



Wuppermann Staal Nederland BV – Moerdijk (NL)

## Good practice Cybersecurity in the supplychain for industry

**William Biemans**

System Administrator at Wuppermann Staal Nederland BV

**Ruud Welschen**

Cybersecurity lead Siemens Digital Industry Nederland NV



# Plant Moerdijk (NL)



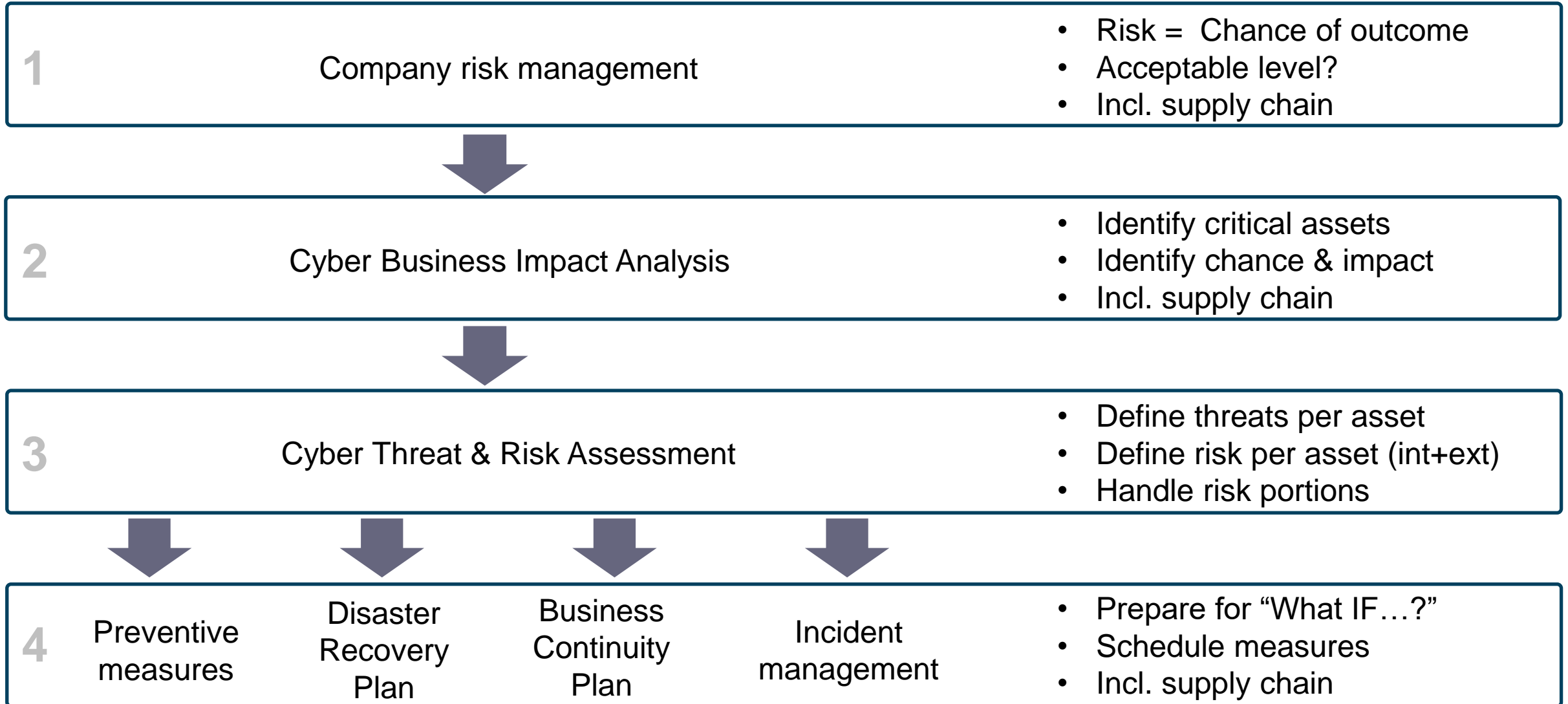
## Quick overview of the process



# Products

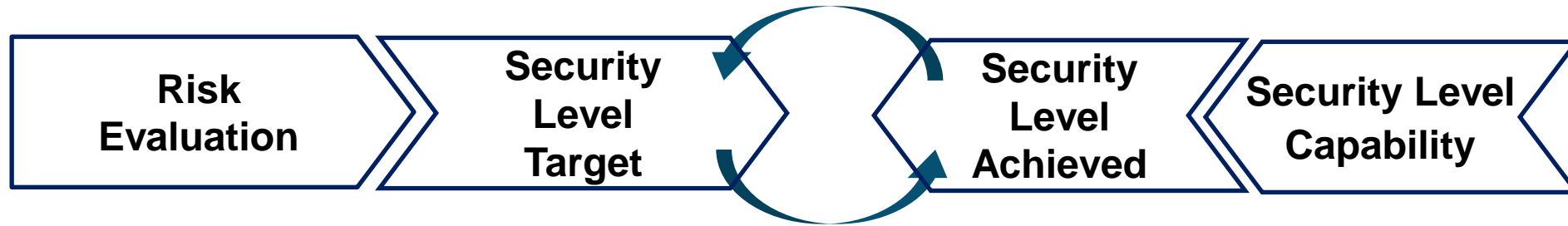


# Core business processes



# Cybersecurity Gap analysis

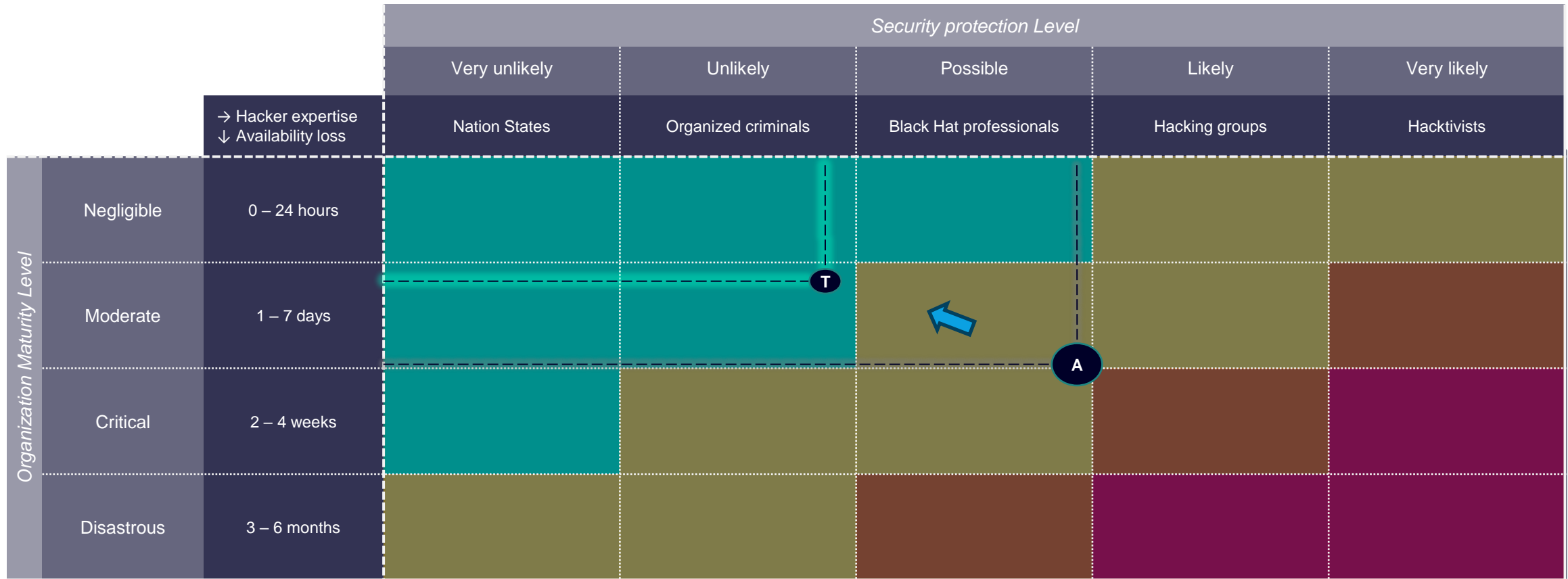
*including the supply chain*



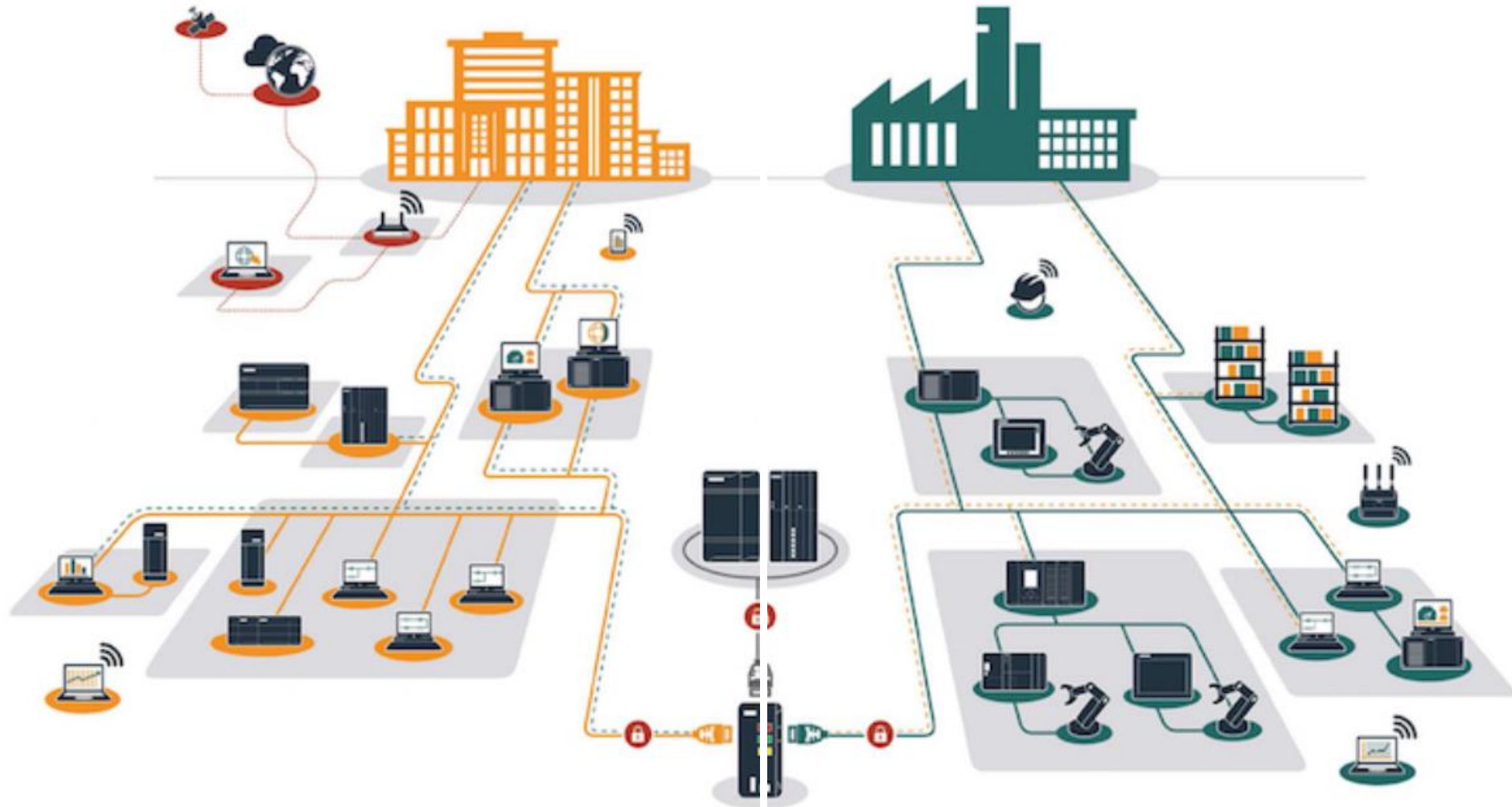
Risk Appetite  Resilience

# Example risk matrix for Cybersecurity

## *In Operational Technology (OT)*



# What is IT/OT?



**IT** Information Technology  
Office Network

**OT** Operation Technology  
Factory Network



# Example: Dependencies of services

*Involve: Company mgt, Production mgt, Facility mgt, Maintenance (E+M), ICT, Purchasing, etc.*

