
Document information

General information

Contact author	Group Cybersecurity Team
Document Type	Policy / Security Requirements
Object	Veolia OT Cybersecurity Policy
Référence	PO-TSE-008
Date	20/03/2024
Validation	Robert AMATU
Scope	Group
Comment	

Version History

Version	Revision date	Change comments
1.0	2015/10/09	Initial version
2.0	2021/02/10	second version
3.0	2024/03/20	Third version

Document Approval

Robert AMATU

Head of group Cybersecurity (Group CISO)
Security Department

Table of Content

1. Introduction	5
1.1. How to read this policy	6
1.2. OT cybersecurity: a Dual Approach	6
1.3. Organisation of the Document	7
2. OT Cybersecurity at the Business Unit Level	8
2.1. High-level OT Cybersecurity Policy Reminder	8
2.2. What the business unit can bring	9
2.2.1. Sponsorship	9
3. OT cybersecurity at site level	14
3.1. FTB-01 - Roles & Responsibilities	15
3.1.1. Reminder of the FTB-01	15
3.1.2. Requirements	15
3.2. FTB-02 - Awareness & Training	17
3.2.1. Reminder of the FTB-02	17
3.2.2. Requirements	17
3.3. FTB-03 - Asset Inventory	19
3.3.1. Reminder of the FTB-03	19
3.3.2. Requirements	19
3.4. FTB-04 - Network Security	20
3.4.1. Reminder of the FTB-04	20
3.4.2. Requirements	20
3.5. FTB-05 - Remote Access	22
3.5.1. Reminder of FTB-05	22
3.5.2. Requirements	22
3.6. FTB-06 - Backup & Recovery	24
3.6.1. Reminder of FTB-06	24
3.6.2. Requirements	24
3.7. FTB-07 - Sites / Contracts Inventory	25
3.7.1. Reminder of FTB-07	25
3.7.2. Requirements	25
3.8. FTB-08 - Identity & Access Management	26
3.8.1. Reminder of FTB-08	26
3.8.2. Requirements	26
3.9. FTB-09 - Antivirus / EDR	28
3.9.1. Reminder FTB-09	28
3.9.2. Requirements	28
3.10. FTB-10 - System Hardening	29
3.10.1. Reminder FTB-10	29
3.10.2. Requirements	29

3.11. FTB-11 - Incident & Crisis Management	31
3.11.1. Reminder FTB-11	31
3.11.2. Requirements	31
3.12. FTB-12 - BCP / DRP	33
3.12.1. Reminder FTB-12	33
3.12.2. Requirements	33
3.13. FTB-13 - Obsolescence Management	34
3.13.1. Reminder FTB-13	34
3.13.2. Requirements	34
3.14. FTB-14 - Vulnerability & Patch Management	35
3.14.1. Reminder FTB-14	35
3.14.2. Requirements	35
3.15. FTB-15 - USB Prevention	37
3.15.1. Reminder FTB-15	37
3.15.2. Requirements	37
3.16. FTB-16 - Detection - Logging & Monitoring	39
3.16.1. Reminder FTB-16	39
3.16.2. Requirements	39
3.17. FTB-17 - Risk Management	41
3.17.1. Reminder FTB-17	41
3.17.2. Requirements	41
3.18. FTB-18 - Audit & Control	42
3.18.1. Reminder FTB-18	42
3.18.2. Requirements	42
3.19. FTB-19 - Security by Design	44
3.19.1. Reminder FTB-19	44
3.19.2. Requirements	44
3.20. FTB-20 - Third-Party Management	46
3.20.1. Reminder FTB-20	46
3.20.2. Requirements	46
4. Annexe	48
4.1. Glossary	48

Executive Summary

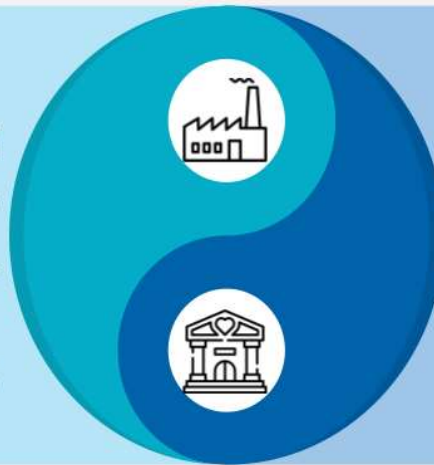
OT cybersecurity policy Dual approach to manage OT cybersecurity

Site level

In the end, industrial sites need to be secured **individually** and a **local approach** will be necessary to maintain a good cybersecurity level over time.

The OT cybersecurity policy is thus focused on **site security methodology**.

6 key principles are defined to drive OT cybersecurity and follow the **20 OT Fix the Basics**.

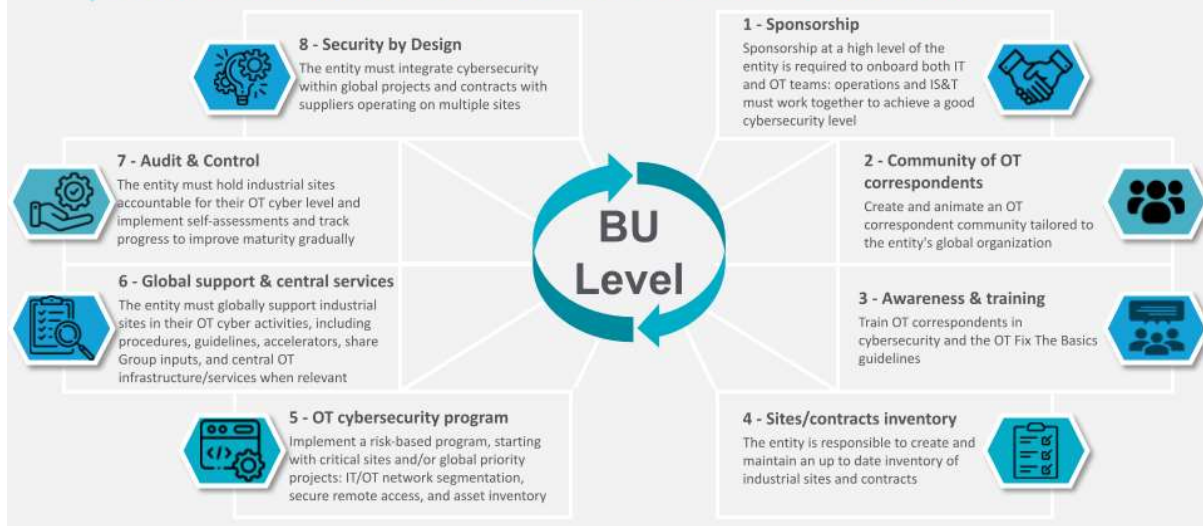


BU level

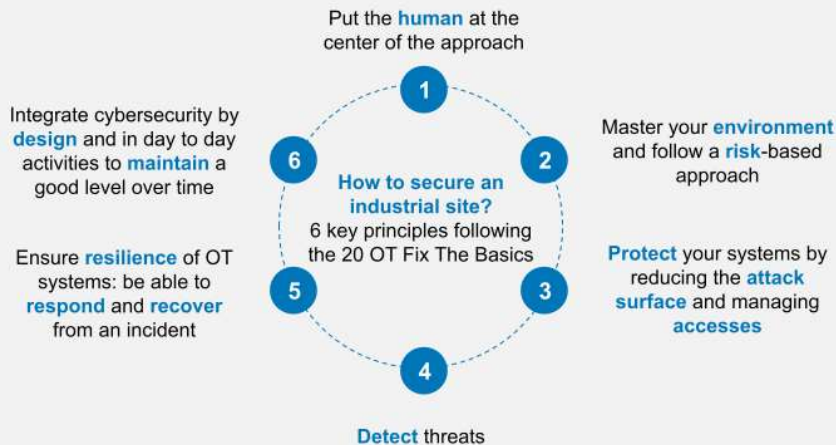
Business units play an **important role** in OT cybersecurity as they manage multiple industrial sites and they must **bring the appropriate support** to help industrial sites achieve and maintain a good cybersecurity level.

Especially, **governance** is key to scale the right OT cybersecurity program.

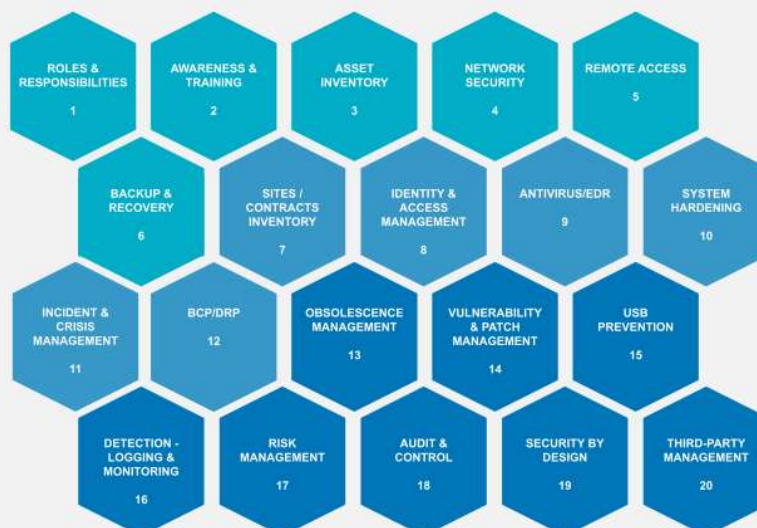
OT cybersecurity at Business unit level Copy and adapt the right governance for the long RUN



OT cybersecurity at the site level 6 key principles to drive the strategy



OT Fix the Basics



OT FIX THE BASICS

In order to **define a long-term local roadmap** to support each site, priorities have been defined on three priority levels, from 1 to 3.

To address the **stakes** specific to each site and to be able to **initiate and then continue** the associated actions, **operational implementation guidelines** are proposed.

They are accompanied by a **maturity scale** to assess the **reality on the ground** and adjust the roadmap.

All the documentation associated with OT Fix the Basics is available.

