# Supply Chain Process 2020 Guidelines

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi 18 - Brussels

T.: +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be

# Table of contents




CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi 18 - Brussels

T.: +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be



CHANCELLERY OF
THE PRIME MINISTER

# 1 Introduction

## 1.1 Purpose

The purpose of this document is to describe control objectives to protect confidentiality, integrity and availability (CIA triad) within the supply chain of network assets and services for Operators of Essential Services (OESs) under the NIS (framework for the security of network and information systems of public interest for public security, publication date 3/5/2019, NUMAC 2019011507).

## 1.2 Contributions

This document came about thanks to the valued contribution of BIPT (Belgian Institute for Postal Services and Telecommunications), various other government organisations as well as experts in (cyber) security.

This document was translated from the original Dutch & French master documents and is provided as a courtesy.

## 1.3 Supply chain of network assets and services

As there is increasing reliance on third parties to optimise owned services and to work cost efficiently, it is becoming increasingly important to gain an insight into the security risks associated with these third parties and their subcontractors. Third parties include integrators, service providers (e.g. maintenance of network components), managed services, hardware and software suppliers, etc…

Supply chain security is the security of assets and services throughout the entire life cycle of a system (design, development, construction, packaging, assembly, distribution, system integration, operational management, maintenance and decommissioning).

Depending on the type of service provider, the supply chain and the use of third parties by the service provider itself, are more complex and less transparent. Both the OESs and the service providers themselves, must consciously handle the supply chain and related risks in order to implement the necessary mitigating controls.

As these controls entail costs for both the OESes and the third parties, they must be based on a substantiated risk assessment for both.

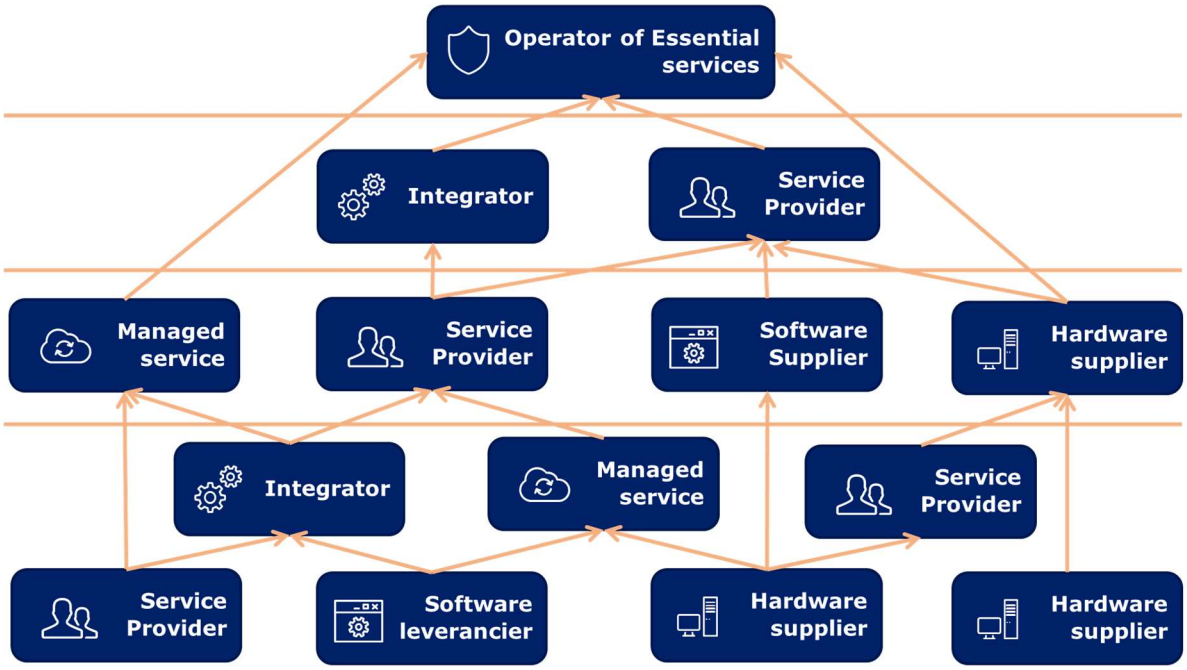


FIGURE 1 - COMPLEXITY OF THE SUPPLY CHAIN FOR OPERATORS OF ESSENTIAL SERVICES

## 1.4 Document structure

This document is composed of several control domains in the supply chain process. For each control domain, general control objectives are drawn up, related to information security.