Entry sheet of services (IT dependende) in the PRODUCTION at the WSN LOCATION																
Service description (ID)	Service description (short)	Does this service belong to "Basic"?	Influence on production: uncritical, disorder, downtime	Service Description: NO / Small / Medium / Large	Service Description	evaluation of the service description if RE, MB&HT PRIO1 = urgent need for action PRIO2 = need for action PRIO3 =	Serv. descr. DoD DATE	Status/Service Description	Risk for production = current situation = (prio: 1 = red, 2 = yellow, 3 = green)	Argumentation for risk value (done by WBiemans)	Datenautsch LINK	Responsibility (Person / Department)	Responsibility agreed upon: Yes/No	Substitute (Person / Department)	Third Party	Contract: YES/NO or ContractData
Admin_PC...		No	uncritical	small	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	2 100% ready	3	No direct link to Prod		WBiemans	Yes	WBiemans		
ADP		No	uncritical	small	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	2 100% ready	3	Is just part of Office, has nothing to do with Prod		WBiemans	Not yet			
Alarm		No	uncritical	small	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	1 100% ready	3			WBiemans	Yes	WBiemans		No Serv. Descr: Pl
Alarm_System		No	uncritical	small	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	0 100% ready	3	Alarm running on MinIO now		WBiemans	Not yet			No Serv. Descr: Pl
ANFR		No	uncritical	medium	<a href="#">link</a>											
AnzeigeTafel		No	uncritical	medium	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	1 100% ready	3	Is part of LVS		WBiemans	Yes			
AutomatischPapierenPrin...		No	uncritical	large	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	1 100% ready	2	Check if WBT has the correct information. Make the solution a little bit more reliable		WBiemans	Yes			
BCD		Yes	disorder	medium	<a href="#">link</a>	PRIO2 = need for action	2023.04.28	1 75% ready	2	Risk evaluation "what-if-then-else" should be made.	Datenautsch LINK: SAP BCD DATEV	WBiemans	Yes			Not in this proj
BDE		No	downtime	large	<a href="#">link</a>	PRIO2 = need for action	2023.04.28	1 75% ready	1	Running stable. External partner in background. Need to check the procedure "just in case something goes wrong"		WBiemans	Yes			
Buspost		No	disorder	medium	<a href="#">link</a>	PRIO3 = recommendation	2023.04.28	1 100% ready	3			WBiemans	Yes	ETD		
Camera_Produktion		No	disorder	medium	<a href="#">link</a>	PRIO3 = recommendation	23.06.2020	0 100% ready	2	Current camera's are connected via Coax. New camera's can be done via IP. Problem are the switchboxes which cannot be delivered any more		WBiemans	Yes	ETD		
Camera_Office		No	disorder	small	<a href="#">link</a>	PRIO1 = urgent need for action	01.05.2023	0 0% done	3			WBiemans	Yes	ETD		

