of CSF 2.0

Created through collaboration between industry and government, the NIST CSF 2.0 provides prioritized, flexible, risk-based, and voluntary guidance that builds on existing standards, guidelines, and practices to help organizations better understand, manage, reduce, and communicate about cybersecurity risks.

The CSF enables organizations — regardless of size, degree of cybersecurity risk, or cybersecurity sophistication — to apply the principles and recommended practices of risk management to improving security and resilience. The framework provides a common language for understanding, managing, and expressing cybersecurity risks and for conducting management-level cybersecurity communications among internal and external stakeholders and across an organization.

The CSF consists of three main components[1]:

1. The **Core** is a taxonomy of high-level cybersecurity outcomes that uses common language to make it easy to understand, regardless of cybersecurity expertise. The Core guides organizations in managing their cybersecurity risks while complementing their existing cybersecurity and management processes.
2. **Tiers** can be used to characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks. Further discussion of Tiers is out of scope for this document, as they do not generally apply directly to Community Profiles. Further description of Tiers is available in "A Guide to Creating Community Profiles" [CSWP_32_ipd].
3. **Profiles** are used to understand, assess, prioritize, and communicate about the Core's outcomes for organizations and communities. Profiles provide a customized alignment of requirements, business and mission objectives, risk appetite, and resources with the desired outcomes of the CSF Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity in a specific context (e.g., an organization's mission needs or a community use case).

3.1. The CSF Core

The Framework Core is organized into six Functions that provide a high-level, strategic view of the life cycle of an organization's cybersecurity risk management: Govern, Identify, Protect, Detect, Respond, and Recover.

- **GOVERN (GV) —** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and

[1] The terms Core, Tiers, Profile, Mission Objectives, Function, Category, and Subcategory are capitalized when they are used to describe elements of the CSF throughout this document.

stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- **IDENTIFY (ID) —** The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.
- **PROTECT (PR) —** Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.
- **DETECT (DE) —** Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.
- **RESPOND (RS) —** Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.
- **RECOVER (RC) —** Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

The six Functions of the CSF 2.0 Core are composed of 22 Categories, which are further broken down into 106 Subcategories of more specific outcomes. Section 4 presents the prioritization for all 106 Subcategories for each Mission Objective with one table for each of the six Functions in the CSF Profile. Section 5 provides more detailed guidance on each Function, Category, and Subcategory as part of defining the Community Profile.

NIST also provides supplemental resources to help organizations understand, adopt, and use the CSF 2.0 and achieve the desired outcome of each Subcategory, including Implementation Examples and Informative References. The NIST CSF website contains the most current information regarding available Implementation Examples and Informative References. Communities and organizations can choose to add their own Implementation Examples and Informative References that are unique to the semiconductor manufacturing context in the future.

3.2. Community Profiles

A *Community Profile* is a baseline of CSF outcomes that represents shared interests and goals for reducing cybersecurity or privacy risks among organizations that share a common context, such as sector or technology. Community Profiles offer a prioritization of CSF Subcategories based on mission and operational considerations for a specific community, industry, or group of stakeholders, such as the semiconductor manufacturing community. Community Profiles can also inform the development of an organization's Target Profile (described further in Sec. 3.3) by providing a useful starting point for identifying and engaging in discussions about cybersecurity activities and outcomes that are important to the Profile's user community. Within an organization, Target Profiles offer a consistent way to discuss cybersecurity objectives across organizational roles—from senior leadership to technical implementors—using common terminology.

Profiles are oriented around an organization's business and mission objectives, identify the Subcategories that are especially relevant to each mission objective, and suggest how those Subcategories could be prioritized. An organization can adapt its business and mission objectives and Subcategory prioritization to fit its unique needs. Community Profiles can also help organizations allocate resources to cybersecurity and privacy improvements or address areas of specific risk.

3.3. Applying the NIST CSF to Semiconductor Manufacturing

This Semiconductor Manufacturing Community Profile prioritizes CSF Subcategories that were designed to help organizations protect their manufacturing systems throughout the semiconductor manufacturing life cycle (illustrated in Fig. 3). Organizations can use the Profile's guidance, rationale, and considerations to examine and potentially improve their existing cybersecurity practices and activities.

Organizations may apply the Semiconductor Manufacturing Community Profile by first identifying and describing their business and mission objectives. Section 4 describes business and mission objectives for the semiconductor manufacturing ecosystem that were developed with stakeholder input. Organizations may apply these or similar objectives or develop their own. Each organization can then prioritize their objectives based on their requirements and strategic goals.

Next, organizations can crosswalk their business and mission objectives to the Semiconductor Manufacturing Community Profile's Subcategories using the tables in Sec. 4.2 to identify priority Subcategories. The General Rationales and Mission Objective Specific Considerations in Sec. 5 can be used to adjust the priority of Subcategories to reflect organizational needs. During this activity, organizations consider any constraints or guidance (e.g., applicable state laws, policies, standards), risks, and other influencing factors that can impact their business and mission objectives or the priority of Subcategories. At each step, organizations can document rationales, considerations, and any additional Informative References. This results in an Organizational Target Profile.

Based on their review and adjustment of business and mission objectives and priority Subcategories, organizations examine their current cybersecurity activities and processes to create an Organizational Current Profile. Organizations can then identify any gaps between their Current and Target Profiles. This gap analysis can help organizations determine whether they need to reallocate cybersecurity resources toward capabilities that help achieve prioritized Subcategories and accomplish their objectives. Additionally, organizations can compare the activities and priorities in their Current Profile to those in the Semiconductor Manufacturing Community Profile.

4. Applying Business and Mission Objectives to Profile Creation

A collaborative community within the semiconductor industry convened to create, adopt, and maintain a tailored NIST CSF Community Profile specifically for semiconductor manufacturing, encompassing device makers, OEMs, suppliers, and solution providers. This Profile fosters industry-wide best practices, shared knowledge, and coordinated efforts to enhance cybersecurity resilience in support of a set of common business and mission objectives.

4.1. Semiconductor Manufacturing Business and Mission Objectives

To provide context for cybersecurity risk mitigation efforts, this Profile identifies five primary business and mission objectives for the semiconductor manufacturing sector, as well as supporting cybersecurity practices for each:

- **Maintain environmental safety:** Manage cybersecurity risks that could adversely affect the environment, including both accidental and deliberate damage. Personnel should understand the interdependencies between cybersecurity and environmental safety.
- **Maintain human safety:** Manage cybersecurity risks that could potentially impact human safety. Personnel should understand the interdependencies between cybersecurity and human safety.
- **Maintain production goals:** Manage cybersecurity risks that could adversely affect production goals, throughput, and yield, including asset damage and unscheduled downtime for lines and equipment. Personnel should understand the interdependencies between cybersecurity and production goals.
- **Maintain the quality of semiconductors:** Manage cybersecurity risks that could adversely affect the quality of the product and/or processes. Ensure that the integrity of the semiconductor manufacturing process, OEM equipment, and associated data throughout the supply chain is maintained.
- **Protect sensitive information:** Manage cybersecurity risks that could lead to the loss or compromise of the organization’s IP and sensitive and/or regulated business data, including information that pertains to semiconductor fabs, OEM equipment, and the supply chain.

4.1.1. Objective 1: Maintain Environmental Safety

Enhancing cybersecurity measures protects infrastructure and environmental safety, ensures compliance with environmental regulations, and maintains public and ecological health. Hazardous environmental incidents can arise from both accidental and intentional cyber disruptions, such as the release of toxic substances or the failure of waste management systems.

Domain-specific security approaches to maintaining environmental safety include:

- **Fab domain:** Sensitive technologies and materials could cause significant environmental damage if compromised. These controls are secured to prevent unauthorized access and mitigate the risks of contamination or hazardous waste leaks.
- **Enterprise IT domain:** Ensuring that these systems are secure prevents manipulations or disruptions that could lead to environmental hazards. Secure and reliable IT systems are vital for continuous monitoring and quick response capabilities.
- **Equipment and tooling domain:** Automated systems to manage materials and waste depend on accurate and timely data from enterprise IT for proper functioning. Protecting the cybersecurity of these systems ensures that the management of materials and waste adheres to environmental safety standards to prevent breaches that could lead to ecological damage. Environmental safety is supported by the safety standards and controls that are integrated into the equipment and tooling development life cycle.

4.1.2. Objective 2: Maintain Human Safety

Focusing on cybersecurity can help prevent incidents that compromise human safety, such as exposure to toxic substances or mechanical failures. The industry can ensure a safe working environment for all personnel by adhering to stringent occupational safety standards and securing systems and processes that, if compromised, could directly harm workers and other stakeholders.

Domain-specific security approaches to maintaining human safety include:

- **Fab domain:** Enhancing cybersecurity measures and mitigations for safety-critical systems that depend on secure communications and data integrity, especially around physical sensor networks related to safety, may prevent potential malfunctions or disruptions that could pose risks to humans. Physical mitigating controls may have corresponding cyber-physical mitigations that could impact safety, such as authentication lockouts and safety-reporting mechanisms. Safety controls that are already in place should not be neglected just because cybersecurity controls are being added. Organizations are encouraged to take a defense-in-depth approach to strengthen assumptions around safety controls.
- **Enterprise IT domain:** Safety protocols ensure the deployment and management of safety measures across the facility and the immediate initiation of emergency responses.
- **Equipment and tooling domain:** Continuous and secure data flows ensure that automated machinery that could endanger human lives is effectively monitored and controlled. Adoption cybersecurity controls in secure software and system development life cycles contributes to the implementation of measures and mitigations that will enhance fail-safe operations.

4.1.3. Objective 3: Maintain Production Goals

Achieving production goals depends heavily on the security and reliability of both physical and IT infrastructure. Cybersecurity risks that disrupt production can lead to significant financial losses and supply chain disruptions. Managing these risks ensures continuous production operations, optimizes throughput and yield, and maintains the industry's ability to meet market demands efficiently.

Domain-specific security approaches to meeting production goals include:

- **Fab domain:** Seamless data integration and system coordination help ensure that production processes are efficiently managed. Securing fab equipment and operational systems against cyber threats is crucial to maintaining continuous production cycles and minimizing downtime.
- **Enterprise IT domain:** Coordinating production schedules and logistics prevents disruptions that can lead to production delays or inaccuracies in the manufacturing process. These systems ensure that logistical and scheduling data are accurately communicated and implemented.
- **Equipment and tooling domain:** Protecting against cyber threats to automated processes and systems is vital for maintaining steady production flows and achieving production goals. This domain depends on the integrity and security of data to effectively manage and control production. Dedicated resources should be provisioned for security mitigating controls to ensure that production is not slowed down and production goals are not impacted.

4.1.4. Objective 4: Maintain the Quality of Semiconductors

4.1.4.1. Objective Overview and Importance to the Semiconductor Industry

Maintaining the quality of semiconductor products is linked to managing cybersecurity risks. Protecting against cyber threats that could compromise the manufacturing process, equipment, and data throughout the supply chain is crucial. Effective cybersecurity practices are an essential pillar in ensuring that the manufacturing process remains uncontaminated and that the end products meet the standards required for their performance and reliability in various applications, including critical infrastructure and consumer electronics.

4.1.4.2. Detailed Domain-Specific Security Approaches for Quality of Semiconductors

- **Fab Domain:** Depends on reliable data, protocols, controls, and system operations from the IT/OT infrastructure to maintain process integrity. Cybersecurity measures in fabs protect the precision and consistency of manufacturing processes, essential for producing high-quality semiconductors.

- **Enterprise IT Domain:** Shares the quality monitoring responsibility (with the Fab domain) and manages production data, providing critical oversight and data to the Tooling and Equipment domain to ensure quality across all stages of manufacturing. Secure IT systems ensure that operational protocols and quality standards are consistently applied.

- **Tooling and Equipment Domain:** Relies on accurate and secure data to ensure that all manufacturing parameters are correctly applied and maintained. Robust cybersecurity in the Tooling and Equipment domain ensures that manufacturing processes run without interference, maintaining the standards necessary for quality assurance in semiconductor products.

Reliability of Fab, Equipment, and Tooling data is central to the IT/OT infrastructure environment, and cyber security protocols and controls provide assurances on data integrity.

4.1.5. Objective 5: Protect Sensitive Information

4.1.5.1. Objective Overview and Importance to the Semiconductor Industry

Protecting sensitive information, including intellectual property and regulated business data, is paramount in the semiconductor industry. Managing cybersecurity risks that could lead to the loss or compromise of this information is crucial for maintaining competitive advantage, complying with regulatory requirements, and ensuring the confidentiality and integrity of business operations.

4.1.5.2. Detailed Domain-Specific Security Approaches for Protecting Sensitive Information

- **Fab Domain:** Ensures that operational data is securely shared and used. It utilizes a variety of proprietary technologies and processes, making it a target for industrial espionage. Secure communication and data integrity are crucial for protecting assets.

- **Enterprise IT Domain:** Provides the necessary security protocols and data integrity assurances that support the Fab and the Tooling and Equipment domains in maintaining secure operations. It handles sensitive corporate and customer data and ensures that all data flows between domains are secure and compliant with data protection requirements.

- **Equipment and Tooling Domain:** Uses security protocols provided by equipment, the Fab, or the Enterprise IT domain to safeguard sensitive information, protecting against unauthorized access to operational data and intellectual property. The equipment and tooling may itself contain sensitive data, such as configurations or metrology data, that may be considered sensitive IP for organization operations.

4.2. Aligning Subcategories to Meet Business and Mission Objectives

The Profile Subcategories are prioritized to align cybersecurity goals with specific business and mission objectives. This allows the manufacturer to focus on implementing cybersecurity measures against threats that could directly and severely compromise their ability to perform their essential mission.

In the Manufacturing Profile [IR 8183r1], the selection of Subcategories to business and mission objectives was based on a broad range of manufacturing sectors and operations. The most critical Subcategories may differ for individual manufacturers.

For semiconductor manufacturers, the criticality determinations were formulaically brought forward from the Manufacturing Profile using the following procedure:

- Given a CSF 1.1 Subcategory's criticality determination within the Manufacturing Profile for a certain mission objective (i.e., Critical or Non-critical), its corresponding CSF 2.0 Subcategories were assigned the same criticality determination for the corresponding semiconductor manufacturing mission objective.
  In other words, there was a “1-to-many" projection of criticality.
- Given a CSF 2.0 Subcategory, the criticality determination was assigned for the corresponding semiconductor manufacturing mission objective for any corresponding CSF 1.1 Subcategory within the Manufacturing Profile.
  In other words, there was a "1-from-many" projection of criticality.
- The “1-to-many" and “1-from-many" projections sometimes conflicted due to the asymmetric nature of CSF 1.1 and 2.0 Subcategory mappings. The resolution to such conflicts was to assume an affirmative designation of Critical. For example, in the Manufacturing Profile, the mission objective of maintaining environmental safety had RC.CO-1 and RC.CO-2 determined Non-Critical but RS.CO-2 determined Critical. Those three Subcategories map into or from RC.CO-04, and because of the criticality of RS.CO-2, RC.CO-04 is deemed Critical.

Tables 1 through 6 show the criticality determinations. Most were brought forward from the Manufacturing Profile. Rows denoted with asterisks are new Subcategories within CSF 2.0 that had no mapping from CSF 1.1 or the Manufacturing Profile. (**Note to reviewers:** During the public comment period, these rows are also bold-faced and denoted as “Proposed” or “Not yet proposed.” Feedback is strongly encouraged with opinions on criticality. All “Proposed” designations will be removed after reviewing public comments. For table cells where a criticality is not yet proposed, if no feedback is received, the cell will default to “Non-critical” from lack of advocacy.)

4.2.1. Govern

The Govern Function is critical for establishing the framework for cybersecurity risk management, aligning policies and expectations with organizational goals, and ensuring continuous improvement and oversight within enterprise risk management.

Table 1. Criticality determinations for GOVERN Function in business and mission objectives

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
GV.OC-01	Critical	Critical	Critical	Critical	Critical
GV.OC-02	Non-critical	Non-critical	Critical	Critical	Critical
GV.OC-03	Critical	Critical	Critical	Non-critical	Non-critical
GV.OC-04	Critical	Critical	Critical	Critical	Non-critical
GV.OC-05	Critical	Critical	Critical	Critical	Critical
GV.RM-01	Critical	Critical	Critical	Critical	Critical
GV.RM-02	Critical	Critical	Critical	Critical	Critical
GV.RM-03	Critical	Critical	Critical	Critical	Critical
GV.RM-04	Critical	Critical	Critical	Critical	Critical
GV.RM-05	Non-critical	Non-critical	Critical	Critical	Critical
GV.RM-06	Critical	Critical	Critical	Critical	Critical
GV.RM-07 *	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**
GV.RR-01 *	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**
GV.RR-02	Non-critical	Non-critical	Non-critical	Non-critical	Critical
GV.RR-03	Critical	Critical	Critical	Critical	Critical
GV.RR-04	Non-critical	Non-critical	Non-critical	Non-critical	Critical
GV.PO-01	Critical	Critical	Non-critical	Non-critical	Critical
GV.PO-02	Critical	Critical	Non-critical	Non-critical	Critical
GV.OV-01 *	**Critical (proposed)**	**Critical (proposed)**	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**	**Critical (proposed)**
GV.OV-02 *	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**
GV.OV-03 *	**Critical (proposed)**	**Critical (proposed)**	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**
GV.SC-01	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-02	Non-critical	Non-critical	Non-critical	Non-critical	Critical
GV.SC-03	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-04	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-05	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-06	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-07	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-08	Non-critical	Non-critical	Non-critical	Critical	Non-critical
GV.SC-09	Non-critical	Non-critical	Critical	Critical	Critical
GV.SC-10	Non-critical	Non-critical	Critical	Critical	Critical

4.2.2. Identify

The Identify Function is critical for developing the foundation for cybersecurity management and understanding cyber risks to assets.

Table 2. Criticality determinations for IDENTIFY Function in business and mission objectives

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
ID.AM-01	Critical	Critical	Critical	Non-critical	Critical
ID.AM-02	Non-critical	Non-critical	Non-critical	Non-critical	Critical
ID.AM-03	Non-critical	Non-critical	Critical	Critical	Critical
ID.AM-04	Non-critical	Non-critical	Critical	Critical	Critical
ID.AM-05	Critical	Critical	Critical	Critical	Critical
ID.AM-07	Non-critical	Non-critical	Critical	Non-critical	Critical
ID.AM-08	Critical	Critical	Critical	Critical	Critical
ID.RA-01	Critical	Critical	Critical	Critical	Critical
ID.RA-02	Critical	Critical	Non-critical	Non-critical	Critical
ID.RA-03	Critical	Critical	Critical	Critical	Critical
ID.RA-04	Critical	Critical	Critical	Critical	Critical
ID.RA-05	Critical	Critical	Critical	Critical	Critical
ID.RA-06	Critical	Critical	Critical	Critical	Critical
ID.RA-07	Critical	Critical	Critical	Critical	Critical
ID.RA-08	Critical	Critical	Critical	Critical	Critical
ID.RA-09	Critical	Critical	Non-critical	Non-critical	Critical
ID.RA-10	Non-critical	Non-critical	Critical	Critical	Critical
ID.IM-01 *	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**	**(Criticality not yet proposed)**
ID.IM-02	Critical	Critical	Critical	Critical	Critical
ID.IM-03	Critical	Critical	Critical	Critical	Critical
ID.IM-04	Critical	Critical	Critical	Critical	Critical

4.2.3. Protect

The Protect Function is critical for preventing many cybersecurity events and limiting the impacts of potential cybersecurity events.

Table 3. Criticality determinations for PROTECT Function in business and mission objectives

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
PR.AA-01	Critical	Critical	Critical	Critical	Critical
PR.AA-02	Critical	Critical	Critical	Critical	Critical
PR.AA-03	Critical	Critical	Critical	Critical	Critical

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
PR.AA-04 *	**Non-critical (proposed)**	**Non-critical (proposed)**	**Non-critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**
PR.AA-05	Critical	Critical	Critical	Critical	Critical
PR.AA-06	Critical	Critical	Critical	Critical	Critical
PR.AT-01	Critical	Critical	Critical	Critical	Critical
PR.AT-02	Critical	Critical	Critical	Critical	Critical
PR.DS-01	Critical	Critical	Critical	Critical	Critical
PR.DS-02	Non-critical	Non-critical	Critical	Critical	Non-critical
PR.DS-10	Non-critical	Non-critical	Non-critical	Critical	Non-critical
PR.DS-11	Non-critical	Non-critical	Critical	Critical	Critical
PR.PS-01	Critical	Critical	Critical	Critical	Critical
PR.PS-02	Critical	Critical	Non-critical	Critical	Critical
PR.PS-03	Critical	Critical	Critical	Critical	Critical
PR.PS-04	Critical	Critical	Critical	Critical	Critical
PR.PS-05	Critical	Critical	Critical	Critical	Critical
PR.PS-06	Non-critical	Non-critical	Critical	Non-critical	Non-critical
PR.IR-01	Critical	Critical	Critical	Critical	Critical
PR.IR-02	Critical	Critical	Critical	Non-critical	Critical
PR.IR-03	Critical	Critical	Non-critical	Critical	Non-critical
PR.IR-04	Non-critical	Non-critical	Critical	Critical	Non-critical

827 4.2.4. Detect

828 The Detect Function is critical for detecting cybersecurity events in real time.

829 **Table 4. Criticality determinations for DETECT Function in business and mission objectives**

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
DE.CM-01	Critical	Critical	Critical	Critical	Critical
DE.CM-02	Critical	Critical	Critical	Critical	Critical
DE.CM-03	Critical	Critical	Critical	Critical	Critical
DE.CM-06	Critical	Critical	Critical	Critical	Critical
DE.CM-09	Critical	Critical	Critical	Critical	Critical
DE.AE-02	Critical	Critical	Critical	Critical	Critical
DE.AE-03	Critical	Critical	Non-critical	Critical	Critical
DE.AE-04	Critical	Critical	Non-critical	Non-critical	Critical
DE.AE-06	Critical	Critical	Critical	Critical	Critical
DE.AE-07	Critical	Critical	Non-critical	Critical	Critical
DE.AE-08	Critical	Critical	Critical	Critical	Critical

4.2.5. Respond

The Respond Function supports the ability to contain the impact of a cybersecurity incident.

Table 5. Criticality determinations for RESPOND Function in business and mission objectives

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
RS.MA-01	Critical	Critical	Critical	Critical	Critical
RS.MA-02	Critical	Critical	Critical	Critical	Critical
RS.MA-03	Critical	Critical	Critical	Critical	Critical
RS.MA-04	Critical	Critical	Critical	Critical	Critical
RS.MA-05	Critical	Critical	Critical	Critical	Critical
RS.AN-03	Critical	Critical	Critical	Critical	Critical
RS.AN-06	Critical	Critical	Critical	Critical	Critical
RS.AN-07 *	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**	**Critical (proposed)**
RS.AN-08	Critical	Critical	Critical	Critical	Critical
RS.CO-02	Critical	Critical	Non-critical	Critical	Non-critical
RS.CO-03	Critical	Critical	Non-critical	Critical	Non-critical
RS.MI-01	Critical	Critical	Critical	Non-critical	Critical
RS.MI-02	Critical	Critical	Critical	Non-critical	Critical

4.2.6. Recover

The Recover Function supports timely recovery to normal operations and reduces the impacts of a cybersecurity incident. Defined recovery objectives are needed when recovering from disruptions.

