

Concept of IPC-1792

Various modern security standards and regulations focus on business continuity, which requires advance preparation to minimize impact and ensure early recovery. IPC-1792, Standard for the Management and Mitigation of Cybersecurity Incidents in the Manufacturing Industry Supply Chain is another modern security standard that focuses on business continuity that also requires advance preparation to minimize impact and ensure early recovery.

The first step in preparation is usually an assessment, which is a comprehensive categorization of critical resources from a business continuity perspective by level of impact, and the design of a compartmentalized plan.

The subsequent process and evidence to be submitted will vary for each country, industry, regulation, and standard. Based on the clarified critical resources and compartmentalized plan, you will proceed to address the requirements of the country, industry, regulation, and standard.

Starting with a back-to-basics assessment ensures efficiency. Efforts done only for compliance often result in wasted work.

IPC-1792 is a purpose-built industry standard focused on business continuity. A back-to-basics assessment will also support compliance with other regulations and standards.

Purpose of IPC-1792

IPC-1792 is a standard for a Trusted Validated Secure Supply Chain.

Customers who pay for and demand visible security value have a significant responsibility to society. For example, this includes companies that develop life-saving medical equipment, equipment that supports the operation of infrastructure that sustains lifelines, and equipment related to defense have a significant responsibility to society.

These customers require the shortest possible recovery time to minimize operational impact in the event of a cybersecurity incident. For this reason, these customers require their suppliers to not only provide protective measures, but also a guarantee of detection within a specified time frame.

IPC-1792 is a standard for a trusted, validated and secure supply chain to meet these requirements.

It does this by setting achievable and quantifiable requirements for:

- Fast notification to customers regarding cybersecurity incidents that affect them along the supply chain, even when unknown attacks have occurred.
- Establishing a framework to quickly detect and notify critical players in the supply chain (and eventually all players) of an attack, even if the attack is of unknown origin.

IPC-1792 Relevance to Other Cybersecurity Standards

IPC-1792 is an industry standard for the electronics manufacturing industry was developed to complement existing standards for cybersecurity. Therefore, there is no conflict with other comprehensively defined standards, and measures taken in response to IPC-1792 will not impede compliance with global standards and regulations.

For instance, while ISO 27000 and NIST SP 800 are comprehensive cybersecurity standards, IPC-1792 is narrower in scope and purpose as follows.

- Particular focused on minimizing social impacts
- Limited to immediate supply chain impact notification
- Defines the minimum requirements for preparation and administrative implementation for immediate notification in advance

IPC-1792 for Web – Overview, Stakeholders and Business Risk Assessment

The European Cyber Resilience Act, which imposes reporting obligations within a certain time frame, is also recognized as a similar regulation. We will continue to investigate this matter, but at this time, there are no conflicts, and measures to comply with IPC-1792 will not prevent compliance with European regulations.

The table below provides a helpful comparison between ISO 27000, NIST SP 800 and IPC-1792.

	ISO 27000	NIST SP 800	IPC-1792
Objective	Comprehensive (subdivided)	Comprehensive (subdivided)	Particularly focused on minimizing Business impacts.
	General security requirements	Diverse in requirements, technology, architecture, etc.	Limited to supply chain impact immediate notification mechanism
	Starting in 2001 (intrusion assumption is optional at this time)	Starting around 2014 (in addition to defense, assumes intrusion and minimizes attack impact)	Starting in 2023 Assuming intrusion and minimizing attack impact
What It Establishes	A system for setting and enforcing organizational rules (management system)	Various mechanisms, rules, architectures, etc.	Defines the minimum requirements for preparation and administrative implementation for immediate notification in advance
Certification System	ISMS Conformity Assessment System	SP800-171 has SPRS for self-declarations (DoD CMMC is under development for defense industries)	Self-assessment
Standardization Organization Standing	International standards among nations	U.S. National Standard	Global industry standards for electronics manufacturing
	Match the level of each country and create a scale	Advance the standard of products and services offered in the U.S.	Customer value realization
	Define "level" as a universal "measure" of the world	Providing various technical information such as requirements and architecture to the world through the supply chain	Part of an ecosystem of IPC standards to establish trusted, validate, secure supply chain standards, supported by education, certification and validation

Stakeholders

Using IPC-1792, supply chain stakeholders work together to communicate information to ensure product authenticity or to notify the supply chain of a cybersecurity incident. The following are explanations of these stakeholders according to IPC-1792.