1. Introduction

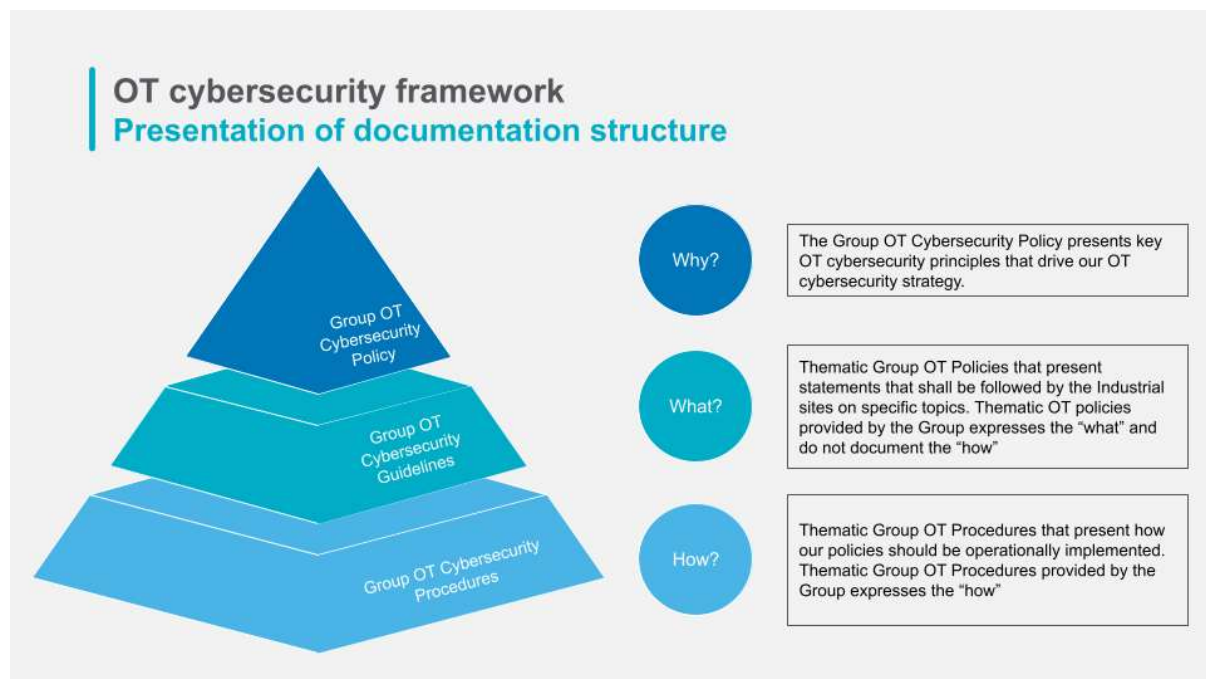
Veolia's main goal is to provide people with services linked to one of those three businesses: Water, Waste and Energy. In order to provide these services, Veolia's industrial sites are equipped with OT (Operational Technology) assets and software such as; Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) or Distributed Control Systems (DCS), etc. If not secured, those technologies can be attacked, leading to physical harm, or causing environmental or health damage. This underscores the essential need for their security.

Considering OT cybersecurity at both the **Site** and **Business unit** levels is important to effectively secure Veolia's industrial sites.

This document is part of the OT cybersecurity framework and answers the question "What?". It describes the main OT cybersecurity requirements and follows the two main "Why?" documents:

- The high-level OT cybersecurity policy explaining the duality of securing industrial control systems:
 - 6 key Principles to Secure an Industrial Site
 - What the business unit can bring to help industrial sites
- The 20 OT Fix the Basics presentation

Here is the global overview of the OT cybersecurity framework.



The OT cybersecurity policy contains a set of requirements defined to achieve a maturity level following the cybersecurity best practices. It reflects the strategic vision of the group's management in terms of cybersecurity of industrial control systems and is intended to define the roadmap for the years to come.

Furthermore, this policy follows the cyber resilience needs and, for the relevant countries, the NIS2 requirements.

1.1. How to read this policy

According to RFC 2119, this document contains two types of requirements that are identifiable through the words "**Must**" and "**Should**".

- **Must**: this word, or the terms "**Required**" or "**Shall**", means that the definition is an absolute requirement of the specification.
- **Should**: this word, or the adjective "**Recommended**", means that there may exist valid reasons, in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. *

* Please note that in this particular document "**Should**" means that this requirement is a way of implementing the musts, but it is not mandatory.

Also, in this document, the word site and/or contract will be used a lot, as the requirements are applicable to industrial sites. Below is a quick definition:

- **Site/Contract**: A site or contract can cover multiple geographically distributed sites, depending on the business and the functioning of the industrial control system. The site consists of every asset/site that together makes the industrial control system as a whole. We also use the word contract because Veolia does not always own industrial sites and the scope of one contract can usually be considered as a site. To give a few examples:
 - Usually, an Energy Recovery Facility will be considered as one site, as the global process is implemented on a single site geographically.
 - However, a water production and distribution site will consist of multiple geographically distributed sites, such as the main production site, the tanks, the boosters, the flow metres, etc.

Each **exception** to this policy should be documented and the way they are managed should also be documented.

1.2. OT cybersecurity: a Dual Approach

OT cybersecurity needs to be tackled at two levels:

- **Site level**
 - In the end, industrial sites need to be secured individually and a local approach will be necessary to maintain a good cybersecurity level over time.
 - The OT cybersecurity policy is thus focused on site cybersecurity methodology.
 - 6 key principles are defined to drive OT cybersecurity and follow the 20 OT Fix the Basics.
- **Business unit level**
 - Business units play an important role in OT cybersecurity as they manage multiple industrial sites and they must bring the appropriate support to help industrial sites achieve and maintain a good cybersecurity level.
 - Governance is the key to scale the right OT cybersecurity program.

It is important to keep in mind that the Fix the Basics were developed for site-level implementation. Therefore, the maturity levels are tailored to the aspects of individual sites. A version of these maturity levels aimed at the BU level has also been developed and is available on the Intranet for the CAP campaign.

1.3. Organisation of the Document

This document is divided into two main sections that follow the dual approach of OT cybersecurity:

- OT cybersecurity at the Business unit level
 - This section provides guidance to Zone and BU CISOs on OT cybersecurity management. It is important to note that nothing in this section is mandatory. Only suggestions on how business units can help sites are provided.
 - This section includes a reminder of the high-level OT cybersecurity policy and then deep dives into the 8 topics where business units can help industrial sites.
- OT cybersecurity at the site level
 - This section introduces the 6 key principles to secure industrial sites.
 - Then, OT cybersecurity requirements are listed following each of the 20 OT Fix the Basics. Each subsection is built as follows:
 - A reminder of the Fix-The-Basics.
 - The list of requirements (each requirement is linked to a maturity level as defined in the framework).
 - A note about implementation advice if needed.
 - A note about how business units can provide help to sites.

Finally, a glossary is available in the appendix part.

2. OT Cybersecurity at the Business Unit Level

Business units have a huge role to play in OT cybersecurity as they manage several industrial sites.

This section provides guidance on how Business units can bring the appropriate support to help industrial sites achieve and maintain a good cybersecurity level.

Nothing is mandatory in this section, but the topics listed are what should be expected from the Business unit to support industrial sites. Everything needs to be adapted to each Business unit's specificity.

2.1. High-level OT Cybersecurity Policy Reminder

The global strategy at the Business unit level is to copy and adapt the right governance for all the sites. This way, OT cybersecurity can be transposed to all sites in the same way, facilitating its implementation, as well as maintenance over time.

This general approach for OT cybersecurity at the Business unit level is focused on 8 topics:

- Sponsorship;
- Community of OT correspondents;
- Awareness & training;
- Sites/contracts inventory;
- OT cybersecurity program;
- Global support & central services;
- Audit & control;
- Security by Design.

Here is a reminder of the [high-level OT cybersecurity policy](#).



2.2. What the business unit can bring

2.2.1. Sponsorship

By nature, OT cybersecurity brings two worlds together: **IT & Operations**

- IT (usually DB&T teams in Business units), in charge of information systems and especially network and system administration.
- Operations, in charge of the business, industrial process and its performance.

Sponsorship at a high level, involving both the CIO and Operations director is required to onboard both IT and OT teams in a common OT cybersecurity strategy and roadmap.

Operations and IT teams must work together to achieve a good cybersecurity level on industrial sites.

2.2.2. Community of OT Correspondents

As mentioned as one of the 6 key principles to secure an industrial site, **putting the human at the centre of the approach** is essential.

This is particularly true in OT, as Industrial Control Systems interact with the physical world. To secure these systems, a physical presence at industrial sites is required at some points.

That is why it is key for business units to build the right **community of OT correspondents** and find the right hierarchy that suits the organisation to make OT cybersecurity work at every level: from the central cybersecurity team of the business unit to the local OT correspondent working on the industrial site.

Below are more details on what can be expected from business units on the corresponding OT Fix the Basics:

FTB01 - Roles & Responsibilities

- Each **business unit should** put together an OT cybersecurity organisation with multiple layers, adapted to the business unit size, specificities and already existing organisation:
 - National organisation with CISO and OT cybersecurity engineers, in charge of relaying Group information and helping business unit's industrial sites
 - Community of local OT correspondents for the sites
 - A layer in between when relevant: split by region, business or business unit organisation, where duos are responsible for OT cybersecurity: one person coming from IT and one coming from operations
- In order to help its sites, the **business unit should** provide a role sheet for the Local OT cybersecurity correspondent.

2.2.3. Awareness & training

Another topic for business units, still focusing on putting the human at the centre of the approach: awareness & training:

- **Awareness** because humans still remain one of the biggest threat factors and it is important to raise awareness among every employee to reduce the risks.
- **Training** because humans are key in securing OT environments as mentioned previously and the community of OT correspondents need to be trained.

Below are more details on what can be expected from business units on the corresponding OT Fix the Basics:

FTB02 - Awareness & Training

- The **business unit should** provide standard awareness materials to all its industrial sites (posters, e-learning, videos, awareness slide presentations, etc.).
- The **business unit should** keep records of all employees following awareness sessions.
- The **business unit should** provide training to local OT cybersecurity correspondents and cybersecurity experts.

2.2.4. Sites/contracts inventory

As stated in another key principle, it is essential to **master its environment**.

Having a list of industrial sites in a business unit is important to know what is the scope that needs to be secured and also prioritise based on sites' criticality.

The "**FTB07 - Sites / Contracts inventory**" is the Fix-The-Basics that gathers all requirements allowing the business units to create and maintain an up-to-date inventory of industrial sites and contracts. Please note that the requirements in this particular section are **musts** for the business units because this whole section is under the business unit's responsibility.

2.2.5. OT cybersecurity program

Common OT cybersecurity projects and targets for industrial sites can be defined at the business unit level. That is why it is important for business units to implement a **risk-based program** and to start their OT cybersecurity journey to raise maturity step by step on their entire scope:

- Start by focusing on **critical sites**, especially when they are subject to cybersecurity regulations. For these sites, you might need to reach pretty quickly an A level of maturity on the OT Fix the Basics.
- Then **scale** and select **top priority projects** to implement on a majority of sites across the business unit: for example, IT/OT network segmentation, secure remote access, asset inventory and backup

Below are more details on what can be expected from business units on the corresponding OT Fix the Basics:

FTB17 - Risk management

- An inventory of all the applicable laws and regulations and their implications for Veolia (in terms of cybersecurity) **should** be maintained at the **business unit** level.