Table 6. Criticality determinations for RECOVER Function in business and mission objectives

Subcategory	Maintain Human Safety	Maintain Environmental Safety	Maintain Quality of Semiconductors	Maintain Production Goals	Protect Sensitive Information
RC.RP-01	Critical	Critical	Critical	Critical	Critical
RC.RP-02	Critical	Critical	Critical	Critical	Critical
RC.RP-03	Non-critical	Non-critical	Critical	Critical	Critical
RC.RP-04	Critical	Critical	Critical	Critical	Critical
RC.RP-05	Critical	Critical	Critical	Critical	Critical
RC.RP-06	Critical	Critical	Critical	Critical	Critical
RC.CO-03	Critical	Critical	Critical	Critical	Critical
RC.CO-04	Critical	Critical	Non-critical	Critical	Non-critical

5. Semiconductor Manufacturing Community Profile Subcategory Guidance

The Semiconductor Manufacturing Community Profile aligns with a semiconductor manufacturer's risk management processes to provide guidance for prioritizing cybersecurity actions across the domains of fab, enterprise IT, and equipment and tooling. It supports continuous risk assessments and the evaluations of business drivers to help semiconductor manufacturers define cybersecurity target states that align with desired outcomes across their operational environments.

Effective risk management requires a thorough understanding of the business drivers and security challenges that are unique to each domain. The risk associated with fab environments, where wafer production and cleanroom operations occur, will differ from those within enterprise IT, where data and communication networks are managed, and equipment and tooling, which focuses on the development, manufacturing, packaging and verification of semiconductor devices. Given these distinct operational elements, the application of the Profile will vary across the domains.

The Semiconductor Manufacturing Community Profile enhances rather than replaces current industry standards and cybersecurity frameworks used in the fab, enterprise IT, and equipment and tooling domains. Manufacturers can assess critical activities within these domains to ensure seamless service delivery and allocate security investments to where they will have the most benefit. The goal is to maximize protection while maintaining efficiency throughout the semiconductor life cycle. By tailoring cybersecurity practices to meet the specific threats and vulnerabilities present in fab, enterprise IT, and equipment and tooling, this Profile helps ensure the confidentiality, integrity, and availability of the systems that are critical to semiconductor manufacturing. The flexibility of the Profile paired with the CSF gives manufacturers the tools to customize risk management approaches to their unique operational and business needs.

The Manufacturing Profile that informs this new Community Profile is structured into three impact levels based on the categorization of the information and processes within the manufacturing system. The Manufacturing Profile also uses business and mission objectives to align a focused set of cybersecurity controls that support critical business goals. Much of that guidance is incorporated by reference, and the referenced guidance points are categorized based on Low, Moderate, and High potential impact levels of incidents or events that jeopardize "a manufacturing system or components, operational assets, individuals, or the organization" [IR 8183r1].

The Manufacturing Profile defines the three impact level configurations as follows:

- "The potential impact is LOW if the loss of integrity, availability, or confidentiality could be expected to have a limited adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment."
- "The potential impact is MODERATE if the loss of integrity, availability, or confidentiality could be expected to have a serious adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment."

- "The potential impact is HIGH if the loss of integrity, availability, or confidentiality could be expected to have a severe or catastrophic adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment."

Section 6 in the Manufacturing Profile further describes the impact levels and gives examples. Section 6.2 describes the hierarchical supporting structure of these impact levels with respect to one other: "Unless otherwise noted, the Moderate and High each include or enhance all of the stipulations from the levels below." For example, "A Moderate categorization includes all Moderate and Low security implementations." Readers should consult Sec. 6 of the Manufacturing Profile [IR_8183r1] for more information on impact levels.

The Semiconductor Manufacturing Community Profile defined in this section makes extensive and tailored references to portions of Sec. 7 of the Manufacturing Profile, according to the two directional mappings between CSF 1.1 and CSF 2.0 [CSF_1to2][CSF_2to1]. Guidance from the Manufacturing Profile is generally drawn into this document from the Moderate impact level, which already includes the Low impact level. At times, guidance is quoted for emphasis and for following mappings.

Table 7 presents the names and identifiers for the Functions and Categories in the CSF. The structure portrayed in this table is used to define the Profile in the tables throughout the rest of this section, with one table dedicated to each Function.

Table 7. CSF 2.0 Functions and Categories

Function's or Category's Unique Identifier	Function or Category
GV	**GOVERN**
GV.OC	Organizational Context
GV.RM	Risk Management Strategy
GV.RR	Roles, Responsibilities, and Authorities
GV.PO	Policy
GV.OV	Oversight
GV.SC	Cybersecurity Supply Chain Risk Management
ID	**IDENTIFY**
ID.AM	Asset Management
ID.RA	Risk Assessment
ID.IM	Improvement
PR	**PROTECT**
PR.AA	Identity Management, Authentication, and Access Control
PR.AT	Awareness and Training
PR.DS	Data Security
PR.PS	Platform Security
PR.IR	Technology Infrastructure Resilience

Function's or Category's Unique Identifier	Function or Category
DE	**DETECT**
DE.CM	Continuous Monitoring
DE.AE	Adverse Event Analysis
RS	**RESPOND**
RS.MA	Incident Management
RS.AN	Incident Analysis
RS.CO	Incident Response Reporting and Communication
RS.MI	Incident Mitigation
RC	**RECOVER**
RC.RP	Incident Recovery Plan Execution
RC.CO	Incident Recovery Communication

5.1. Govern

Table 8. Subcategory-level guidance for GOVERN Function

Function – **Category** – **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
GOVERN – **GV.OC:** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood – **GV.OC-01** The organizational mission is understood and informs cybersecurity risk management	Ecosystem	**Rationale:** The implementation of information systems and associated risk factors are directly influenced by the organization's mission and business processes, as detailed in Section 2.4.1 of SP 800-39. This section emphasizes that understanding the organization's objectives and processes is crucial for tailoring risk management strategies that effectively support and align with its overarching goals. **Guidance:** • "Define and communicate the manufacturer's place in critical infrastructure and its industry sector. Define and communicate critical infrastructure and key resources relevant to the manufacturing system." IR 8183r1: ID.BE-2 • "Develop, document, and maintain a critical infrastructure and key resources protection plan." IR 8183r1: ID.BE-2 • "Define and communicate priorities for manufacturing missions, objectives, and activities with consideration for security and the resulting risk to manufacturing operations, components, and individuals." IR 8183r1: ID.BE-3	[IR_8183r1]: ID.BE-2, ID.BE-3 [SP_800_39]
GV.OC-02 Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are	Ecosystem	**Rationale:** Internal stakeholders within the semiconductor industry prioritize manufacturing availability and the protection of trade secrets, as disruptions can have immediate and significant impacts on revenue. Understanding the cybersecurity expectations of external stakeholders is essential. In this context, external stakeholders can include customers or partners involved in the semiconductor manufacturing process, such as developers or producers of specialized equipment, regulatory bodies, and other entities integrated into the supply chain. This definition distinguishes these	[IR_8183r1]: ID.GV-2, ID.SC-2

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
understood and considered		stakeholders/customers from the broader category of end consumers who ultimately purchase goods that contain semiconductors. This perspective complements the internal focus on supplier management outlined in GV.SC. While GV.SC addresses how the organization manages its suppliers, GV.OC-02 expands this to include meeting the cybersecurity requirements of the organization's stakeholders within their supply chains. Standard organizational cybersecurity practices may not be fully applicable in these specialized environments and may necessitate tailored approaches to meet these unique demands. **Guidance:** • Develop policies including, for example, the identification and assignment of roles and responsibilities, management commitment, coordination among organizational entities, and compliance. The policies should also reflect coordination among organizational entities that are responsible for different aspects of security (e.g., physical, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring). • "Develop and disseminate a security program for the manufacturing system that includes, for example, the identification of personnel security roles and assignment of responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements, roles and responsibilities for third-party providers. Review and update the security program as determined necessary." IR 8183r1: ID.GV-2 • "Conduct and document cyber supply chain risk assessments at least annually or when a change to the manufacturing system, operational environment, or supply chain occurs. This assessment should identify and prioritize potential negative impacts to the organization from the sharing of sensitive information or the use of information technology, operational technology, services, technology-based input products, or non-technology-based input products supporting the manufacturing system. Disseminate results to relevant stakeholders	

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		including those responsible for informational technology and operational technology systems." IR 8183r1: ID.SC-2	
GV.OC-03 Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	Ecosystem	**Rationale:** The escalating demands of external stakeholders (e.g., compliance with global privacy regulations, like GDPR; cybersecurity mandates, like the CRA) significantly influence the controls that organizations have organizational requirements to implement, thereby increasing organizational liability. As these requirements intensify, customers are increasingly requesting cybersecurity attestations or certifications, likely spurred by laws and regulations similar to the CRA. Adherence to recognized industry frameworks becomes critical to guide the selection and implementation of internal controls. Where these external expectations are formalized through laws, regulations, or contracts, there is overlap with GV.OC-02. **Guidance:** • "Ensure that legal and regulatory requirements affecting the manufacturing operations regarding cybersecurity are understood and managed." IR 8183r1: ID.GV-3 • "Review assessments of suppliers and third-party partner compliance with contractual obligations by routinely reviewing third-party independent audits, test results, and other evaluations." IR 8183r1: ID.SC-4	[IR 8183r1]: ID.GV-3, ID.SC-4 [SEMI E187] [SEMI E188]
GV.OC-04 Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	Ecosystem	**Rationale:** This subcategory helps ensure that all organizational controls are aligned with both internal and external expectations to enhance the organization's ability to protect its operations against potential security breaches and compliance issues. **Guidance:** • "Identify and prioritize supporting services for critical manufacturing system processes and components." IR 8183r1: ID.BE-4 • "Provide an uninterruptable power supply for identified critical manufacturing system components to facilitate the transition of the manufacturing system to long-term alternate power in the event of a primary power source loss." IR 8183r1: ID.BE-4	[IR 8183r1]: ID.BE-4, ID.BE-5

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		• "Identify alternate and redundant supporting services for critical manufacturing system processes and components." IR 8183r1: ID.BE-4 • "Define resilience requirements for the manufacturing system to support delivery of critical services." IR 8183r1: ID.BE-5 • "Define recovery time objective and recovery point objective for the resumption of essential manufacturing system processes." IR 8183r1: ID.BE-5 • "Identify critical manufacturing system assets that support essential manufacturing system processes." IR 8183r1: ID.BE-5 • "Conduct capacity planning for manufacturing system processing, telecommunications, and environmental support as required during contingency operations." IR 8183r1: ID.BE-5 • "Conduct contingency planning for the continuance of essential manufacturing functions and services with little or no loss of operational continuity and sustain that continuity until full system restoration." IR 8183r1: ID.BE-5	
GV.OC-05 Outcomes, capabilities, and services that the organization depends on are understood and communicated	Ecosystem	**Rationale:** This includes internal and supply chain inputs that are essential to satisfying the organization's mission. It is key to understanding and prioritizing the threats and vulnerabilities that are controlled to manage risk (GV.RM, GV.SC), protecting the organization's information assets (PR), and managing the response to (RS) and recovery from (RC) cybersecurity incidents. **Guidance:** • "Define and communicate the organization's role in the supply chain. Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system." IR 8183r1: ID.BE-1 • "Protect against supply chain threats to the manufacturing system, system components, or system services by employing security safeguards as part of a comprehensive, defense-in-depth security strategy." IR 8183r1: ID.BE-1 • "Identify and prioritize supporting services for critical manufacturing system processes and components." IR 8183r1: ID.BE-4	[IR 8183r1]: ID.BE-1, ID.BE-4

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Identify alternate and redundant supporting services for critical manufacturing system processes and components." IR 8183r1: ID.BE-4	
GV.RM: The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions – **GV.RM-01** Risk management objectives are established and agreed to by organizational stakeholders	Ecosystem	**Rationale:** Incorporating risk management at a strategic level enables the alignment of risk-related activities with the broader goals of the organization. This approach allows for a proactive stance in identifying and mitigating risks while leveraging them as opportunities where possible. **Guidance:** • "Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally." IR 8183r1: ID.RM-1	[IR 8183r1]: ID.RM-1
(GV.RM-01)	Fab	**Guidance:** • To ensure alignment with organizational standards, it is vital to clearly define the roles and responsibilities of field service engineers. This alignment should be consistent with the risk management objectives that are established and agreed upon by organizational stakeholders, as noted in GV.OC-01. Implementing robust governance to control the activities of field service engineers will help maintain clarity in their duties, support effective risk management, and foster accountability within the framework of agreed-upon organizational objectives.	
GV.RM-02 Risk appetite and risk tolerance statements are established,	Ecosystem	**Rationale:** Formally documenting the organization's risk appetite in policies and procedures establishes clear processes for defining risk tolerance boundaries and ensures control and consistency. Communicating this information across the organization maintains uniformity	[IR 8183r1]: ID.RM-2, ID.RM-3

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
communicated, and maintained		in risk management actions. Regular updates to risk statements are essential to keeping them relevant. **Considerations:** Risk appetite and tolerance statements may need customization for each domain and specific operational needs. **Guidance:** • "Define the risk tolerance for the manufacturing system." IR 8183r1: ID.RM-2 • "Ensure the risk tolerance for the manufacturing system is informed by the organization's role in critical infrastructure and sector-specific risk analysis." IR 8183r1: ID.RM-3	
GV.RM-03 Cybersecurity risk management activities and outcomes are included in enterprise risk management process	Ecosystem	**Rationale:** This subcategory ensures that cybersecurity risks are recognized and incorporated into enterprise risk management (ERM) and all incident response activities alongside financial, regulatory, reputational, and other key risk areas. This ensures that cybersecurity measures are maintained, even during recovery from non-cyber incidents. Incorporating elements such as vulnerability management, physical security, and access controls is essential.	[IR 8183r1]: Not available [SP 800 53r5]: PM-3, PM-9, PM-30, RA-7, SR-2
GV.RM-04 Strategic direction that describes appropriate risk response options is established and communicated	Ecosystem	**Rationale:** Establishing a strategic direction for risk response with specific processes and procedures is essential for comprehensive risk management and immediate risk management activities, such as incident response and mitigation. It also allows for broader strategic risk responses to be incorporated in the future. This approach balances immediate needs with long-term strategic goals.	[IR 8183r1]: ID.RM-2
GV.RM-05 Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Ecosystem	**Rationale:** These standards ensure that communication lines across the organization are robust. This setup systematically includes the handling of risks from suppliers and other third parties and fosters an environment in which cybersecurity risks are managed cohesively and comprehensively across all levels of the organization. **Guidance:** • Implement a cyber supply chain risk management process that effectively identifies, assesses, communicates, and addresses risk-related issues associated with the sharing of sensitive information or the use of information technology, operational	[IR 8183r1]: ID.SC-1

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		technology, services, technology-based input products, and non-technology-based input products that support the manufacturing system.	
GV.RM-06 A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Ecosystem	**Rationale:** Establishing and communicating a standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks ensures that resources are directed toward effectively reducing significant risks. **Guidance:** • "Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally." IR 8183r1: ID.RM-1	[IR 8183r1]: ID.RM-1 [SP 800 30r1]
GV.RM-07 Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Ecosystem	**Rationale:** Aligning the goal of advancing organizational maturity in managing negative risks with the inclusion of strategic opportunities (i.e., positive risks) in cybersecurity discussions can broaden the scope of risk management. This integration ensures that while organizations strive to mitigate threats, they also recognize and leverage potential opportunities to enhance their cybersecurity posture and strategic objectives.	[IR 8183r1]: Not available
GV.RR Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated_ **GV.RR-01** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a	Ecosystem	**Rationale:** Effective cybersecurity risk management requires clear direction and support from all members of organizational leadership, who are collectively responsible and accountable for cybersecurity risk. Each leader needs to understand their role in fostering a culture that is risk-aware, ethical, and continually improving. While appointing a cyber champion or executive sponsor is important for providing specific accountability and leadership focus, it is equally vital that all leadership act as "cyber champions" to support and promote a cyber-aware culture. This combined approach underscores the need for designated advocates while also emphasizing the shared responsibility across the leadership team. Although a CISO may hold primary authority for cybersecurity risk strategy, effective risk management demands active involvement and accountability from every leader within the organization.	[IR 8183r1]: Not available [SP 800 53r5]: PM-2, PM-19, PM-23, PM-24, PM-29

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
culture that is risk-aware, ethical, and continually improving			
GV.RR-02 Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Ecosystem	**Rationale:** Clearly establishing, defining, communicating, understanding, and enforcing roles, responsibilities, and authorities ensures accountability and strengthens overall cybersecurity governance. **Guidance:** • "Develop and disseminate a security program for the manufacturing system that includes, for example, the identification of personnel security roles and assignment of responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements, roles and responsibilities for third-party providers. Review and update the security program as determined necessary." IR 8183r1: ID.GV-2 • "Define roles and responsibilities for detection activities on the manufacturing system and ensure accountability." IR 8183r1: DE.DP-1 • "Establish and maintain personnel cybersecurity roles and responsibilities for the manufacturing system. Include cybersecurity roles and responsibilities for third-party providers." IR 8183r1: ID.AM-6 • "Require third-party providers to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components." IR 8183r1: ID.AM-6 • "Third-party providers include, for example, service providers, contractors, and other organizations providing manufacturing system development, technology services, outsourced applications, or network and security management." IR 8183r1: ID.AM-6 • Document the roles and responsibilities of third-party providers for incident eradication in accordance with the organization's security and privacy requirements.	[IR 8183r1]: DE.DP-1, ID.AM-6, ID.GV-2

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
GV.RR-03 Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	Ecosystem	**Rationale:** Adequate resources should be allocated in alignment with the organization's cybersecurity risk strategy, roles, responsibilities, and policies. This ensures that support and resources are both sufficient and appropriately distributed to effectively manage cybersecurity risks across the organization and achieve the goals set out in GV.OC and GV.RM. **Guidance:** • "Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally." IR 8183r1: ID.RM-1	[IR 8183r1]: ID.RM-1
(GV.RR-03)	Equipment and Tooling	**Guidance:** • Provide an incident response support resource to determine the appropriate handling of security incidents, including the mention of third-party providers, if applicable.	
GV.RR-04 Cybersecurity is included in human resources practices	Ecosystem	**Rationale:** Integrate cybersecurity risk management considerations into human resources processes (e.g., personnel screening, change notification, offboarding) to uphold the security of sensitive information. Access control processes are required for processes such as termination (leavers) and internal transfers (movers) and for personal data privacy, which is less likely to be a concern in the context of manufacturing availability. **Guidance:** • "Ensure that third-party providers understand their responsibilities regarding the security of the manufacturing system and the responsibilities of their assignments. Require notifications be given for any personnel transfers, termination, or transition involving personnel with physical or logical access to the manufacturing system components." IR 8183r1: PR.AT-3 • "Develop and maintain a personnel security program for the manufacturing system. Personnel security program should include policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions." IR 8183r1: PR.IP-11	[IR 8183r1]: PR.AT-3, PR.IP-11

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
(GV.RR-04)	Fab	**Considerations:** In fabrication environments, deprovisioning plays a crucial role in maintaining cybersecurity as an integral part of human resources practices. It is essential to promptly remove former employees from Identity and Access Management (IAM) systems and local user databases to prevent unauthorized access. Additionally, changing passwords for shared accounts is a necessary measure to mitigate the risk of former employees, who had access to the shared account, using prior known passwords to gain unauthorized access. This practice helps to safeguard sensitive information and maintain security protocols within the fabrication domain.	
(GV.RR-04)	Equipment and Tooling	**Considerations:** It is crucial to understand the implications of personnel departures, such as the handling of sensitive responsibilities like firmware signing keys. A dedicated security operations team is essential to ensure comprehensive coverage of all cybersecurity functions. HR practices should be tightly integrated with deprovisioning processes to secure the organization effectively and ensure a smooth transition when employees leave.	
GV.PO Organizational cybersecurity policy is established, communicated, and enforced – **GV.PO-01** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Ecosystem	**Rationale:** Establish a policy for managing cybersecurity risks based on the organizational context, cybersecurity strategy, and priorities. The policy should be tailored to address the unique characteristics, specific risks, and requirements of each domain within the semiconductor manufacturing ecosystem while ensuring that they are effectively communicated and enforced across all domains. **Guidance:** • "Develop and disseminate a security policy that provides an overview of the security requirements for the manufacturing system. The policy includes, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the manufacturing system. Review and update the security policy as determined necessary. Ensure the security policy is approved by a senior official with	[IR 8183r1]: ID.GV-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		responsibility and accountability for the risk being incurred by manufacturing operations." IR 8183r1: ID.GV-1	
(GV.PO-01)	Fab	**Guidance:** • Make considerations to address the unique challenges related to equipment integration, process control systems, and high-availability requirements that differ from typical IT environments. This ensures that fab-specific cybersecurity policies adequately mitigate risks while supporting operational efficiency.	
(GV.PO-01)	Equipment and Tooling	**Considerations:** Cybersecurity risk management policies, which are usually inherited from enterprise IT, should be customized to address specific threats associated with OT. This tailored approach is necessary because the equipment and tooling domain often requires distinct policies that are heavily influenced by external standards and requirements, diverging from conventional IT policies.	
GV.PO-02 Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Ecosystem	**Rationale:** Cybersecurity concerns that are specific to the manufacturing context should be incorporated into organizational policy, including expectations for confidentiality, availability, and integrity. Additionally, semiconductor and manufacturing OT has unique vulnerabilities, threats, and impacts that require the tailoring of typically IT-focused cybersecurity risk management policies. (See GV.PO-01.) **Guidance:** • "Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by manufacturing operations." IR 8183r1: ID.GV-1	[IR 8183r1]: ID.GV-1
GV.OV Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk	Ecosystem	**Rationale:** Cybersecurity risk management programs should swiftly integrate lessons learned from significant cybersecurity incidents, as outlined in RC.RP-04. This integration is crucial for ensuring that the outcomes of the cybersecurity risk management strategy are continuously reviewed and used to refine and adjust the organization's overall strategy and direction. This process promotes an adaptive and responsive cybersecurity posture that evolves in line with emerging threats and organizational needs.	[IR 8183r1]: Not available