# Example: Risk inventory

*Per supplier and per asset > 1-2-3 rule / I-T-T-T*

Name of the OT Service	Plants area	Contact in case of FAILURE	Responsible person or department	Documentation available y/n	Supportability given (EOL EndOfLife)	Supportability - not given --> Measure	Reference to the measure (project,change,...)	Patch Mgmt: Patch management policy is adhered to y/n (LINK) Overall state: 1 = not started, 2 = in progress, 3 = up-to-date	Patch Mgmt Responsible Person /Team2	Patch Mgmt Current Patch version / New Patch version	Patch Mgmt Date of security check	Service is backed up using backup procedures according to its criticality y/n
Alarm system	General	<a href="#">LINK - Servicebeschreibung</a>	1. WBiemans / 2. WBiemans / 3. Esteme Ima XYZ Control room operator tel: [redacted] Manager ETO [redacted] Manager PTh [redacted]	ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	07.04.2024	No
System	BVZ - Bandverzinkung	<a href="#">LINK - Servicebeschreibung</a>		ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	12.08.2023	Yes, once every week
BOE08_WSNB238	Produktion - Gesamt	<a href="#">LINK - Servicebeschreibung</a>	1. Inhouse IT Abteilung WSTB/WBIT 2. Firma XYZ	ja / yes	ja / yes		04.04.2024: SAP Maintenance is to be [redacted]	1 - not started	ME	fbu	02.01.2024	Yes
Buispost	General	<a href="#">LINK - Servicebeschreibung</a>	1. ETO voor operationeel/jaar werken van de buispost infrastructuur 2. WBiemans / voor [redacted] 3. Firma XYZ	ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	12.08.2023	No
Case	Produktion - Gesamt	<a href="#">LINK - Servicebeschreibung</a>	WES	ja / yes	ja / yes			3 - up-to-date	TK	fbu	12.08.2023	Yes
Cognex	BVZ - Bandverzinkung	<a href="#">LINK - Servicebeschreibung</a>	1. QS afdeling 2. Electisch: ETO 3. ICT vragers: WBiemans 4. Esteme Ima XYZ	ja / yes	In progress	Windows 10 OS - Questions: -What spare parts do you have in stock for the system?	D.02 IT Sicherheit: DB Flar (übergeordnet) // D.02.02 Budget 2022: Bemerkung1: this project is not a pure IT project therefore it will be removed from the IT budget planning and discussed elsewhere decided and planned by Quality Department (QS)	2 - in progress	RV + WBiemans	6.0.18	13.12.2023	No
DMC code	Logistiek	<a href="#">LINK - Servicebeschreibung</a>	1. WBiemans / 2. WBIT - [redacted] 3. Esteme Ima XYZ	ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	12.08.2023	Yes
FileServer	General	<a href="#">LINK - Servicebeschreibung</a>	WES	niet / no	ja / yes			3 - up-to-date	FE	fbu	12.08.2023	Yes
Horizon	BVZ - Bandverzinkung ULTA	<a href="#">LINK - Servicebeschreibung</a>	1. Inhouse/IK Horizon (Tags/Walves) ETO 2. Functionele werking (Inkl netwerk): WBiemans 3. Esteme Ima XYZ	ja / yes	In progress	24.08.2022: Angebot wird in Auftrag gegeben	<b>Budget 2022: Bemerkung2: this project is not a pure IT project therefore it will be removed from the IT budget planning and discussed elsewhere decided and planned by PRODUCTION (ETO)</b>	2 - in progress	ETD + WBiemans	2020-P2	13.12.2023	Yes
Igelterminal	Produktion - Gesamt	<a href="#">LINK - Servicebeschreibung</a>	WES	ja / yes	ja / yes			2 - in progress	WBiemans	fbu	12.08.2023	Yes
Jungle	General	<a href="#">LINK - Servicebeschreibung</a>	1. WBiemans 2. XYZ 3. XYZ	ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	12.08.2023	Yes
KABA	General	<a href="#">LINK - Servicebeschreibung</a>	WBiemans / XYZ	ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	12.08.2023	Yes
Klimaat-PC	Control of climate Moedijk (Klimaat-PC)	<a href="#">LINK - Servicebeschreibung</a>	1. ETO 2. ICT 3. externe Ima	ja / yes	ja / yes			3 - up-to-date	WBiemans	fbu	12.08.2023	No
Kransteuerung	BVZ - Bandverzinkung ULTA	<a href="#">LINK - Servicebeschreibung</a>	1. ETO voor netwerkverbinding, VO, etc 2. WBiemans / voor overige ICT zaken 3. Firma XYZ	ja / yes	In progress	MSO Maßnahme --> Aktualisierung der KRAN Umgebung - [redacted] - WSN 24.08.2022: Angebot wird in Auftrag gegeben	D.02 IT Sicherheit: DB Flar (übergeordnet) // D.02.02. <b>Will be done in Q1-2024</b>	2 - in progress	WBiemans	v24052	13.12.2023	No
LAN network environment	General	<a href="#">LINK - Servicebeschreibung</a>	WES	niet / no	ja / yes			3 - up-to-date	ZB	fbu	12.08.2023	Yes