A control domain can be supplemented with one or more sub-domains describing more specific control objectives. In order to achieve a control objective, one or more measures can be implemented. It is not the scope of this document to provide an exhaustive list of measures, but where possible reference is made to existing international standards.

In this document, the life cycle of a service or asset is broken down into five control domains, with "risk management" being considered the sixth key domain.

The various chapters relate to different steps in the life cycle of an asset or service.


## 1.5 Related documents

This document is consistent within the framework of ISO 28000 "Supply chain security management systems" as a control objective for the supply chain security management to be drawn up and implemented. However, the scope of this document is limited to control objectives for information security of network-assets and - services. More general control objectives and specific measures can be found in standards such as ISO 27001 or the CCB's "Baseline Information Security Guidelines" (BSG).

The following documents were used as references for the text:

- ISO/IEC 27000, 27001,27002 & 27005
- ISO/IEC 27017 Cloud Security
- ISO/IEC 27036 Information security for supplier relationships
- ISO/IEC 28000
- NIST SP800-161
- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation
- ISO/IEC 20243:2015 Open Trusted Technology Provider Standard
- NIST Cybersecurity Framework Version 1.1 (2018)
- Baseline Information Security Guidelines (CCB, edition 2019)

## 1.6 Terms and definitions

| Term | Definition |
|---|---|
| CERT | Cyber Emergency Response Team.<br>See CSIRT. |
| CIA - triad | CIA stands for Confidentiality, Integrity & Availability. |
| Control | Measure affecting the related risk (in accordance with ISO). |
| Control domain | A control domain describes a subject for which control objectives are set. |
| Control objective | A control objective describes a specific objective against which the effectiveness of the measures to be implemented can be evaluated (in accordance with ISO). |
| CSIRT | Computer Security Incident Response team. See CERT. |
| CTI | Cyber Threat Intelligence |
| EWS | Early warning System |
| GDPR | General Data Protection Regulation. A regulation aimed at standardising the rules relating to the processing of personal data. |
| ISO | International Organization for Standardization |
| KPI | KPI stands for Key Performance Indicator. This is a measure for assessing performance. |
| NIS Directive | Refers to the European Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union ('NIS' Directive).<br>This Directive was transposed into Belgian law on 7 April 2019. |
| NIST | National Institute for Standards and Technology (US) |
| Non-EU supplier | This also includes providing services in a non-EU country. |
| OES | Operator of Essential Services |

| Term | Definition |
|---|---|
| | As defined in the 'Framework for the security of network and information systems of general interest for public security' Act, Article 6 § 11 (publication date 3/5/2019, NUMAC 2019011507) |
| RPO | Recovery point objective<br>The minimum status of data that must be restored, it indicates how much data a company can allow to lose (RPO of 1 day means possibly lose 1 day of data) |
| RTO | Recovery Time Objective.<br>This is the maximum time required to return to normal service after an incident. |
| SLA | Service Level Agreement.<br>This is the definition of the minimum service or quality that customers can expect. |
| Supply Chain | The supply chain for services and assets. |

Terms not defined in the table above are used in accordance with their meaning in the existing standards (cf. ISO and NIST).

# 2 Risk Management

Identifying and analysing risks within the organisation related to the supply chain of network assets and services.

## 2.1 Setting the context

### 2.1.1 Asset and service inventory

| Objective: To establish and maintain an overview of all network assets, services and their criticality. |
|---|

Guide: OESes set up a process for the inventory of assets and services. This inventory contributes to a central and overarching overview. Features such as ownership can be managed in this inventory.

### 2.1.2 Evaluate dependency on other service providers

| Objectives: To evaluate the service's dependency on other service providers. |
|---|

Guide: OESes should evaluate the extent to which their services are dependent on other vital services (e.g. supply of electricity) and their impact in the event of failure or disruption and how (preventive) measures can minimise this impact.

### 2.1.3 Threat assessment and threat scenarios

| Objective: to determine and monitor the threat assessment and related threat scenarios for network assets and services. |
|---|

Guide: changes in the threat assessment are monitored in periodic reviews of industry security notices and recommendations (security bulletins from suppliers or national CERTs). Changes in the threat assessment, e.g. new threat scenarios, may require the risks within the supply chain to be reassessed.