Function – **Category** – **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
management strategy – **GV.OV-01** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction			
GV.OV-02 The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risk	Ecosystem	**Guidance:** Regularly review and adjust the cybersecurity risk management strategy to align with the industry's unique requirements and risks. Given the sector's high susceptibility to operational disruptions and the rapid evolution of technological threats, this dynamic approach ensures the robust protection of critical assets and sustains competitive advantage.	[IR 8183r1]: Not available
GV.OV-03 Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	Ecosystem	**Rationale:** Performance in cybersecurity risk management should be closely tied to key performance indicators (KPIs) and key risk indicators (KRIs). This approach ensures that the organization's cybersecurity efforts are measurable and align with broader risk management objectives. Regular evaluation and review of these performance metrics help identify areas that need adjustment and enhance the overall security posture.	[IR 8183r1]: Not available [SP 800 53r5]: PM-4, PM-6, RA-7, SR-6
GV.SC Cyber supply chain risk management processes are identified, established, managed, monitored, and	Ecosystem	**Rationale:** Establishing a cyber supply chain risk management process is essential to systematically identify, assess, communicate, and address risks associated with sensitive information and the use of various technologies and services in the manufacturing system. SCRM should take a comprehensive approach that considers supply chain risks to both technology-based inputs (e.g., software, hardware) and non-technology-based inputs (e.g., personnel, physical facilities). This process requires	[IR 8183r1]: ID.SC-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
improved by organizational stakeholders – **GV.SC-01** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders		approval from key stakeholders, including those in charge of IT and OT systems, to align with the organization's broader cybersecurity strategies and objectives, ensuring cohesive risk management across all operational facets. **Guidance:** • "Implement a cyber supply chain risk management process that effectively identifies, assesses, communicates, and facilitates addressing risk-related issues associated with the sharing of sensitive information or the use of information technology, operational technology, services, technology-based input products, and non-technology-based input products supporting the manufacturing system. The cyber supply chain risk management process should be approved by organizational stakeholders including those responsible for informational technology and operational technology systems." IR 8183r1: ID.SC-1	
(GV.SC-01)	Fab	**Considerations:** Addressing single points of failure within the supply chain, particularly scenarios that involve sole suppliers, is critical for enhancing supply chain resilience. Contingency planning plays a vital role in this context. Additionally, refining purchasing specifications can further bolster supply chain resilience. These strategies are integral components of a comprehensive cybersecurity supply chain risk management program, ensuring that the organization's policies and processes are robust enough to handle disruptions effectively.	
(GV.SC-01)	Equipment and Tooling	**Considerations:** Addressing single points of failure in equipment and tooling within the supply chain is crucial, particularly in single-supplier scenarios. Implementing robust contingency plans is vital for ensuring equipment and tooling resilience. These measures are essential for a comprehensive cybersecurity supply chain risk management strategy, continuous operations, and minimal disruptions in critical supply areas.	
GV.SC-02 Cybersecurity roles and responsibilities for suppliers, customers, and partners are established,	Ecosystem	**Rationale:** Aligning suppliers' expectations and incentives with the organization's mission and cybersecurity objectives is crucial for establishing clear and effective cybersecurity roles and responsibilities. This strategic alignment ensures that cybersecurity measures are consistently communicated and coordinated both internally and across the extensive network of suppliers, customers, and partners that are integral to this industry.	[IR 8183r1]: ID.AM-6

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
communicated, and coordinated internally and externally		Such a unified approach enhances the security posture of the entire semiconductor supply chain and mitigates risks more effectively. **Guidance:** • "Establish and maintain personnel cybersecurity roles and responsibilities for the manufacturing system. Include cybersecurity roles and responsibilities for third-party providers. Require third-party providers to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components. Third-party providers include, for example, service providers, contractors, and other organizations providing manufacturing system development, technology services, outsourced applications, or network and security management." IR 8183r1: ID.AM-6	
GV.SC-02	Equipment and Tooling	**Guidance:** • Ensure that third-party providers can comply with the organization's security and privacy requirements.	
GV.SC-03 Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Ecosystem	**Rationale:** Performing annual assessments of cybersecurity risks, with the timing adjusted based on specific risks, is essential. This practice is part of integrating cybersecurity supply chain risk management into broader cybersecurity and enterprise risk management frameworks. It ensures that risk assessments and improvement processes are continuously updated, remain effective, and align with the organization's overall risk management strategy. This guidance supports the proactive monitoring and enhancement of security measures across the supply chain. **Guidance:** • "Conduct and document cyber supply chain risk assessments at least annually or when a change to the manufacturing system, operational environment, or supply chain occurs. This assessment should identify and prioritize potential negative impacts to the organization from the sharing of sensitive information or the use of information technology, operational technology, services, technology-based input products, or non-technology-based input products supporting the manufacturing system. Disseminate results to relevant stakeholders	[IR 8183r1]: ID.SC-2

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		including those responsible for informational technology and operational technology systems." IR 8183r1: ID.SC-2	
GV.SC-04 Suppliers are known and prioritized by criticality	Ecosystem	**Rationale:** Maintain an inventory that assesses the risks posed by direct and indirect suppliers. Prioritizing suppliers by their criticality ensures that controls are strategically implemented, safeguard operational integrity, and align with best practices in supply chain management. Without this, other controls cannot be effectively applied. **Guidance:** • "Identify and document key personnel from suppliers and third-party partners to include as stakeholders in response and recovery planning activities." IR 8183r1: ID.SC-5	[IR 8183r1]: ID.SC-2, ID.SC-5
GV.SC-05 Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Ecosystem	**Rationale:** When establishing requirements to address cybersecurity risks in supply chains, considerations should extend beyond the supplier's internal cybersecurity practices to include the security of the equipment and tools that they provide. This comprehensive assessment ensures that cybersecurity requirements are not only established and prioritized but are also effectively integrated into contracts and agreements with suppliers and other relevant third parties. **Guidance:** • "Implement contract requirements permitting the organization to review the cybersecurity programs implemented by suppliers and third-party partners." IR 8183r1: ID.SC-3 • "Implement contract requirements for suppliers and third-party partners to implement a documented development life cycle for the information technology, operational technology, services, technology" IR 8183r1: ID.SC-3	[IR 8183r1]: ID.SC-3, PR.AC-3 [SEMI E187]
(GV.SC-05)	Fab	**Considerations:** Purchasing specifications (i.e., specs) and service-level agreements (SLAs) should be rigorously defined to align with the unique operational demands of semiconductor fabrication. Additionally, there should be clear flow-down requirements established with vendors to ensure that their products and services meet the stringent quality and security standards necessary for fab operations.	
(GV.SC-05)	Equipment and Tooling	**Consideration:** Software Bills of Materials (SBOMs) provide detailed transparency about the software components	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		used in manufacturing equipment and tooling. This ensures that all software dependencies are known, vulnerabilities can be tracked, and updates managed effectively.	
GV.SC-06 Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Ecosystem	**Rationale:** Assessing the criticality of suppliers (e.g., their role in providing specialized materials or proprietary technology) ensures that risk reduction strategies are precisely targeted toward suppliers that are integral to the production chain's stability and security. Prioritizing these efforts before entering into formal relationships with suppliers mitigates potential disruptions and enhances the overall resilience of semiconductor operations. **Guidance:** "Include security requirements into the acquisition process of the manufacturing system and its components." IR 8183r1: PR.IP-2	[IR 8183r1]: ID.SC-1, PR.IP-2
(GV.SC-06)	Fab	**Considerations:** Planning and due diligence are especially critical when dealing with suppliers for specific production nodes that may rely on sole-source providers.	
GV.SC-07 The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Ecosystem	**Rationale:** Understanding and managing the risks associated with suppliers, their products, services, and other third parties is crucial for maintaining a secure and reliable supply chain. **Guidance:** • "Review assessments of suppliers and third-party partner compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations." IR 8183r1: SC-4 • An annual review is the minimum recommendation for suppliers involved in nested supply chains that are critical to semiconductor manufacturing. However, the review cadence should be adjusted based on the risk level, the criticality of the supplier to specific production nodes, and specific events that may alter risk profiles.	[IR 8183r1]: ID.SC-2, ID.SC-4
GV.SC-08 Relevant suppliers and other third parties are included in incident planning, response, and	Ecosystem	**Rationale:** Integrate relevant suppliers and third parties into incident planning, response, and recovery activities. **Considerations:** To strengthen these collaborative efforts, both parties should maintain onboard emergency contacts and validate their information at least annually. **Guidance:** • "Identify and document key personnel from suppliers and third-party partners to include as	[IR 8183r1]: ID.SC-5, RS.CO-3, RS.CO-4 [SEMI E188]

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
recovery activities		stakeholders in response and recovery planning activities." IR 8183r1: ID.SC-5 • "Identify and document key personnel from suppliers and third-party partners to include as stakeholders in testing and execution of the response and recovery plans." IR 8183r1: ID.SC-5 • "Share cybersecurity incident information with relevant stakeholders per the response plan" IR 8183r1: RS.CO-3 • "Coordinate cybersecurity incident response actions with all relevant stakeholders." IR 8183r1:RS.CO-4 • Procurement teams should include specific incident response and recovery language and service-level agreements in contracts to ensure timely responsiveness.	
GV.SC-09 Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	Ecosystem	**Rationale:** The cadence of performance reviews for supply chain security practices should be determined by event-driven factors, commensurate risks, and the criticality of the suppliers. This approach ensures that reviews are timely, relevant, and reflect the dynamic nature of risks throughout the technology product and service life cycle. By integrating these practices into broader cybersecurity and enterprise risk management programs, the ecosystem can maintain a vigilant and responsive security posture.	[IR 8183r1]: ID.SC-1
GV.SC-10 Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	Ecosystem	**Rationale:** Cybersecurity supply chain risk management plans should explicitly include provisions for managing post-engagement risks to safeguard sensitive information (e.g., enterprise data, contractual information, and intellectual property) and maintain system integrity after the conclusion of a partnership or service agreement. Effective management in this context involves ensuring that all data associated with the partnership is securely handled through proper return, destruction, or archival in compliance with contractual and regulatory requirements. Access controls should also be addressed to revoke or terminate permissions that were previously granted to	[IR 8183r1]: ID.SC-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		partners to prevent unauthorized access to systems, networks, or data repositories. End-of-life maintenance considerations should be addressed, particularly for systems or components that are tied to the former relationship. Additionally, consider any legal requirements to provide product support for a defined number of years after the engagement. **Guidance:** • Include data retention/deletion and post-event coordination in contracts and SLAs. • Address nested supply chain issues. • Clarify roles for execution of final data destruction and related activities. • “Conduct and document cyber supply chain risk assessments at least annually or when a change to the manufacturing system, operational environment, or supply chain occurs.” IR 8183r1: ID.SC-1	
(GV.SC-10)	Fab	**Considerations:** Evaluate the feasibility of implementing IT best practices within legacy systems and OT. Cybersecurity supply chain risk management plans should address current processes and include specific mitigation strategies for identified risks that are associated with equipment and tooling. These plans should also provide for ongoing activities and responsibilities after the conclusion of a partnership or service agreement.	
(GV.SC-10)	Equipment and Tooling	**Considerations:** Assess the feasibility of end-of-service (EOS) requirements for equipment and tooling with plans that address the risks and challenges associated with equipment and software nearing the end of their support life cycle.	

901 5.2. Identify

902 **Table 9. Subcategory-level guidance for IDENTIFY Function**

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
IDENTIFY The organization's current cybersecurity risks are understood – **ID.AM: Asset Management** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy – **ID.AM-01** Inventories of hardware managed by the organization are maintained	Ecosystem	**Rationale:** Maintain inventories of organization-managed hardware to enable effective asset management, risk assessment, and cybersecurity across the complex network of equipment involved in chip manufacturing. **Guidance:** • "Identify individuals who are both responsible and accountable for administering manufacturing system components." 8183r1: ID.AM-1 • "Establish and maintain an accurate inventory of physical devices. Include detailed attributes like asset ID, manufacturer, model, location, ownership, and operational status." 8183r1, ID.AM-1 • "Update the inventory of manufacturing system components as an integral part of component installations, removals, and system updates." IR 8183r1: PR.MA-1 • "Implement automated mechanisms where safe and feasible to maintain an up-to-date, complete, accurate, and readily available inventory of manufacturing system components." IR 8183r1: PR.MA-1	[IR_8183r1]: ID.AM-1, PR.MA-1 [SEMI_E169]: Equipment Information Asset, Section 7 [ANSI_IEC_62443_3_3]: SR 7.8
(ID.AM-01)	Fab	**Considerations:** Smart devices, sensors, networked devices, and OT equipment may have interfaces that could create an attack surface.	[IR_8183r1]: ID.AM-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		Guidance: • "Document an inventory of manufacturing system components that reflects the current system." IR 8183r1: ID.AM-1	
(ID.AM-01)	Equipment and Tooling	**Considerations:** Real-time production requirements may limit the ability to take systems offline for inventory, and automated asset discovery tools may not work with all industrial control systems.	
ID.AM-02 Inventories of software, services, and systems managed by the organization are maintained	Ecosystem	**Rationale:** Maintain inventories of software, services, and systems to manage licensing, patches, and vulnerabilities and to ensure operational integrity across the supply chain. Software platforms and applications within the organization should be inventoried. SBOMs may be required by organizations and/or legislation. Indexing SBOMs can support inventory efforts. **Guidance:** • "Identify individuals who are both responsible and accountable for administering manufacturing system software." IR 8183r1: ID.AM-2 • "Monitor for system inventory discrepancies." IR 8183r1: DE.CM-7 • Develop and maintain a comprehensive inventory of all software used within the organization. Include metadata, software name, version, vendor, deployment location (e.g., server, endpoint, controller), and licensing and expiration details.	[IR_8183r1]: ID.AM-2, DE.CM-7 [SEMI_E169]: Section 7, Equipment Information Asset [ANSI_IEC_62443_2_1]: 4.2.3.4 [ANSI_IEC_62443_3_3]: SR 7.8
(ID.AM-02)	Enterprise IT	**Considerations:** Maintain clear boundaries and inventories between IT and OT, and include cloud and virtualized assets in inventories. **Guidance:** • Inventories should include systems that interface with the OT space.	
ID.AM-03 Representations of the organization's authorized network communication and internal and external network data	Ecosystem	**Rationale:** Maintain representations of authorized network communications and data flows to understand and secure information exchange across the infrastructure and support the identification of critical data paths and potential attack surfaces. Severe breaches (e.g., theft of intellectual property or operational degradation) may greatly increase national security risks. **Considerations:** Connection information includes, for example, the interface characteristics, data characteristics,	[IR_8183r1]: ID.AM-3, DE.AE-1 [SEMI_E187]: Section 8, Network Security Requirement

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
flows are maintained		ports, protocols, addresses, description of the data, security requirements, and the nature of the connection. **Guidance:** • "Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed." IR 8183r1: ID.AM-3 • "Map the flow of information within the manufacturing system and to external systems." IR 8183r1: ID.AM-3 • Data flow between the equipment and fab should be established, particularly for anomaly detection.	[ANSI_IEC_62443_2_1]: 4.2.3.4
(ID.AM-03)	Fab	**Considerations:** Fabs have complex data flows between equipment, control systems, and data historians. Mapping real-time process control communications can be challenging. Proprietary protocols may complicate flow mapping. **Guidance:** • "Ensure that a baseline of network operations and expected data flows for the manufacturing system are developed, documented, and maintained to detect events." IR 8183r1: DE.AE-1	
(ID.AM-03)	Enterprise IT	**Considerations:** Data is often exchanged between enterprise systems, manufacturing systems, external partners, and cloud services.	[IR_8183r1]
(ID.AM-03)	Equipment and Tooling	**Considerations:** Production environments have critical data flows for process control and quality management. Mapping flows without disrupting production can be challenging. OT network segmentation should be reflected in flow maps.	
ID.AM-04 Inventories of services provided by suppliers are maintained	Ecosystem	**Rationale:** Various business processes rely on a complex network of components and suppliers, including ultra-pure materials, precision equipment, and specialized facility services. Maintaining accurate inventories of these services and components ensures production continuity, effective risk management, and operational stability. **Guidance:** • "Identify and document all external connections for the manufacturing system." IR 8183r1: ID.AM-4 • "Require external providers to identify the functions, ports, protocols, and other services required for use with the manufacturing system." IR 8183r1: ID.AM-4	[IR_8183r1]: ID.AM-4 [SEMI_E187] - Specification for Cybersecurity of Fab Equipment [SEMI_E188]

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• Inventory and record the purpose of all external services used by the organization, including IaaS, platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other application services. Where feasible, external information systems providing these services should be catalogued.	
ID.AM-05 Assets are prioritized based on classification, criticality, resources, and impact on the mission	Ecosystem	**Rationale:** Prioritizing assets based on classification, criticality, and impact on the mission is essential for effectively allocating security efforts. It also supports risk-based decision-making and resource allocation across the supply chain. **Guidance:** Identify and prioritize manufacturing system components and functions based on their classification, criticality, and business value. "Identify the types of information in possession, custody, or control for which security safeguards are needed (e.g., sensitive or protected information)." IR 8183r1: ID.AM-5	[IR_8183r1]: ID.AM-5
(ID.AM-05)	Fab	**Considerations:** Fabs have many critical systems that directly impact product quality and yield. Prioritizing these systems while also considering support systems can be complex. Criticality may change based on current production needs. Operations are responsible for labelling (e.g., classification, criticality, resources, and mission impact).	
ID.AM-07 Inventories of data and corresponding metadata for designated data types are maintained	Ecosystem	**Rationale:** Maintaining inventories of data and metadata is crucial for the semiconductor ecosystem to manage and protect sensitive information, intellectual property, and process data across the supply chain. **Guidance:** • Develop and maintain inventories of data and corresponding metadata for designated data types within the manufacturing system. Include data classification, storage locations, access controls, and retention policies in the inventory.	[IR_8183r1]: Not available [ANSI_IEC_62443_2_1]: 4.2.3.4
(ID.AM-07)	Fab	**Considerations:** Fabs generate large volumes of process data and equipment telemetry. Challenges include managing real-time data streams and historical data archives and maintaining metadata for process recipes and product specifications.	
(ID.AM-07)	Enterprise IT	**Considerations:** Enterprise systems handle various data types, including financial, HR, and research data. Data discovery and classification tools may be useful.	

Function – Category – Subcategory	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		Guidance: • Ensure consistency between IT and OT data inventories.	
(ID.AM-07)	Equipment and Tooling	**Considerations:** Production environments generate critical quality-control and traceability data. Inventorying and managing metadata for high-volume, high-velocity data can be challenging. Data retention requirements may vary based on product type and customer requirements.	
ID.AM-08 Systems, hardware, software, services, and data are managed throughout their life cycles	Ecosystem	**Rationale:** Managing assets throughout their life cycles is essential to maintain security, performance, and compliance across the complex manufacturing environment. This supports risk management, operational efficiency, and the secure decommissioning of assets. **Guidance:** "Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items." IR 8183r1: PR.DS-3 "Manage the manufacturing system using a system development life cycle that includes security considerations." IR 8183r1: PR.IP-2 "Require the developer of the manufacturing system and system components to provide a description of the functional properties of security controls, and design and implementation information for security-relevant system interfaces." IR 8183r1: PR.IP-2	[IR_8183r1]: PR.DS-3, PR.IP-2, PR.IP-6, PR.MA-1, PR.MA-2
(ID.AM-08)	Fab	**Considerations:** Fabs have long-lived equipment alongside rapidly evolving control systems. Balancing operational stability with security updates can be challenging. Failure to maintain equipment can degrade operations or cause an abrupt stop, leading to significant mission impact and ceased production. Managing the life cycle of custom hardware and software requires special attention. **Guidance:** • Define a system development life cycle that incorporates information security practices. • Develop a continuous monitoring strategy informed by the organization's risk strategy (developed in support of GV.RM-06). • Implement configuration management during system development.	[SEMI_E187]

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
(ID.AM-08)	Enterprise IT	**Considerations:** Enterprise IT typically has established life cycle management processes that may need adaptation for OT systems, which unique dependencies, vendors, and service contracts (e.g., warranties). As such, life cycle management processes may starkly differ from the organization's IT processes. Cloud services and virtualized assets introduce new life cycle management challenges. **Guidance:** • "Ensure that manufacturing system data is destroyed according to policy." IR 8183r1: PR.IP-6	
(ID.AM-08)	Equipment and Tooling	**Considerations:** Production environments should manage asset life cycles and coordinate updates and replacements across interdependent systems without disrupting manufacturing processes. Legacy systems may also require extended life cycle support. **Guidance:** • Equipment should provide logging capabilities.	
ID.RA: Risk Assessment – **ID.RA-01** Vulnerabilities in assets are identified, validated, and recorded	Ecosystem	**Rationale:** Identifying, validating, and recording vulnerabilities is crucial for effectively managing cybersecurity risks. This supports proactive risk mitigation, patch management, and secure supply chain practices. Since vulnerabilities can exist in any hardware, software, or service, identification and validation are key in prioritizing remediation. **Guidance:** • "Conduct vulnerability scans on the manufacturing system where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process." IR 8183r1: DE.CM-8	[IR_8183r1]: DE.CM-8, ID.RA-1, PR.IP-12 [SEMI_E187]: 7.1.1, 9.1 [EU_CRA]: Annex I, part 1, part 2 [ISA_IEC_62443_2_3]
(ID.RA-01)	Fab	**Considerations:** Fabs contain sensitive equipment that may be disrupted by active scanning. Identifying vulnerabilities in proprietary or custom systems can be challenging. Balancing vulnerability management with production uptime is crucial. OT and legacy equipment may require special considerations related to vulnerability scanning. **Guidance:** • "Implement control system-specific vulnerability scanning tools and techniques where safe and feasible." IR 8183r1: DE.CM-8 • "Active vulnerability scanning, which introduces network traffic, is used with care on manufacturing systems to ensure that system functions are not	

Function – Category – Subcategory	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		adversely impacted by the scanning process." IR 8183r1: DE.CM-8	
(ID.RA-01)	Enterprise IT	**Considerations:** Enterprise IT systems typically have established vulnerability management processes that should also cover OT systems and consider their operational constraints. **Guidance:** Regularly perform vulnerability scans.	
(ID.RA-01)	Equipment and Tooling	**Considerations:** Production environments require vulnerability assessments to be scheduled carefully to avoid disrupting operations. Identifying vulnerabilities in real-time control systems and embedded devices may require specialized tools and expertise. **Guidance:** • Perform vulnerability scans prior to release.	
ID.RA-02 Cyber threat intelligence is received from information sharing forums and sources	Ecosystem	**Rationale:** Staying informed about emerging threats and vulnerabilities that are specific to the industry requires cyber threat intelligence. This supports proactive risk management and enhances incident response capabilities. **Guidance:** • "Establish and maintain ongoing contact with security groups and associations to receive security alerts and advisories. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Implement a threat awareness program that includes a cross-organization information-sharing capability. Organizations should consider having both an unclassified and classified information sharing capability." IR 8183r1: ID.RA-2	[IR_8183r1]: ID.RA-2 [SP_800_150]
(ID.RA-02)	Fab	**Guidance:** Fabs should focus on general threat intelligence while also analyzing intelligence that is relevant to industrial control systems and specialized semiconductor manufacturing equipment.	
(ID.RA-02)	Enterprise IT	**Considerations:** Enterprise IT typically has established threat intelligence processes. This intelligence should be shared with OT teams and contextualized for manufacturing environments.	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
(ID.RA-02)	Equipment and Tooling	**Considerations:** Production environments should focus on threats that could impact product quality, safety, and operational continuity. The need for current threat intelligence should be balanced with the stability requirements of production systems.	
ID.RA-03 Internal and external threats to the organization are identified and recorded	Ecosystem	**Rationale:** Identifying and recording internal and external threats is crucial for understanding the risk landscape of the semiconductor ecosystem. This supports comprehensive risk management and helps prioritize security efforts across the supply chain. **Guidance:** • "Conduct and document periodic assessment of risk to the manufacturing system to identify threats and likelihood of impact to manufacturing operations and assets. The risk assessment includes threats from insiders and external parties." IR 8183r1: ID.RA-3	[IR_8183r1]: ID.RA-3 [SP_800_30r1]
ID.RA-04 Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Ecosystem	**Rationale:** Assessing the potential impacts and likelihoods of threats is crucial for effectively prioritizing risks and allocating resources. This approach supports risk-based decision-making across the industry and allows organizations to address the most pressing vulnerabilities first. Additionally, it is important to acknowledge the challenges of applying these assessments to legacy systems, which may not have been designed with modern cybersecurity threats in mind. **Guidance:** • "Conduct criticality reviews of the manufacturing system that define the likelihood and potential adverse impacts to manufacturing operations, assets, and individuals if compromised or disabled." IR 8183r1: ID.RA-4	[IR_8183r1]: ID.RA-4 [SP_800_30r1]
(ID.RA-04)	Fab	**Consideration:** Impacts can include production downtime, yield loss, and compromised product integrity. Likelihood assessments should consider the unique attack vectors in fab environments.	
(ID.RA-04)	Enterprise IT	**Considerations:** Impacts in enterprise IT can range from data breaches to operational disruptions. Likelihood assessments should consider both external and insider threats.	
(ID.RA-04)	Equipment and Tooling	**Considerations:** Impacts in production environments can directly affect product quality and safety. Likelihood assessments should consider the potential for cascading effects across interconnected systems.	