# Agree on company alignment for: Scope of services, time window, response time, roles, point of contact, actual information, certificates etc.

**SIEMENS**

**Annex I**  
**Remote Industrial Operations Services**  
Description and Terms & Conditions applicable to your Service Contract

**Contract specific agreements**

**Digital Enterprise Services**

Fastest time to market. Better quality. More efficient production. Nowadays, being competitive means becoming digital – which can be overwhelming. Where do I start? Who can help me to digitalize my processes to my standards? Digitalization in an industrial environment requires specialized expertise and knowledge. Let us be part of your digitalization journey. From day one of the entire transformation process.

**Digital Enterprise Consulting**

The beginning of our consulting is a thorough assessment of your company's digitalization maturity that our experts perform together with you. It's important to understand where, when and how to digitalize in your plants, value streams, and business models.

The result of our consulting is a digitalization road map that's based on selected digital enterprise scenarios and is tailored to your needs and your installed base. That's the beginning of your digital transformation.

Our contract for Digital Enterprise Consulting also includes:

- Initiation** – Get ready for your digital transformation by co-creating digitalization use cases
- Strategy** – We analyze your readiness for an end-to-end transformation and propose the Digital Enterprise Implementation Roadmap
- Process** – Design your digital solution architecture based on a benchmark process blueprint
- Solution** – Connect digitalization strategy with solutions and projects
- Security** – Evaluate the current security status of your industrial environment

**Industrial Security Services**

Comprehensive protection of your plant using Industrial Security Services is based on the recommendations of the international standard IEC 62443. With "Defense in Depth", Siemens has developed a multilevel security strategy that includes not only the technology you need but also taking measures for your employees by service experts and improvements to your organizational structure.

Industrial Security Services include the necessary hardware and software, and especially service experts who combine expertise in automation, digitalization, and security. You enjoy support from the experts right from the start as they work with you to develop the strategy you need, put it in place, and make ongoing improvements to protection. This service follows the end-to-end approach of Digital Enterprise Services in the three steps of consulting, implementation, and optimization, including the corresponding modules.

Please note: work may result in the temporary unavailability of the system. Therefore, the time of the planned work must be agreed in advance.

**Vulnerability management**

Based on your installed base data, an overview of known vulnerabilities is periodically offered. This overview will be discussed to assess possible follow-up actions and, if necessary, to plan them separately.

**Software & firmware updates**

As part of the Siemens software support license (see also section Software support license) you will receive updates for:

- Minor functional improvements.
- The delivery of security enhancements.

These updates are made available according to product release cycles or instant updates in case of a security improvement for a product's vulnerability.

**Windows updates**

Microsoft makes updates available on a monthly basis. In case of very serious vulnerabilities (security problems), then Microsoft also releases instant security improvements. This service module covers the implementation of Microsoft Windows updates on the OT systems for security improvements. This keeps Microsoft Windows up to date within the installation, reducing Windows-related security risks on your installation. This makes the installation less susceptible to cyberattacks. Based on the frequency agreed with you, the Windows updates available at that time will be implemented.

