Charter of Trust

Common risk-based approach for the Digital Supply Chain

1 Summary

On February 16, 2018 at the Munich security conference, the cornerstone for the Charter of Trust was laid to make the digital world more secure.

A continuously growing group of global companies have signed off on this cybersecurity initiative and endorsed its 10 fundamental principles to foster three important objectives:

- To **protect the data** of individuals and companies
- To **prevent damage** to people, companies and infrastructures and
- To **create a reliable foundation** on which confidence in a networked, digital world can take root and grow

The second of these 10 principles includes the responsibility for companies to expand such objectives throughout their digital supply chain, stating:

> **Responsibility throughout the digital supply chain**
>
> Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as
>
> - **Identity and access management**: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
> - **Encryption**: Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.
> - **Continuous protection**: Companies must offer updates, upgrades, and patches throughout a reasonable life cycle for their products, systems, and services via a secure update mechanism.

Based on this statement, the CoT members developed a common risk-based approach aligned with international norms to help improve cybersecurity and provide visibility through the supply chain. Three elements form this risk-based approach:

- **Baseline requirements**
  are common for all digital suppliers and define the fundamentals that a supplier must address in order to ensure the cybersecurity foundations for their product/service
- **Supplier criticality**
  Digital suppliers have different criticalities depending on risk factors, which are also dependent on the context viewed by the purchaser
- **Verification**
  Verification to the baseline requirements is dependent on the criticality of the supplier

The purpose of this document is to describe such a risk-based approach and its impact on the digital supply chain with a focus on the various stakeholders throughout the digital supply chain.

2 Common risk-based approach

2.1 Baseline requirements

Seventeen (17) baseline requirements have been developed to which relevant suppliers within the digital supply chain should adhere.

Individual members may have additional specific requirements for particular suppliers that supplement these baseline requirements.

The baseline requirements are organized into eight categories covering people, process, and technology:

- Data Protection
- Security Policies
- Incident Response
- Site Security
- Access, Intervention, Transfer and Separation
- Integrity and Availability
- Support
- Training

These baseline requirements form the fundamental cybersecurity base for the supply chain. They have been developed from best practices and are in alignment with a number of international frameworks, standards, and guidelines (e.g. ISO 27001 & 20243, IEC 62443, NIST CSF, METI CPSF, etc.).

Category	Baseline Cybersecurity Supply Chain Requirements
Data Protection	– Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data – Data shall be protected from unauthorized access throughout the data life cycle – The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	– Security policies consistent with industry best practices such as ISO27001, ISO20243, SOC2, IEC62443 shall be in effect (including access control, security education, employment verification, encryption, network isolation/segmentation, operational security, physical security, vendor management) – Guidelines on secure configuration, operation and usage of products or services shall be available to customers – Policies and procedures shall be implemented so as not to consent to include back doors, malware and malicious code in products and services
Incident Response	– For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	– Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer and Separation	– Encryption and key management mechanisms shall be available, when appropriate, to protect data – Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	– Regular security scanning, testing and remediation of products, services and underlying infrastructure shall be performed – Asset management, vulnerability management and change management policies shall be implemented that are capable of mitigating risks to service environments – Business continuity and disaster-recovery procedures shall be in place and shall incorporate security during disruption, where applicable – A process shall be in place to ensure that products and services are authentic and identifiable
Support	– The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made available – Based on risk and during the time frame of support, processes shall be in place for 1. Contacting Support 2. Security Advisories 3. Vulnerability Management 4. Cybersecurity-related Patch Delivery and Support
Training	– A minimum level of security education and training for employees shall be regularly deployed (e.g. through training, certifications, awareness)

2.2 Method to define supplier criticality

The criticality of a Digital Supplier will vary depending on specific context. Therefore, criticality level should be assigned to suppliers based on a simple and robust method.

Typically, the criticality level will be assigned based on a risk graph approach, which should be tailored to the specific context and needs.

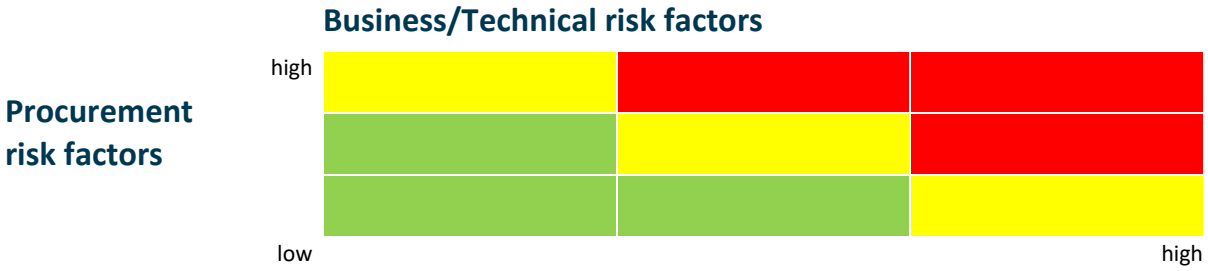
The criticality level of a digital supplier should be assessed as High/Medium/Low based upon specific business or technical risk factors and/or appropriate procurement data.

Business/Technical risk factors

- Types of Data (e.g. public, confidential, source code)
- Data governance (storing and processing of data)
- Product function (e.g. monitoring, control, safety)
- Threat and risk analysis trough business analyses

Procurement risk factors

- Cost of procured product
- Supplier competition (e.g. supplier dependency)
- Material fields (e.g. firmware as high-risk)



Definitions

High criticality supplier | Medium criticality supplier | Low criticality supplier

2.3 Verification

A standard verification process shall be used to ensure that digital suppliers are adhere to the baseline requirements. The process allows for three verification elements, which will be used according to the criticality of the digital supplier. Therefore, the verification element to be employed is aligned to the criticality level of the supplier being assessed.

Verification Element	Verification Element description	Supplier criticality
DP **Document proof**	Supplier shall provide evidence that it complies with the baseline requirements	**High**
SA **Self-Assessment**	Supplier shall demonstrate compliance to the baseline requirements by completing a self-assessment questionnaire	**Medium**
SD **Self-Declaration**	Supplier shall declare its compliance with the baseline requirements, e.g. through accepting T&Cs	**Low**

The verification process is designed to have minimum impact on existing procurement processes.

It has been specifically designed to be “light” while at the same time raising awareness and compliance with foundational cybersecurity requirements and best practices that should be adopted by all digital suppliers.

3 Context and further resources

The Charter of Trust believes that cybersecurity is a foundational element of trust in the digital economy for all. For creating this foundation, Charter of Trust partners aim to lead by example driving applicable Charter of Trust requirements through their companies and connected ecosystems (e.g. suppliers, partners and others). Furthermore, the partners aim at demonstrating the effectiveness of collaborative private enterprise efforts to regulators and policymakers.

The members of the Charter of Trust are continuously working on advancing the ten principles, defining clear baseline requirements and best practices where applicable. These are widely shared with a broad network of stakeholders to ensure a far-reaching level of trust.

To learn about the work of the Charter of Trust and find the latest releases, please refer to our website www.charter-of-trust.com.