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
ID.RA-05 Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Ecosystem	**Guidance:** - "Conduct risk assessments of the manufacturing system incorporating threats, vulnerabilities, likelihood, and impact to manufacturing operations, assets, and individuals. Disseminate risk assessment results to relevant stakeholders." IR 8183r1 ID.RA-5	[IR 8183r1]: ID.RA-5 [SP 800 30r1] [EU CRA]: art. 1(c)
(ID.RA-05)	Fab	**Considerations:** Risk assessment in fabs should balance cybersecurity risks with operational requirements and potential impacts on highly sensitive processes.	
(ID.RA-05)	Enterprise IT	**Considerations:** Enterprise IT risk assessments should consider both IT and OT risks to ensure a holistic view of the organization's risk posture.	
(ID.RA-05)	Product	**Considerations:** Risk assessments in production environments should consider potential impacts on product quality, safety, and regulatory compliance.	
ID.RA-06 Risk responses are chosen, prioritized, planned, tracked, and communicated	Ecosystem	**Rationale:** Effectively managing risk responses is critical for systematically addressing risks and supporting continuous improvement of the industry's cybersecurity posture. Develop and implement a comprehensive strategy to manage risks to the manufacturing system that includes the identification and prioritization of risk responses. **Guidance:** - "Develop and implement a comprehensive strategy to manage risk to the manufacturing system that includes the identification and prioritization of risk responses." IR 8183r1: ID.RA-6 - "Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks." IR 8183r1: RS.MI-3	[IR 8183r1]: ID.RA-6, RS.MI-3 [SP 800 30r1]
(ID.RA-06)	Fab	**Considerations:** Risk responses in fabs should be carefully planned to minimize disruption to sensitive manufacturing processes. Communication of risk responses should consider the diverse stakeholders in fab operations.	
(ID.RA-06)	Enterprise IT	**Considerations:** Risk responses in enterprise IT should align with overall business objectives and consider potential impacts on both IT and OT environments.	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
(ID.RA-06)	Equipment and Tooling	**Considerations:** Risk responses in production environments should be implemented without compromising product quality or safety. Tracking and communicating risk responses is crucial for maintaining operational integrity.	
ID.RA-07 Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Ecosystem	**Rationale:** Managing changes and exceptions is crucial for maintaining operational integrity and adapting to new requirements or technologies. This supports risk management across the supply chain and ensures the traceability of decisions. **Guidance:** • "Implement configuration change control for the manufacturing system and its components. Conduct security impact analyses in connection with change control reviews." IR 8183r1: PR.IP-3 • "Test, validate, and document changes to the manufacturing system before implementing the changes on the operational system. Review and authorize proposed configuration-controlled changes prior to implementing them on the manufacturing system." IR 8183r1: PR.IP-3 • "Implement automated mechanisms where feasible to support the change control process. Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to the manufacturing system." IR 8183r1: PR.IP-3	[IR 8183r1]: PR.IP-3 [EU CRA]
(ID.RA-07)	Fab	**Considerations:** Changes in fab environments can have significant impacts on product quality and yield. Rigorous change management processes are necessary to prevent unintended consequences.	
(ID.RA-07)	Enterprise IT	**Considerations:** Change management in enterprise IT should consider potential impacts on both IT and OT systems. Coordination between IT and OT teams is essential for managing cross-domain changes.	
(ID.RA-07)	Equipment and Tooling	**Considerations:** Changes in production environments should be carefully managed to avoid disruptions to manufacturing processes. Exception handling is critical for maintaining production continuity.	
ID.RA-08 Processes for receiving, analyzing, and	Ecosystem	**Rationale:** Establishing processes for handling vulnerability disclosures is crucial for enabling rapid responses to newly discovered vulnerabilities, supporting proactive risk management, and fostering industry-wide trust. This	[IR 8183r1]: RS.AN-5

Function – Category – Subcategory	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
responding to vulnerability disclosures are established		approach meets regulatory demands and enhances the ecosystem's overall security posture. **Guidance:** • "Implement vulnerability management processes and procedures to incorporate processing, analyzing, and remediating vulnerabilities identified from internal and external sources." IR 8183r1: RS.AN-5 • "Implement automated mechanisms to disseminate and track remediation efforts for vulnerability information captured from internal and external sources to key stakeholders." IR 8183r1: RS.AN-5	[SEMI_E187]-0122, Section 9.2 [EU_CRA]
(ID.RA-08)	Fab	**Considerations:** Vulnerability disclosure processes in fabs should consider the potential impacts on sensitive manufacturing equipment and processes. Coordination with equipment vendors is crucial.	
(ID.RA-08)	Enterprise IT	**Considerations:** Enterprise IT typically has established vulnerability management processes that may need to be adapted to include OT systems and semiconductor-specific vulnerabilities.	
(ID.RA-08)	Equipment and Tooling	**Considerations:** Vulnerability disclosure processes in production environments should balance the need for quick responses with potential impacts on ongoing manufacturing operations.	
ID.RA-09 The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Ecosystem	**Rationale:** This is critical for preventing supply chain attacks, ensuring the trustworthiness of manufacturing systems, and supporting overall product integrity and security. **Guidance:** • "Implement hardware integrity checks to detect unauthorized tampering (e.g., tamper evident tape or labels, computer port protection, power-on self-tests, etc.) to manufacturing system hardware determined to be critical." IR 8183r1: PR.DS-8 • "Incorporate the detection of unauthorized tampering to the manufacturing system hardware into the organization incident response capability." IR 8183r1: PR.DS-8	[IR_8183r1]: PR.DS-8 [SS]
(ID.RA-09)	Fab	**Considerations:** Fabs use specialized equipment and software that may require unique verification processes. Ensuring the authenticity of components is crucial for maintaining product quality and protecting intellectual property.	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		Guidance: • Utilize automated mechanisms where possible to detect unauthorized components.	
(ID.RA-09)	Enterprise IT	**Considerations:** Enterprise IT should verify the authenticity and integrity of both IT and OT systems. This includes verifying software updates and patches before deployment.	
(ID.RA-09)	Equipment and Tooling	**Considerations:** Production environments should ensure the authenticity and integrity of control systems and software to prevent tampering that could affect product quality or safety.	
ID.RA-10 Critical suppliers are assessed prior to acquisition	Ecosystem	**Rationale:** Assessing critical suppliers is essential for effectively managing supply chain risks as they spread across many countries and geographical regions. This supports the integrity and security of the entire manufacturing process. **Guidance:** • "Conduct and document cyber supply chain risk assessments at least annually or when a change to the manufacturing system, operational environment, or supply chain occurs. This assessment should identify and prioritize potential negative impacts to the organization from the sharing of sensitive information or the use of information technology, operational technology, services, technology-based input products, or non-technology-based input products supporting the manufacturing system. Disseminate results to relevant stakeholders including those responsible for informational technology and operational technology systems." IR 8183r1: ID.SC-2 • "Review assessments of suppliers and third-party partner compliance with contractual obligations by routinely reviewing audits, test results, and other evaluations." IR 8183r1: ID.SC-4	[IR 8183r1]: ID.SC-2, ID.SC-4 [SS]
(ID.RA-10)	Fab	**Considerations:** Fabs rely on specialized suppliers for critical equipment and materials. Assessing these suppliers is crucial for maintaining product quality and protecting intellectual property.	
(ID.RA-10)	Enterprise IT	**Considerations:** Enterprise IT should assess suppliers of both IT and OT systems, including evaluating the cybersecurity practices of cloud service providers and software vendors.	
(ID.RA-10)	Equipment and Tooling	**Considerations:** Production environments should assess suppliers of control systems, raw materials, and other	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		critical components that directly impact manufacturing processes.	
ID.IM Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF Functions – **ID.IM-01** Improvements are identified from evaluations	Ecosystem	**Rationale:** Identifying improvements from evaluations is crucial for continuously enhancing an organization's cybersecurity posture. This supports ongoing adaptation to evolving threats and technological advancements across the industry. **Guidance:** • "Ensure that the security plan for the manufacturing system facilitates the review, testing, and continual improvement of the security protection processes." IR 8183r1: PR.IP-7 • "Implement independent teams to assess the protection process. Independent teams, for example, may include internal or external impartial personnel. Impartiality implies that assessors are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the manufacturing system under assessment or to the determination of security control effectiveness." IR 8183r1: PR.IP-7	[IR 8183r1]: PR.IP-7
(ID.IM-01)	Fab	**Considerations:** Evaluations in fabs should balance cybersecurity improvements with potential impacts on highly sensitive and precisely calibrated manufacturing processes. Any proposed changes should be carefully assessed for their impact on product quality and yield. **Guidance:** • Continuously evaluate systems to protect critical processes. • Adopt and utilize equipment, and add automated features for cyber continuous evaluations, where feasible.	
(ID.IM-01)	Enterprise IT	**Considerations:** Identifying improvements from evaluations helps align cybersecurity measures with evolving business needs and technological advancements. **Guidance:** Conduct regular internal and third-party IT assessments for continuous cybersecurity evaluation.	
(ID.IM-01)	Equipment and Tooling	**Considerations:** Identified improvements should be carefully vetted to ensure that they do not disrupt ongoing production processes. The high cost of downtime in semiconductor manufacturing means that any changes	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		should demonstrate clear benefits that outweigh potential risks. **Guidance:** • Establish criteria to determine the ROI required to adopt improvements in this area.	
ID.IM-02 Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	Ecosystem	**Rationale:** Identifying improvements from security tests and exercises, especially those that involve suppliers and third parties, helps in identifying potential weaknesses across the supply chain and improves overall industry resilience. **Guidance:** • "Test response and recovery plans to determine the effectiveness of the plans and the readiness to execute the plans." IR 8183r1: PR.IP-10 • "Related plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans." IR 8183r1: PR.IP-10 • "Validate that event detection processes are operating as intended." IR 8183r1: DE.DP-3	[IR 8183r1]: DE.DP-3, ID.SC-5, PR.IP-10
(ID.IM-02)	Fab	**Considerations:** Security tests in fabs should be carefully designed to avoid disrupting both sensitive and routine manufacturing processes. Coordination with equipment suppliers is crucial but may be complicated by proprietary technologies and competitive concerns. **Guidance:** • Identify and address barriers to penetration testing in fab settings. • Conduct essential security tests and exercises with extreme caution, an emphasis on thorough planning, and risk mitigation. • Conduct regular tabletop exercises to validate and enhance cybersecurity processes.	
(ID.IM-02)	Enterprise IT	**Considerations:** Tests should cover the intersection of IT and OT systems, which is particularly important in the semiconductor industry. Cloud services and other third-party IT solutions that are common in the industry should be included in testing scenarios. **Guidance:**	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• Implement regular IT tests that are conducted both internally and by third-party experts.	
(ID.IM-02)	Equipment and Tooling	**Considerations:** Tests should be carefully scheduled to minimize impacts on production. Involving suppliers of production equipment and materials in these tests requires careful planning and coordination. **Guidance:** • Perform targeted testing to identify cybersecurity improvements for production assets. • Conduct regular tabletop exercises to validate and enhance cybersecurity processes.	
ID.IM-03 Improvements are identified from the execution of operational processes, procedures, and activities	Ecosystem	**Rationale:** For the semiconductor ecosystem, identifying improvements from operational processes is crucial for maintaining competitiveness and security. It enables industry to adapt quickly to new threats and technological advancements. **Guidance:** • "Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions." IR 8183r1: DE.DP-5 • "Ensure the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security detection processes." IR 8183r1: DE.DP-5	[IR 8183r1]: DE.DP-5, PR.IP-7, PR.IP-8, RC.IM-1, RC.IM-2, RS.IM-1, RS.IM-2
(ID.IM-03)	Fab	**Considerations:** Changes to operational processes in fabs can have significant impacts on product quality and yield. Any improvements should be thoroughly tested and gradually implemented to avoid disruptions. **Guidance:** • Integrate continuous improvement processes into all fab operations and prioritize non-disruptive enhancements.	
(ID.IM-03)	Enterprise IT	**Considerations:** Improvements should be considered in both IT and OT environments. The rapid pace of technological change in the semiconductor industry requires agile improvement processes. **Guidance:** • Embed continuous improvement practices across all IT operations and emphasize adaptability and cross-domain integration.	

Function – Category – Subcategory	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
(ID.IM-03)	Equipment and Tooling	**Considerations:** Improvements should be carefully vetted to ensure that they do not disrupt ongoing production. The high cost of downtime in semiconductor manufacturing means that any changes should demonstrate clear benefits that outweigh potential risks. **Guidance:** • Implement a structured continuous improvement program across all production operations with a focus on risk-benefit analysis for proposed changes.	
ID.IM-04 Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Ecosystem	**Rationale:** For the semiconductor ecosystem, comprehensive incident response and cybersecurity plans are crucial due to the interconnected nature of the industry. These plans ensure coordinated responses to incidents that could affect multiple stakeholders across the supply chain. **Guidance:** • "Develop a configuration management plan for the manufacturing system. The plan includes, for example, configuration processes, roles, lifecycle definition, configuration items, and control methods." IR 8183r1: PR.IP-1 • "Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as providing a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information. Address maintaining essential functions despite system disruption, and the eventual restoration of the manufacturing system." IR 8183r1: PR.IP-9 • "Define incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities." IR 8183r1: PR.IP-9 • "Coordinate contingency plan development with stakeholders responsible for related plans." IR 8183r1: PR.IP-9 • "Review response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans." IR 8183r1: PR.IP-10	[IR 8183r1]: PR.IP-1, PR.IP-9, PR.IP-10, RS.IM-1, RC.IM-1

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		• "Test response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans." IR 8183r1: PR.IP-10 • "Coordinate testing of response and recovery plans with relevant stakeholders." IR 8183r1: PR.IP-10 • "Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly." IR 8183r1: RS.IM-1 • "Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly." IR 8183r1: RC.IM-1	
(ID.IM-04)	Fab	**Considerations:** Plans should be tailored to the unique operational requirements of fabs, including considerations for cleanroom environments and specialized equipment. The potential for physical damage or contamination should be addressed alongside cybersecurity concerns. **Guidance:** • Establish, communicate, maintain, and improve cybersecurity plans as an integral part of regular fab operations.	
(ID.IM-04)	Enterprise IT	**Considerations:** Plans should address both IT and OT systems and recognize the increasing convergence of these domains in the semiconductor industry. They should also consider the global nature of many semiconductor companies and address international regulatory requirements and cross-border incident response. **Guidance:** • Implement comprehensive, integrated cyber plans that cover both IT and OT domains.	
(ID.IM-04)	Equipment and Tooling	**Considerations:** Plans should balance the need for rapid response with potential impacts on ongoing production. They should address scenarios that are specific to semiconductor manufacturing, such as threats to process control systems and potential product tampering. **Guidance:** • Prioritize robust cybersecurity plans to ensure operational cyber resilience in the production environment.	

903 ## 5.3. Protect

904 **Table 10. Subcategory-level guidance for PROTECT Function**

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
PROTECT – **PR.AA: Identity Management, Authentication, and Access Control** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access – **PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization	Ecosystem	**Rationale:** This enables the organization to protect sensitive information and critical systems by ensuring that only authenticated and authorized entities can access them. It supports compliance with regulatory requirements and enhances accountability through traceable access logs. This practice extends to vendor and other third-party user accounts. **Guidance:** • "Establish and manage identification mechanisms and credentials for users of the manufacturing system." IR 8183r1: PR.AC-1 • "Implement automated mechanisms where feasible to support the management and auditing of information system credentials." IR 8183r1: PR.AC-1 • "Issue unique credentials bound to each verified user, device, and process interacting with the manufacturing systems." IR 8183r1: PR.AC-6 • "Ensure credentials are authenticated and the unique identifiers are captured when performing system interactions." IR 8183r1: PR.AC-6 • Managed local accounts or those that are isolated from management systems on the factory floor require different management procedures. • Administrator, shared, and vendor accounts for support should be carefully managed through established processes to mitigate risks.	[IR 8183r1]: PR.AC-1, PR.AC-6
(PR.AA-01)	Fab	**Considerations:** Access to both industrial control systems and IT systems should be controlled, including the use of Identity and Access Management (IAM) controls and system logging to detect malicious activity on user accounts.	
(PR.AA-01)	Enterprise IT	**Considerations:** An Identity and Access Management (IAM) system that integrates with both IT and OT environments provides a unified approach to managing identities across the organization. This system supports compliance with data protection regulations and improves	

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		operational efficiency through automated provisioning processes.	
(PR.AA-01)	Equipment and Tooling	**Considerations:** In production environments, managing identities and credentials is critical for maintaining the integrity of manufacturing processes and ensuring product quality and safety. It helps prevent unauthorized changes to production systems that could lead to defects or safety issues.	
PR.AA-02 Identities are proofed and bound to credentials based on the context of interactions	Ecosystem	**Rationale:** This practice ensures that each identity is accurately verified and linked to the appropriate credentials to provide a reliable means of authentication. Organizations can implement dynamic and context-aware access controls by considering the context of interactions, such as the sensitivity of accessed resources or the environment in which access occurs. While shared accounts are commonly used in the industry, organizations should try to integrate authentication, authorization, and accounting (AAA) where feasible. **Guidance:** • "Issue unique credentials bound to each verified user, device, and process interacting with the manufacturing systems." IR 8183r1: PR.AC-6 • "Ensure credentials are authenticated and the unique identifiers are captured when performing system interactions." IR 8183r1: PR.AC-6 • When issuing credentials to third-parties or other external users, ensure appropriate access controls to limit available assets to a basis of "need to know," or more specifically, "need to use or access." (See also PR.AA-05.)	[IR_8183r1]: PR.AC-3, PR.AC-6, PR.AC-7 [ANSI_IEC_62443_2_1]: 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 [ANSI_IEC_62443_3_3]: SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 [ISO_IEC_27001]: A.7.1.1, A.9.2.1
(PR.AA-02)	Fab	**Considerations:** This feature enables fabs to implement robust security measures in various applications (e.g., bound to credentials and based on context to control access to cleanrooms).	
(PR.AA-02)	Equipment and Tooling	**Considerations:** Embedding context-aware identity proofing capabilities provides a hardware-based foundation for secure authentication in end products.	
PR.AA-03 Users, services, and hardware are authenticated	Ecosystem	**Rationale:** This ensures that only legitimate entities gain access to sensitive information and critical resources by preventing unauthorized access and potential breaches. Authentication verifies the identity of users and devices to safeguard against impersonation and credential theft. It also ensures that only trusted applications interact with	[IR_8183r1]: PR.AC-3, PR.AC-7 [ANSI_IEC_62443_2_1]: 4.3.3.6.1,

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		the organization's infrastructure, reducing the risk of malicious software infiltrating the network. **Guidance:** • "Implement multi-factor or certificate-based authentication for transactions within the manufacturing systems determined to be critical." IR 8183r1: PR.AC-7	4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 [ANSI_IEC_62443_3_3]: SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 [ISO_IEC_27001]: A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 [SP_800_53r4]: IA-5, IA-8
(PR.AA-03)	Fab	**Considerations:** Implementing robust authentication mechanisms for all equipment, including legacy systems (when possible), ensures the integrity of manufacturing processes. This practice prevents unauthorized modifications to critical parameters, enhances the traceability of actions, and supports compliance with industry standards.	
(PR.AA-03)	Enterprise IT	**Considerations:** Implementing context-aware or adaptive authentication that is supported by PR.AA-02 and considers various factors (e.g., device health, location, and user behavior patterns) strengthens security for remote work and cloud-based design tools. This approach supports the principle of least privilege, enhances the protection of intellectual property, and enables more accurate risk assessments for access requests. Consistent authentication policies across all systems, including chip design and simulation tools, strengthen the overall security posture. This approach protects valuable intellectual property, supports secure collaboration in distributed design teams, and enables more effective audit trails.	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
(PR.AA-03)	Equipment and Tooling	**Considerations:** Implementing robust authentication mechanisms for all equipment, including legacy systems (when possible), ensures the integrity of manufacturing processes. This practice prevents unauthorized modifications to critical parameters, enhances the traceability of actions, and supports compliance with industry standards.	
PR.AA-04 Identity assertions are protected, conveyed, and verified	Ecosystem	**Rationale:** Identity assertions should be safeguarded against interception and tampering to prevent unauthorized access and identity fraud. Securely conveying these assertions ensures that they are only transmitted through trusted channels and reduces the risk of compromise during transit. Organizations should ensure that identity assertions used to access IP are protected, conveyed, and verified before access is granted. **Guidance:** • Ensure that identity assertions are encrypted in transit using trusted channels (e.g., Transport Layer Security [TLS]). Any encryption mechanisms used should leverage the most recently updated algorithms. • “Ensure credentials are authenticated and the unique identifiers are captured when performing system interactions.” IR 8183r1: PR.AC-6 • “Implement procedures for verifying identity of individuals before issuing credentials that provide access to the manufacturing systems.” IR 8183r1: PR.AC-6	[IR 8183r1]: PR.AC-6 [SAML v2] [OpenID CC1] [IETF JWT] [SP 800 207], [SP 800 63C], [SP 800 53r5]: SC-8, SC-11, SC-12
(PR.AA-04)	Fab	**Considerations:** Implementing secure protocols for conveying identity assertions between fab systems and equipment ensures the integrity of manufacturing processes. This practice can help prevent machine-in-the-middle attacks, support the secure integration of diverse equipment types, and enhance overall operational reliability. **Guidance:** • Organizations should strive to meet certain identity-assertion outcomes in a defined amount of time, such as having no shared accounts, minimizing the use of shared accounts, or leveraging compensating controls. • Establish MFA on all critical systems to limit access and validate all access attempts, though this could	

Function – Category – Subcategory	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		be challenging on certain systems (e.g., those that are air-gapped).	
(PR.AA-04)	Enterprise IT	**Considerations:** Using industry-standard protocols for secure identity federation across the enterprise enables seamless and secure access to resources. This approach supports efficient collaboration, reduces administrative overhead, and enhances the user experience while maintaining strong security.	
(PR.AA-04)	Equipment and Tooling	**Considerations:** Designing systems to securely handle and verify identity assertions increases the resiliency of fab operations.	
PR.AA-05 Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed and incorporate the principles of least privilege and separation of duties	Ecosystem	**Rationale:** Defining, managing, enforcing, and regularly reviewing access permissions, entitlements, and authorizations in accordance with a policy that incorporates the principles of least privilege and separation of duties is essential for maintaining robust security and operational integrity. **Guidance:** • Define a policy related to authentication, authorization, and accounting (AAA). Document and implement review processes for the policy to support policy improvement. • “Deactivate system credentials after a specified time period of inactivity, unless this would result in a compromise to safe operation of the process.” IR 8183r1: PR.AC-1 • “Implement separation of duties for manufacturing system users. Limit, document, and explicitly authorize privileged user access to the manufacturing system. Audit the execution of privileged functions on the manufacturing system. Separation of duties includes, for example: dividing operational functions and system support functions among different roles; conducting system support functions with different individuals; and ensuring security personnel administering access control functions do not also administer audit functions.” IR 8183r1: PR.AC-4 • “Enforce account usage restrictions for specific time periods and locality. Monitor manufacturing system usage for atypical use. Disable accounts of users posing a significant risk. Specific restrictions can include, for example, restricting usage to certain	[IR_8183r1]: PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6 [SP_800_53r4]: AC-1, AC-2, AC-3, AC-5, AC-6, AC-17 [ANSI_IEC_62443_2_1]: 4.3.3.7.3 [ANSI_IEC_62443_3_3]: SR 2.1 [ISO_IEC_27001]