2.2.6. Global support & central services

Besides defining a business unit OT cybersecurity program, to easily implement the same cybersecurity targets, business units might want to **provide central support and services to all their industrial sites**. Both **organisational** and **operational** support can be provided. To give a few examples:

- At operational level:
 - A common WAN architecture can be implemented with the same IT/OT firewall solution, centrally managed, including a red button procedure to isolate sites quickly in case of a cyber attack.

- A central OT DMZ at the business unit level can be implemented, in AWS for instance, with the following infrastructure services:
 - Remote access
 - Antivirus and/or EDR
 - Patch management server, such as a WSUS
 - Backup repository
 - NTP server
 - Syslog server
 - Active Directory
 - Etc.
- At the organisational level:
 - Business unit procedures and processes can be defined, formalised, and applicable to the entire OT scope:
 - Incident and crisis management procedure
 - Guidelines and templates such as hardening guidelines, a disaster recovery procedure, identity and access management procedure, a patch management procedure, a log management procedure, etc.
 - Cyber crisis exercises can be organised annually and spread across multiple sites of the business unit

Below are more details on what can be expected from business units on the corresponding OT Fix the Basics:

FTB05 - Remote access

- A dedicated and central remote access solution **should** be put in place at the **business unit** level. The solution can be implemented in a central OT DMZ for the **business unit**.

FTB08 - Identity & Access management

- A central OT Active Directory **can** be implemented at the **business unit** level. The number of Active Directory and the OU (Organisation Unit) organisation must be adapted to the **business unit**.

FTB11 - Incident & Crisis management

- At the **business unit** level, a cyber incident management plan and a cyber crisis management procedure **should** be defined and documented and should be applicable to all industrial sites.
- In case of compromise, the **business unit should** have the ability to isolate a specific site.
- At the **business unit** level crisis management exercises simulating a cyber attack **should** be organised on multiple industrial sites.

FTB16 - Detection - Logging & Monitoring

- A SIEM (Security Information and Event Management) **should** be implemented at the **business unit** level to analyse logs.
- OT logs **should** be sent to the Global SOC for analysis, review and security monitoring.

2.2.7. Audit & Control

The Business unit is **accountable** for the level of cybersecurity of its industrial sites. Audit & Control activities must be organised at the business unit level and be adapted to the sites' volume, typology, criticality, as well as regulatory requirements. Indeed, it is important to know its cybersecurity level and be able to **track progress** to improve maturity gradually.

For example, self-assessments, internal assessments and 3rd party audits should be organised and a specific plan should be defined.

Below are more details on what can be expected from business units on the corresponding OT Fix the Basics:

FTB18 - Audit & Control

- Each **business unit should** define and implement a self-assessment program for each industrial site, and adapt the frequency based on site criticality. Annual self-assessments **should** be performed on critical sites.
- Each **business unit should** define and implement a global audit plan based on the sites' criticality.
- An OT audit carried out by an independent third party **should** be conducted on some sites based on the **business unit's** plan.

2.2.8. Security by Design

Many projects are conducted on multiple sites and some 3rd parties operate on multiple sites as well. In order to have consistency, but also for efficiency, the business unit should support industrial sites on these projects and 3rd party management:

- BU CISO team should be involved in projects, share cybersecurity requirements and make sure best practices are implemented.
- Standard requirements should be shared with 3rd parties involved on multiple sites.

Below are more details on what can be expected from business units on the corresponding OT Fix the Basics:

FTB19 - Security by design

- **Business unit should** be involved in projects affecting multiple industrial sites.

FTB20 - Third-party management

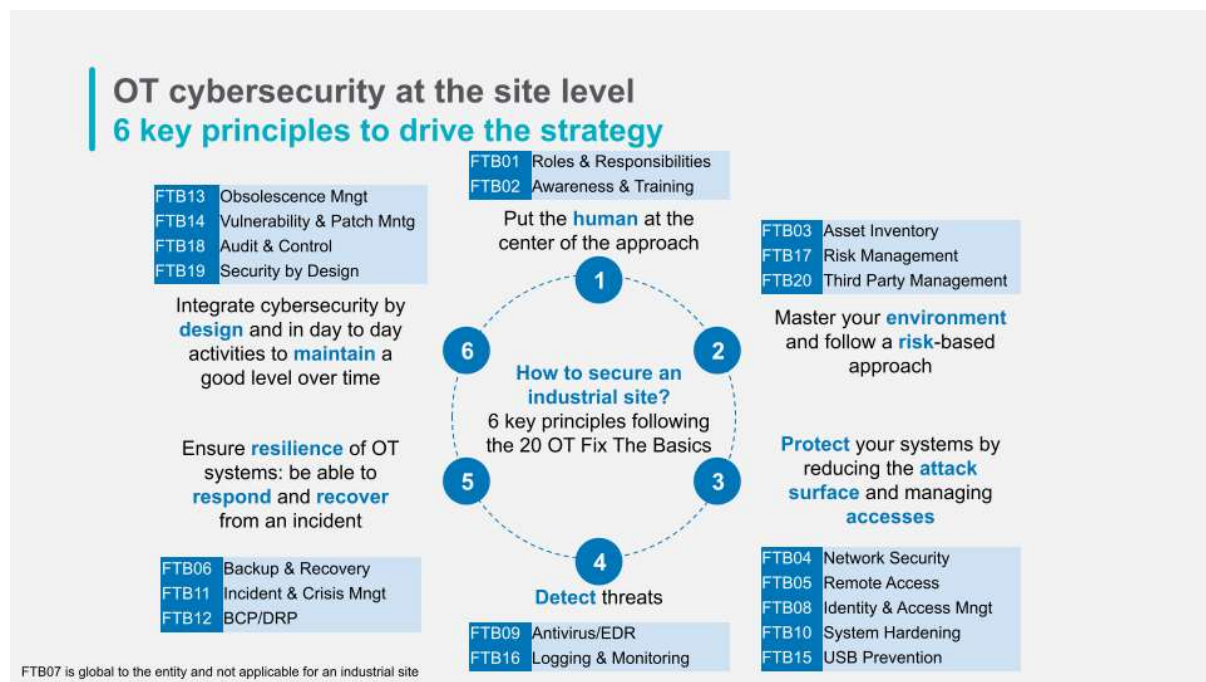
- If a 3rd party is involved on multiple sites of the **business unit**, a service agreement, defining mutual responsibilities in terms of cybersecurity, **should** be drawn up between this third party and the business unit.
- For sites not owned by Veolia, an appendix with OT cybersecurity activities conducted by Veolia **should** be added by the **business unit** to all bids to clearly position cybersecurity as a differentiator in the Veolia business offers.

3. OT cybersecurity at site level

In the end, industrial sites need to be secured individually and a local approach will be necessary to maintain a good cybersecurity level over time.

How to secure an industrial site? 6 key principles are defined to drive OT cybersecurity and follow the 20 OT Fix the Basics.

- Put the **human** at the centre of the approach.
- Master your **environment** and follow a **risk**-based approach.
- **Protect** your systems by reducing the **attack surface** and managing **accesses**.
- **Detect** threats.
- Ensure **resilience** of OT systems: be able to **respond** and **recover** from an incident.
- Integrate cybersecurity by **design** and in day-to-day activities to **maintain** a good level over time.



3.1. FTB-01 - Roles & Responsibilities

3.1.1. Reminder of the FTB-01

1. Roles & Responsibilities

An OT correspondent in charge of cyber must be identified for each industrial site
Entity level: Has a formal OT cybersecurity organization been defined and implemented with the appropriate correspondents across the entity? / **Site level:** Has a local OT correspondent been identified for the site?

General principle
Effective governance makes it possible to significantly increase the level of cyber maturity of sites and to ensure that a **good level is maintained over time**. A **local OT correspondent** must be identified on each site. His role is, among other things, to share procedures and good practice guides to the teams, report any cybersecurity incident, enforce cybersecurity requirements, etc.

Operational implementation

1. Set up a **local correspondent** for cybersecurity actions: appointment of a cybersecurity referent to the established missions.
2. Ensure **exchanges** between the entity's cybersecurity team and the local correspondent and the **feedback** of information, needs, etc.

Group available resources

- General Job Description - OT Cybersecurity Correspondant (EN)
- RACI Chart (EN)
- General Job description - CISO (EN)

What's expected from the site

- ❑ Identification of the local correspondent
- ❑ Formalization of a job description for the local OT correspondent
- ❑ Complete Organization Charts (by priority, OT, sites, BU, Zone, IT)

Cyber Maturity

0
No one is locally in charge of industrial cybersecurity.

1
A person on the site is partially responsible for relaying certain industrial cybersecurity topics.

2
A business correspondent aware of industrial cybersecurity provides local relay and information feedback to the entity referent.

3
Local industrial cybersecurity is fully supported by a business correspondent trained in OT and cyber aspects. He organizes the local governance of industrial cybersecurity and ensures security actions.

Priority 1

3.1.2. Requirements

FTB01 - R01 - A Local OT cybersecurity correspondent **must** be identified for each industrial site.

FTB01 - R02 - The Local OT cybersecurity correspondent **must** be aware of OT cybersecurity.

FTB01 - R03 - The Local OT cybersecurity correspondent **must** be trained in OT cybersecurity.

FTB01 - R04 - The Local OT cybersecurity correspondent **must** be responsible for sharing information from the Group/business unit and raising alerts.

FTB01 - R05 - The Local OT cybersecurity correspondent **must** be in charge of the OT cybersecurity action plan for the site.

Implementation advice:

- One person can be the local OT cybersecurity correspondent for multiple sites depending on the business unit organisation.
- The local OT cybersecurity correspondent does not usually work full-time in cybersecurity.
- The local OT cybersecurity correspondent can have an IT background but usually comes from the business (automation engineer, operations manager, etc.)

What the business unit can bring:

- Each **business unit should** put together an OT cybersecurity organisation with multiple layers, adapted to the business unit size, specificities and already existing organisation:

- A national organisation with CISO and OT cybersecurity engineers, in charge of relaying Group information and helping business unit's industrial sites
 - Community of local OT correspondents for the sites
 - A layer in between when relevant: split by region, business or business unit organisation, where duos are responsible for OT cybersecurity: one person coming from IT and one coming from operations
- In order to help its sites, the **business unit should** provide a role sheet for the Local OT cybersecurity correspondent.