## 2.2 Risk Analysis

### 2.2.1 Supply Chain Risk Analysis

| Objective: to identify and analyse supply chain security risks as part of the organisation's broader risk management strategy. |
|---|

Guide: OESes determine a risk analysis methodology including related impact and probability scales.

It is defined which assets are part of the essential services in the supply chain as well as the risks that need to be considered. It is important to integrate Supply Chain Risk Assessment into the broader (enterprise) risk management.

The impact tables that must be created take into account the impact criteria such as the number of users affected by the disruption of the essential service, the duration of the incident and the extent of the geographical area affected by the incident.

The measures to be implemented for an asset or service are determined based on a risk analysis. A high-risk asset or service will require stricter measures than a low-risk asset or service.

## 2.3 Risk communication and monitoring

### 2.3.1 Risk communication

| Objective: to share risk information with relevant stakeholders. |
|---|

Guide: communicating risks is important for monitoring the threat posture and determining the measures to be implemented with third parties.

### 2.3.2 Risk monitoring

| Objective: to monitor the existing and emerging risks within the organisation. |
|---|

Guide: risks within an organisation are not static. The threat landscape is changing constantly and, as a result, the risks within the organisation may change or new risks may arise.

A regular reassessment of the risks within an organisation is necessary for proper risk monitoring. In addition, changes within the organisation can also lead to a change in risks.

# 3 Security Management and architecture

General management of information security for network assets and services, and security architecture of network assets and services.

## 3.1 Management

### 3.1.1 Roles and responsibilities

| Objective: to formalise main buyer and outsourcer responsibilities and governance structure regarding the supply chain. |
|---|

Guide: there are major responsibilities that must be assigned when outsourcing, both in the buyer's organisation and in the outsourcer's organisation, like:

- Identify which stakeholders have to be involved in the decision-making process, who makes the final decision, who is liable for an action/result, and who should be consulted or informed, i.e. an RACI matrix must be drawn up (e.g. legal department, HR, finance, Enterprise risk management, IT, procurement, program management, etc.).

Assign the necessary resources to carry out processes and measures relevant to information security for the supply chain.

### 3.1.2 Procurement Strategy

| Objective: to define a management-supported procurement strategy covering business, operational, legal, architectural and regulatory requirements. |
|---|

Guide: an OES should define the procurement strategy for the essential services and implement this strategy in template contracts and procurement methods.

Organisations should encourage third parties to implement information security measures, to create transparency in organisational processes, in their own use of third parties and information security practices, and to provide additional controls of employees and other third parties related to service delivery for the essential service.

### 3.1.3 Definition and monitoring of KPIs for supply chain security

| Objective: to define and monitor KPIs for supply chain security. |
|---|

Guide: an OES defines internal and external KPIs for monitoring supply chain security requirements.

### 3.1.4 Risk Treatment

| Objective: to deal with risks associated with a network asset or service. |
|---|

Guide: the measures to be implemented for an asset or service are determined based on a risk analysis.

### 3.1.5 Incident management

| Objective: to be prepared for handling and monitoring incidents. |
|---|

Guide: defining a formal incident handling procedure contributes to an efficient response to incidents. This procedure includes at least the following phases:

- Preparation;
- Detection and Analysis;
- Contain, eradicate and recover;
- Post-incident activities.

When defining this procedure, an OES will have to assign the various roles and responsibilities during incident handling to internal or external parties. Furthermore the OES will also have to define in the contract with third parties when the AED wishes to be informed of incidents at the third party.

In the incident handling, an OES will also integrate the legal obligation to report incidents to the National CSIRT, the sectoral authorities and the National Crisis Centre.

## 3.2 Network security architecture

### 3.2.1 Network architecture layout

| Objective: to establish and maintain a schematic overview of all network assets and related services, and their connections. |
|---|

Guide: an OES keeps an overview of how the various network assets and services communicate and interact with each other.

### 3.2.2 Network information security measures

| Objective: to determine network information security measures based on a risk analysis (taking into account at least the different information flows and the sensitivity of the data). |
|---|

Guide: based on the network architecture diagram, the risks and relevant measures on the network layer can be examined. The risk analysis will include at least the different information flows, known vulnerabilities and sensitivity of the data.

