Agrifood Cyberweerbaarheid

AgroConnect-winterseminar

24 November 2022

AgroConnect

Why this initiative?

- Because there is a need for knowledge and information sharing on IT/OT security solutions.
- Because there is a need for a harmonized and integral application of privacy & security legislation and standards (ISO, IEC, ISA, GDPR etc.)
- Because there is a need for a community that can speak for the agricultural sector on the topic of cyber security.

The initiative started with the collaboration of ForFarmers and Nutreco, followed by Vion, Royal Friesland Campina, Eurofins and De Heus. All providing their cyber security experts to help develop a cyber security sector standard, supported by other stakeholders.

The ‘Agrifood Cyberweerbaarheid’ project

- Bringing the cyber resilience of the sector to a higher level by:

1. Developing the cyber security baseline
   To be used by small, medium and large companies to determine where they stand with the level of cyber resilience.

2. Cyber Security assessment tool
   A cloud application for performing a cyber security resilience analysis.

3. Cyber Security workshops
   Series of workshops (physical and virtual) for the agricultural sector, for knowledge exchange and dissemination of information in the field of cyber resilience.

Agrifood Cyberweerbaarheid, project team

organisatie	persoon
De Heus	Michel Teuwen
Digital Trust Center (DTC)	Farid Boutiba
EurofinsAgro	Fred Verbeek
ForFarmers	Johan Rambi
ForFarmers	Yuri Weseman
Nutreco	Mirsad Murtic
Royal Friesland Campina	Maik Timmermans
Vion	Twan van Rhee
AgroConnect	Conny Graumans

Agrofood Cybersecurity, self-assessment tool

Developed by:

- Stark Narrative (Omara Naha) and Berkeley Bridge (Oskar Snijders), supported by Twan van Rhee (Vion, on behalf of the projectteam)
- Test-url: https://agroconnect-test.bridge-to-knowledge.nl/?modelname=agroconnect

Covers:

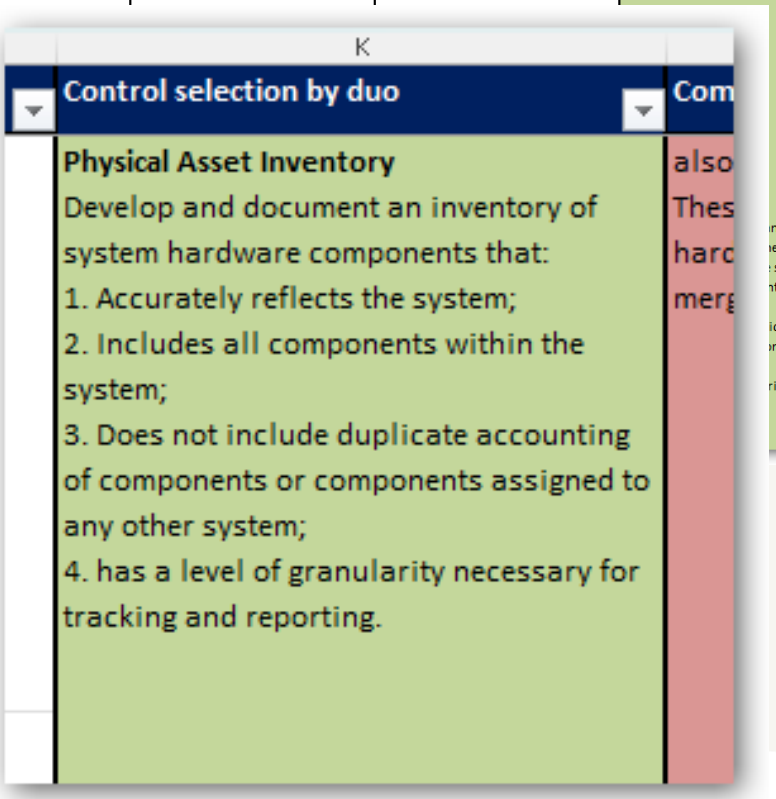
- IDENTIFY → PROTECT → DETECT → RESPOND → RECOVER

Based on the Agrifood Cybersecurity baseline.

Meant for cybersecurity experts in agrifood.