3.2. FTB-02 - Awareness & Training

3.2.1. Reminder of the FTB-02

2. Awareness & Training

Priority 1

- Everyone must be made aware of OT cybersecurity
- People with cybersecurity responsibilities must follow dedicated OT cyber training

*Is there a dedicated industrial cybersecurity training in place for the OT cybersecurity team and is there an awareness program in place for OT Cybersecurity for plants' staff, visitors and suppliers ?**

General principle
Cybersecurity is everyone's business, even in an industrial environment. Beyond raising awareness and training industrial cybersecurity managers, involving all the teams working on the industrial information system (management, operations, maintenance, etc.) ensures the relevance and effectiveness of the hardware and software solutions deployed on the site.

Operational implementation

1. Train the local OT correspondent in awareness raising.
2. Set up mandatory awareness sessions for the different user populations.
3. Train local OT correspondent and managers in OT cybersecurity
4. Raise the awareness of suppliers, partners and service providers working on the industrial network.
5. Provide easily accessible awareness-raising materials (posters, reminders of good practices, reflex sheets, etc.).

Group available resources

- Group OT awareness e-learning (Siemens)
- All Posters Awareness Raising IT/OT - EN/FR
- Intranet Awareness Support

What's expected from the site

- ☐ OT Awareness material
- ☐ OT Awareness planning
- ☐ List of people who have followed the awareness
- ☐ Sharing of Group documents to sites (entity)
- ☐ List of people who followed a training (which training and when)

*Note: training and awareness material should be provided at the entity level and then implemented at site level

Cyber Maturity

No one on site is aware or trained in industrial cybersecurity. **0**

The local OT correspondent is trained in industrial cybersecurity and he himself able to raise awareness among the teams. **1**

Some of the teams are made aware of industrial cybersecurity. Nevertheless, some stakeholders still need to be made aware of OT cybersecurity. **2**

An awareness program is applied to all populations accessing the industrial network. Mandatory sessions are regularly given and feedback integrated. **3**

3.2.2. Requirements

FTB02 - R01 - Every employee working on an industrial site **must** be made aware of OT cybersecurity and follow an OT cybersecurity awareness session.

FTB02 - R02 - OT awareness posters **must** be displayed on site, including incident posters.

FTB02 - R03 - The site's service suppliers **must** follow an OT cybersecurity awareness session either provided by the site or by the supplier in itself.

FTB02 - R04 - Specific OT cybersecurity training **must** be provided to sites' employees and service suppliers in charge of maintaining OT environments, including the local OT correspondent.

FTB02 - R05 - Specific OT cybersecurity training **should** be provided to the Local OT Cybersecurity Correspondent.

FTB02 - R06 - A quick cybersecurity awareness session **should** be provided on-site to visitors with the physical security induction.

Implementation advice:

- OT awareness sessions can be provided through e-learning or on-site physical sessions.

What the business unit can bring:

- The **business unit should** provide standard awareness materials to all its industrial sites (posters, e-learning, videos, awareness slide presentations, etc.).
- The **business unit should** keep records of all employees following awareness sessions.
- The **business unit should** provide training to local OT cybersecurity correspondents and cybersecurity experts.

3.3. FTB-03 - Asset Inventory

3.3.1. Reminder of the [FTB-03](#)

3. Asset Inventory

Each industrial site must have a cartography, including a complete asset inventory as well as a network diagram

Are all plant assets tracked in an asset inventory and kept up to date under the responsibility of the CISO with the support of the OT Correspondent? Is there a network diagram for the site?

General principle
Having a **complete documentation** of the OT makes it possible to identify the equipment, software, critical data and **associated flows**. Centralizing this information facilitates the **management of the OT fleet**: monitoring of obsolescence, deployment of solutions, etc. **Precisely locating each of the assets on the network** makes it possible to **consolidate the architecture** and protect the heart of production.

Operational implementation

1. Formalize the complete **inventory** of the industrial information system, covering **all equipment with an IP address** (including physical security systems).
2. Formalize the cartography of the entire industrial network (**architecture diagram**), if necessary using probes.
3. Regularly **update**, after each change, the formalized asset inventory and network cartography.

Group available resources

- Nozomi (including Master Service Agreement)
- [Asset inventory Guidelines - FN](#)
- [Asset inventory Template](#)

What's expected from the site

- ❑ Complete OT asset inventory
- ❑ OT full cartography (network architecture diagram)

Priority 1

Cyber Maturity

No inventory or cartography of the industrial network is formalized. The OT documentation is incomplete or even non-existent. **0**

An asset inventory and a cartography are formalized on some part of the OT (some mandatory information are filled in: typology, IP address, etc.). **1**

The asset inventory covers the entire network and all mandatory information is filled in. The associated cartography is complete. **2**

The entire OT is documented. The asset inventory as well as the network cartography are regularly updated and all the recommended information is filled in. **3**

3.3.2. Requirements

FTB03 - R01 - All assets linked to industrial control systems **must** be listed on an asset inventory which contains all relevant information (IP addresses, name, type of asset, versions, obsolescence, asset's criticality, etc.).

FTB03 - R02 - The asset inventory **must** be kept up-to-date.

FTB03 - R03 - An OT network diagram **must** be formalised for the site.

FTB03 - R04 - The OT network diagram **must** be kept up-to-date.

FTB03 - R05 - Prior to leaving Veolia's premises, all equipment **must** be removed from the asset inventories.

FTB03 - R06 - The deletion of sensitive information prior to the disposal of assets **must** be done to ensure that cybersecurity is not compromised as assets reach the end of their useful life.

FTB03 - R07 - The asset inventory **should** be maintained through an automatic and passive asset discovery if the site size is important or if the site is critical.

FTB03 - R08 - A process explaining how to manage the asset inventory and the linked network diagram **should** be formalised.

3.4. FTB-04 - Network Security

3.4.1. Reminder of the FTB-04

4. Network Security

The OT network must be segmented from other networks

Does the network architecture of the industrial site respect the standard established by the group? Including:

- Prohibit the exposure of OT assets on the Internet
- Implement a firewall between the IT and OT networks and limit communications to the only necessary flows
- Implement a DMZ between IT and OT: favor protocol break and incoming flows to the DMZ when possible
- Segment the OT network internally

General principle

Building a **resilient industrial network** reduces the attack surface against threats seeking to enter and propagate to the production. This requires **isolating** industrial equipment within a dedicated network, at least input/output filtered and equipped with a **DMZ** and finally developing **partitioning** into sub-networks.

Operational implementation

1. Install an IT/OT **firewall** to ensure isolation of the industrial network.
2. Configure a **DMZ** intended for assets shared or accessed from outside the OT.
3. Attach industrial network assets to **sub-networks** dedicated to their application.
4. Ensure that industrial assets are not exposed to the **Internet**.

Group available resources

- [Architecture Guideline - EN](#)
- [Network architecture diagram Template](#)

What's expected from the site

- ❑ Complete OT architecture diagram
- ❑ Flow Matrix(s)
- ❑ Implementation of a secure architecture

Cyber Maturity

The industrial network is not isolated: uncontrolled connections exist between industrial assets and the outside (IT or Internet). **0**

There is a dedicated industrial network and its connections to the outside (IT or Internet) are filtered by a firewall, but uncontrolled connections remain. **1**

All connections within the industrial network and with the outside (IT or Internet and all connections included) are documented and filtered by a firewall and a DMZ is used for exchanges with the outside of the OT. **2**

The OT is segmented/partitioned into sub-networks by type of assets. Filtering is performed between the different subnets. **3**

3.4.2. Requirements

FTB04 - R01 - All OT assets **must** be installed on a dedicated OT network, segmented from the rest of the networks.

FTB04 - R02 - A firewall **must** be implemented at the interconnection of OT network with other external networks (IT network, 3rd party network, Internet, etc.).

FTB04 - R03 - Interconnections between OT and external networks **must** be minimised, to reduce the attack surface.

FTB04 - R04 - Restricted firewall rules **must** be implemented in the firewall and only allow legitimate communications, either wired or wireless (limited source IP address, destination IP address, port and services). The directive "any" **must** be prohibited, or limited to the strict necessary.

FTB04 - R05 - A DMZ (Demilitarized Zone) **must** be implemented between the OT network and the external networks to further protect incoming and outgoing communications to the OT. All communications between IT and OT **must** be subject to a protocol break, or at least flow analysis.

FTB04 - R06 - Data **should** be pushed to the DMZ and pulled from the DMZ. Exceptions **should** be justified.

FTB04 - R07 - All network flows **must** be inventoried within a network flow matrix (source IP address, destination IP address, protocol, port, description) with an identification and a documentation of all legitimate network flows.

FTB04 - R08 - Direct communications between OT and the Internet (including Cloud resources) **must** be prohibited.

FTB04 - R09 - If a wireless network is necessary for OT, it **must** be dedicated to OT and follow firewall, authentication and encryption best practices.

FTB04 - R10 - Network segmentation **must** be implemented as well within the OT network. The segmentation can follow the Purdue model and/or the use of different applications within the site, especially when different parties are involved. Here are possible examples of segmented zones within the OT network:

- DMZ, including assets communicated outside the network, such as the remote access solution or the antivirus,
- Supervision network with the SCADA/DCS servers and workstations,
- Production network with PLCs, sensors and actuators,
- Infrastructure network with services such as backup, NTP, Active Directory, etc.
- Administration network with dedicated workstations,
- Isolated zones dedicated to each type of system and/or supplier, ensuring communication flows vertically.

This network organisation has to be adapted depending on site requirements and activities.

FTB04 - R11 - Dedicated administration and engineering workstations **must** be used and comply with the following principles:

- Engineering workstations dedicated to PLC programming and OT devices management,
- Administration workstations authorised only for network and system administration,
- Not connected outside of the OT network,
- Hard drive encrypted.

FTB04 - R12 - All communications going in or out of the OT network **must** be authenticated and encrypted wherever possible.

FTB04 - R13 - Two sets of firewalls **should** be implemented on each critical site:

- One dedicated to IT/OT segmentation,
- One to segment the OT network internally.

3.5. FTB-05 - Remote Access

3.5.1. Reminder of [FTB-05](#)

5. Remote Access

Secure remote access to OT assets must be implemented

Do you have a secure remote access process ?

Remote access solution with the following characteristics: Present in a DMZ / Use of nominative accounts / 2FA authentication / Encryption of the communication / Monitoring and recording of the communication / Limited access to the network / Process respecting the account management policy (access reviews, least privilege principle, etc.)

General principle

Controlling all remote accesses to the OT assets is vital to restrict direct exposure outside the industrial site, and in particular on the internet, of production infrastructures, in reading and controlling the industrial process. It is necessary to **limit these accesses** (people, remote access solutions) and to **secure these connections** (authentication, encryption, etc.).

Operational implementation

1. **Streamline** remote access: number of authorized users and machines, targeted assets, access validation workflow, etc.
2. Implement a **centralized remote access solution**
3. Use **nominative accounts** for all users
4. Implement **strong authentication and encryption** of associated flows.
5. **Trace** all actions performed remotely.