## 3.3 Cloud solutions

Cloud solutions such as Software as a Server (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) are increasingly used. These are subject to specific control objectives.

### 3.3.1 Cloud Criticality

| Objective: to map the data flows to the cloud service provider and the criticality of the service. |
|---|

Guide: an OES determines a Cloud service's impact on the entire supply chain for the provision of an essential service. These results are an indication of the mitigating controls to be implemented by the cloud service provider and by the OES.

Risks associated with cloud solutions will have to be managed and mitigated differently than traditional risks managed by the organisation

### 3.3.2 Cloud information security measures

| Objective: to define the measures needed for storing data in the Cloud with adequate protection and considering other guidance and legislation. |
|---|

Guide: data stored in the Cloud must be subject to the same access controls as data stored locally.

In addition, it must be checked whether the geographical location of the data and any backups comply with other directives or legislation (e.g. GDPR).

### 3.3.3 Data sovereignty of services provided by non-EU suppliers

| Objective: to protect data sovereignty with non-EU suppliers |
|---|

Guide: the use of IT services including Cloud services by non-EU suppliers poses risks to data sovereignty. This means that all data stored, processed or transmitted by the Service is subject to the laws and regulations of those countries where data is stored, processed and transmitted.

Similarly, a non-EU supplier operating a service within Belgium may be subject to the laws of the country in which its registered office is located. For example, a service provider may be forced by a non-EU security body to provide information about its customers without informing the customer of this request. An OES must therefore identify the legal rules governing data storage, processing or transmission.

They also need to understand how the laws of those countries may affect the confidentiality, integrity, availability and data protection. When a service provider outsources part of the

service provision to a third party, the OES must also determine whether this entails additional data sovereignty risks.

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi 18 - Brussels

T.: +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

# 4 Procurement

Supplier relationship management and procurement of network assets and services from delivery up to storage.

## 4.1 Relationship Management

Managing the relationship with suppliers spans initial contact to completion of the contract.

### 4.1.1 Exchange of information

| |
|---|
| Objective: to carefully handle the exchange of information with (potential) suppliers during the procurement process. |

Guide: during the procurement process, information will be exchanged between the organisation and (potential) suppliers.

This information sharing starts with the drawing up of a list of specifications or Request For Proposal (RFP). It should be clear what information is shared during this exchange. If necessary, a binding agreement can be made with (potential) suppliers for contractual protection of the information shared. This includes sharing information with subcontractors or third parties of the (potential) supplier, and how long the information can be retained.

### 4.1.2 Information security measures from suppliers must be written in a contract

| |
|---|
| Objective: to collect, analyse and report on information security controls related to procurement of assets or services in order to demonstrate the maturity of information security in the supplier relationship, before starting a new relationship and at regular intervals for existing relationships. |

Guide: when selecting a supplier for an asset or service, a certain level of maturity of information security should be enforced. This should be monitored in existing relationships, either actively (via audits) or passively (via reporting). If the security needs change, the information security controls measures may need to be reviewed together with the third party.

### 4.1.3 Suppliers' security maturity

| |
|---|
| Objective: to select suppliers with adequate information security maturity and to regularly monitor this. |

Guide: the choice of supplier is based on various parameters. One of these parameters is the desired level of information security. An OES is also able to determine information security maturity for itself by performing an audit or a maturity assessment.

### 4.1.4 Suppliers comply with European and national laws and regulations

| Objective: to select suppliers that comply with European and national laws and regulations. |
|---|

Guide: the supplier must be evaluated and a assessment should be made as to whether they might be subject to regulations that are contrary to European or Belgian regulations.

### 4.1.5 Mapping all partners and parties involved in service delivery.

| Objective: to identify all (strategic) partners and parties, such as subcontractors, their services and their relationship to essential services. |
|---|

Guide: an OES maps its (strategic) partners and parties, as well as the services it provides and how they relate to the essential services provided by the OES. This inventory will create an overview of the risks.

### 4.1.6 OES will consider information about threats

| Objective: to integrate threat information on non-EU suppliers into the OES risk analysis process. |
|---|

Guide: an OES will have access to the central Cyber Threat Intelligence / Early warning System (CTI/EWS) platform for the threat-related information needed for their risk analysis. Through this CTI platform, the competent intelligence services will share their threat assessments of certain technical and geopolitical risks. Specific analyses are be coordinated by the CCB in consultation with the competent security and intelligence services.