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		days of the week, time of day, or specific durations of time. Privileged user access through non-local connections to the manufacturing system is restricted and managed." IR 8183r1: PR.AC-4 • Access permissions in local system accounts should be separate from access permissions in factory floor management systems accounts.	
(PR.AA-05)	Fab	**Considerations:** Implementing granular access controls for different fab areas, equipment types, and process stages enhances operational security and efficiency. This practice supports compliance with industry regulations, reduces the risk of accidental or malicious process interference, and facilitates more effective auditing. **Guidance:** • Establish role-based access control [RBAC] on all critical systems to limit access and validate all access attempts, though this could be challenging on certain systems (e.g., those that are air-gapped).	
(PR.AA-05)	Enterprise IT	**Considerations:** Establishing controls (e.g., RBAC policies) that align with job functions across the semiconductor value chain ensures appropriate access to sensitive information, protects intellectual property, supports regulatory compliance, and enhances collaboration by enabling secure information sharing.	
(PR.AA-05)	Equipment and Tooling	**Considerations:** Designing products with the ability to enforce least privilege and separation of duties in their operation and management enhances their security in various deployment scenarios.	
PR.AA-06 Physical access to assets is managed, monitored, and enforced commensurate with risk	Ecosystem	**Rationale:** Managing, monitoring, and enforcing physical access to assets based on assessed risks are essential steps in safeguarding an organization's critical resources and confidential information. Organizations can effectively prevent unauthorized access to sensitive areas by instituting comprehensive physical access controls, including the monitoring and logging of entries and exits for personnel, visitors, and vendors (see also DE.CM-02) and the deployment of physical barriers. **Guidance:** • "Protect physical access to the manufacturing facility. Determine access requirements during emergency situations." IR 8183r1: PR.AC-2	[IR_8183r1]: PR.AC-2, PR.DS-5, PR.PT-4 [ANSI_IEC_62443_2_1]: 4.3.3.3.2, 4.3.3.3.8 [ISO_IEC_27001]: A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6,

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• “Protect power equipment, power cabling, network cabling, and network access interfaces for the manufacturing system from accidental damage, disruption, and physical tampering. Ensure availability and integrity of wireless systems, especially safety related systems.” IR 8183r1: PR.AC-2 • “Control physical access to the manufacturing system in addition to the physical access for the facility.” IR 8183r1: PR.AC-2 • “Protect the system from information leakage due to electromagnetic signals emanations.” IR 8183r1: PR.DS-5 • Protect data and media during transportation. • Protect and control portable storage devices that contain manufacturing system data while in transit and in storage.	A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8
(PR.AA-06)	Fab	**Considerations:** Implementing physical access controls for cleanrooms protects critical manufacturing assets and processes, helps to ensure cleanroom integrity, prevents unauthorized access to sensitive areas, and supports compliance with industry standards.	
(PR.AA-06)	Enterprise IT	**Considerations:** Ensuring the physical security of data centers and development environments that house critical semiconductor design assets protects valuable intellectual property. This approach also complements logical access controls, supports compliance with data protection regulations, and enhances business continuity.	
(PR.AA-06)	Equipment and Tooling	**Considerations:** Considering physical tamper resistance and detection features in product design, especially for security-critical components, enhances the overall security of end products.	
PR.AT: Awareness and Training The organization’s personnel are provided with cybersecurity awareness and training so that they can	Ecosystem	**Rationale:** As the first line of defense against cyber threats, employees should understand the importance of cybersecurity practices, how to recognize potential threats, and how to respond appropriately. Regular training helps cultivate a security-conscious culture and reduces the risk of human errors that can lead to data breaches and other security incidents. The security awareness and training of third-party providers should also be considered to help reduce cybersecurity risk. **Guidance:**	[IR_8183r1]: PR.AT-1, PR.AT-3, RS.CO-1 [ANSI_IEC_62443_2_1]: 4.3.2.4.2 [ISO_IEC_27001]: A.7.2.2, A.12.2.1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
perform their cybersecurity-related tasks – **PR.AT-01** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind		• "Provide security awareness training for all manufacturing system users and managers." IR 8183r1: PR.AT-1 • "Incorporate insider threat recognition and reporting into security awareness training." IR 8183r1: PR.AT-1	
(PR.AT-01)	Fab	**Considerations:** Providing specialized training on cybersecurity risks in manufacturing environments and equipment security enhances overall operational security, reduces the risk of human error leading to security breaches, and supports compliance with industry standards. **Guidance:** • "Provide security awareness training for all manufacturing system users and managers. Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, responding to suspected cybersecurity incidents, and awareness of operational security." IR 8183r1: PR.AT-1 • Visitors should be required to complete basic cybersecurity awareness and understand cybersecurity requirements before being granted access.	
(PR.AT-01)	Enterprise IT	**Considerations:** Offering regular cybersecurity awareness training that is tailored to different roles strengthens the organization's security posture.	
(PR.AT-01)	Equipment and Tooling	**Considerations:** Educating personnel on secure design principles and the potential security implications of product features ensures that security is integrated into the product development life cycle.	

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
PR.AT-02 Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with security risks in mind	Ecosystem	**Rationale:** Organizations should identify individuals with specialized roles (e.g., those that support incident response and recovery) and ensure that they have specialized training in cybersecurity and OT operations to support their roles. **Guidance:** • "Ensure that users with privileged access to the manufacturing system understand the requirements and responsibilities of their assignments." IR 8183r1: PR.AT-2 • "Establish standards for measuring, building, and validating individual qualifications for privileged users." IR 8183r1: PR.AT-2 • "Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them." IR 8183r1: PR.AT-4 • "Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility are trained and understand their responsibilities." IR 8183r1: PR.AT-5 • "Establish standards for measuring, building, and validating individual qualifications for physical security personnel." IR 8183r1: PR.AT- 5 • "Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response." IR 8183r1: RS.CO-1	[IR_8183r1]: PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, RS.CO-1 [ANSI_IEC_62443_2_1]: 4.3.2.4.2, 4.3.2.4.3 [ISO_IEC_27001]: A.6.1.1, A.7.2.2 [SP_800_53r4]: AT-3, PM-13
(PR.AT-02)	Fab	**Considerations:** Providing advanced training for process engineers and operators on securing manufacturing equipment and detecting anomalies that may indicate cyber threats enhances the fab's ability to maintain process integrity, improves early threat detection capabilities, and supports the development of secure manufacturing workflows.	
(PR.AT-02)	Enterprise IT	**Considerations:** Offering specialized training on secure hardware design principles and tools enables personnel to understand the environment that they are trying to protect.	
(PR.AT-02)	Equipment and Tooling	**Considerations:** Training product security teams on the latest hardware security techniques, side-channel attacks,	

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		and the secure implementation of cryptographic functions is vital.	
PR.DS: Data Security Data is managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information – **PR.DS-01:** The confidentiality, integrity, and availability of data at rest are protected	Ecosystem	**Rationale:** Protecting the confidentiality, integrity, and availability of data at rest ensures that sensitive information remains secure when stored within an organization's systems. Data at rest, which includes all data that is not actively being transmitted or processed, is often a target for unauthorized access, theft, or tampering. **Guidance:** • "Protect the manufacturing system against data leaks." IR 8183r1: PR.DS-5 • "Implement cryptographic mechanisms where determined necessary to prevent unauthorized access, distortion, or modification of system data and audit records." IR 8183r1: PR.DS-2 • Protect and control portable storage devices that contain manufacturing system data while in transit and in storage.	[IR_8183r1]: PR.DS-2, PR.DS-5, PR.DS-6, PR.PT-2 [ANSI_IEC_62443_3_3]: SR 3.4, SR 4.1 [ISO_IEC_27001]: A.8.2.3 [SP_800_53r4]: MP-8, SC-12, SC-28
(PR.DS-01)	Fab	**Considerations:** Data at rest includes sensitive operational data (e.g., equipment configuration files, process recipes, and tool settings) that is critical to manufacturing yields and maintaining operational efficiency. Tools may be independently owned by the fab and simultaneously managed by OEMs, meaning that support agreements may complicate data access.	
(PR.DS-01)	Enterprise IT	**Considerations:** Semiconductor companies store vast amounts of sensitive data in enterprise IT systems, including design schematics, product roadmaps, and customer contracts. Protecting this data at rest ensures that the company remains competitive and avoids legal repercussions from data breaches.	
(PR.DS-01)	Equipment and Tooling	**Considerations:** Protecting data at rest is essential for preventing tampering and reverse engineering.	
PR.DS-02: The confidentiality, integrity, and	Ecosystem	**Rationale:** Protecting the confidentiality, integrity, and availability of data in transit is essential for securing information as it moves between systems, networks, and devices. Data in transit is particularly vulnerable to	[IR_8183r1]: PR.DS-2, PR.DS-5

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
availability of data in transit are protected		interception, eavesdropping, and machine-in-the-middle attacks, which can lead to unauthorized access, data breaches, and tampering. **Guidance:** - "Regulate the information flow within the manufacturing system and to outside systems." IR 8183r1: PR.DS-5 - "Enforce controls restricting connections to only authorized interfaces." IR 8183r1: PR.DS-5 - Protect and control portable storage devices that contain manufacturing system data while in transit and in storage.	[ANSI_IEC_62443_3_3]: SR 3.1, SR 3.8, SR 4.1, SR 4.2 [ISO_IEC_27001]: A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
(PR.DS-02)	Fab	**Considerations:** Machine-to-machine (M2M) communications often include the transmission of sensitive data between process control systems, fabrication equipment, and monitoring devices. Securing this data in transit ensures operational integrity by preventing unauthorized alterations to process parameters that could result in manufacturing errors or yield loss. Securing this data can be aided by the data-in-transit protection mechanisms provided by the equipment and tooling present in the fab. In situations where such capabilities are not provided, consider compensatory controls that can help in addressing control gaps or risks. **Guidance:** - "Protect manufacturing system information determined to be critical when in transit." IR 8183r1: PR.DS-2	
(PR.DS-02)	Enterprise IT	**Considerations:** Securing data in transit within enterprise IT environments is crucial, especially with the frequent use of remote design collaborations, vendor negotiations, and internal R&D efforts across global teams. Protecting data as it traverses internal and external networks ensures confidentiality and maintains a company's competitive advantage by preventing the exposure of sensitive IP or business-critical data. Additional capabilities may be necessary to support operations-borne requirements to send and receive sensitive information by email.	
(PR.DS-02)	Equipment and Tooling	**Considerations:** Semiconductor equipment, particularly those embedded in connected systems, often involve the transmission of sensitive data during operation.	

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
PR.DS-10: The confidentiality, integrity, and availability of data in use are protected	Ecosystem	**Rationale:** Protecting the confidentiality, integrity, and availability of data in use is crucial for ensuring that sensitive information remains secure while being processed or actively accessed by applications and users. Data in use is particularly vulnerable to threats that can lead to data breaches and tampering, such as unauthorized access, malware, and insider attacks. Security measures (e.g., memory encryption, secure enclaves, and stringent access controls) help safeguard data during its active phase and prevent unauthorized viewing or manipulation. **Guidance:** • "Regulate the information flow within the manufacturing system and to outside systems." IR 8183r1: PR.DS-5 • "Enforce controls restricting connections to only authorized interfaces." IR 8183r1: PR.DS-5	[IR_8183r1]: PR.DS-5 [SP_800_207] SP 800-125B [ISO_IEC_27002_2013] Clause 10: [ANSI_IEC_62443_3_3] [IEEE_2700] [OWASP]
(PR.DS-10)	Fab	**Considerations:** Data in use is often related to real-time process monitoring and control. Protecting this operational data ensures that process adjustments, yield monitoring, and equipment diagnostics can proceed without interference or manipulation; reduces the risk of faulty production runs; and safeguards the proprietary data involved in high-precision manufacturing environments.	
(PR.DS-10)	Enterprise IT	**Considerations:** Enterprise IT systems handle significant volumes of sensitive data in use, such as active design projects, customer interactions, and real-time R&D data. Protecting this data is critical to preventing unauthorized access that could result in IP theft, project delays, or compliance failures, particularly in an industry where time-to-market and protecting competitive advantages are key business drivers.	
(PR.DS-10)	Equipment and Tooling	**Considerations:** Many pieces of semiconductor equipment rely on active, real-time data in use for decision-making. Protecting this data ensures the reliability and security of production and prevents malicious actors from exploiting vulnerabilities in data processing to cause malfunctions, degrade performance, or alter safety-critical behaviors in real-world applications. Customers should not be able to access the owner's IP.	
PR.DS-11: Backups of data	Ecosystem	**Rationale:** Creating, protecting, maintaining, and testing backups of data ensure data recovery and business	[IR_8183r1]: PR.IP-4

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
are created, protected, maintained, and tested		continuity in the event of data loss, corruption, or cyber attacks. Regular backups provide a safeguard against unforeseen incidents (e.g., hardware failures, ransomware attacks, natural disasters) and enable the organization to restore critical information quickly. **Guidance:** • "Include into contingency plan testing the conducting of restorations from backup data." IR 8183r1: PR.IP-4 • "Store critical manufacturing system backup information separately." IR 8183r1: PR.IP-4 • "Verify the reliability and integrity of backups." IR 8183r1: PR.IP-4 • "Coordinate backup testing with organizational elements responsible for related plans." IR 8183r1: PR.IP-4 • "Establish a separate alternate storage site for system backups and ensure the same security safeguards are employed." IR 8183r1: PR.IP-4	[CIS_v8]: CSC 10 [COBIT5] APO13.01, DSS01.01, DSS04.07 [ANSI_IEC_62443_2_1]: 4.3.4.3.9 [ANSI_IEC_62443_3_3]: SR 7.3, SR 7.4 [ISO_IEC_27001]: A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 [SP_800_53r4]: CP-4, CP-6, CP-9
(PR.DS-11)	Fab	**Considerations:** Regularly backing up sensitive operational data (e.g., tool configurations, process recipes) ensures rapid recovery from both physical and cyber incidents. To reduce backup storage requirements and speed restoration, consider whether there is ephemeral, intermediate, or transient process data that does not require backup.	
(PR.DS-11)	Enterprise IT	**Considerations:** Enterprise IT systems in the semiconductor industry house vital data, such as design files, production schedules, and customer contracts. Regularly backing up this data and ensuring that it can be recovered in case of incidents like ransomware attacks or system crashes ensures business continuity and compliance with regulations (e.g., data protection laws) while also protecting the company's reputation and financial standing.	
(PR.DS-11)	Equipment and Tooling	**Considerations:** Maintaining backups of configuration data, firmware, and critical software components helps ensure that the product can be restored to its fully functional and secure state in the event of a malfunction or cyber attack.	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
PR.PS: Platform Security The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability – **PR.PS-01:** Configuration management practices are established and applied	Ecosystem	**Rationale:** Systematically managing and documenting the configuration of systems, software, and hardware can increase consistency, prevent unauthorized changes, and quickly identify and resolve issues. These practices help mitigate risks associated with misconfigurations and reduce the potential for security vulnerabilities **Guidance:** • "Review and update the baseline configuration of the manufacturing system as an integral part of system component installations and upgrades. Retain previous versions of the baseline configuration to support rollback." IR 8183r1: PR.IP-1 • "Define configuration parameters, capabilities, and fail to known state procedures such that, upon a system failure (or failure conditions), assets revert to a state that achieves a predetermined mode of operation." IR 8183r1: PR.IP-1 • "Implement configuration change control for the manufacturing system and its components." IR 8183r1: PR.IP-1 • "Conduct security impact analyses in connection with change control reviews." IR 8183r1: PR.IP-1 • "Implement automated mechanisms where feasible to support the change control process." IR 8183r1: PR.IP-1 • "Test, validate, and document changes to the manufacturing system before implementing the changes on the operational system." IR 8183r1: PR.IP-3 • "Review and authorize proposed configuration-controlled changes prior to implementing them on the manufacturing system." IR 8183r1: PR.IP-3 • "Configure the manufacturing system to provide only essential capabilities." IR 8183r1: PR.PT-3 • "Disable defined functions, ports, protocols, and services within the manufacturing system deemed to be unnecessary." IR 8183r1: PR.PT-3 • "Manage for false positives during malicious code detection and eradication." IR 8183r1: DE.CM-4	[IR_8183r1]: PR.IP-1, PR.IP-3, PR.PT-2, PR.PT-3, DE.CM-4 [ANSI_IEC_62443_2_1]: 4.3.4.3.2, 4.3.4.3.3 [ANSI_IEC_62443_3_3]: SR 7.6 [ISO_IEC_27001]: A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 [SEMI_E187]
(PR.PS-01)	Fab	**Considerations:** Fabs often use a mix of new and legacy equipment, making automated tools critical for efficiently	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		tracking and managing configurations. However, there may be legacy devices that are not compatible with these tools, which adds a layer of complexity to the configuration management activity.	
(PR.PS-01)	Enterprise IT	**Considerations:** In hybrid environments that combine on-premises and cloud infrastructure, maintaining configuration consistency requires robust change management processes and automated tools.	
(PR.PS-01)	Equipment and Tooling	**Considerations:** Configuration management in production environments should account for collaboration with external partners, as well as the need for strong access controls to prevent unauthorized changes to production systems.	[ANSI_IEC_62443_2_1]: 4.3.4.3.2 [ANSI_IEC_62443_3_3]: SR 2.3, 7.6, CM-2, CM-6, MP-2
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	Ecosystem	**Rationale:** Regular maintenance — including updates and patches — addresses vulnerabilities, improves functionality, and protects systems from emerging threats. Replacing outdated or unsupported software reduces exposure to risks associated with obsolete technologies. Removing unnecessary or deprecated software minimizes the attack surface and lowers the risk of exploitation. **Guidance:** • "Require that diagnostic services pertaining to remote maintenance be performed from a system that implements a security capability comparable to the capability implemented on the manufacturing system." IR 8183r1: PR.MA-2 • "Deploy malicious code protection mechanisms throughout the manufacturing system where safe and feasible to detect and eradicate malicious code." IR 8183r1: DE.CM-4 • "Update malicious code protection mechanisms whenever new releases are available in accordance with the configuration management policy and procedures for the manufacturing system." IR 8183r1: DE.CM-4 • "Automatically update malicious code protection mechanisms where safe and feasible." IR 8183r1: DE.CM-4	[IR_8183r1]: PR.IP-12, PR.MA-2, DE.CM-4

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		• Establish and maintain a formal patch management program that aligns with vulnerability management processes, ensuring timely identification, validation, testing, and deployment of security updates to mitigate known exposures and maintain the integrity of manufacturing systems.	
(PR.PS-02)	Fab	**Considerations:** There should be timely updates for equipment-specific software and legacy systems that may no longer receive official updates or support from vendors. Fabs may lease, license, or rely heavily on vendor-managed support agreements, which can dictate who is authorized to apply updates, when maintenance can be scheduled, and under what conditions. As a result, operations may need to be closely coordinated with vendors or governed by strict contractual and warranty obligations that can hinder the timely deployment of patches and limit control over security and maintenance processes.	
(PR.PS-02)	Enterprise IT	**Considerations:** Software management is essential for maintaining the security and efficiency of business operations, data management, and support systems for manufacturing processes.	
(PR.PS-02)	Equipment and Tooling	**Considerations:** Software management is critical for ensuring the integrity, quality, and security of the final product, as well as the efficiency and reliability of the production process. Software embedded in semiconductor products requires stringent version control and security measures throughout its life cycle.	
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	Ecosystem	**Rationale:** Replacing outdated or vulnerable hardware mitigates risks associated with obsolescence and enhances performance and security. Removing redundant or compromised hardware reduces potential attack surface and prevents unauthorized access to sensitive data. **Guidance:** • “Enforce accountability for all manufacturing system components throughout the system lifecycle, including removal, transfers, and disposition.” IR 8183r1: PR.DS-3 • “Enforce approval requirements, control, and monitoring of maintenance tools for use on the manufacturing system. Maintenance tools can include, for example, hardware/software diagnostic	[IR_8183r1]: PR.DS-3, PR.MA-1 [CIS_v8]: Control 1 [COBIT5] BAI09.03 [ANSI_IEC_62443_2_1]: 4.3.3.3.9, 4.3.4.4.1 [ANSI_IEC_62443_3_3]: SR 4.2 [ISO_IEC_27001]:

Function **–** **Category** **–** **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		test equipment, hardware/software packet sniffers, and laptops." IR 8183r1: PR.MA-1 • "Perform preventative maintenance at defined intervals." IR 8183r1: PR.MA-1 • "Inspect maintenance tools brought into the facility." IR 8183r1: PR.MA-1 • "Scan maintenance tools and portable storage devices for malicious code before they are used on the manufacturing system." IR 8183r1: PR.MA-1 • "Ensure that disposal actions are approved, tracked, documented, and verified." IR 8183r1: PR.MA-1	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7
(PR.PS-03)	Fab	**Considerations:** Hardware maintenance is critical due to the reliance on highly specialized and precise equipment. Maintaining and replacing hardware based on risk assessments ensures that production remains uninterrupted and that equipment continues to perform at the required specifications and commensurate with risk.	
(PR.PS-03)	Enterprise IT	**Considerations:** Managing hardware encompasses servers, storage devices, workstations, and network equipment that support business operations. Regular maintenance and the timely replacement of IT hardware ensure continued performance and security. Obsolete hardware can pose risks, such as security vulnerabilities, performance degradation, and non-compliance with data protection regulations.	
(PR.PS-03)	Equipment and Tooling	**Considerations:** Specialized equipment and tooling are foundational to production quality and throughput, so hardware maintenance demands a structured approach that is guided by risk assessments. Regular inspections, calibrations, and timely replacements should align with performance requirements, contractual obligations, vendor support agreements, and warranty terms.	
PR.PS-04: Log records are generated and made available for continuous monitoring	Ecosystem	**Rationale:** Logs provide detailed records of system activities, user actions, and network events, enabling the detection of suspicious behavior, the identification of potential security incidents, and the facilitation of forensic investigations. Continuous monitoring of these logs ensures real-time awareness of anomalies and threats and allows for prompt response and mitigation. **Guidance:** • "Conduct time correlation of audit records." IR 8183r1: PR.PT-1	[IR 8183r1]: PR.PT-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Enable authorized individuals to extend audit capabilities when required by events." IR 8183r1: PR.PT-1 • "Ensure that audit processing failures on the manufacturing system generate alerts and trigger defined responses." IR 8183r1: PR.PT-1 "Implement automated mechanisms to integrate audit review, analysis, and reporting." IR 8183r1: PR.PT-1	
(PR.PS-04)	Fab	**Considerations:** Implementing comprehensive logging can be challenging due to legacy equipment that may lack built-in logging capabilities or interfaces for data extraction. Challenges emerge when the technology stack is not fully owned, as obtaining the necessary data from OT equipment often requires suppliers or OEMs to integrate this capability. Additionally, the vast amount of data generated requires efficient storage and analysis solutions to prevent straining resources. Enabling these tools to communicate and export logs for analysis is essential.	[SEMI_E187]
(PR.PS-04)	Enterprise IT	**Considerations:** Integrating different logging systems and formats across various IT assets can hinder comprehensive monitoring, and extensive logging should be balanced with respect for employee privacy rights and adherence to local data protection laws.	
(PR.PS-04)	Equipment and Tooling	**Considerations:** Logs should capture a wide range of data — from machine activity to user access logs and software interactions. Challenges include managing the volume of data generated by high-precision equipment, ensuring the secure storage of log records, and setting up effective monitoring systems that can act on real-time data.	
PR.PS-05: The installation and execution of unauthorized software are prevented	Ecosystem	**Rationale:** Unauthorized software can introduce vulnerabilities, malware, or other malicious activities that compromise system integrity and data security. By enforcing strict controls over software installation and execution, organizations can minimize the risk of security breaches, ensure consistent system performance, and uphold business standards. **Guidance:** • "Identify mechanisms for detecting the presence of unauthorized software within the manufacturing system. Where safe and feasible, these mechanisms should be automated." IR 8183r1: ID.AM-2	[IR_8183r1]: ID.AM-2, DE.CM-7, PR.DS-6, PR.IP-1, PR.PT-2, DE.CM-3, DE.CM-7 [ISO_IEC_27001]: A.12.6.2 [CIS_v8]: Control 2 [SANS_SIP]