**Virus & malware detection**

The starting point of this module is that the servers and clients within your installation are equipped with virus & malware detection software. A network facility has also been set up to keep virus detection up to date. With this service module we periodically check the operation of the virus & malware detection software, we check whether the virus detection is up to date and we check the scan results. If this check shows that the virus detection is not up to date, we will manually update the status thereof.

If the scan results show that the servers or clients have a form of infection, you will be notified immediately. After this notification, it will be determined in consultation which actions are required. If there are suitable updates for the virus & malware detection software, these will be implemented as part of this service module on the installation.

**Backup PC systems**

The starting point of this module is that your installation is equipped with a backup facility on which backups of the PC systems are automatically made and stored. With this service module, we periodically check the consistency of the recently made backups. If the backup is not done correctly, we will restore the backup after consultation. A correct and up-to-date backup of systems is a requirement for a short recovery time in the event of (Cybersecurity) incidents.

**Backup (historic data)**

The starting point of this module is that your installation is equipped with a backup facility with which backups of the historic data (for example trend data) are automatically stored. With this service module we periodically check the correctness of the recently made backup. If the backup is not done correctly, we will restore the automatic backup after consultation. A correct and up-to-date backup of systems is a requirement for a short recovery time in the event of (Cybersecurity) incidents.

**Virtualization and IT firmware updates/updates**

The starting point of this module is that the servers within the installation are equipped with a virtualization software. Update/updates may also be made available for this software to mitigate identified vulnerabilities.

The IT systems, server(s) and client PC(s), within the installation are equipped with firmware (formerly also called BIOS). For this firmware, updates may also be made available by the hardware vendors to mitigate identified vulnerabilities.

This service module provides for the implementation of these virtualization and IT firmware update/updates on the IT systems within the installation. This makes your installation less susceptible to cyberattacks.

**Network maintenance including cybersecurity**

This service module concerns the periodic monitoring and, where necessary, updating of the operation and security of the OT network. If necessary, in consultation, it is initially offered to put the network in order.

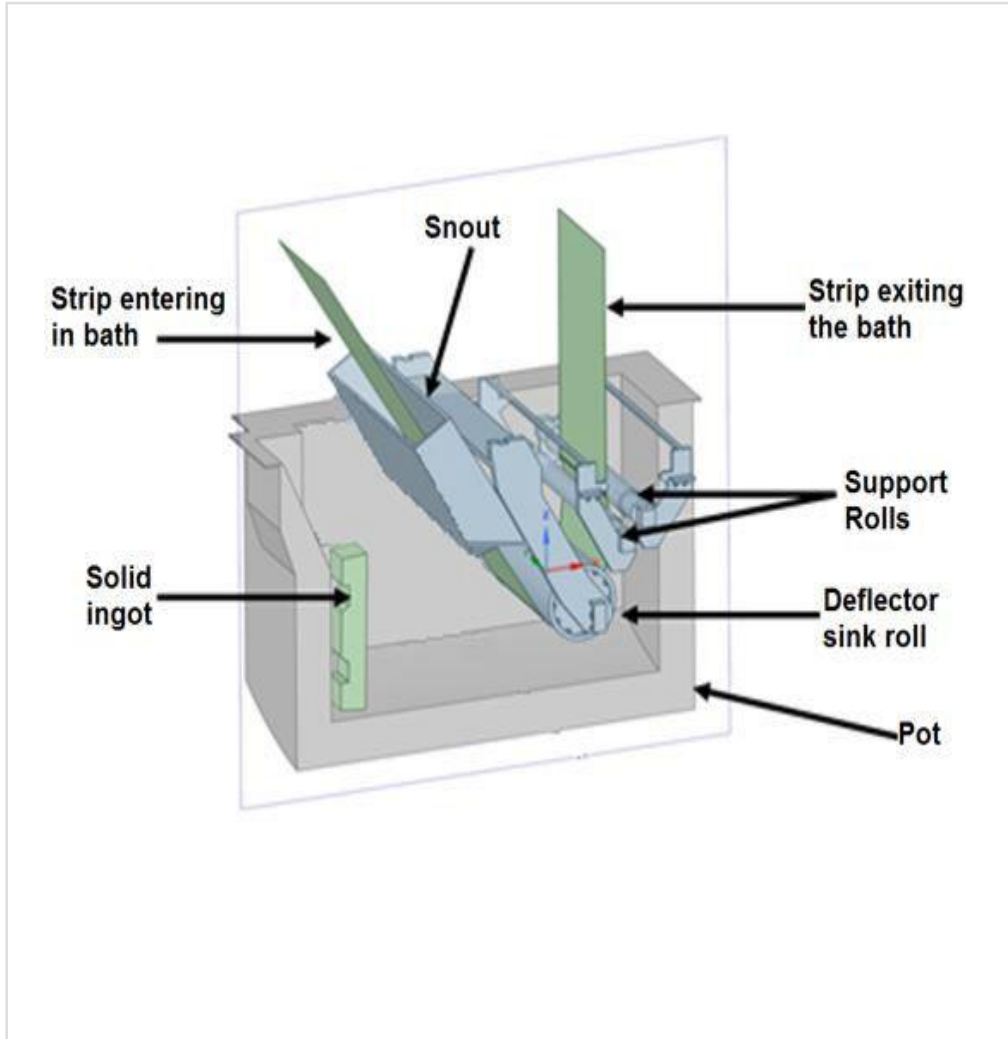
This service concerns the following predictive maintenance activities to be carried out periodically:

- Checking and, where necessary, updating the firmware of the network equipment within your installation.
- Checking log files for network problems / cyberattacks.
- If applicable: reporting the findings from the log files.
- If applicable: improve network security by adjusting the configuration of the network equipment.

## Example: Drive Converter & Transformer



## Example: stones for the pot of the sink bath



Cybersecurity strongly demands for:

Professional company management

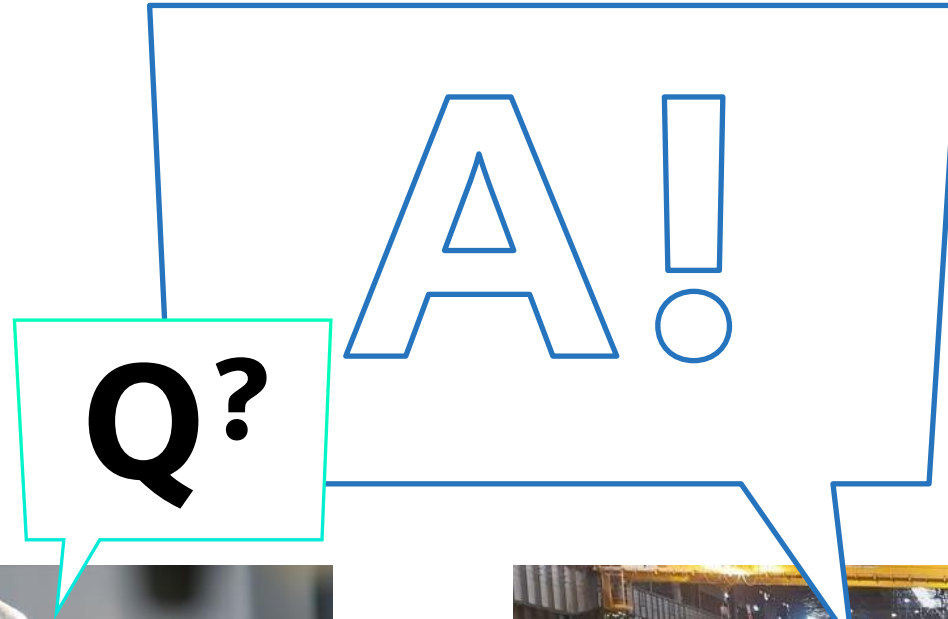
Risk management

Preparation & Training

COLLABORATION



# Q&A



Thank you