## 4.2 Shipping, delivery and storage

Assets that are sent and stored may be exposed to external threats. Digital downloads or files can also be compromised during transport over the network or during storage.

### 4.2.1 Protecting the integrity, confidentiality and availability of an asset

| Objective: to protect assets against tampering during transport, delivery and storage. |
|---|

Guide: assets will be monitored to detect anomalies during transport, delivery or storage. This may require sealed packaging during transport and storage. Control of the shipment, delivery and storage of digital assets is also required. If necessary, the integrity of digital downloads and stored files will also have to be confirmed before they are used.

## 4.3 Self-assessment statement for suppliers of IT security services or systems

| Objective: compliance with the supply chain process guidelines by OES subcontractors or suppliers. |
|---|

Suppliers shall provide a self-assessment statement prior to the provision or purchase of IT security services or systems confirming compliance with the various control objectives of this guideline.

Annex 1 to the guideline contains an example of a self-assessment statement.

# 5 Operational Management

Operational management includes recurring management and maintenance tasks performed by a third party or services purchased from a service provider.

## 5.1 General security measures

### 5.1.1 Awareness-raising

| Objective: to raise staff awareness about sharing corporate information with outside parties and the potential associated risks for the supply chain. |
|---|

Guide: information can be shared with third parties on a need-to-know basis.

### 5.1.2 Operational procedures

| Objective: to establish and manage Security Operating Procedures related to network assets and services. |
|---|

Guide: the organisation will draw up and comply with a set of Security Operating Procedures in order to keep the residual risks related to information security at an acceptable level.

### 5.1.3 Contracts

| Objective: to protect corporate information against theft and misuse by external parties. |
|---|

Guide: binding agreements between all parties involved to adequately protect information (cf. risk assessment) and to ensure CIA will be included in contracts with external parties to ensure legal protection against theft and misuse of corporate information.

### 5.1.4 Access to network assets

| Objective: to prevent and monitor unauthorised access to network assets. |
|---|

Guide: for in-house and external staff, a clear Identity and Access Management (IAM) lifecycle process is needed. Access to network assets may only be granted if this is necessary for them to carry out their function. This access should therefore be revoked once it is no longer necessary.

### 5.1.5 Logging & Monitoring

| Objective: logging and monitoring of network assets and services to detect information security incidents. |
|---|

Guide: the various network assets must be configured with logging and monitoring to detect information security incidents (e.g. unauthorised access).

### 5.1.6 Information encryption

| Objective: to ensure the correct and effective use of encryption to protect the Confidentiality, Integrity and Availability (CIA) of information. |
|---|

Guide: use end-to-end encryption and tunnels when communicating across devices that are not managed by the organisation or whose security cannot be sufficiently ensured.

### 5.1.7 Information exchange

| Objective: to maintain the security of information exchanged within an organisation and with an external party. |
|---|

Guide: draw up clear rules and measures on e-mailing to third parties and sharing documents.

### 5.1.8 Supplier dependency

| Objective: to reduce dependence on a single supplier. |
|---|

Guide: an OES must be vigilant not to become dependent on one single supplier or manufacturer for network assets or services.

Measures may include placing the source code of applications developed by third parties with an escrow service, purchasing a second data centre from a different supplier, etc.

The network and cloud architecture should take sufficient account of the extent to which it is dependent on a single supplier or manufacturer. A modular architecture with components supplied by multiple suppliers and/or manufacturers will make the organisation less dependent on a single third party.

## 5.2 Consultants/External staff

All long-term and short-term external staff are consultants within the scope of this document. This is in supplement to the controls in 5.1.

### 5.2.1 Physical access

| Objective: to prevent unauthorised physical access , damage to and interference with information and information processing facilities of the organisation. |
|---|

Guide: an external staff member is only allowd to gain access to rooms and buildings that are necessary for the performance of his duties. This access may include autonomous or supervised access.

## 5.3 Third-party administrators

Third parties sometimes manage various aspects of the organisation.

Examples include network management, server management or data centre management. This is in supplement to the controls in 5.1.