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Implement software, firmware, and information integrity checks to detect unauthorized changes to manufacturing system components during storage, transport, startup and when determined necessary." IR 8183r1: PR.DS-6 • "Implement software program usage restrictions." IR 8183r1: PR.IP-1 • "Implement a deny-all, permit-by-exception policy to allow the execution of only authorized software programs." IR 8183r1: PR.IP-1 • "Scan all portable storage devices for malicious code before they are used on the manufacturing system." IR 8183r1: PR.PT-2 • "Enforce software usage and installation restrictions." IR 8183r1: DE.CM-3	[SP_800_167] [ISO_IEC_27001]: Annex A.12.5 [ANSI_IEC_62443_3_3]
(PR.PS-05)	Fab	**Considerations:** All software changes should be strictly controlled and audited in real time, particularly for legacy equipment that may not support modern security mechanisms.	
(PR.PS-05)	Enterprise IT	**Considerations:** Challenges include managing a large number of endpoints across different departments and preventing unauthorized software installations while balancing productivity and security.	
(PR.PS-05)	Equipment and Tooling	**Considerations:** Challenges include managing the software environments of globally distributed teams and external collaborators while ensuring that only authorized software is used in the product development process.	
PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Ecosystem	**Rationale:** Integrating secure software development practices and monitoring their performance throughout the software development life cycle (SDLC) is vital for producing secure, reliable software. These practices, which include threat modeling, secure coding standards, code reviews, and security testing, help identify and mitigate vulnerabilities early in the development process and reduce the risk of security breaches. **Guidance:** • "Apply security engineering principles into the specification, design, development, implementation, and modification of the manufacturing system." IR 8183r1: PR.IP-2 • "Implement configuration management and change control during the development of the	[IR_8183r1]: PR.IP-2 [CIS_v8]: Control 18 [CISA_SBD] [COBIT5] APO13.01, BAI03.01, BAI03.02, BAI03.03 [ANSI_IEC_62443_2_1]: 4.3.4.3.3

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		manufacturing system and its components, and include flaw tracking and resolution, and security testing." IR 8183r1: PR.IP-2	[ISA_IEC_62443_4_1] [ISO_IEC_27001]: A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 [SP_800_53r4]: PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
(PR.PS-06)	Fab	**Considerations:** Ensure that legacy systems used in fabs are integrated with secure software updates and that third-party vendors comply with secure development standards.	
(PR.PS-06)	Enterprise IT	**Considerations:** Key challenges include managing secure development practices across geographically dispersed development teams and ensuring that all software, whether developed in-house or outsourced, meets security standards.	
(PR.PS-06)	Equipment and Tooling	**Considerations:** Challenges include coordinating secure development practices across global teams and ensuring that security is prioritized without compromising innovation and efficiency in the product development cycle.	
PR.IR: Technology Infrastructure Resilience Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability and organizational resilience	Ecosystem	**Rationale:** Organizations can prevent unauthorized entities from infiltrating their networks by implementing access controls, monitoring network activity, and deploying security technologies, such as firewalls and intrusion prevention systems. Incorporating network segmentation further reinforces this protection by dividing the network into smaller, secure sections and ensuring that only authorized users and systems can interact with critical resources. **Guidance:** • "Provide an explicit indication of active remote access connections to users physically present at the devices." IR 8183r1: PR.AC-3 • "Allow remote access only through approved and managed access points." IR 8183r1: PR.AC-3	[IR_8183r1]: PR.AC-3, PR.AC-5, PR.DS-7, PR.PT-4 [ANSI_IEC_62443_2_1]: 4.3.3.4 [ANSI_IEC_62443_3_3]: SR 3.1, SR 3.8 [ISO_IEC_27001]: A.13.1.1, A.13.1.3, A.13.2.1,

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
– **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage		• Protect network integrity of the manufacturing system, incorporating network segmentation and segregation where appropriate. Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries within the manufacturing system. Implement boundary protection devices.” IR 8183r1: PR.AC-5 • “Implement an off-line development and testing system for implementing and testing changes to the manufacturing system.” NISTIR 8183r1: PR.DS-7 • “Control the flow of information within the manufacturing system and between interconnected systems.” IR 8183r1: PR.PT-4	A.14.1.2, A.14.1.3
(PR.IR-01)	Fab	**Considerations:** Unauthorized logical access to OT networks that control manufacturing equipment poses significant risks, including operational disruption, the manipulation of production processes, and theft of proprietary data. Protecting fab environments from unauthorized access requires strong network segmentation, strict access controls, and continuous monitoring of network traffic.	
(PR.IR-01)	Enterprise IT	**Considerations:** Protecting networks from unauthorized access ensures the security of business-critical systems, including financial systems, IP databases, and communication platforms. Unauthorized access to these systems can result in data breaches, IP theft, and operational downtime.	
(PR.IR-01)	Equipment and Tooling	**Considerations:** Unauthorized logical access can disrupt manufacturing processes, compromise product quality, and lead to IP theft or sabotage. For example, unauthorized access to machines controlling the production of semiconductor components could lead to defective products or production delays.	
PR.IR-02: The organization's technology assets are protected from environmental threats	Ecosystem	**Rationale:** Environmental threats (e.g., fire, flooding, extreme temperatures, and power outages) can cause significant damage to hardware, data, and critical systems, leading to downtime and data loss. Implementing measures like climate control, fire suppression systems, uninterruptible power supplies (UPS), and disaster recovery plans helps mitigate these risks by maintaining optimal operating conditions and providing immediate response capabilities **Guidance:**	[IR 8183r1]: PR.IP-5

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls for the manufacturing system." IR 8183r1: PR.IP-5 • "Fire suppression mechanisms should take the manufacturing environment into account (e.g., water sprinkler systems could be hazardous in specific environments)." IR 8183r1: PR.IP-5 • "Implement fire detection devices that activate and notify key personnel automatically in the event of a fire." IR 8183r1: PR.IP-5 • Protect media during transportation.	
(PR.IR-02)	Fab	**Considerations:** Environmental threats can cause significant production disruptions. The cleanroom environment, where semiconductor wafers are produced, maintains strict controls on temperature, humidity, and particulate levels. Any deviations from established environmental parameters can lead to product contamination or yield losses.	
(PR.IR-02)	Enterprise IT	**Considerations:** Enterprise IT environments are susceptible to environmental threats (e.g., overheating, power failures, and water damage) that can compromise data centers, servers, and critical IT infrastructure.	
(PR.IR-02)	Equipment and Tooling	**Considerations:** Environmental threats (e.g., temperature fluctuations, dust, and humidity) can directly impact the quality and reliability of the final product.	
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Ecosystem	**Rationale:** These mechanisms (e.g., redundancy, failover systems, disaster recovery plans, and regular testing of emergency procedures) help the organization quickly adapt to and recover from disruptions, whether they are caused by cyber attacks, natural disasters, or technical failures. By proactively preparing for adverse situations, organizations can minimize downtime, protect sensitive data, and maintain service delivery to customers and stakeholders. **Guidance:** • "Implement IT resiliency mechanisms to support normal and adverse manufacturing situations." IR 8183r1: PR.PT-5	[IR_8183r1]: PR.PT-5 [SP_800_160v1r1]: Appendices G—K [SP_800_53r5]: SA-14, SA-15 [ISO_IEC_27001]: Annex A.17 [ISO_IEC_22301]: Clause 8.4 & 9.1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Implement OT resiliency mechanisms to support normal and adverse manufacturing situations." IR 8183r1: PR.PT-5	
(PR.IR-03)	Fab	**Considerations:** Ensuring resilience is key to maintaining continuous production. Equipment failure, environmental anomalies, or cyber incidents can cause substantial disruptions.	
(PR.IR-03)	Enterprise IT	**Considerations:** Enterprise IT's resilience maintains access to critical business systems, including design tools, supply chain management, and financial operations. Resilience in IT environments includes disaster recovery, data backups, and system redundancy to ensure that the organization can recover from cyber attacks, system failures, and other disruptions.	
(PR.IR-03)	Equipment and Tooling	**Considerations:** Resilience mechanisms are critical to maintaining product quality and meeting production deadlines. Unplanned interruptions in production — whether caused by power outages, equipment failures, or external threats — can lead to defects, costly delays, or the need for rework.	
PR.IR-04: Adequate resource capacity to ensure availability is maintained	Ecosystem	**Rationale:** Organizations can handle peak loads, accommodate growth, and respond to unexpected increases in demand without compromising performance by ensuring that sufficient computational, storage, and network resources are in place. This proactive approach helps prevent service outages, reduces latency, and ensures that critical applications and services remain accessible to users. Adequate resource capacity also supports scalability and enables the organization to efficiently adapt to changing business needs and technological advancements. **Guidance:** • "Protect the manufacturing system against, or limit the effects of, denial of service attacks." IR 8183r1: PR.DS-4 • "Ensure that adequate resources are maintained for manufacturing system information processing, networking, telecommunications, and data storage." IR 8183r1: PR.DS-4	[IR_8183r1]: PR.DS-4 [ANSI_IEC_62443_3_3]: SR 7.1, SR 7.2 [ISO_IEC_27001]: A.12.1.3, A.17.2.1 [SP_800_53r4]: AU-4, CP-2, SC-5
(PR.IR-04)	Fab	**Considerations:** Ensuring an adequate resource capacity is crucial to production running smoothly and meeting tight timelines. This includes ensuring that manufacturing equipment, cleanroom environments, and supporting	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		systems have sufficient power, cooling, and physical space to operate at peak efficiency.	
(PR.IR-04)	Enterprise IT	**Considerations:** Enterprise IT systems are integral to supporting business operations, design processes, and supply chain management. Maintaining adequate resource capacity in this domain means ensuring that servers, storage systems, and networks can handle both routine tasks and sudden spikes in demand.	
(PR.IR-04)	Equipment and Tooling	**Considerations:** Adequate resource capacity ensures that production lines can continue operating efficiently, even during periods of high demand or unexpected challenges. Production machinery, testing equipment, and supporting infrastructure should have sufficient capacity to handle varying workloads without experiencing delays or quality issues.	

5.4. Detect

Table 11. Subcategory-level guidance for DETECT Function

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
DETECT – **DE.CM: Detect Continuous Monitoring** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events – **DE.CM-01** Networks and network	Ecosystem	**Rationale:** Continuous monitoring allows for the detection of cybersecurity events and potential indicators of threats. Given the critical nature of semiconductor production processes and the potential impacts of cyber incidents on product quality, yield, and intellectual property, robust network monitoring is critical for the early detection of any potential network intrusions and unauthorized connections and services. Network monitoring and early detection enable timely intervention to prevent or minimize production disruptions. **Guidance:** • "Heighten system monitoring activity whenever there is an indication of increased risk to manufacturing operations and assets." IR 8183r1: PR.DS-5 • "Monitor for and report atypical usage of the manufacturing system." IR 8183r1: DE.CM-1	[IR_8183r1]: PR.DS-5, DE.CM-1, DE.CM-4, DE.CM-7, RS.CO-2 [ANSI_IEC_62443_3_3]: SR 6.2

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
services are monitored to find potentially adverse events		- “Implement automated mechanisms to support detection of cybersecurity events.” IR 8183r1: DE.CM-1 - “Conduct ongoing security status monitoring of the manufacturing system network to detect defined cybersecurity events and indicators of potential cybersecurity events.” IR 8183r1: DE.CM-1 - “Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system.” IR 8183r1: DE.CM-1 - “Generate audit records for defined cybersecurity events.” IR 8183r1: DE.CM-1 - “Monitor network communications at the external boundary of the system and at key internal boundaries within the system.” IR 8183r1: DE.CM-1 - “Heighten system monitoring activity whenever there is an indication of increased risk.” IR 8183r1: DE.CM-1 - “Deploy malicious code protection mechanisms throughout the manufacturing system where safe and feasible to detect and eradicate malicious code.” IR 8183r1: DE.CM-4 - “Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software.” IR 8183r1: DE.CM-7 - “Implement automated mechanisms to assist in the reporting of cybersecurity events.” IR 8183r1: RS.CO-2	
(DE.CM-01)	Fab	**Considerations:** Semiconductor fabrication facilities have unique OT and ICS that require specialized monitoring solutions. Sometimes, the unique nature of legacy systems and OT prevents the use of conventional means of detection, so other methods may be required. Cleanroom environments and sensitive manufacturing processes pose challenges for traditional monitoring approaches. High-speed, high-volume data flows are typical in semiconductor manufacturing environments. Networks are segmented, and traffic that deviates from the established baselines (e.g., traffic patterns, communication protocols, device behaviors) is monitored to detect anomalies and minimize the attack surface. Anti-	[IR_8183r1]: PR.AC-3, PR.DS-5, DE.CM-1, DE.CM-4, DE.CM-7 [ISA_IEC_62443_4_2]: Section 4.3 [ISO_IEC_27001], Annex A.12.4

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		malware software may not run on equipment due to the speed and precision required. **Considerations:** "Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use." IR 8183r1: PR.DS-5	
(DE.CM-01)	Enterprise IT	**Considerations:** Continuous monitoring should include all access points, data centers, and remote connections to identify any potential compromises, protect intellectual property, and maintain the reliability of business operations. Enterprise IT systems often interface with OT systems in semiconductor manufacturing, and lateral movement from IT to OT systems is possible. Intellectual property protection is a significant concern in the semiconductor industry. **Guidance:** • "Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest." IR 8183r1: DE.CM-7 • "Monitor for unauthorized configuration changes to the manufacturing system." IR 8183r1: DE.CM-7 • "Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software". IR 8183r1: DE.CM-7	[SP_800_41r1]: Section 5.3 [ISO_IEC_27002_2022]: Section A.12.1 CA-3
(DE.CM-01)	Equipment and Tooling	**Considerations:** There are significant challenges in deploying monitoring systems without disrupting continuous operations. These environments utilize automated machinery and interconnected devices, and integrating new monitoring solutions may not be feasible. This is exacerbated by the fact that many systems were not originally designed with network monitoring capabilities. Additionally, resource constraints can directly impact operations. Network anomalies in such setups could halt production and result in substantial financial losses. Thus, monitoring strategies should prioritize real-time visibility and minimal downtime. Challenges also extend to maintaining an accurate system inventory, especially when the technology stack is not directly controlled by the end user.	
DE.CM-02 The physical environment is	Ecosystem	**Rationale:** Monitoring the physical environment is essential for detecting potential cybersecurity events that could impact the broader ecosystem, including physical	[IR_8183r1]: PR.DS-3, DE.CM-2

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
monitored to find potentially adverse events		breaches or unauthorized access to sensitive areas. Timely detection and response are vital to ensuring the safety and security of the entire supply chain. **Guidance:** • "Maintain and review visitor access records to the facility where the manufacturing system resides." IR 8183r1: PR.AC-2 • "Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items." IR 8183r1: PR.DS-3 • "Conduct ongoing security status monitoring of the manufacturing system facility to detect physical security incidents." IR 8183r1: DE.CM-2 • "Implement independent teams to monitor the security of the physical environment." IR 8183r1: DE.CM-2 • "Monitor physical intrusion alarms and surveillance equipment." IR 8183r1: DE.CM-2 • "Monitor physical access to the manufacturing system and devices in addition to the facility." IR 8183r1: DE.CM-2	
(DE.CM-02)	Enterprise IT	**Considerations:** Physically monitoring enterprise IT environments protects critical IT infrastructure from unauthorized physical access that could compromise security. **Guidance:** Continuously monitor surveillance systems, physical intrusion alarms, and access and badge controls that cover critical areas and entry points to prevent unauthorized access. House critical devices in secure enclosures. Periodically conduct integrity inspections to detect unauthorized access or tampering. Make records of integrity information at time of deployment for future comparisons.	
DE.CM-03 Personnel activity and	Ecosystem	**Rationale:** Monitoring user and entity behavior analytics, account access, authentication, and authorization is vital for gaining insights on insider threats and detecting	[IR 8183r1]: PR.AC-1, PR.AC-3,

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
technology usage are monitored to find potentially adverse events		potential cybersecurity events. Having a strong baseline is a requirement, and generating a baseline could be a challenge. **Guidance:** “Monitor the manufacturing system for atypical use of system credentials. Credentials associated with significant risk are disabled.” IR 8183r1: PR.AC-1 “Conduct security status monitoring of personnel activity associated with the manufacturing system.” IR 8183r1: DE.CM-3 “Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest.” IR 8183r1: DE.CM-7 “Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use.” IR 8183r1: PR.DS-5	PR.DS-5, DE.CM-3, DE.CM-7 [ANSI_IEC_62443_3_3]: SR 6.2
(DE.CM-03)	Fab	**Considerations:** Fab facilities often contain intellectual property and sensitive processes. Monitoring personnel activity helps detect unauthorized access and actions that could negatively impact operations or security.	
(DE.CM-03)	Equipment and Tooling	**Considerations:** Personnel activity during the production process should be monitored to prevent unauthorized changes or actions that could compromise product quality, safety, or security.	
DE.CM-06 External service provider activities and services are monitored to find potentially adverse events	Ecosystem	**Rationale:** Monitoring external service provider activities and services helps detect and mitigate adverse events or security incidents that could arise from the additional attack vectors and potential vulnerabilities introduced into the organization’s environment by external service providers (both on-site and off-site). **Guidance:** • “Conduct ongoing security status monitoring of external service provider activity on the manufacturing system.” IR 8183r1: DE.CM-6 • “Detect defined cybersecurity events and indicators of potential cybersecurity events from external service providers.” IR 8183r1: DE.CM-6 • “Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.” IR 8183r1: DE.CM-6	[IR_8183r1]: PR.AC-3, DE.CM-6, DE.CM-7

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest." IR 8183r1: DE.CM-7 • "Monitor for unauthorized configuration changes to the manufacturing system." IR 8183r1: DE.CM-7	
(DE.CM-06)	Fab	**Considerations:** Fab facilities rely on specialized external service (i.e., remote connectivity) providers for equipment maintenance and critical functions, which require specific monitoring approaches. **Guidance:** • "Conduct ongoing security status monitoring of external service provider activity on the manufacturing system." IR 8183r1: DE.CM-6 • "Detect defined cybersecurity events and indicators of potential cybersecurity events from external service providers." IR 8183r1: DE.CM-6 • "Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements." IR 8183r1: DE.CM-6 • Monitor privileged access that is given to external service providers and the activities performed by individuals on critical systems.	
(DE.CM-06)	Equipment and Tooling	Consideration: External providers who are involved in product development or manufacturing may have access to sensitive IP and critical systems.	
DE.CM-09 Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	Ecosystem	**Rationale:** Monitoring and integrity-checking mechanisms proactively detect configuration changes and block unsupported or unauthorized software and hardware to prevent adverse events and security breaches. The detection of artifacts related to system degradation could be useful in understanding adverse events. **Guidance:** • "Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software." IR 8183r1: DE.CM-7 • "Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest." IR 8183r1: DE.CM-7	[IR_8183r1]: DE.CM-4, DE.CM-5, DE.CM-7, PR.DS-6, PR.DS-8 [ANSI_IEC_62443_2_1]: 4.3.4.3.8 [ANSI_IEC_62443_3_3]: SR 2.4, 3.1, 3.2, 3.3, 3.4

Function – **Category** – **Subcategory**	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		• "Monitor for unauthorized configuration changes to the manufacturing system." IR 8183r1: DE.CM-7 • "Implement software, firmware, and information integrity checks to detect unauthorized changes to manufacturing system components during storage, transport, startup and when determined necessary." IR 8183r1: PR.DS-6 • "Incorporate the detection of unauthorized changes to the manufacturing system into the system's incident response capability." IR 8183r1: PR.DS-6 • "Implement hardware integrity checks to detect unauthorized tampering (e.g., tamper-evident tape or labels, computer port protection, power-on self-tests) to manufacturing system hardware determined to be critical." IR 8183r1: PR.DS-8 • Verify the integrity and authenticity of product software releases.	
DE.AE: Adverse Event Analysis Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents – **DE.AE-02** Potentially adverse events are analyzed to better understand associated activities	Ecosystem	**Rationale:** Analyzing and responding to adverse events early is vital for detecting threats before they can cause significant damage and helps prevent operational disruptions to ensure the continuity of critical processes and services. Abnormal situations should be considered when reviewing and evaluating unauthorized access events (e.g., an emergency evacuation should be differentiated from malicious, unauthorized access). **Guidance:** • "Review and analyze detected events within the manufacturing system to understand attack targets and methods." IR 8183r1: DE.AE-2 • "Implement automated mechanisms where feasible to review and analyze detected events within the manufacturing system." IR 8183r1: DE.AE-2	[IR_8183r1]: DE.AE-2 [ANSI_IEC_62443_2_1]: 4.3.4.5.6 [ANSI_IEC_62443_3_3]: SR 2.8, 2.9
(DE.AE-02)	Fab	**Considerations:** Adverse events and related activities within industrial control systems are analyzed to identify potential threats.	[SEMI_E187]: Req 11 &12

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
(DE.AE-02)	Equipment and Tooling	**Considerations:** Balancing thorough analysis with the demands of high-volume, continuous production remains a low priority, largely due to customer demand not driving this requirement. Traditionally, equipment operates openly under the assumption of an air-gapped environment, and there is minimal spare computational power, as most of the capacity is dedicated to wafer production. Diverting resources would impact operations. There is currently no established or agreed-upon protocol for such analysis. **Guidance:** • Analyze threats and design the product to protect itself from adversarial events. • "Implement automated mechanisms where feasible to review and analyze detected events within the manufacturing system." IR 8183r1: DE.AE-2	
DE.AE-03 Information is correlated from multiple sources	Ecosystem	**Rationale:** Correlating information from multiple sources helps identify hidden patterns, connections, and indicators of compromise (IOCs) involved in various stages of an attack. Effective threat communication requires IT and OT to share available information, especially geopolitical concerns that may impact threat landscapes. **Guidance:** • "Ensure that event data is compiled and correlated across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports." IR 8183r1: DE.AE-3 • "Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity." IR 8183r1: DE.AE-3	[IR 8183r1]: DE.AE-3
(DE.AE-03)	Equipment and Tooling	**Consideration:** Balancing the need for comprehensive monitoring with potential impacts on production speed and efficiency is essential. Some products rely on a single source and lack redundancy or alternative suppliers.	
DE.AE-04 The estimated impact and scope of	Ecosystem	**Rationale:** Knowing the estimated impact and scope of adverse events is crucial for developing targeted incident response plans that are proportional to the severity of the threat while minimizing operational disruptions and maintaining business continuity.	[IR 8183r1]: DE.AE-4