Agrofood Cybersecurity, baseline controls

Function	Category	Subcategory	Controls ISA 62443-3-3:2013	Controls ISF ICS	OWASP Top Ten	Control selection by duo	Comments
		ID.AM-1: Physical devices and systems within the organization are inventoried	SR 7.8 Control system component inventory The control system shall provide the capability to report the current list of installed components and their associated properties.	1.5 Network devices To support secure network communications, by: – enabling and controlling approved network devices – preventing unauthorised network traffic from disrupting ICS environments – protecting the confidentiality and integrity of data in transmitted to ICS environments and between ICS network zones.		**Physical Asset Inventory** Develop and document an inventory of system hardware components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. has a level of granularity necessary for tracking and reporting.	also inventory the parent/child relationship of the ci. These relationships can be both softw.are and hardware merge AM1+2 to 1 control
		ID.AM-2: Software platforms and applications within the organization are inventoried	SR 7.8 Control system cc The control system shall to report the current list components and their a			n inventory of ents that: system; nts within the icate accounting nents assigned to rity necessary for	also inventory the parent/child relationship of the ci. These relationships can be both softw.are and hardware merge AM1+2 to 1 control



AgroConnect

Agrofood Cybersecurity, selection controls

A	B	C	D	E	F
Function	**Category**	**Subcategory**	**Control selection by duo**	**Risk level**	**Assessment question**
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**Physical Asset Inventory** Develop and document an inventory of system hardware components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. has a le	Low	ID1. Is an inventory of system hardware components developed and documented, reflecting the complete IT/OT infrastructure?
		ID.AM-2: Software platforms and applications within the organization are inventoried	**Digital As** Develop a 1. Accurat 2. Include 3. Does nc 4. has a le	Low	ID2. Is an inventory of system software components developed and documented, reflecting the complete IT/OT infrastructure?
		ID.AM-3: Organizational communication and data flows are mapped	**Communi** Develop a 1. Accurat 2. Include 3. Does nc system; 4. has a le	Medium	ID3. Is an inventory of data communication components developed and documented, reflecting the complete IT/OT infrastructure interfaces?
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**Security C** Categoriz a. Identify b. Identify c. Identify d. Docum e. Verify t	Medium	ID4. Do the inventoried components of the IT/OT infrastructure have a security categorization based on e.g. classification, criticality and value to the business?
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**Security o** - Establish implemer - Impleme (prioritizi - Identify	Medium	ID5. Is a security organization established including roles & responsibilities for te entire workforce and stakeholders, security awareness and training programs and needed skills and competences?

Assessment question
ID1. Is an inventory of system hardware components developed and documented, reflecting the complete IT/OT infrastructure?
ID2. Is an inventory of system software components developed and documented, reflecting the complete IT/OT infrastructure?
ID3. Is an inventory of data communication components developed and documented, reflecting the complete IT/OT infrastructure interfaces?
ID4. Do the inventoried components

AgroConnect

Agrifood Cyber Resilience Self-Assessment Tool

Home

Agrifood Cyber Resilience Self-Assessment Tool

How to increase your organization's level of cyber resilience

This self-assessment tool has been developed to help determine your organization's level of cyber resilience. The outcome of the assessment serves as a snapshot of, or insight into the 'as-is' situation of your organization. Having this insight will help establish possible shortcomings, as well as determine what measures are needed for your organization to achieve a higher level of cyber resilience. Required measures will vary from organization to organization. Please first proceed to the classification questions to determine your organization's cyber resilience category High, Medium, or Low.

Agrifood Cyber Resilience

Reducing the vulnerability of the agrifood chain to cyber-attacks requires a sector-wide approach. Seven leading agribusiness organizations have taken the lead in setting up an agrifood cybers
supervision of sector organization AgroConnect. Separate initiatives by individual companies are now being combined and reinforced into a network and joint approach of measures to establis

One of the aids the network is pleased to provide is a Self-Assessment Tool, which can be used to determine an organization's level of cyber resilience - on a strategic as well as a tactical and op

Agrifood Cyber Resilience Self-Assessment Tool

Home

Agrifood Cyber Resilience Self-Assessment Tool

1 — 2 — 3 — 4

IT/OT systems

How much damage is done if the IT/OT systems are down for 2-3 days due to a cyber-attack?