Group available resources

- [Architecture Guideline \(chapter on remote access\) - FN](#)

What's expected from the site

- ❑ List of stakeholders with a need for remote access to the industrial network present in the inventory
- ❑ Description of the remote access solution

Cyber Maturity

0 Direct remote access to the OT is not controlled: non-validated solutions, simple authentication, extended access, lack of documentation...

1 Remote access is rationalized, in number, users and scope. Accesses are performed with a protocol break (DMZ). Access is targeted and the process is documented.

2 Any remote access solution to the production network is validated and its different uses justified by a business need (eg: remote maintenance). Their accesses are traced and require MFA.

3 All industrial remote access is carried out using a solution that complies with the Group Industrial cybersecurity policy. Sessions are logged and privileged access is validated.

Priority 1

3.5.2. Requirements

FTB05 - R01 - All remote access needs **must** be identified and documented.

FTB05 - R02 - Only remote access solutions validated by the business unit **must** be allowed. All others **must** be disabled/prohibited by default.

FTB05 - R03 - All remote access connections **must** be authenticated with a nominative account.

FTB05 - R04 - Each user **must** have limited rights and access on the OT network (least privilege principle).

FTB05 - R05 - MFA **must** be enforced for all remote access to the site network.

FTB05 - R06 - All remote access communications **must** be logged and monitored to include all the relevant information to identify connections and trace all the actions performed on the OT equipment.

FTB05 - R07 - Remote access communications **must** be encrypted.

FTB05 - R08 - Remote access solution **must** be hosted in a DMZ.

FTB05 - R09 - All accesses from the Internet **should** access OT through a DMZ with a dedicated OT jump host for OT-specific communications. This system **should** leverage its own identity and access management system.

FTB05 - R10 - If possible, remote access **should** only be enabled when needed, that can be done logically or physically.

What the business unit can bring:

- A dedicated and central remote access solution **should** be put in place at the **business unit** level. The solution can be implemented in a central OT DMZ for the **business unit**.

3.6. FTB-06 - Backup & Recovery

3.6.1. Reminder of [FTB-06](#)

6. Backup & Restore

Necessary backups must be implemented, copied offline and tested regularly
Is there a documented and implemented backup management procedure that takes into account the complete backup of industrial equipment, recovery tests, offline data storage and business data retention?

General principle
Mastering the **backup and restoration** of the entire OT makes it possible to be able to **react in the event of an incident** (hardware failure, cyber attack, etc.) and quickly bring production back to a degraded but acceptable operating mode, without major consequence on the **data and industrial processes** deployed.

Operational implementation

1. Define and formalize a **backup plan** for all systems in the OT scope (backup owner, backup data, backup methodology, online storage, offline storage, frequency, retention)
2. **Perform backups** using different storage media (connected to the network, offline, on a cloud). Always have an **offline copy** of your backup.
3. Document **operational procedure** for backup & restore
4. Regularly **test** the restore procedure on samples from the OT to verify the integrity of the backups.

Group available resources

- [ICS Guideline - Maintenance in security conditions](#)
- [Backup & Restore guideline - EN](#)
- [Backup & Restore procedure template - EN](#)

What's expected from the site

- ☐ Local backup & restore backup plan
- ☐ Operational backup & restore procedure

Cyber Maturity

No formal OT backup and restore process is developed. **0**

A backup process covering critical data and systems (SCADA, PLC programs and configurations, etc.) is applied following changes or during maintenance periods. **1**

The backup process concerns all assets. Data is backed up and available offline. Unitary restoration tests are carried out. **2**

The backup process is automated as much as possible and performed periodically according to the criticality of the assets. The restoration process is regularly tested for improvement. **3**

3.6.2. Requirements

FTB06 - R01 - A backup plan **must** be formalised for the site OT entities. It **must** include all relevant information: system name and function, supplier, data, data storage, backup owner, backup methodology, online and offline backup media, frequency, retention, and any comments.

FTB06 - R02 - Asset backups **must** be performed on all industrial equipment according to the backup plan.

FTB06 - R03 - An offline copy of the backup **must** be performed for each industrial asset (on an external hard drive or a Google Shared Drive for example) according to the backup plan.

FTB06 - R04 - A backup and restore procedure **must** be formalised for the site OT perimeter.

FTB06 - R05 - Restoration tests **must** be performed on a regular basis (e.g. once a year). The restoration tests can be partial (e.g. on specific assets) or complete (e.g. on all OT assets).

FTB06 - R06 - All backups **must** be physically protected or encrypted.

FTB06 - R07 - Offline backup **should** be stored outside of the site (e.g. another place or site).

3.7. FTB-07 - Sites / Contracts Inventory

This section is under the **business unit's** responsibility.

3.7.1. Reminder of [FTB-07](#)

7. Sites/contracts inventory

An inventory of all industrial sites / contracts must be formalized and kept up to date at the entity level

Are all contracts and plants listed with an identification of their criticality performed on a regularly basis at the entity level?

General principle
It is essential to have the **list of sites and contracts** in order to know the entire perimeter to be secured. **Identifying the risks** inherent in industrial site activity is essential to prioritizing a **cybersecurity action plan**.

Operational implementation

1. Formalize the **list of contracts** with local authorities/customers.
2. List the factories/plants/industrial sites included in these contracts.
3. Specify the **level of criticality** of each plant and contract, both on the basis of proven risks.

Priority 2

Group available resources

- To be defined

What's expected from the site

- List of contracts/sites with their level of criticality

Cyber Maturity

There is no list of sites and contracts. **0**

A partial list of contracts and sites has been formalized. **1**

Contracts and sites are completely listed. **2**

All contracts and sites are subject to a regular criticality assessment based on a risk analysis. **3**

3.7.2. Requirements

FTB07 - R01 - All contracts and sites of the **business unit must** be listed in an inventory.

FTB07 - R02 - The **business unit must** classify each industrial installation following its criticality.

FTB07 - R03 - The **business unit CISO must** be informed when a new site is managed by the business unit or when a site is no longer part of Veolia. All new contracts and sites **must** be reported to sites/contracts inventory.

3.8. FTB-08 - Identity & Access Management

3.8.1. Reminder of [FTB-08](#)

8. Identity & Access Management

Accounts allowing access to OT assets must be managed through proper identification, authentication and access rights

Is there a documented and enforced process for access control, account and password management and access rights that takes into account the criticality of assets and user authorization? Use of nominative accounts / Strong password policy / Respect of least privilege principle / Dedicated accounts for administration / Regular account reviews

General principle

Proper **identification**, **authentication** and **access rights** of **system and application accounts** guarantees access to plant resources (data, processes, etc.) **only to people authorized** to acquire (read) and manipulate (write) them. This also reduces the **risk of modification** (accidental or voluntary) of data critical to the proper functioning of the industrial site and makes it possible to individually trace the sensitive actions carried out on the system (system and application logs). As the password is the main authentication factor, it is crucial to generalize its use and prevent its bypass by applying **strict rules** (sharing, complexity, renewal).

Operational implementation

1. Implement **nominative accounts** on **supervision** applications for **write access**.
2. Implement **nominative accounts** dedicated to **administration** and **remote access** on all assets.
3. For each type of machine in the industrial perimeter, apply a **robust password policy** adapted to the type of machine and its use (length, complexity, lifespan) and store passwords securely (e.g.: passwords managers).
4. Disable when possible default, generic, and unused accounts and change default passwords.
5. Apply the principle of **least privilege**: users have necessary and sufficient roles.
6. Perform an **annual review of accounts**, renew passwords annually and justify each security exception / trace the implemented countermeasures.

Group available resources

- [ICS Veolia Policy - Password Chapter - EN](#)
- [User Management Security Policy - EN](#)
- [User account and access management Guideline - EN](#)

What's expected from the site

- ❑ Accounts inventory
- ❑ Local procedure for managing accounts and passwords
- ❑ Extract of password strategy for workstations and servers

Cyber Maturity

0

Accounts and passwords are not subject to any particular policy. Default and generic accounts or passwords are mostly used and unused accounts remain.

1

Some workstations and servers comply with an account management policy. Basic hygiene principles are respected, at least for administration tasks: nominative accounts, no default password, periodic renewal, etc.

2

All workstations and servers comply with an account management policy adapted to their criticality. The authentication of administration accounts is subject to a strict policy imposing criteria of length, complexity and periodic renewal. Exceptions are listed and justified.

3

All accounts and accesses are inventoried and subject to an annual rights review. Authentication follows a strict policy. The entry/exit process is applied to all users (agents, service providers, etc.). Exceptions are justified and traced.

3.8.2. Requirements

FTB08 - R01 - An identity and access management process **must** be documented following those four topics: identification, authentication, access control and administration accounts.

FTB08 - R02 - Accounts **must** be nominative, both at the application level for modification access and the system level.

FTB08 - R03 - Generic accounts **must** be avoided everywhere it is technically possible.

FTB08 - R04 - When a generic account is used, it **must**:

- Be inventoried,
- Not have elevated privileges,
- Be valid on a limited number of machines,
- Have a justification.

FTB08 - R05 - All passwords **must** be compliant with the [PO-TSE 004 User Management Security Policy](#). For the OT environment, passwords can be changed annually.

FTB08 - R06 - Default passwords used for example for service accounts, databases, applications, and access in console mode (PLC, gateways, network devices), **must** be changed, according to the [PO-TSE 004 User Management Security Policy](#).

FTB08 - R07 - Passwords of generic accounts **must** be changed when someone leaves the site.

FTB08 - R08 - The least privilege principle **must** be applied to every OT application and system. Only necessary rights **must** be granted to users and administration privileges **must** not be granted by default.

FTB08 - R09 - All accounts **must** be listed in a user's inventory.

FTB08 - R10 - All accounts, including remote access accounts and third-party accounts, **must** be reviewed annually. A noteworthy attention **must** be paid to privileged accounts.

FTB08 - R11 - All default accounts **must** be disabled when technically possible.

FTB08 - R12 - A check-out / check-in process **must** be documented and applied to make sure that when an employee leaves the company, all accounts and access rights are removed from all OT components in a timely manner.

FTB08 - R13 - Dedicated nominative accounts **must** be implemented for system administration on servers, workstations, firewalls and network switches.

FTB08 - R14 - Passwords **must** be stored securely in password managers.

FTB08 - R15 - An Active Directory **can** be implemented for OT authentication at the application or system level. The Active Directory **must** be dedicated to OT, with no trust relationship with an IT Active Directory. The Active Directory **must** be hardened and follow the Microsoft tiering model.

Implementation advice:

- No authentication is required for read-only access on supervision applications.
- Autologon can be configured for operation workstations in the control room. A robust password must be configured.