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
adverse events are understood		**Guidance:** • "Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes." IR 8183r1: DE.AE-4 • "Implement automated mechanisms to support impact analysis." IR 8183r1: DE.AE-4 • "Correlate detected event information and responses to achieve perspective on event impact across the organization." IR 8183r1: DE.AE-4	
(DE.AE-04)	Equipment and Tooling	**Consideration:** Assessing impacts on production equipment, quality control systems, and overall manufacturing output is essential. Critical systems such as AMHS should be considered.	
DE.AE-06 Information on adverse events is provided to authorized staff and tools	Ecosystem	**Rationale:** Provisioning information on adverse events in a timely fashion to authorized personnel is crucial for managing cybersecurity incidents. **Guidance:** • "Generate system alerts when indications of compromise or potential compromise occur." IR 8183r1: DE.CM-1 • "Communicate event detection information to defined personnel." IR 8183r1: DE.DP-4 • "Implement automated mechanisms and system generated alerts to support event detection communication." IR 8183r1: DE.DP-4	[IR 8183r1]: DE.CM-1, DE.DP-4
(DE.AE-06)	Equipment and Tooling	Consideration: Sharing information should be balanced with the need to protect sensitive details about manufacturing processes and potential vulnerabilities. Consider presenting threat intelligence in a context that is accessible and actionable for production staff without deep cybersecurity expertise.	
DE.AE-07 Cyber threat intelligence and other contextual information are integrated into the analysis	Ecosystem	**Rationale:** Incorporating contextual information and CTI helps to better understand the relevance and potential impact and to proactively identify and mitigate threats. This should be done whenever feasible. **Guidance:** • "Ensure that event data is compiled and correlated across the manufacturing system using various sources such as event reports, audit monitoring,	[IR 8183r1]: DE.AE-3

Function – Category – Subcategory	**Domain**	**Semiconductor Manufacturing Profile Rationale / Considerations / Guidance**	**Reference**
		network monitoring, physical access monitoring, and user/administrator reports." IR 8183r1: DE.AE-3 • "Integrate analysis of events where feasible with the analysis of vulnerability scanning information, performance data, manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity." IR 8183r1: DE.AE-3	
(DE.AE-07)	Fab	**Considerations:** Threat intelligence feeds are integrated into monitoring tools to provide targeted intelligence and contextual insights on emerging threats.	
(DE.AE-07)	Equipment and Tooling	Consideration: Consider presenting threat intelligence in a context that is accessible and actionable for production staff without deep cybersecurity expertise.	
DE.AE-08 Incidents are declared when adverse events meet the defined incident criteria	Ecosystem	**Rationale:** Timely incident declaration, including mandatory reporting to meet legal obligations, ensures the prompt activation of response measures, keeps all relevant internal and external stakeholders informed, and minimizes the impact of adverse events. **Guidance:** • "Define incident alert thresholds for the manufacturing system." IR 8183r1: DE.AE-5 • "Implement automated mechanisms where feasible to assist in the identification of security alert thresholds." IR 8183r1: DE.AE-5	[IR 8183r1]: DE.AE-5
(DE.AE-08)	Fab	**Considerations:** Define incident criteria that balance sensitivity to potential issues with the need to avoid unnecessary disruptions to manufacturing processes. **Guidance:** • Incident declaration criteria are clearly defined, tailored to the unique aspects of OT/ICS, and regularly tested and updated.	
(DE.AE-08)	Equipment and Tooling	**Consideration:** Integrate cybersecurity incident criteria with existing quality control and production incident processes. **Guidance:** • Thresholds should be configurable on the equipment.	

5.5. Respond

Table 12. Subcategory-level guidance for RESPOND Function

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
RESPOND – **RS.MA: Incident Management** Responses to detected cybersecurity incidents are managed – **RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared	Ecosystem	**Rationale:** Semiconductor manufacturing facilities operate within a complex ecosystem of specialized equipment, processes, and third-party relationships. Effective incident response requires careful coordination among multiple parties to maintain clean-room integrity, prevent equipment damage, and minimize production impacts. **Guidance:** • Ensure that in-house personnel or trained contractors/external resources are identified and cleared to respond. • Validate that the response team has the needed physical access to the response areas. • Ensure access to and awareness of the latest version of the incident response plan. Extend access and awareness to appropriate stakeholders. Additionally, ensure that vendors provide ample information to facilities personnel who maintain respective equipment. • "Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include for example; mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices." IR 8183r1: RS.CO-4 • Implement predetermined communication mechanisms to support stakeholder coordination. • "Execute the response plan during or after a cybersecurity event on the manufacturing system." IR 8131r1: RS.RP-1	[IR 8183r1]: RS.CO-4, RS.RP-1
(RS.MA-01)	Fab	**Considerations:** Semiconductor fab facilities require specialized response coordination due to the complex integration of OT systems, cleanroom environments, and precision manufacturing equipment. The incident response plan should include special training for each manufacturing environment to ensure that personnel have the proper training (i.e., health and safety),	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		prevent undue delays in response, and ensure that responses are inconsistent with the processes outlined in the response plan.	
(RS.MA-01)	Enterprise IT	Consideration: Enterprise IT managers should effectively orchestrate response efforts across business systems to ensure seamless integration and communication with manufacturing networks, maintain operational continuity, and secure data flows between different segments of the enterprise. The managers should also consider the global nature of many semiconductor companies and address international regulatory requirements and cross-border incident response. **Guidance:** • Plan for trusted external communications and secure remote connectivity for remote support personnel during incidents. • Test this connectivity routinely. • Implement predetermined mechanisms to support stakeholder coordination.	
(RS.MA-01)	Equipment and Tooling	Consideration: Production-related incident response requires coordination with design tool vendors, IP providers, and foundry partners while maintaining strict confidentiality and protecting intellectual property throughout the response process.	
RS.MA-02: Incident reports are triaged and validated	Ecosystem	**Rationale:** Semiconductor manufacturing incidents require specialized triage and validation procedures due to the complex interplay between manufacturing equipment, cleanroom environments, and integrated systems. Proper incident validation is critical for determining the scope of impact and preventing unnecessary production disruptions. **Guidance:** • "Investigate cybersecurity-related notifications generated from detection systems." IR 8183r1: RS.AN-1 • "Implement automated mechanisms to assist in the investigation and analysis of cybersecurity-related notifications." IR 8183r1: RS.AN-1 • "Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results." IR 8183r1: RS.AN-2	[IR 8183r1]: RS.AN-1, RS.AN-2

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• “Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.” IR 8183r1: RS.AN-2	
RS.MA-02	Fab	**Considerations:** Fab environments present unique triage challenges due to the interconnected nature of process tools, AMHS, and environmental controls. Triage processes and actions should be auditable to ensure the validity of responsive measures taken.	
RS.MA-02	Enterprise IT	**Considerations:** Enterprise IT incidents should be triaged consider potential impacts on both business systems and manufacturing operations. **Guidance:** • “Implement automated mechanisms to assist in the investigation and analysis of cybersecurity-related notifications.” IR 8183r1: RS.AN-1 • “Implement automated mechanisms to support incident impact analysis.” IR 8183r1: RS.AN-2	
RS.MA-03: Incidents are categorized and prioritized	Ecosystem	**Rationale:** Semiconductor manufacturing requires specialized incident categorization and prioritization frameworks due to the critical nature of production processes, cleanroom environments, and high-value equipment. **Guidance:** “Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results.” IR 8183r1: RS.AN-2 “Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.” IR 8183r1: RS.AN-4	[IR 8183r1]: RS.AN-2, RS.AN-4
RS.MA-03	Fab	**Considerations:** Fab environments require specific categorization schemes that account for complex manufacturing processes, equipment conditions, and cleanroom requirements.	
RS.MA-03	Enterprise IT	**Considerations:** Enterprise IT incident categorization should align with manufacturing operations while addressing traditional IT security concerns.	
RS.MA-03	Equipment and Tooling	**Considerations:** Production-related incidents require categorization that addresses design tool availability, IP protection, and product integrity. Incidents should be	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		triaged to restore normal operations while also enabling operators to conduct investigations as necessary. Production environments require a specialized categorization that considers continuous operations, automated machinery, and real-time process control.	
RS.MA-04: Incidents are escalated or elevated as needed	Ecosystem	**Rationale:** The semiconductor industry requires precise escalation procedures due to the high value of manufacturing processes, complex equipment dependencies, and the potential widespread impact of incidents. Once incidents have been discovered and investigations have commenced, responses should be prioritized accordingly to consider impact, the mission criticality of affected systems, and more. **Guidance:** • "Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results." IR 8183r1: RS.AN-2 • "Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization." IR 8183r1: RS.AN-2 • "Coordinate cybersecurity incident response actions with all relevant stakeholders." IR 8183r1: RS.CO-4	[IR 8183r1]: RS.AN-2, RS.CO-4
RS.MA-04	Fab	**Considerations:** Fab escalation procedures should account for complex tool dependencies, cleanroom integrity, and specialized expertise requirements.	
RS.MA-04	Enterprise IT	**Considerations:** Enterprise IT escalations should balance traditional IT security protocols with manufacturing system requirements.	
RS.MA-04	Equipment and Tooling	**Considerations:** Production environment escalations require careful consideration of ongoing manufacturing processes, quality control systems, and automated equipment operations. During incident response, operators should consult documentation or support teams from vendor-provided equipment and tooling.	
RS.MA-05: The criteria for initiating incident	Ecosystem	**Rationale:** Ecosystem-wide recovery initiation criteria are crucial because premature or uncoordinated recovery across the supply chain can cause additional disruptions and complications. Clear criteria ensure that all affected parties are ready to begin coordinated	[IR 8183r1]: RC.RP-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
recovery are applied		recovery efforts. The incident response plan should define decision-making authorities. GV.RR-02 includes the responsibility of defining a decision-making authority.	
RS.MA-05	Fab	**Considerations:** The sophisticated nature of fab operations requires recovery criteria that verify environmental controls, tool readiness, and process stability before resuming operations. Incident recovery efforts should be carefully balanced with the sensitive nature of ongoing operations so as not to impede mission-critical functions.	
RS.MA-05	Enterprise IT	**Considerations:** The integrated nature of enterprise systems requires recovery criteria that verify the readiness of interconnected business and manufacturing support components. Dependencies between systems affect recovery sequencing.	
RS.MA-05	Equipment and Tooling	**Considerations:** The continuous nature of semiconductor production requires recovery criteria that address process stability, material handling, and quality control readiness. A work-in-progress status significantly impacts recovery timing, decisions and operations.	
RS.AN: Incident Analysis Investigations are conducted to ensure an effective response and support forensics and recovery activities – **RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Ecosystem	**Rationale:** Incident analysis and root cause determination are critical due to the complex interactions between manufacturing systems, specialized equipment, and automated processes. Incident analysis should inform recovery processes to ensure that systems are restored to a known or otherwise safe state. This includes the validation of system backups, an assessment of how severely systems have been impacted, and a timeline of when they may be operationalized. **Considerations:** Limitations on analysis due to systems' proprietary nature may limit root cause analysis. **Guidance:** • "Conduct forensic analysis on collected cybersecurity event information to determine root cause" IR 8183r1: RS.AN-3	[IR_8183r1]: RS.AN-3

Function _ Category _ Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
RS.AN-03	Fab	**Considerations:** Fab environments present unique analysis challenges due to the interaction between process tools, automated systems, and environmental controls. Challenges include root cause analysis, the enumeration of potentially affected systems, and the triage/eradication of malicious artifacts upon discovery.	
RS.AN-03	Enterprise IT	**Considerations:** Enterprise IT incident analysis should examine both IT and OT system interactions while considering potential impacts on manufacturing operations.	
RS.AN-03	Equipment and Tooling	**Considerations:** Production environment analysis requires an examination of manufacturing process data, quality control systems, and automated equipment behaviors to determine incident impact and cause.	
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Ecosystem	**Rationale:** The proper collection and preservation of pertinent incident data and metadata are critical due to the complex nature of manufacturing systems, proprietary processes, and quality requirements. **Guidance:** • "Provide on-demand audit review, analysis, and reporting for after-the-fact investigations of cybersecurity incidents." IR 8183r1: RS.AN-3	[IR_8183r1]: RS.AN-3
RS.AN-06	Fab	**Considerations:** Fab investigations require detailed documentation of actions taken in cleanroom environments, on specialized equipment, and with sensitive processes.	
RS.AN-06	Enterprise IT	**Considerations:** Enterprise IT investigation records should maintain integrity while documenting actions across both IT and OT systems.	
RS.AN-06	Equipment and Tooling	**Considerations:** Production environment investigations require a careful documentation of actions that could affect manufacturing processes, quality control, or automated systems.	
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	Ecosystem	**Rationale:** The proper collection and preservation of incident data are critical due to the complex nature of manufacturing systems, proprietary processes, and quality requirements. **Guidance:** • Collect, preserve, and safeguard the integrity of all pertinent incident data and metadata (e.g.,	[IR_8183r1]: Not available [CRI_v2]: RS.AN-07, RS.AN-07.01 [SP_800_53r5]: AU-7,

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		equipment logs, production environment data, process parameters, data source, date/time of collection) in accordance with evidence preservation and chain-of-custody procedures that are specific to semiconductor manufacturing operations.	IR-4, IR-6
RS.AN-07	Fab	**Considerations:** Fab environments generate extensive data from multiple systems, including process tools, environmental controls, and material handling systems.	
RS.AN-07	Enterprise IT	**Considerations:** Enterprise IT data collection should capture both IT and OT system information while preserving the relationships between interconnected systems.	
RS.AN-07	Equipment and Tooling	**Considerations:** Production environment data collection requires the preservation of process control data, quality measurements, and equipment operational data while maintaining production continuity.	
RS.AN-08: An incident's magnitude is estimated and validated	Ecosystem	**Rationale:** The accurate estimation and validation of incident magnitude are crucial due to the high cost of production disruption, potential equipment damage, and quality impacts. **Guidance:** • "Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results." IR 8183r1: RS.AN-2	[IR_8183r1]: RS.AN-2 [CRI_v2]: RS.AN-08: RS.AN-08.01 [SP_800_53r5]: IR-4, IR-8, RA-3, RA-7
RS.AN-08	Fab	**Considerations:** Fab incident magnitude assessments should account for complex tool interdependencies, cleanroom impacts, and potential effects on in-process wafers.	
RS.AN-08	Enterprise IT	**Considerations:** Enterprise IT incident magnitude assessments should evaluate impacts across business and manufacturing systems and consider potential disruptions to production support systems.	
RS.AN-08	Equipment and Tooling	**Considerations:** Production environment magnitude assessments require an evaluation of impact on manufacturing processes, quality control systems, and automated equipment operation.	
RS.CO:	Ecosystem	**Rationale:** Notifications across the semiconductor ecosystem are critical because incidents can affect	[IR_8183r1]: PR.IP-9,

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
Incident Response Reporting and Communication Response activities are coordinated with internal and external stakeholders, as required by laws, regulations, or policies – **RS.CO-02:** Internal and external stakeholders are notified of incidents		multiple points in the supply chain, and a coordinated response often requires timely information sharing among interdependent partners. **Guidance:** • "Execute the response plan during or after a cybersecurity event on the manufacturing system." IR 8183r1: RS.RP-1 • "Implement prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system." IR 8183r1: RS.CO-2 • "Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan." IR 8183r1: RS.CO-2	RS.RP-1, RS.CO-1, RS.CO-2, RS.CO-3 [DFARS] [FAR]
RS.CO-02	Fab	**Considerations:** The complex nature of fab operations requires notifications to consider impacts across multiple process areas, shifts, and support teams. Cleanroom access restrictions and contamination controls can affect how notifications are delivered and acknowledged.	
RS.CO-02	Enterprise IT	**Considerations:** The interconnected nature of business and manufacturing systems requires the careful coordination of notifications across different organizational units and external service providers. Regulatory requirements and customer agreements may mandate specific notification time frames.	
RS.CO-02	Equipment and Tooling	**Considerations:** The continuous nature of semiconductor production requires notifications to consider impacts on in-process materials and downstream operations. Quality control requirements may necessitate specific notification protocols for potentially affected products. Products used for manufacturing should be monitored for weaknesses, including vulnerabilities and other bugs. If substantial weaknesses are found, communication with stakeholders may be necessary for remedial action.	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
RS.CO-03: Information is shared with designated internal and external stakeholders	Ecosystem	**Rationale:** Information sharing is essential across the semiconductor ecosystem — both internally within the organization and through voluntary information sharing through channels such as ISACs. Detailed technical and impact information should flow between fabs, suppliers, customers, senior leadership, and industry peers to effectively manage incidents that affect multiple supply chain participants. **Guidance:** • "Share cybersecurity incident information with relevant stakeholders per the response plan." IR 8183r1: RS.CO-3 • "Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness." IR 8183r1: RS.CO- 5 • "Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident." SP 800-53r5: IR-6	[IR_8183r1]: RS.CO-3, RS.CO-5 [SP_800_53r5]: IR-6
RS.CO-03	Fab	**Considerations:** The complex nature of fab operations means that incident information often contains sensitive details about proprietary processes, custom tool configurations, and yield data.	
RS.CO-03	Enterprise IT	**Considerations:** The mix of business and manufacturing systems means that incident information may contain sensitive corporate data, customer information, and production details.	
RS.CO-03	Equipment and Tooling	**Considerations:** The continuous nature of semiconductor production means that incident information often includes real-time process data, quality metrics, and product-tracking details. **Guidance:** • Product suppliers should have a communication channel so that the incident response team can understand the impact of the incident and provide a remediation plan in a timely manner.	
RS.MI: Incident Mitigation Activities are performed to	Ecosystem	**Rationale:** Containment across the semiconductor ecosystem is critical because incidents can rapidly spread through supply chain connections and shared technology infrastructure.	[IR_8183r1]: RS.MI-1

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
prevent the expansion of an event and mitigate its effects – **RS.MI-01:** Incidents are contained		**Guidance:** • "Contain cybersecurity incidents to minimize impact on the manufacturing system." IR 8183r1: RS.MI-1	
RS.MI-01	Fab	**Considerations:** The sensitive nature of semiconductor manufacturing processes means that containment actions should maintain cleanroom protocols and environmental controls. Tool configurations, process recipes, and material flows should be preserved while implementing containment measures. **Guidance:** • "Contain cybersecurity incidents to minimize impact on the manufacturing system." IR 8183r1: RS.MI-1	
RS.MI-01	Enterprise IT	**Considerations:** The integrated nature of business and manufacturing systems requires containment actions that maintain necessary connections while isolating affected components.	
RS.MI-01	Equipment and Tooling	**Considerations:** The continuous nature of semiconductor production means that containment actions should account for work in progress and maintain critical process parameters.	
RS.MI-02: Incidents are eradicated	Ecosystem	**Rationale:** Ecosystem-wide eradication is vital because remnants of incidents can resurface and spread through supply chain connections and potentially reinfect multiple industry participants. **Guidance:** • "Mitigate cybersecurity incidents occurring on the manufacturing system." IR 8183r1: RS.MI-2 • "Implement automated mechanisms to support the cybersecurity incident mitigation process." IR 8183r1: RS.MI-2	[IR 8183r1]: RS.MI-2
(RS.MI-02)	Fab	**Considerations:** The complex web of ecosystem relationships means that eradication should address shared systems, data exchanges, and common infrastructure without disrupting critical supply chain	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		operations. Cultural and regulatory differences across global partners can affect eradication procedures.	
(RS.MI-02)	Enterprise IT	**Considerations:** The sophisticated nature of fab equipment and processes requires eradication procedures that do not compromise tool calibration or process recipes.	
(RS.MI-02)	Equipment and Tooling	**Considerations:** The continuous nature of semiconductor manufacturing requires eradication procedures that account for in-process materials and maintain quality control systems. Production tool configurations and process recipes should be protected during eradication. **Guidance:** • Ensure that supply chain risks (with regard to third-party incident handlers) are identified, documented, and reported to stakeholders where necessary.	[SP_800_53r5]: IR-4, IR-7, SA-9, SR-3

5.6. Recover

Table 13. Subcategory-level guidance for RECOVER Function

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
RECOVER – **RC.RP** **Incident Recovery Plan Execution** – **RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from	Ecosystem	**Rationale:** In the semiconductor manufacturing industry, recovery after a cybersecurity incident should be approached systematically and focus on restoring critical operational capabilities to minimize downtime and production losses. The primary focus area for recovery should be getting the manufacturing systems back online, with a clear emphasis on the tools and systems directly involved in wafer processing, such as lithography, etching, and deposition equipment. The order of recovery should be prioritized based on the impact on production. **Considerations:** The prioritization of recovery based on production impact may require that tools and systems be recovered prior to the finalization of all response operations. However, it is important to consider root cause analysis and other artifacts of response operations when	[IR_8183r1]: RC.RP-1 [SP_800_53r5]: IR-8 [ANSI_IEC_62443_2_1]: 4.4.3.4