- ○ No or very limited damage
- ○ Serious damage with financial losses we can sustain
- ○ The continued existence of the company may be threatened

‹ Prior Next ›

Low

None of the organization's identified cyber resilience risks classify as category Medium or High

Medium

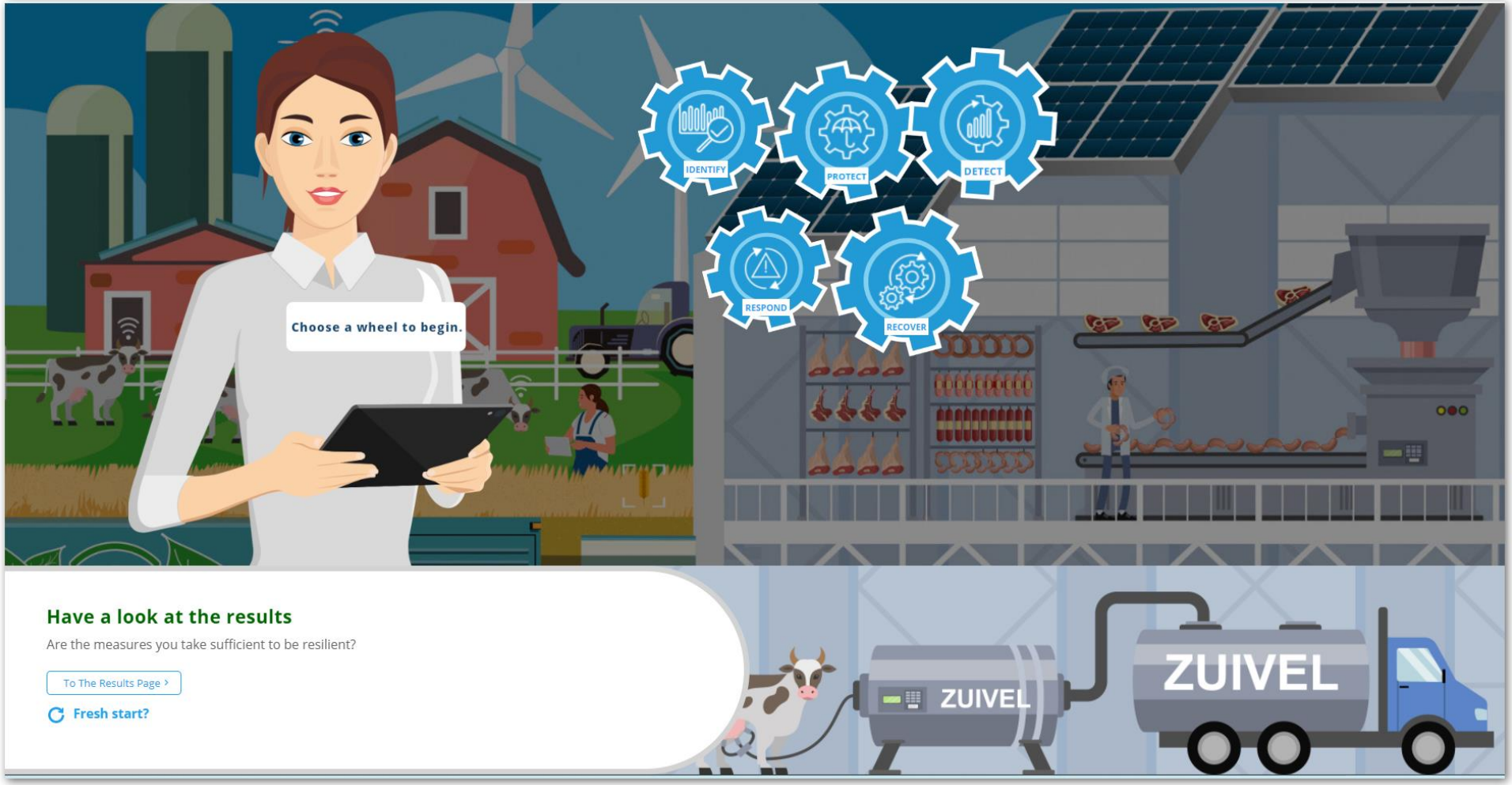
There is a risk that the security of the organization is not fully effective. As a result, and in the worst-case scenario, a cyber incident could result in:

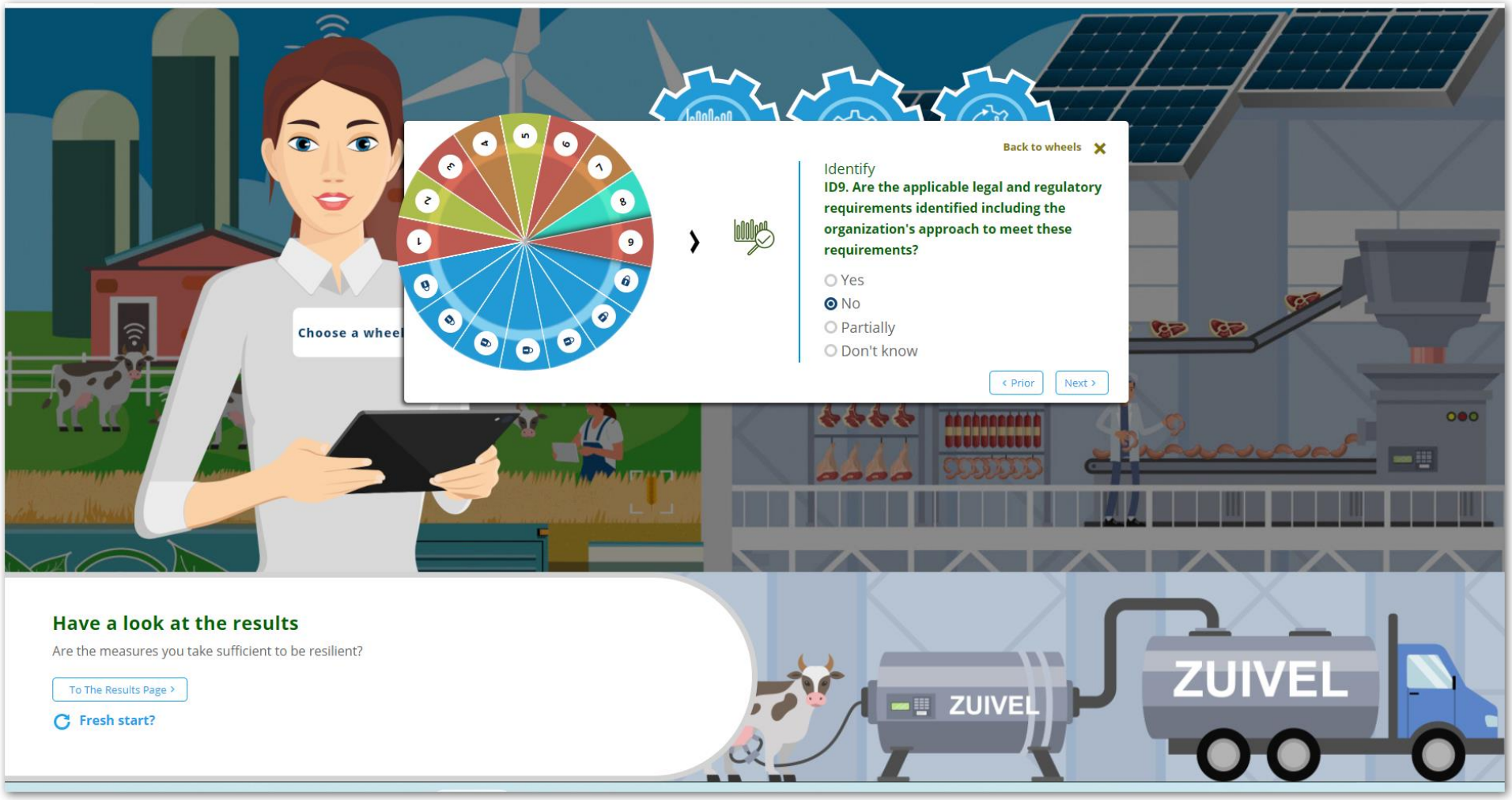
- Financial consequences, which can still be absorbed by your company; AND/OR
- Violation of company policy or ethics with limited consequences; AND/OR
- Unsafe situations that may lead to hospitalization; AND/OR
- Failure to achieve business objectives; AND/OR
- Moderate or minor damage to the environment.