What the business unit can bring:

- A central OT Active Directory **can** be implemented at the **business unit** level. The number of Active Directory and the OU (Organisation Unit) organisation must be adapted to the **business unit**.

3.9. FTB-09 - Antivirus / EDR

3.9.1. Reminder [FTB-09](#)

9. Antivirus/EDR
An antivirus and/or EDR must be installed on all OT workstations and servers
Is there an Antivirus/EDR deployed on the workstations and servers?

Priority 2

General principle
Ensuring relevant **antivirus/EDR protection** with **daily signatures updates** limits the exposure of the OT to known attacks.

Operational implementation

1. Generalize the deployment of an **antivirus/EDR** on all workstations and servers.
2. Implement a **daily antivirus update process**.

Group available resources

- To be defined

What's expected from the site

- ❑ Installation of an antivirus/EDR

Cyber Maturity

- 0** There is no antivirus/EDR on servers and workstations.
- 1** Some of the workstations and servers have an antivirus.
- 2** Antiviral databases are regularly updated at least on critical assets.
- 3** All OT assets have an antivirus/EDR with daily updates.

3.9.2. Requirements

FTB09 - R01 - All workstations and servers **must** have an antivirus installed.

FTB09 - R02 - All workstations and servers **must** have their antivirus database updated daily.

FTB09 - R03 - When used, the EDR (Endpoint Detection and Response) **must** be updated on a regular basis.

FTB09 - R04 - An EDR (Endpoint Detection and Response) **should** be installed on the OT perimeter when possible and compatible (servers and workstations with recent OS). Therefore, the EDR, if possible, is a replacement for the antivirus.

3.10. FTB-10 - System Hardening

3.10.1. Reminder [FTB-10](#)

10. System Hardening

Hardening measures must be implemented on all OT assets

Is there an asset configuration hardening in place (workstations, servers, network equipments, PLCs)?

General principle

Restricting the capabilities of OT devices involves **granular filtering** on each device, **disabling non-essential services** and **blocking unused ports**, if possible through the machine's local firewall.

Operational implementation

1. Define and implement a local **hardening** procedure for OT workstations and servers.
 - a. Disable or even delete non-essential or unused services or programs (e.g. network sharing).
 - b. Enable local firewall when possible.
2. Define and implement **hardening** measures on network devices
3. Define and implement **hardening** measures on PLCs and other OT devices

Group available resources

- [PRO-TSE-01 - ICS Security Procedure - Switch Hirschmann - EN](#)
- [Windows Hardening Guideline - EN](#) [To publish]

What's expected from the site

- ❑ Hardening procedures (workstation, servers, network devices, PLCs)
- ❑ Hardening follow-up document

Priority 2

Cyber Maturity

The software configuration of OT assets is not listed (open ports, types of flows, etc.) and no hardening is implemented **0**

A few hardening measures are implemented on some OT assets (Non-essential services/protocols are disabled). **1**

Main hardening measures are implemented on critical industrial assets (supervision workstation, SCADA, main OT switches/firewalls). For example: secure version of protocols are used, non-essential services are disabled, filtering rules are configured. **2**

Hardening measures are implemented on all OT assets including servers, workstations, network devices, PLCs and other OT devices and hardening is controlled/monitored. **3**

3.10.2. Requirements

FTB10 - R01 - Hardening measures **must** be implemented on workstations and servers.

FTB10 - R02 - Hardening measures **must** be implemented on network devices (firewalls and switches).

FTB10 - R03 - Hardening measures **must** be implemented on OT devices such as PLCs, where possible.

FTB10 - R04 - All unused programs, software, network ports, protocols or services running on any OT component **must** be removed or disabled.

FTB10 - R05 - Hardening measures for all OT assets **must** be documented in a procedure.

FTB10 - R06 - Laptops **must** have their hard drive encrypted.

Implementation advice: Hardening measures usually include the following:

- Uninstall all unnecessary software or programs,
- Disable unused ports or services such as SMB or RDP on Windows machines, or HTTP, FTP, SSH on network devices,
- Harden necessary services and protocols, for example:
 - SMB: disable SMBv1, enable SMB signing
 - RDP: harden encryption parameters
 - Use the encrypted version of protocols: HTTPS vs HTTP, SFTP vs FTP

- SNMP: disable SNMP v1/v2 or change default community names
- Disable unused network ports on network devices,
- Etc.

3.11. FTB-11 - Incident & Crisis Management

3.11.1. Reminder [FTB-11](#)

11. Incident & Crisis Management

An incident and crisis management process must be defined and implemented

*Is there an incident management plan, including reporting of incident to the entity CISO and Group Cybersecurity, and a crisis management plan, including cybersecurity event scenarios, documented?**

General principle

Putting in place a cybersecurity incident and crisis management process allows all stakeholders to have the right security reflexes in the event of an incident. This allows rapid acknowledgement and efficient handling of incidents to limit any possible spread. Good crisis management allows rapid decision-making and to address the required people and authorities.

Operational implementation

1. Develop **operational procedures** applicable in the event of a cybersecurity incident or crisis (classification of the incident/crisis, definition of roles and responsibilities, processing, etc.).
2. Formalize an **alert escalation procedure** so that the CISO of the entity and the Group are informed of the incident or crisis.
3. Periodically **test** incident/crisis management procedures in order to improve them (**crisis exercise**).
4. Formalize and update a **list of incidents** that have taken place on the site for traceability and to secure the OT accordingly.

Group available resources

- [ICS Guideline - Incident & Crisis management](#)
- [Crisis management procedure - EN](#)
- [Crisis management Poster - Exec Sum - EN](#)
- [Crisis management toolkit - EN](#)

What's expected from the site

- ☐ Incident management plan
- ☐ Crisis management procedure
- ☐ Crisis exercise debrief

*Note: the process should be defined at the entity level and then shared to industrial sites and adapted locally when necessary

Cyber Maturity

No cybersecurity incidents and crises management process is formalized for the OT. No report is made. 0

An incident management process is formalized for critical OT assets. 1

An incident management process is formalized for all OT assets. The incident escalation procedure takes into account the CISO of the entity and the Group. A crisis management process is formalized. 2

The incident and crisis management process is regularly tested and improved. The reporting procedure is updated regularly. 3

3.11.2. Requirements

FTB11 - R01 - An incident management plan defining roles as well as phases of incident handling/management **must** be documented.

FTB11 - R02 - A cyber crisis management procedure **must** be defined and documented, including industrial cybersecurity event scenarios, as well as an escalation process.

FTB11 - R03 - In case of compromise, the site **must** have the ability to isolate itself from other networks (IT, Internet, third-party network, etc.). This can be formalised through a red button procedure.

FTB11 - R04 - A crisis management exercise simulating a cyber attack **must** be organised on-site.

FTB11 - R05 - A list of all cybersecurity incidents that took place **should** be maintained and annually reviewed in order to learn from previous experiences.

FTB11 - R06 - Incident posters **should** be displayed on-site to help users memorise and have good reflexes in case of an incident.

Implementation advice:

- Many documents and procedures can be provided at the business unit level, and do not need to be formalised for each individual site (incident and crisis management procedure).
- IT documents can usually be applicable to OT.

What the business unit can bring:

- At the **business unit** level, a cyber incident management plan and a cyber crisis management procedure **should** be defined, documented and applied to all industrial sites.
- In case of compromise, the **business unit should** have the ability to isolate a specific site.
- At the **business unit** level crisis management exercises simulating a cyber attack **should** be organised on multiple industrial sites.

3.12. FTB-12 - BCP / DRP

3.12.1. Reminder [FTB-12](#)

Priority 2

12. BCP/DRP

Business continuity and disaster recovery process must be defined and implemented
Is there a BCP/DRP documentation and processes in place that include industrial cybersecurity aspects?

General principle
Implementing a **DRP** process allows **rapid reconstruction or recovery** of activity (nominal or degraded mode) following an incident, or even a disaster. The **BCP** allows to **identify critical activities** for production to **avoid any interruption** (switch to manual mode for example). These plans must be **tested** to ensure their effectiveness under operational conditions.

Operational implementation

1. Develop a **Business Continuity Plan** and a **Disaster Recovery Plan**, linked to the business, or include industrial cybersecurity in existing procedures.
2. Formalize a technical operational procedure for **rebuilding the systems** (including a prioritization of the assets to be rebuilt, as well as the minimum assets to be rebuilt to restart the activity)
3. Periodically **test** the BCP/DRP in order to improve them and carry out a **reconstruction exercise** (at least the main control system)

Group available resources

- [Disaster Recovery Plan - EN](#)

What's expected from the site

- ☐ BCP
- ☐ DRP
- ☐ Systems Rebuild Operational Procedure

Cyber Maturity

No BCP/DRP is defined for the site. **0**

A DRP is defined for critical assets. It defines the degraded mode and the reconstruction or recovery procedures. **1**

A BCP is consolidated and applicable to critical OT assets. It details the roles, objectives, escalation steps, detailed operational procedures, etc. **2**

A complete BCP and DRP are consolidated and applicable to the OT. They are regularly tested and improved: reconstruction tests, feedback from stakeholders, etc. **3**

3.12.2. Requirements

FTB12 - R01 - IT disruption and OT cyber attack scenarios **must** be taken into account in the BCP (Business Continuity Plan) managed by the business.

FTB12 - R02 - A DRP (Disaster Recovery Plan) **must** be formalised for the OT perimeter at the site level. It can include:

- Roles and responsibilities, including emergency contacts, and suppliers,
- Systems business impact analysis and prioritisation,
- Degraded mode,
- Minimum requirements to rebuild OT systems,
- Recovery procedure,
- etc.

FTB12 - R03 - An operational system rebuilding procedure with a prioritisation of assets to be rebuilt **must** be formalised. It can either be on its own or included in the DRP.

FTB12 - R04 - BCP and DRP **must** be periodically tested and improved through reconstruction exercises. Tests can occur on the whole OT perimeter or just on parts of it according to asset criticality.

3.13. FTB-13 - Obsolescence Management

3.13.1. Reminder [FTB-13](#)

13. Obsolescence Management

Obsolescence of assets must be managed

Are obsolete assets formally tracked within the asset inventory? Is there an obsolescence remediation plan?

General principle

Controlling the obsolescence of the industrial scope limits the vulnerabilities of its assets and software, thus allowing it to be maintained in security conditions over time. It is important to anticipate the renewals of this system in order to improve the overall OT cybersecurity of the site. Especially since the newer solutions generally offer more cybersecurity functions.

Operational implementation

1. Identify **obsolete assets and software** as well as related vulnerabilities.
2. Implement a short, medium and long term **renewal plan**.
3. Integrate requirements into contracts, tenders, etc. ensuring the support and maintenance of solutions over time.