### 5.3.1 Time-restricted access

| Objective: to restrict access to systems and applications to specified time intervals. |
|---|

Guide: the access of a third party administrator will be limited in time. Access can be granted within a time window (e.g. office hours) or based on a request (e.g. support ticket).

## 5.4 Managed Service Providers

Outsourced services. This is in supplement to the controls in 5.1.

### 5.4.1 External information transport

| Objective: to maintain the security of information exchanged inside an organisation and with an external entity. |
|---|

Guide: when purchasing a managed service that has access to or control over the organisation's core network, the information shared must be adequately secured.

### 5.4.2 An OES will take into account information about threats

| Objective: to integrate threat information on non-EU suppliers into the OES risk analysis process. |
|---|

**The same rule applies here as in 4.1.6 in the Procurement chapter (above).**

# 6 Incident Recovery & Major Changes

Emergency interventions on network assets and services and the modification and replacement of network assets.

This is out of the scope of day-to-day operational management.

## 6.1 General

### 6.1.1 Ensuring access for emergency interventions

| |
|---|
| Objective: to provide temporary authorisation to access network assets and services during emergency interventions. |

Guide: external support teams should be able gain temporarily access the necessary network assets or services.

### 6.1.2 Contingency plans

| |
|---|
| Objective: to develop contingency plans for restoring critical assets and services. |

Guide: implement contingency plans that include supply chain aspects, ensuring supply chain integrity and reliability during potential incidents (e.g. cyber-attack or strike)

### 6.1.3 Secure access

| |
|---|
| Objective: to provide secure communication channels for remote support teams. |

Guide: remote access to parts of the basic network infrastructure is possible during repairs and major extensions. Remote access can be initiated in various forms, for example services such as RDP or SSH.

Secure communication channels (e.g. protected with VPN and multi-factor authentication) will be used to provide remote access to external support teams.

### 6.1.4 Secured areas

| |
|---|
| Objective: to prevent unauthorised physical access to, damage to and interference with information and information processing facilities of the organisation. |

Guide: in case of repairs or major changes, access to certain rooms or facilities for repairing or replacing network components may be required.

Excessive or unplanned access rights must be avoided. How is the physical access granted? By request, ad hoc, or in case of emergency? Do people need to be accompanied by someone?

## 6.2 Returns

Assets can be returned to the supplier for repairs, in a process known as Return Merchandise Authorization (RMA).

### 6.2.1 Secure returns

| |
|---|
| Objective: to protect company data stored on assets that are returned to the supplier or manufacturer. |

Guide: during the return process, an inventory will have to be made of which parties (courier service, postal service, etc.) have access to these assets and which information is located on the assets.

# 7 Secure disposal

Decommissioning equipment and shutting down or transitioning services.

## 7.1 Data carriers

### 7.1.1 Prevention of data leakage

| Objective: to protect data against leakage when network assets are decommissioned. |
|---|

Guide: decommissioning equipment raises the question of whether it can be reused or should be destroyed. A decision can be taken based on the risk analysis. When equipment is intended for reuse, either by being sold or reused within the organisation, all data must first be adequately erased from the device.

## 7.2 Service transition plan

### 7.2.1 Management of supplier data in the event of decommissioning

| Objective: to protect corporate information shared with a supplier in the event of decommissioning of a service contract. |
|---|

Guide: when a service is terminated, all data transfers to/from the supplier will be stopped. Corporate information stored at the supplier will have to be removed and, if applicable, returned to the OES.

When services are migrated to another supplier, the necessary company data will also have to be transferred from the original supplier to the new supplier. This transfer will be adequately secured.

## Annex 1: Example of a supply chain security self-assessment statement

[Supplier]

I hereby confirm as [Supplier] that the supply chain security of the product [Product] has been assessed against the requirements set by [OES].

With this supply chain security statement, I confirm that for product [Product], the control objectives are handled as described by [OES] for the following control domains:

Risk management

- Security & Architecture
- Procurement
- Operational management
- Incident Recovery & Major Extensions
- Secure Disposal

I can provide the necessary supporting evidence if needed.

Supplier:

Signature

DATE

**Responsible publisher:**
Centre for Cyber Security Belgium
M. De Bruycker, Director
Rue de la Loi, 16
1000 Brussels

**Legal deposit**
D/2020/14828/001

Supply Chain Process guidelines - December 2019

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi 18 - Brussels

T.: +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be