High

There is a significant risk - that in the worst-case scenario - a cyber inc will result in:

- Serious financial consequences, possibly leading to redundancy or bankruptcy; OR
- Unsafe, life-threatening situations; AND/OR
- Failure to achieve key business objectives; AND/OR
- Serious damage to the environment; AND/OR
- Failure to comply with laws and regulations.

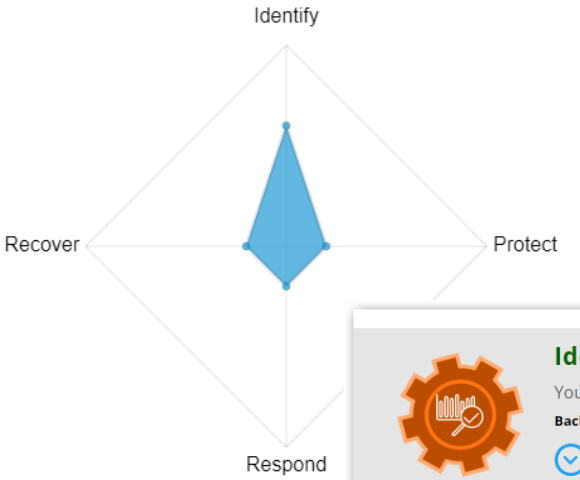

Choose a wheel to begin.
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Have a look at the results
Are the measures you take sufficient to be resilient?
To The Results Page ›
Fresh start?
ZUIVEL
ZUIVEL


Choose a wheel
Back to wheels
Identify
ID9. Are the applicable legal and regulatory requirements identified including the organization's approach to meet these requirements?
Yes
No
Partially
Don't know
‹ Prior
Next ›
Have a look at the results
Are the measures you take sufficient to be resilient?
To The Results Page ›
Fresh start?
ZUIVEL
ZUIVEL

Agrifood Cyber Resilience Self-Assessment Tool

Result

You need to answer more assessment questions to determine your score.



Agrifood Cyber Resilience Self-Assessment Tool

How to increase your organization's level of cyber resilience

This self-assessment tool has been developed to help determine your organization's level of cyber resilience. The outcome of the assessment serves as a snapshot of, or insight into the 'as-is' situation of your organization. Having this insight will help establish possible shortcomings, as well as determine what measures are needed for your organization to achieve a higher level of cyber resilience. Required measures will vary from organization to organization. Please first proceed to the classification questions to determine your organization's cyber resilience category High, Medium, or Low.

IT/OT systems

How much damage is done if the IT/OT systems are down for 2-3 days due to a cyber-attack?	Serious damage with financial losses we can sustain

Intellectual Property (IP)

How severe is the damage if business critical information or intellectual property is stolen due to a cyber attack?	The impact is so significant that corrective measures are hardly sufficient

Identify

You are doing well, but there is

Back to overview

More information

Protect

You need to answer more questions in this section to determine your score.

Back to overview

Respond

You need to answer more questions in this section to determine your score.

Back to overview

Recover

You need to answer more questions in this section to determine your score.

Back to overview

AgroConnect

Identify

Please proceed and answer further questions to see what could be improved.

Back to overview

Hide information

- ✔ ID1. Is an inventory of system hardware components developed and documented, reflecting the complete IT/OT infrastructure?
- ✔ ID2. Is an inventory of system software components developed and documented, reflecting the complete IT/OT infrastructure?
- ✔ ID3. Is an inventory of data communication components developed and documented, reflecting the complete IT/OT infrastructure interfaces?
- ✔ ID4. Do the inventoried components of the IT/OT infrastructure have a security categorization based on e.g. classification, criticality and value to the business?
- ✔ ID5. Is a security organization established including roles & responsibilities for the entire workforce and stakeholders, security awareness and training programs and needed skills and competences?
- ✔ ID6. Is the organization's role towards security in the business supply chain identified?

Cyber security policy

A set of policies for cyber security shall be defined, approved by management, published and communicated to employees and relevant external parties.

Legal and Regulatory requirements

Identify all relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

Privacy & Protection of Personally Identifiable Information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.