Group available resources

- Nozomi

What's expected from the site

- ❑ List of "end of support" dates for devices and software (included in the inventory template, but information could be provided with Nozomi or with a dedicated follow-up file)
- ❑ Obsolescence remediation plan

Priority 3

Cyber Maturity

The obsolescence of assets and software is not subject to specific monitoring and no renewal is planned. **0**

The obsolescence of the main assets and software is globally identified and ad-hoc replacement measures are studied. **1**

The obsolescence of critical assets and software is formally inventoried. A renewal program is defined and resources are allocated to it. **2**

Measures limiting the obsolescence of all assets and software are anticipated and integrated into contracts: system version upgrades, software updates, support, etc. **3**

3.13.2. Requirements

FTB13 - R01 - Obsolete assets (hardware) **must** be formally tracked within the asset inventory.

FTB13 - R02 - Obsolete software **must** be formally tracked within the asset inventory.

FTB13 - R03 - A renewal plan **must** be identified and formalised in short, medium and/or long term.

FTB13 - R04 - The renewal plan **must** include a tracking of the end of the contract or version of software and hardware.

Implementation advice:

- Obsolescence is a reality in the OT environment. The policy is not asking to have 0 obsolescence but to manage obsolescence through inventory and renewal plan, even if the plan is a long-term one.

3.14. FTB-14 - Vulnerability & Patch Management

3.14.1. Reminder FTB-14

14. Vulnerability & Patch Management

Vulnerabilities must be identified on OT assets and appropriate patches implemented for remediation

Is there a patch management process defined, documented and applied at plant level associated with a vulnerability management process to ensure related-risks are managed appropriately?

General principle

Installing the latest available security patches quickly reduces OT exposure to known preventable attacks. Beyond defining a frequency and deadlines for application, this requires the implementation of a vulnerability management process, reflected in **detailed monitoring of all software versions** deployed, **monitoring of their vulnerabilities** and **remediation plan** associated with their criticality.

Operational implementation

1. Implement a **local patch management procedure** taking into account the frequency and application deadlines on each type of assets. Justify exceptions.
2. Implement a **security watch** of available critical patches and analyze the possibility of deploying them on sensitive assets as a matter of urgency. Do this on network devices (firewalls) exposed on the Internet and on the IT network.
3. Implement a mechanism for **detecting vulnerabilities** and alerting in order to strengthen monitoring (e.g. Nozomi industrial probe).

Group available resources

- [Maintenance in security conditions Guideline - EN](#)
- Nozomi

What's expected from the site

- Local patch management procedure

Cyber Maturity

There is no process for tracking OT vulnerabilities. No recent patch is installed. **0**

A patch management process exists and monitoring of OT vulnerabilities allows to identify critical patches, installed ad-hoc. **1**

The patch management process is broken down by type of assets throughout the OT. It specifies the frequency and deadlines for applying the patches. Software update monitoring is performed for critical assets. **2**

Vulnerability monitoring is reinforced by a mechanism for detecting and alerting anomalies and vulnerabilities within the OT (e.g. Nozomi industrial probe). A list of missing patches is formalized. **3**

3.14.2. Requirements

FTB14 - R01 - A vulnerability management process **must** be documented in order to make sure that:

- All vulnerabilities are:
 - Identified,
 - Tracked,
- All related risks are:
 - Assessed,
 - Treated (remediation, mitigation or acceptance).

All of this must be done in a timely manner.

FTB14 - R02 - A periodical patch management process, automated or manual, that suits the functional constraints and risks of patching **must** be defined, documented and applied at site level.

FTB14 - R03 - A specific procedure for urgent patching **must** be formalised for critical vulnerabilities.

FTB14 - R04 - Automated vulnerability scans **should** be performed on a regular basis against systems exposed (within DMZ, within OT exposed to a third-party network) and alert if vulnerabilities are detected on a system.

Implementation advice:

- OT devices exposed to external networks (such as firewalls and assets in the DMZ) should be patched more frequently than other OT assets.
- OT assets in the core OT network can be patched only annually.
- It is not necessary to patch old PLCs as they do not offer cybersecurity functionalities.

3.15. FTB-15 - USB Prevention

3.15.1. Reminder [FTB-15](#)

15. USB Prevention

The use of removable media must be controlled

Are USB keys sanitized before being connected to industrial workstations to avoid the introduction of malware within the OT environment and disabled for non admin usage?

General principle

Restricting the use of removable media (USB) limits the direct attack surface inside the site. This involves cleaning authorized media (virus scanning), which must be identified and kept protected. Also, USB ports should not be enabled for users who do not need them.

Operational implementation

1. Define and implement a local procedure for managing USB devices (dedicated USB key, whitelist, storage, cleaning via antivirus scan, etc.).
2. Disable the use of USB devices on all workstations and servers that do not need them (justify the exceptions).
3. Install a white station to sanitize USB devices or use a dedicated file sharing solution and ban USB media.
4. If using a white station, block the use of USB devices that have not been verified by this white station.

Group available resources

- [Poster USB devices good practices](#)
- [Malware cleaner documentation - configuration guide - EN](#)
- [Malware cleaner documentation - user guide - EN](#)

What's expected from the site

- ☐ Procedure for managing USB removable media
- ☐ Awareness

Cyber Maturity

Removable media are not subject to any dedicated security constraints or procedures. 0

The use of removable media is only regulated on critical machines. It is justified by a business need, restricted to identified systems and people. 1

The use of removable media peripherals is regulated throughout the OT scope. It is justified by a business need, restricted to identified systems and people. 2

The use of removable media is strictly regulated and subject to a security procedure: identified and physically protected devices, antivirus analysis (ex: white station), formatting, etc. 3

3.15.2. Requirements

FTB15 - R01 - All USBs' key use cases and needs **must** be identified to protect their use.

FTB15 - R02 - Dedicated USB keys **must** be used for OT (no personal or IT USB keys for example).

FTB15 - R03 - All USB keys **must** be scanned through an antivirus before being connected to an OT asset.

FTB15 - R04 - USB ports **must** be disabled on all machines where USB keys are not required.

FTB15 - R05 - A procedure on how to manage USB devices **should** be formalised for the site.

FTB15 - R06 - A clean station **should** be installed on-site to analyse USB keys for viruses.

FTB15 - R07 - An agent **should** be installed on machines to make sure that the USB devices are scanned by the clean station before being plugged into OT.

FTB15 - R08 - Only USB storage devices that have been explicitly approved and authorised **should** be permitted for use, to mitigate the risk of data breaches and malware infections.

Implementation advice:

- The use of USB devices can be banned completely and replaced by another file exchange solution, such as an SFTP server hosted in a DMZ.

3.16. FTB-16 - Detection - Logging & Monitoring

3.16.1. Reminder [FTB-16](#)

16. Detection - Logging & Monitoring

Logs must be implemented on OT assets and sent to a central collection point for correlation and analysis

Are event logs with relevant security information (source, date, user and timestamps) implemented on the systems that support them? Are these logs collected into a SIEM and analyzed by a SOC?*

General principle
Ensuring the **logging** of all OT assets allows to **trace security events** and **trace the actions** of users, services, etc. Their **centralization** and **use** allows, following a failure or an attack, to identify its origin and facilitates the development of a remediation plan.

Operational implementation

1. Identify **assets** in the industrial environment to prioritize for logging activation.
2. Identify the information to be collected on all the assets allowing it and **activate logging**: user connections, use of administrative rights, etc.
3. **Centralize the logs** collected locally on the industrial network.
4. Implement a correlation/analysis of logs (ex: **SOC**).

Group available resources

- [Log management Policy - EN](#)
- [Log management Policy settings - EN](#)

What's expected from the site

- ☐ Enabling logging on industrial assets
- ☐ Integration of the industrial scope into the SOC

*Note: the SOC should be implemented at entity or Group level

Cyber Maturity

Logging is not enabled on the industrial environment. **0**

The main events on the industrial environment are collected locally (connections, administration actions, etc.). **1**

All the events to be collected locally on the industrial environment are precisely configured. Clock synchronization is performed. **2**

All recorded logs are centralized (eg Syslog) and analyzed (eg SOC). Incidents reported are analyzed and enriched with feedback from stakeholders (users, administrators, etc.). **3**

3.16.2. Requirements

FTB16 - R01 - Events logs **must** be configured on systems that support it and stored locally.

FTB16 - R02 - All devices that support time synchronisation **must** be synchronised from a global and consistent time source so that timestamps in logs are consistent.

FTB16 - R03 - Log **must** be collected, either locally on-site or centrally at the business unit level.

FTB16 - R04 - Appropriate logs **must** be identified and aggregated to a SIEM (Security Information and Event Management) for collection and correlation.

FTB16 - R05 - Logs **must** be sent to a Global SOC for analysis, review and security monitoring.

FTB16 - R06 - A network probe **should** be implemented to enhance OT detection capabilities.

What the business unit can bring:

- A SIEM (Security Information and Event Management) **should** be implemented at the **business unit** level to analyse logs.
- OT logs **should** be sent to a Global SOC for analysis, review and security monitoring.

3.17. FTB-17 - Risk Management

3.17.1. Reminder [FTB-17](#)

17. Risk Management

A risk based approach must be followed to identify appropriate measures to be implemented

*Has a risk analysis been conducted, validated by the business, and a budget allocated to deploy the appropriate action plan?**

General principle
To define the appropriate OT cybersecurity **strategy** and raise the global **maturity level** of an industrial site, it is key to follow a **risk-based approach** to **prioritize** the right projects, define a **pragmatic action plan** and planning, and allocate the right resources and budget.

Operational implementation

1. Perform a **risk analysis** for the industrial site
2. Develop an OT cybersecurity **roadmap** and action plan and formalize the associated **budget**.
3. Plan and **communicate** the application of this roadmap as well as the associated expenses.

Group available resources

- To be defined

What's expected from the site

- ☐ Risk analysis
- ☐ Formalization of an OT cybersecurity roadmap with associated costs

*Note: A risk analysis should be conducted at the entity level first to define appropriate action plan and budget globally and then site specific risk analysis should be conducted when relevant

Cyber Maturity

0
Cyber is not a project: no risk analysis is performed, cyber is not the subject of any specific allocation of funds, even in current contracts.

1
Some OT cyber actions are planned in the short term, human resources are allocated. However they do not rely on any risk analysis.

2
A risk analysis is performed and a medium-term site security action program is in place. A budget is available but not dedicated to industrial cyber. The entity is informed of the planned actions and the associated needs.

3
OT cyber is the subject of a real action plan, following a detailed risk analysis, monitored on the basis of a cyber budget dedicated to OT and adequate human resources. The entity is regularly involved and consulted on the actions to be implemented.