Supply Chain Entity is any factory involved in the supply chain that produces certified products using certified materials and is an entity subject to IPC-1792 certification. It has the necessary systems to meet the necessary security requirements and to undertake the operation of IPC-1792.

Cybersecurity Diploma Manager is an organization that issues a Diploma to a supply chain entity. To issue a Diploma to a supply chain entity, the Cyber Security Diploma Manager accepts issuance requests and manages issued Diplomas (new registrations, renewals, and expirations).

Certificate Authority is an organization that uses a public key infrastructure (PKI) mechanism to manage the digital diploma issued by a cybersecurity diploma manager to authenticated supply chain entities. An audit conducted by the cybersecurity diploma manager also results in the revocation of the digital diploma.

Cybersecurity Auditor audits whether a supply chain entity meets the security requirements set forth in IPC-1792 and is eligible to be granted the Cyber Security Diploma.

Customer is the organization (company) that uses the final certification product.

Because there are no operational entities such as the Cybersecurity Diploma Manager, Certificate Authority or Cybersecurity Auditor, to implement this standard, each Supply Chain Entity will tentatively declare that it meets the security requirements and allow a mechanism to communicate and operate Digital Certificates without Digital Diploma.

Information exchanged between stakeholders

The elements exchanged by stakeholders in the operation of IPC-1792 include the following:

A **Diploma**, which are credentials that certify that the supply chain entity is eligible to issue a **Digital Certificate**.

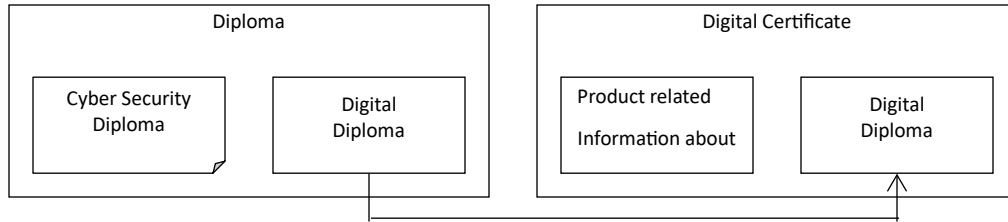
Conditions for issuance include meeting the applicable requirements specified in IPC-1792 and having a mechanism to transmit information to other supply chain entities. The conditions also include certifying that the public key information has been duly registered with a certificate authority.

A **Cyber Security Diploma**, which certifies that the supply chain entity meets the applicable requirements set forth in IPC-1792 and has a mechanism for transmitting information to other supply chain entities. The Cyber Security Diploma is managed by the Cyber Security Diploma Manager and evaluated by the Cyber Security Auditor.

A **Digital Diploma**, which is a certificate of a public key provided by a supply chain entity to ensure the legitimacy of the source of the product. Third-party certification of certificates based on requests from other supply chain entities are done by a certificate authority working with a cybersecurity diploma manager.

A **Digital Certificate**, which is a secure digital record identified by a unique identity that contains information about a certified product or material. It contains information about the product and a **Digital Diploma** to **prove** the factory (supply chain entity) of the product.

IPC-1792 for Web – Overview, Stakeholders and Business Risk Assessment



The following is an example of how these stakeholders work together in an IPC-1792 supply chain.

First, the supply chain entity (factory) that wants to be certified requests the cybersecurity diploma manager to join the supply chain (issue a diploma).

This is where the process begins.

Upon receiving the request, a cybersecurity diploma manager will check the validity of the request.

This will include an audit of the stakeholder to IPC-1792 to ensure the stakeholder implements security measures in accordance with the security requirements of the IPC-1792 and has an information transmission mechanism in accordance with IPC-1792. This audit should be predicated by a stakeholder self-assessment.