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
the incident response process		conducting recovery operations to avoid critical information being lost. **Guidance:** • All teams (i.e., stakeholders and environments) should be coordinated and respond based on the agreed-upon playbook. • When defining, practicing, and executing the recovery playbook, teams should consider the overlap with ongoing response efforts. • "Execute the recovery plan during or after a cybersecurity incident on the manufacturing system." IR 8183r1: RC.RP-1 • "Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components." IR 8183r1: RC.RP-1 • "Continue essential manufacturing functions and services with little or no loss of operational continuity and sustain continuity until full system restoration." IR 8183r1: RC.RP-1	
(RC.RP-01)	Fab	**Considerations:** In a fab environment, it is crucial to balance rapid system restoration with thorough analysis to prevent similar incidents from happening again. Environmental and safety considerations should remain top priorities during recovery to ensure that the reactivation of equipment complies with established safety protocols and that all hazardous materials are handled appropriately.	
(RC.RP-01)	Enterprise IT	**Consideration:** Recovery processes should prioritize restoring manufacturing execution systems (MES), engineering data analysis systems, and supply chain management applications while maintaining data integrity. If IT infrastructure that is outsourced to or managed by a third party is impacted by a cybersecurity event, the organization will have to consider communication and coordination with the third-party provider in their recovery planning.	
(RC.RP-01)	Equipment and Tooling	**Consideration:** Recovery procedures for processing equipment should include maintaining calibration data, preventive maintenance records, and process recipes while preserving qualified process windows. Tool recovery would benefit from coordinated collaboration between	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		equipment vendors, process engineers, and maintenance teams to restore parameters within specification.	
RC.RP-02 Recovery actions are selected, scoped, prioritized, and performed	Ecosystem	**Rationale:** Prioritizing recovery actions requires careful balancing of multiple critical factors, including equipment costs, throughput impact, and potential yield loss. The wrong sequence of recovery actions can cascade into extensive production delays, scrapped wafers, or quality excursions. When considering risk tolerance, stakeholders should consider acceptable thresholds of yield loss. Recovery actions should be consistent within the determined bounds of risk tolerance, which will vary from organization to organization.	[IR 8183r1]: RC.RP-1
RC.RP-03 The integrity of backups and other restoration assets is verified before using them for restoration	Ecosystem	**Rationale:** Verifying the integrity of backups before restoration is essential for ensuring a reliable recovery and preventing the introduction of corrupted data or errors into critical systems. Backups serve as a vital safety net, and their integrity should be prioritized to provide a stable fallback state. **Guidance:** • "Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components." IR 8183r1: RC.RP-1 • Verify restoration assets for compromise indicators, corruption, and integrity issues before use to safeguard production.	[IR 8183r1]: RC.RP-1
(RC.RP-03)	Fab	**Considerations:** Verifying the integrity of backups is critical given the unique and highly specialized nature of fab equipment, which often operates continually and with only an eight-hour maintenance window each year. Add "backup capability status" to the fab assets inventory.	
(RC.RP-03)	Enterprise IT	Consideration: Verification procedures should confirm the integrity of manufacturing execution system (MES) databases, lot-tracking data, process control parameters, and other production-critical datasets before restoration.	
(RC.RP-03)	Equipment and Tooling	Consideration: Verification procedures should verify the integrity of equipment configuration backups, calibration data, and maintenance records before restoration. Verification should include OEM-specified validation procedures for control software, firmware versions, and parameter settings to ensure proper tool operation and to	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		prevent equipment damage or process excursions during recovery.	
RC.RP-04 Critical mission functions and cybersecurity risk management are considered to establish a post-incident operational norm	Ecosystem	**Rationale:** While there may be intense pressure to restart production, establishing proper operational norms is essential to preventing recurring incidents that could cause even longer disruptions or product quality issues. Recovery operations should still be informed by critical mission functions and prioritize the recovery of critical operation capabilities to minimize downtime and production losses.	[IR 8183r1]: Not available
RC.RP-05 The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	Ecosystem	**Rationale:** Failure to verify the integrity of restored assets can expose the semiconductor ecosystem to risks (e.g., introducing malware into production environments, or compromising product quality). Risk-based prioritization that considers business, safety, security, and environmental factors should guide decision-making in the restoration process.	[IR 8183r1]: Not available
(RC.RP-05)	Fab	**Considerations:** Verifying the integrity of restored systems includes ensuring that critical machines (e.g., photolithography and etching tools) are calibrated correctly after restoration.	
(RC.RP-05)	Enterprise IT	**Considerations:** Verifying restored assets focuses on data integrity and system functionality. Critical enterprise software, including MES and ERP tools, should be thoroughly checked after restoration to ensure correct configuration and data consistency.	
(RC.RP-05)	Equipment and Tooling	**Consideration:** Verifying integrity after restoration means ensuring that all automation protocols, firmware, and software configurations are consistent with baseline settings.	
RC.RP-06 The end of incident recovery is declared based on criteria, and incident-related	Ecosystem	**Rationale:** Knowing when the recovery period has ended is crucial for defining the end of the overall response phase. However, recognizing that root cause determination is not always achievable, a structured declaration of recovery completion is essential to maintain efficiency and prevent cascading failures that could impact product quality, machine availability, or personnel safety.	[IR 8183r1]: Not available

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
documentation is completed			
(RC.RP-06)	Fab	**Considerations:** The declaration of the end of recovery ensures that all tools — including lithography, deposition, and metrology — are fully operational and synchronized.	
(RC.RP-06)	Enterprise IT	Consideration: Declaring recovery is crucial for ensuring that all IT systems (e.g., MES, ERP, and other business-critical applications) are functioning correctly without residual issues from the incident. Incident-related documentation is essential for tracking the recovery process, noting any data loss, carrying out restoration efforts, and ensuring compliance with cybersecurity policies.	
(RC.RP-06)	Equipment and Tooling	Consideration: The end of recovery declaration involves verifying that all automated processes, tooling software, and hardware are functioning as intended. Proper documentation is essential for tracking configuration changes and ensuring that any firmware or software adjustments made during recovery are recorded for future reference.	
RC.CO-03 Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Ecosystem	**Rationale:** Effective communication during recovery is crucial for ensuring alignment among stakeholders (e.g., suppliers, maintenance teams, and customers). The incident response plan should prioritize communication with stakeholders over the public and clearly define these communication duties and ownership. **Guidance:** • "Communicate recovery activities to all relevant stakeholders, and executive and management teams." IR 8183r1: RC.CO-3	[IR_8183r1]: RC.CO-3 [COBIT5] EDM03.02
(RC.CO-03)	Fab	**Considerations:** Communication about recovery progress is essential for coordinating across different sections (e.g., etching, deposition, and photolithography) and effectively synchronizing their activities. Providing updates on recovery status to fab operators helps them adjust operational plans and minimize the risk of rework due to system instabilities.	
(RC.CO-03)	Enterprise IT	**Consideration:** Recovery communications should focus on informing management and operational teams about the status of critical IT systems (e.g., MES, ERP, and production scheduling software). Keeping internal teams updated about the availability of these systems helps them adjust	

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		workflows, mitigate disruptions, and maintain a balance in production scheduling. External stakeholders (e.g., suppliers and logistics partners) may also need to be informed to adjust their delivery schedules based on any production delays.	
(RC.CO-03)	Equipment and Tooling	**Consideration:** Progress in restoring operational capabilities should be communicated to the engineering and maintenance teams that are responsible for tool uptime. Many tools in a semiconductor fab are interdependent, so informing technicians about recovery stages helps efficiently coordinate the recalibration and testing of machines. Additionally, equipment suppliers may need updates on the status of tools that they support to expedite replacement parts, provide technical assistance, or prepare for any future maintenance needs. Organizations should consider existing contracts with suppliers and determine information-sharing responsibilities.	
RC.CO-04 Public updates on incident recovery are shared using approved methods and messaging	Ecosystem	**Rationale:** Sharing public updates about incident recovery is crucial for maintaining transparency with customers, suppliers, investors, and regulatory bodies. Failure to communicate effectively could lead to mistrust, reputational damage, and even disruptions in contractual obligations. **Guidance:** • "Centralize and coordinate information distribution and manage the public facing representation of the organization. Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies." IR 8183r1: RC.CO-1 • "Assign a Public Relations Officer." IR 8183r1: RC.CO-1 • "Pre-define media contacts." IR 8183r1: RC.CO-1 • "Implement external assets to manage public relations." IR 8183r1: RC.CO-1	[IR 8183r1]: RC.CO-1, RS.CO-2

Function – Category – Subcategory	Domain	Semiconductor Manufacturing Profile Rationale / Considerations / Guidance	Reference
		• "Implement prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system." IR 8183r1: RS.CO-2	
(RC.CO-04)	Fab	**Considerations:** Public updates may involve notifying clients (e.g., fabless semiconductor companies) about the current status of manufacturing capabilities and expected production timelines. Approved communication methods (e.g., official press releases) can help alleviate concerns related to production delays, yield impact, or order fulfillment.	
(RC.CO-04)	Enterprise IT	Consideration: Updates on incident recovery may need to be shared with a broader audience. Using approved channels (e.g., an official statement) ensures consistency in messaging and prevents misinformation.	

References

[ANSI_IEC_62443_2_1] The International Society of Automation (2009) Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. Available at https://webstore.ansi.org/standards/isa/ansiisa624439902012009

[ANSI_IEC_62443_3_3] American National Standards Institute (ANSI) / International Electrotechnical Commission (IEC) (2013). Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Available at https://webstore.ansi.org/standards/iec/iec62443ed2013

[CIS_v8] Center for Internet Security (2021) CIS Critical Security Controls Version 8. Available at https://www.cisecurity.org/controls/v8

[CISA_SBD] Cybersecurity & Infrastructure Security Agency (CISA) (2024) Secure by Design. Available at https://www.cisa.gov/securebydesign

[COBIT5] ISACA (2012) COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Available at https://www.isaca.org/resources/cobit/cobit-5

[CRI_v2] Cyber Risk Institute (2024) CRI Profile v2.0. Available at https://cyberriskinstitute.org/the-profile/

[CSF_1to2] National Institute of Standards and Technology (2024) CSF 1.1 to 2.0 Core Transition Changes Overview. Available at https://www.nist.gov/document/csf-11-csf-20-core-transition-changes

[CSF_2to1] National Institute of Standards and Technology (2024) Cybersecurity Framework v1.1 to Cybersecurity Framework v2.0. Available at https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=119#/

[CSF_v2] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (Department of Commerce, Washington, D.C.), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[CSWP_32_ipd] Pascoe C, Snyder JN, Scarfone KA (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSW) NIST CSWP 32 ipd. https://doi.org/10.6028/NIST.CSWP.32.ipd

[DFARS] Defense Federal Acquisition Regulation Supplement, 48 CFR 252.204-7012, 7020 (2024). Available at https://www.ecfr.gov/current/title-48/section-252.204-7012 and https://www.ecfr.gov/current/title-48/section-252.204-7020

[EU_CRA] European Commission (2024) Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products With Digital Elements and Amending Regulation (EU) 2019/1020 / Cyber Resilience Act (CRA). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

[FAR] Basic Safeguarding of Covered Contractor Information Systems, 48 CFR 52.204-21 (2021). Available at https://www.ecfr.gov/current/title-48/section-52.204-21

[IEEE_2700] IEEE Standards Association (2014). IEEE Standard for Sensor Performance Parameter Definitions. Available at https://standards.ieee.org/ieee/2700/5821/

[IETF_JWT] Internet Engineering Task Force (IETF) (2015) JSON Web Token (JWT). Available at https://datatracker.ietf.org/doc/html/rfc7519

[IR_8183r1] Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, Pease M, McCarthy J (2020) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8183r1. https://doi.org/10.6028/NIST.IR.8183r1

[IR_8477] Scarfone K, Souppaya M, Fagan M (2024) Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings. https://doi.org/10.6028/NIST.IR.8477

[ISA_IEC_62443_2_3] International Society of Automation (ISA) / International Electrotechnical Commission (IEC) (2015) Security for industrial automation and control systems – Part 2-3: Patch management in the IACS Environment. Available at https://www.isa.org/products/isa-tr62443-2-3-2015-security-for-industrial

[ISA_IEC_62443_4_1] International Society of Automation (ISA) / International Electrotechnical Commission (IEC) (2018) Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. Available at https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au

[ISA_IEC_62443_4_2] International Society of Automation (ISA) / International Electrotechnical Commission (IEC) (2018) Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, 2nd Printing. Available at https://www.isa.org/products/ansi-isa-62443-4-2-2018-security-for-industrial-au

[ISO_IEC_22301] International Standards Organization (ISO) (2019) ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Available at https://www.iso.org/standard/75106.html

[ISO_IEC_27001] International Standards Organization (ISO) (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Available at https://www.iso.org/standard/27001

[ISO_IEC_27002_2013] International Standards Organization (ISO) (2013) ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. Available at https://www.iso.org/standard/54533.html

[ISO_IEC_27002_2022] International Standards Organization (ISO) (2022) ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Available at https://www.iso.org/standard/75652.html

[NCSIP] Executive Office of the President (2024) National Cybersecurity Implementation Plan Version 2. Available at https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf

[OpenID_CC1] OpenID Foundation (OIDF) (2023) OpenID Connect Core 1.0 incorporating errata set 2. Available at https://openid.net/specs/openid-connect-core-1_0.html

[OWASP] Open Worldwide Application Security Project (OWASP) (2023) OWASP Data Security Top 10. Available at https://owasp.org/www-project-data-security-top-10/

[SAML_v2] OASIS Open (2005) Security Assertion Markup Language (SAML) v2.0. Available at https://www.oasis-open.org/standard/saml/

[SANS_SIP] SANS (2022) Software Installation Policy. Available at https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltde86aaea6bdfc430/636f12e0b03dfe44a65395ab/Software_Installation_Policy.pdf

[SEMI_E169] SEMI (2023) SEMI E169 - Guide for Equipment Information System Security. Available at https://store-us.semi.org/products/e16900-semi-e169-guide-for-equipment-information-system-security

[SEMI_E187] SEMI (2022) SEMI E187 - Specification for Cybersecurity of Fab Equipment. Available at https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment

[SEMI_E188] SEMI (2022) SEMI E188 - Specification for Malware Free Equipment Integration. Available at https://store-us.semi.org/products/e18800-semi-e188-specification-for-malware-free-equipment-integration

[SEMI_Terms] SEMI (2024) SEMI International Standards Compilation of Terms. Available at https://www.semi.org/sites/semi.org/files/2024-07/CompilationTerms0624.pdf

[SP_1800_12] Newhouse N, Bartock M, Cichonski J, Ferraiolo H, Souppaya M, Brown C, Dog S E, Prince S, Sexton J (2019) Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 1800-12. https://doi.org/10.6028/NIST.SP.1800-12

[SP_800_150] Johnson C, Badger M, Waltermire D, Snyder J, Skorupka C (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-150. http://dx.doi.org/10.6028/NIST.SP.800-150

[SP_800_160v1r1] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems, NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[SP_800_167] Sedgewick A, Souppaya M, Scarfone K (2015). Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-167. http://dx.doi.org/10.6028/NIST.SP.800-167

[SP_800_207] Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-207. https://doi.org/10.6028/NIST.SP.800-207

[SP_800_218] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-218. https://doi.org/10.6028/NIST.SP.800-218

[SP_800_30r1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-30r1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP_800_39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP_800_41r1] Scarfone K, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-41r1. https://doi.org/10.6028/NIST.SP.800-41r1

[SP_800_53r4] Joint Task Force Transformation Initiative (2015) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-53r4. https://doi.org/10.6028/NIST.SP.800-53r4

[SP_800_53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-53r5, includes updates as of 12-19-2023. https://doi.org/10.6028/NIST.SP.800-53r5

[SP_800_63C] Grassi P, Richer J, Squire S, Fenton J, Nadeau E, Lefkovitz N, Danker J, Choong YY, Greene K, Theofanos M (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-63C, Includes updates as of 03-02-2020. https://doi.org/10.6028/NIST.SP.800-63c

[SP_800_82r3] Stouffer K, Pease M, Tang CY, Zimmerman T, Pillitteri V, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) Guide to Operational Technology (OT) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-82r3. https://doi.org/10.6028/NIST.SP.800-82r3

[SS] National Institute of Standards and Technology (2024) Supplier Scouting. Available at https://www.nist.gov/mep/supply-chain/supplier-scouting

Appendix A. Selected Bibliography

- Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-161r1-upd1. https://doi.org/10.6028/NIST.SP.800-161r1-upd1
- Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. Available at https://www.govinfo.gov/app/details/DCPD-201300091
- International Society of Automation (ISA) / International Electrotechnical Commission (IEC) (2020). ISA/IEC 62443 Series of Standards. Available at https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- Kissel R, Stine K, Scholl M, Rossman H, Fahlsing J, Gulick J (2008) Security Considerations in the System Development Life Cycle. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-64r2. https://doi.org/10.6028/NIST.SP.800-64r2
- National Institute of Standards and Technology (2018) Cybersecurity Framework 1.1. (Department of Commerce, Washington, D.C.), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Institute of Standards and Technology (2022) Cyber and Network Security. Available at https://www.nist.gov/itl/cyber-and-network-security
- Quinn S, Ivy N, Chua J, Scarfone K, Barrett M, Feldman L, Topper D, Witte G, Gardner R K (2023) Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-221A. https://doi.org/10.6028/NIST.SP.800-221A

Appendix B. List of Symbols, Abbreviations, and Acronyms

AAA
Authentication, authorization, and accounting

AI
Artificial intelligence

ANSI
American National Standards Institute

CAIQ
Consensus Assessments Initiative Questionnaire

CCM
Cloud Controls Matrix

CFR
Code of Federal Regulations

CIS
Center for Internet Security

CISA
Cybersecurity & Infrastructure Security Agency

CISO
Chief information security officer

CRA
Cyber Resiliency Act

CRI
Cyber Risk Institute

CSA
Cloud Security Alliance

CSF
Cybersecurity Framework

CSWP
Cybersecurity white paper

CTI
Cyber threat intelligence

DFARS
Defense Federal Acquisition Regulation Supplement

EO
Executive Order

EOS
End of service

ERM
Enterprise risk management

ERP
Enterprise resource planning

EU
European Union

fab
Factory ecosystem or semiconductor fabrication plant

FAR
Federal Acquisition Regulation

GDPR
General Data Protection Regulation

HR
Human resources

IACS
Industrial automation and control system

IAM
Identity and access management

ICS
Industrial control system

ICT
Information and Communications Technology

IEC
International Electrotechnical Commission

IEEE
The Institute of Electrical and Electronics Engineers

IETF
Internet Engineering Task Force

IOC
Indicator of compromise

IP
Intellectual property

IR
(NIST) Interagency Report or Internal Report

ISA
International Society of Automation

ISAC
Information sharing and analysis center

ISO
International Organization for Standardization

IT
Information technology

ITL
Information technology laboratory

JSON
JavaScript Object Notation

JWT
JSON Web Token

KPI
Key performance indicator

KRI
Key risk indicator

LLC
Limited liability company

M2M
Machine-to-machine

masks
Photomasks

MCS
Material control system

MES
Manufacturing execution system

NCSIP
National Cybersecurity Implementation Plan

NIST
National Institute of Standards and Technology

OEM
Original equipment manufacturer

OIDF
OpenID Foundation

OWASP
Open Worldwide Application Security Project

PIV
Personal Identity Verification

R&D
Research and development

ROI
Return on investment

SAML
Security Assertion Markup Language

SBOM
Software bill of material

SCRM
Supply chain risk management

SLA
Service-level agreement

SMCC
Semiconductor Manufacturing Cybersecurity Consortium

SP
(NIST) Special Publication

SSDF
Secure Software Development Framework

TLS
Transport Layer Security

WG4
Working-group 4, a group within SMCC

WLA
Wafer-level assembly

Appendix C. Glossary

Automated material handling system

An automated system to store and transport materials within the factory. [SEMI_Terms]

fab

In semiconductor manufacturing, “Fab” is short for “Fabrication facility” or “Foundry.” It is a highly specialized and controlled environment where semiconductor devices, such as integrated circuits (ICs), are manufactured.

legacy system

An outdated or older system that is no longer actively supported, maintained, or updated by its developer.

multifactor authentication

Authentication using two or more factors to achieve authentication. Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric). [SP_1800_12, Volume B, Appendix B]

operational technology

A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. [SP_800_82r3, Appendix B]

Note: OT is a known environmental term used for industrial control systems and manufacturing systems where the technology or technical systems are used outside normal IT environments.

role-based access control

Access control based on user roles (i.e., a collection of access authorizations that a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. [SP_800_53r5, Appendix A]

software development life cycle (SDLC)

A formal or informal methodology for designing, creating, and maintaining software (including code built into hardware). [SP_800_218, Introduction]

Appendix D. Figure Descriptions

The following sections contain detailed textual descriptions of figures appearing in this document.

D.1. Description of Fig. 1

Figure 1 denotes spaces within a semiconductor fabrication facility using illustrative blocks. Spaces are meant to be physical and/or logical. For example, the Factory and Warehouse are physically bounded spaces, and the Vendor/Supplier Room is also a physically bounded space. Some blocks are labeled as being managed in cooperation with vendor or supplier organizations, such as the Vendor/Supplier Room.

Arrows represent the many ways process, data flows, and material flows between parts of the facility. The arrows only cover a few example flows, like raw materials flowing from the warehouse to the factory, and metrology data flowing from the factory to a vendor room and vendor equipment so optimization parameters can flow back to the factory. The raw example material flow is an example of a manufacturer-owned flow, while the example metrology flow is an example of a vendor-managed flow.

D.2. Description of Fig. 2.

Figure 2 illustrates the functional domains of Enterprise IT, Fab, and Equipment & Tooling, represented as concentric ovals. The ovals nest within one another to suggest containment, with Enterprise IT the outermost, and Equipment & Tooling the innermost. Vendors also have a set of concentric ovals, representing vendors for each of the functional domains. The vendors' ovals overlap at each functional domain layer, illustrating their own involvement with each of the functional domains. The vendors' ovals also expand outside of the functional domains to show vendors' domains necessarily including functional spaces outside of the manufacturer's functional domains.

D.3. Description of Fig. 3.

Figure 3 illustrates the semiconductor manufacturing lifecycle and, separately, a hierarchy of security topics. A highlighting overlay denotes the areas of focus for the current document and purposefully does not include some topics and lifecycle phases.

The lifecycle phases are arranged in a sequence:

- Design
- Development
- Manufacturing
- Packaging
- Integration

- Provisioning
- Maintenance
- End of Life

The highlighted phases include “Manufacturing” and “Packaging,” with some overlap backwards to the end of “Development,” and forwards to the beginning of “Integration,” indicating that some of the topical coverage within this document includes interfacing with the transitions from and to those lifecycle phases.

The hierarchy of hardware security topics houses:

- Hardware Security
    - Security OF Semiconductors
        - These topics are grouped under the umbrella of "Design & Development", and work towards the goal of "Security Closure Power/Area/Timing"
        - Vulnerabilities
        - Secure Communication
        - Authentication
        - Secure firmware
        - Lifecycle management
    - Security OF and FOR Semiconductors
        - These topics are grouped under the umbrella of "Supply Chain", and work towards the goal of "Establish Trust & Provenance"
        - Counterfeiting
        - IP Protection
        - Malware
        - Trojans
        - Supply Vulnerabilities
        - Material Supply
        - Device, Firmware alteration
        - Re-mark
    - Security FOR Semiconductors
        - These topics are grouped under the umbrella of "Manufacturing", and work towards the goal of "Industrial Security"
        - IT Security Risks
        - Weak Security Controls

    - IT Network Attacks
    - Data Security

The highlighted topics include all of the topics under the Manufacturing umbrella; include all of the topics at and after "Supply Vulnerabilities" under the "Supply Chain" umbrella; and partially include all of the topics between Counterfeiting and Trojans, inclusive, under the "Supply Chain" umbrella. The highlight leaves uncovered space under the "Supply Chain" and "Manufacturing" umbrellas because of topics that are pertinent to those higher-order groupings but still outside the scope of this document.

D.4. Description of Fig. 4.

Figure 4 is a picture of how some CSF 1.1 subcategories map to other subcategories. Subcategories are represented with oval-shaped nodes, each labeled with the subcategory short identifier. Nodes are arranged in two rows, the top row representing CSF 1.1 subcategories, the bottom row representing CSF 2.0 subcategories. The nodes are also grouped into three clusters, with two nodes on the left, six nodes in the middle, and four nodes on the right. Arrows either point from some nodes in the top row to some nodes in the bottom row, or from some nodes in the bottom row to some rows in the top row. Each arrow pointing represents Subcategory-level mappings [IR 8477], as recorded by the CSF 1.1 to 2.0 [CSF 1to2] and CSF 2.0 to 1.1 [CSF 2to1] mapping resources. The Subcategories in this figure have no further mappings within those mapping resources.

Figure 4 has three clusters, arranged left-to-right:

- The left cluster of two nodes is labeled "1-to-1 mapping," and has CSF 1.1 DE.AE-2 linking to CSF 2.0's DE.AE-02, and vice-versa.
- The middle cluster of six nodes is labeled "1-to-2 mappings." The left three nodes of the middle cluster link CSF 2.0 GV.OC-01 to CSF 1.1's ID.BE-3 and ID.BE-2. The right three nodes of the middle cluster link CSF 1.1's DE.AE-3 to CSF 2.0's DE.AE-03 and DE.AE-07.
- The right cluster of four nodes is labeled "Asymmetric mapping." The CSF 1.1 row of the right cluster has ID.AM-3 and DE.AE-1. The CSF 2.0 row of the right cluster has ID.AM-07 and ID.AM-03. CSF 1.1's ID.AM-3 links to CSF 2.0's ID.AM-07 and ID.AM-03. CSF 2.0's ID.AM-03 links to CSF 1.1's ID.AM-3 and DE.AE-1. The shape of the cluster shows two unidirectional links and one bi-directional link.