3.17.2. Requirements

FTB17 - R01 - A risk analysis **must** be performed at the site level, to help prioritise cybersecurity activities. All risks identified **must**:

- be taken into account;
- have adequate compensatory measures;
- be added to the risk treatment plan;
- accepted and validated by the relevant authorities.

FTB17 - R02 - An action plan and an OT roadmap **must** be defined following the risk analysis, and include the necessary resources and budget.

FTB17 - R03 - The roadmap and its implementation **must** be followed and communicated to relevant stakeholders, including Top Management.

FTB17 - R04 - An inventory of all the applicable laws and regulations and their implications for Veolia (in terms of cybersecurity) **must** be maintained.

What the business unit can bring:

- An inventory of all the applicable laws and regulations and their implications for Veolia (in terms of cybersecurity) **should** be maintained at the **business unit** level.

3.18. FTB-18 - Audit & Control

3.18.1. Reminder [FTB-18](#)

18. Audit & Control

The level of cybersecurity must be controlled through regular assessments
*Are there periodic audits and/or self-assessments based on the Fix the Basics including the supplier's managed perimeter? Are results shared to the relevant stakeholders (the Group, clients, etc.)?**

General principle
Identifying the overall level of maturity of the site and its teams allows to specify the associated risks and technical needs. It is thus possible to **define the OT security actions** to be implemented quickly. **Involving the stakeholders** (entity, local authorities, etc.) at this level helps them take local stakes into account and allows to strengthen the support available to the site.

Operational implementation

1. Carry out the industrial cybersecurity maturity **self-assessment** each year and communicate it to entity managers.
2. Organize periodic industrial cybersecurity **audits**.
3. **Share results** to the relevant stakeholders (the Group, clients, etc.)

Group available resources

- 2024 Fix-The-Basics Framework - with detailed cyberlevel and cyberscore - can be use for sites assessment
- [Cyber maturity calculation sheet](#)

What's expected from the site

- ☐ Complete self-assessment (site)
- ☐ Audit report
- ☐ Consolidation of self-assessment at entity level and communication to the group

*Note: An assessment program must be defined at the entity level and implemented at site level

Cyber Maturity

The site's cybersecurity maturity level is neither evaluated nor communicated. **0**

The site's maturity is globally identified on the basis of an initial high-level self-assessment. **1**

The site assesses its maturity on the basis of a precise assessment. **2**

The maturity of the site is precisely identified on the basis of a third-party assessment (audit) communicated and periodically renewed. **3**

3.18.2. Requirements

FTB18 - R01 - A self-assessment **must** be performed regularly on the industrial site.

FTB18 - R02 - A precise assessment **must** be performed regularly on the industrial site (either by the Group, the zone or the business unit).

FTB18 - R03 - A 3rd party audit **must** be performed regularly on critical industrial sites.

FTB18 - R04 - Audits and self-assessment conclusions **must** be shared with all relevant stakeholders, including Top Management.

FTB18 - R05 - Penetration tests **should** be conducted on some sites based on the business unit's plan. Be careful while performing penetration tests directly on the production environment to avoid any impact on the site's activities.

What the business unit can bring:

- Each **business unit should** define and implement a self-assessment program for each industrial site, and adapt the frequency based on site criticality. Annual self-assessments **should** be performed on critical sites.
- Each **business unit should** define and implement a global audit plan based on the sites' criticality.
- An OT audit carried out by an independent third party **should** be conducted on some sites based on the **business unit's** plan.

3.19. FTB-19 - Security by Design

3.19.1. Reminder [FTB-19](#)

19. Security by Design

Cybersecurity must be taken into account from end to end in all projects
*Is OT cybersecurity taken into account from end to end in projects with the involvement of the entity CISO or the local OT correspondent? Provide Cybersecurity requirements during the project's conception phase and/or during the tenders / Validate the design / Control the implementation**

General principle
 Including cybersecurity in every stage of an industrial project guarantees the commissioning of **safe systems** and thus contributes to the **defense in depth** of the industrial site. Cybersecurity requirements and their verification on project delivery ensure **good control of the OT** and contribute to **maintaining it in secure conditions** over time.

Operational implementation

1. Implement local/entity follow-up of all the projects carried out on the OT allowing the **intervention** (risk analysis, definition of requirements, validation of the architecture, etc.) of an industrial cybersecurity manager **throughout the project**: consultation, specification, development, testing and validation.
2. Implement a **verification** of the compliance of the solutions delivered with cybersecurity requirements (FAT/SAT).

Group available resources

- To be defined

What's expected from the site

- ❑ Addition of a cyber clause in all future site/entity projects (new projects and renewals)

*Note: projects can be the construction of a new site, the installation of a solution on industrial site, etc.

Cyber Maturity

0
No industrial cybersecurity manager is involved in the site/entity's projects.

1
An industrial cybersecurity manager is consulted on projects with a cyber dimension.

2
An industrial cybersecurity manager defines cybersecurity requirements and ensures compliance with them in projects.

3
An industrial cybersecurity manager is involved in all project phases: design, specifications, development and compliance (FAT/SAT).

3.19.2. Requirements

FTB19 - R01 - A cybersecurity stakeholder **must** be informed and involved in any new OT projects to include cybersecurity in the project.

FTB19 - R02 - A cybersecurity due diligence **must** be conducted prior to the start of operations in specific new projects (buying a new plant or business unit) in order to prepare the application of minimum security measures.

FTB19 - R03 - A cybersecurity stakeholder **must** be involved during the project specification phase in order to provide high-level cybersecurity requirements and ensure that cybersecurity principles will be applied throughout the development.

FTB19 - R04 - OT cybersecurity requirements **must** be included in all tenders.

FTB19 - R05 - Risk evaluation of the project **must** be conducted under the responsibility of a cybersecurity stakeholder.

FTB19 - R06 - Residual risks **must** be formally accepted by Top Management.

FTB19 - R07 - A cybersecurity stakeholder **must** be involved during the design phase and present during the main gate/milestones reviews.

FTB19 - R08 - A verification of compliance with cybersecurity requirements **must** be done (FAT -Factory Acceptance Test- /SAT -Site Acceptance Test-) for all projects.

FTB19 - R09 - A cybersecurity audit **must** be conducted for all projects before systems commissioning.

FTB19 - R10 - Penetration testing **should** be completed:

- After a new industrial installation is commissioned,
- When an existing site is handed over from another vendor,
- After any major changes or upgrades to OT infrastructure or applications (e.g. DMZ, segmentation, new application).

Be careful while performing penetration tests directly on the production environment to avoid any impact on the site's activities.

FTB19 - R11 - Technical evaluations of products and IT/OT solutions **should** be undertaken.

What the business unit can bring:

- **Business units** **should** be involved in projects affecting multiple industrial sites.

3.20. FTB-20 - Third-Party Management

3.20.1. Reminder [FTB-20](#)

20. Third-party Management

Cybersecurity requirements must be defined, included in contracts with all third parties and their implementation controlled

*Are security requirements included and checked in tenders and contract with suppliers (incident handling, provision of security fixes, conditions for Remote Access or use of contractors' tools) ?**

General principle

In order to **increase the resilience** of the industrial site, it is necessary to **control its contractual relations** by formalizing **strict industrial cybersecurity requirements**. Ensuring **compliance** with all of these security principles with suppliers guarantees the **compliance** of the installations and allows them to be **maintained in security conditions** over time.

Operational implementation

1. Review all **contracts** with solution and service providers and verify the applicability of missing cybersecurity requirements in order to update them.
2. Integrate all industrial **cybersecurity requirements** (patches, AV, remote access, etc.) into any new contract.
3. **Check** contractors' compliance with requirements by means of tests (SAT - Site Acceptance Test).

Group available resources

- [Managing ICS cybersecurity in contracts with clients and suppliers Guideline - EN](#)
- [Due Diligence Guideline - EN](#)

What's expected from the site

- Contracts with cyber requirements

*Note: Contracts can be managed at the entity level when the same supplier operates at multiple sites

Cyber Maturity

Cybersecurity is not specifically integrated into supplier and service provider contracts. **0**

Generic cybersecurity requirements are incorporated into new contracts with vendors, maintainers, etc. **1**

OT-specific industrial cybersecurity requirements are integrated into all contracts (existing and new) with suppliers and service providers. **2**

The industrial cybersecurity requirements communicated to suppliers and service providers are subject to verification. **3**

3.20.2. Requirements

FTB20 - R01 - All contracts with 3rd parties **must** include cybersecurity requirements such as:

- Asset inventory and network diagrams,
- Device maintenance, including backups and patch management,
- Device hardening, including antivirus,
- Conditions for Remote Access,
- Incident handling,
- Use of contractors' tools,
- Audits.

FTB20 - R02 - Roles and responsibilities **must** be clearly defined in each contract.

FTB20 - R03 - Contractor's compliance **must** be verified periodically.

What the business unit can bring:

- If a 3rd party is involved on multiple sites of the **business unit**, a service agreement, defining mutual responsibilities in terms of cybersecurity, **should** be drawn up between this third party and the business unit.
- For sites not owned by Veolia, an appendix with OT cybersecurity activities conducted by Veolia **should** be added by the **business unit** to all bids to clearly position cybersecurity as a differentiator in the Veolia business offers.

4. Annexe

4.1. Glossary

Abbreviation	Meaning	Definition
BCP	Business Continuity Plan	A document that puts together all critical information needed to continue all operations during a disaster.
DCS	Distributed Control Systems	A solution that collects data to provide supervision/programming over industrial equipment (PLCs for example).
DMZ	Demilitarized Zone	Physical or logical subnetwork that contains services exposed to external networks (IT, Internet, third parties, etc.).
DRP	Disaster Recovery Plan	A document explaining the process to follow to execute recovery in case of a disaster.
EDR	Endpoint Detection and Response	A tool that can detect attacks and launch remediations against those attacks on endpoints.
FAT	Factory Acceptance Test	Test that is conducted on assets and/or software before their delivery to the site.
IT	Information Technology	Technology that protects, stores and manipulates data processes.
MFA	Multi-Factor Authentication	An additional layer of security is used to prevent unauthorized access to accounts even in the event of a password breach.
OT	Operational Technology	Technology that does, controls and monitors physical processes.
OU	Organisational Unit	Active Directory file that contains a group of components.
PLC	Programmable Logic Controller	An industrial device used to control and/or monitor other industrial assets (sensors, actuators).
SAT	Site Acceptance Test	A process used to verify that the assets and/or software are meeting the site's expectations.
SIEM	Security Information and Event Management	Solution collecting and correlating all threats detected within the network.

SOC	Security Operation Center	A Team that analyses, reviews and monitors all threats reported by the SIEM.
SCADA	Supervisory Control and Data Acquisition	A Solution that collects data to provide supervision over industrial equipment (PLCs for example).