If auditor deems the stakeholder participation in the supply chain to be appropriate, a cybersecurity diploma manager will issue a Cyber Security Diploma to the stakeholder.

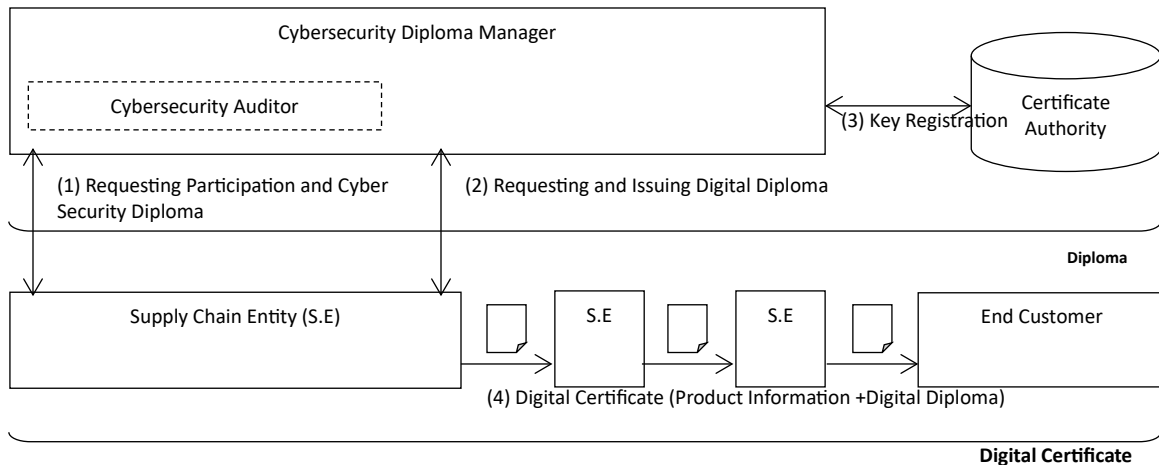
The stakeholder will then request the cybersecurity diploma manager to issue a Digital Diploma that will be attached to the stakeholder product's Digital Certificate.

The public key certification scheme uses the Public Key Infrastructure (PKI) scheme commonly used on the Internet. Therefore, when a stakeholder requests a Digital Diploma, that organization will need to generate its own “private” and “public” key pair and apply for the Digital Diploma with the “public” key. The cybersecurity diploma manager will register the “public” key with a certificate authority and provide the issued Digital Diploma to the supply chain entity.

After obtaining the Cyber Security Diploma and Digital Diploma, the stakeholder attaches the Digital Certificate to each certified product each time it is shipped. The Digital Certificate consists of the authorization issued by the Diploma Manager along with key product information, such as lot number and shipping date.

This verifies the authenticity and compliance of the product.

The diagram below provides a visual of this process.



Business Risk Assessment

IPC-1792 recommends that, when an event occurs that is suspected to be a cyber security incident, the criteria for determining the event as an incident be prepared in advance. Based on these criteria, a decision can be made regarding whether or not to transmit the incident to the supply chain.

It is difficult to uniquely define these criteria because it depends on the characteristics of the products and materials produced by the stakeholder. IPC-1792 recommends a business risk assessment to set these criteria.

Pre-assessment of Business Risks

Aligned with customer requirements and the IPC Product Classification (Class 1, 2, or 3), a business risk assessment helps determine the appropriate level of response to a cybersecurity incident. The required response level depends on the degree of risk that customers and suppliers are willing to accept for the intended use of the material or final product.

Risk assessments may vary by industry, region, product characteristics and key materials. These assessments are often expressed in a risk assessment matrix, as illustrated in the table below.

A variety of methodologies can be applied, such as Failure Mode and Effects Analysis (FMEA), depending on the standards in force within a given industry. As a specific example, the severity–probability mapping table from MIL-STD-882E: Standard Practice for System Safety can be used. Preparing such a matrix provides an effective preliminary assessment of business risk.

The stakeholder should conduct this risk analysis in normal times and document the risk analysis tailored to the relevant business.

Table: MIL-STD-882E Risk Assessment Matrix

Severity Probability	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High (Urgent)	High (Urgent)	Serious (Rapid)	Medium (No)
Probable (B)	High (Urgent)	High (Urgent)	Serious (Rapid)	Medium
Occasional (C)	High (Urgent)	Serious (Rapid)	Medium (No)	Low (No)
Remote (D)	Serious (Rapid)	Medium (No)	Medium (No)	Low (No)
Improbable (E)	Medium (No)	Medium (No)	Medium (No)	Low (No)
Eliminated (F)	Eliminated (No)	Eliminated (No)	Eliminated (No)	Eliminated (No)

Exploration of influence segmentation

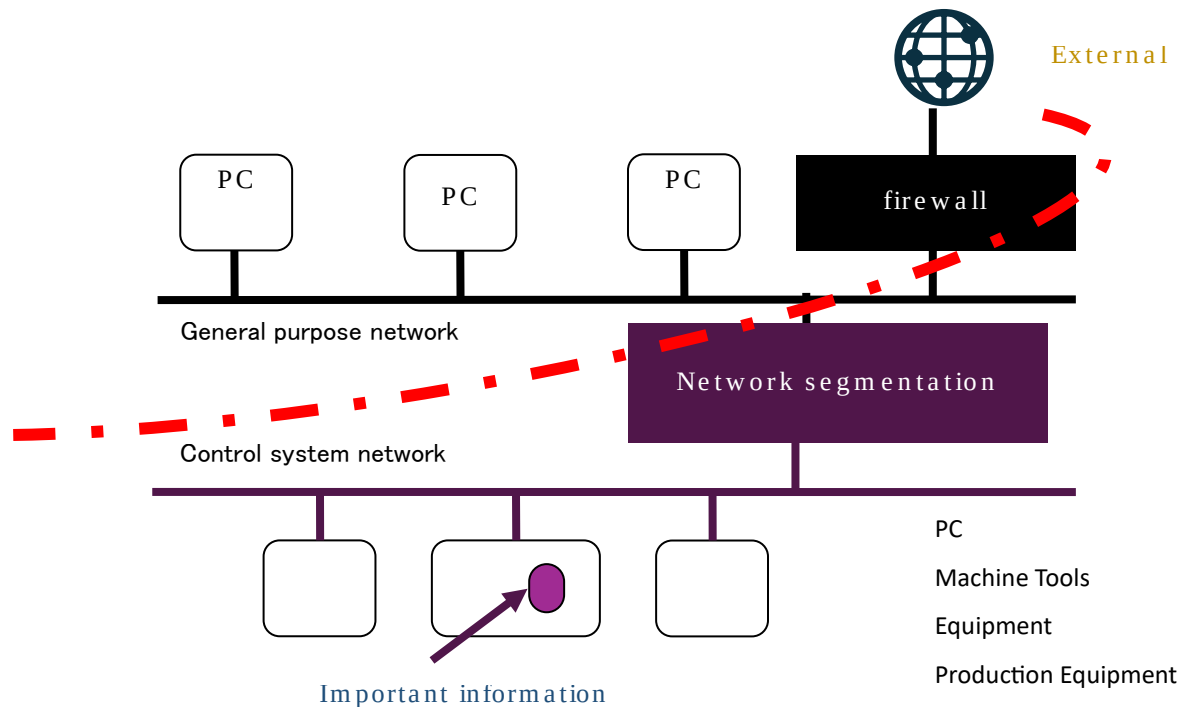
In addition, "network segmentation" improves the accuracy of the risk assessment matrix and further contributes to risk reduction.

Segmentation is generally important for early identification of the impacted area of a cybersecurity attack. Factory network segmentation can help reduce the time to analyze an incident. Segments should be defined according to product and business characteristics, and risk in each production environment should be properly assessed to ensure appropriate risk management.

IPC-1792 for Web – Overview, Stakeholders and Business Risk Assessment

The following are key considerations for an efficient segmentation implementation:

- Create a list of units affected by the incident for each segmented network
- Establish an incident response flow for each network to serve as an early communication tool



It is recommended that the stakeholder perform this risk analysis in normal times through the above devices and other means and document the risk analysis tailored to the business.