



Increasing OT Cyber resilience in Food industry

NISDUC 2025

Ruud Welschen

Siemens Nederland

Mark Schut

FrieslandCampina



OT in cyber security: How to increase your cyber resilience in the OT-domain of your company

P **Purpose:** Share with participants the challenges that the industry is facing when improving the cyber resilience and raise awareness about the blind spot that most companies/IT have for the OT domain.

O **Outcome:** **Call for actions** to C-level and CISO's actively **investigate the required actions** in their **OT domain**.

S **Structure:** Dual Presentation Siemens & FrieslandCampina

T **Timing:**
05min – Setting the Scene (Siemens)
20min – Presentation
05min – Q&A

Table of content



1. Intro – Risk management for OT;
2. Complexity of OT within FrieslandCampina;
3. Looking back – our challenges and successes from 2019 till now;
4. Moving forward – our current roadmap for NIS2 to provide inspiration for your organization;
Risks: Compliance vs Control
5. Q&A.

From Compliance to Control *for Operation Technology*

Duty to Care

- Organization
 - > Based on risk management
 - > Cyber Security Management System
- Operation
 - > Duty to Train the board
- Technical
 - > Conform relevant standard

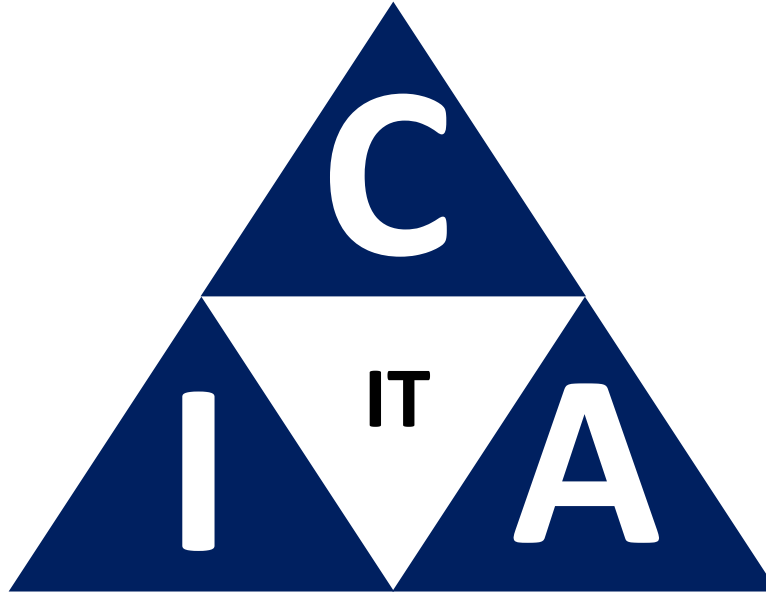


For industrial applications use IEC62443

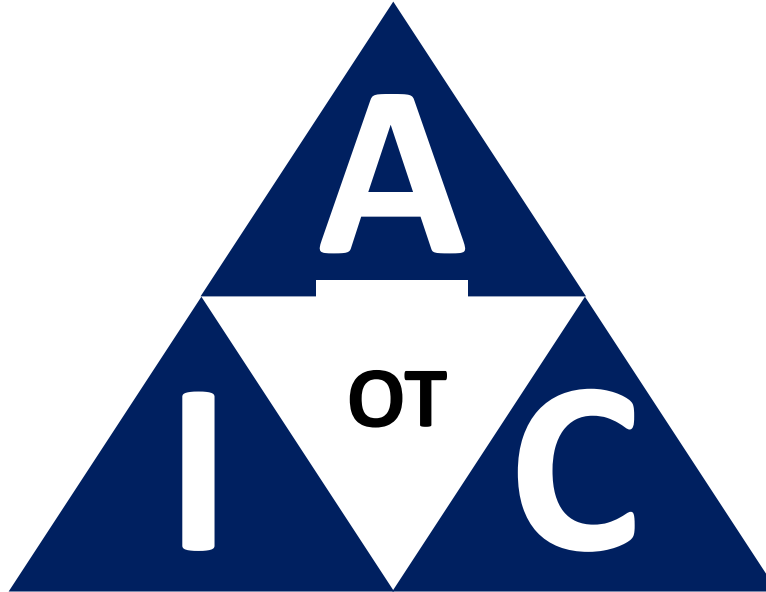
Even with low probability, there is always high

IMPACT

For information security the confidentiality is key



For production availability is more relevant

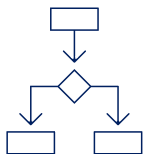


Because this directly impacts HSEQ



Production has low maturity in security, however, is very mature in risk management

RI&E

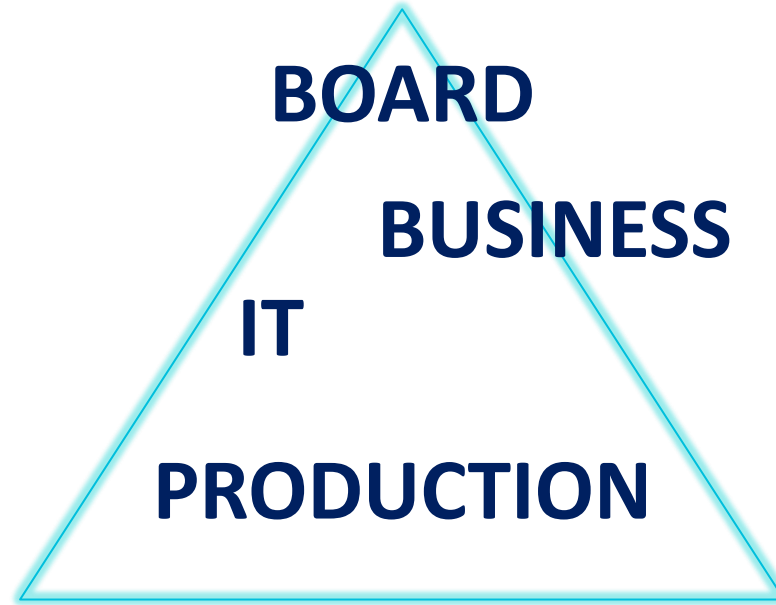


LMRA

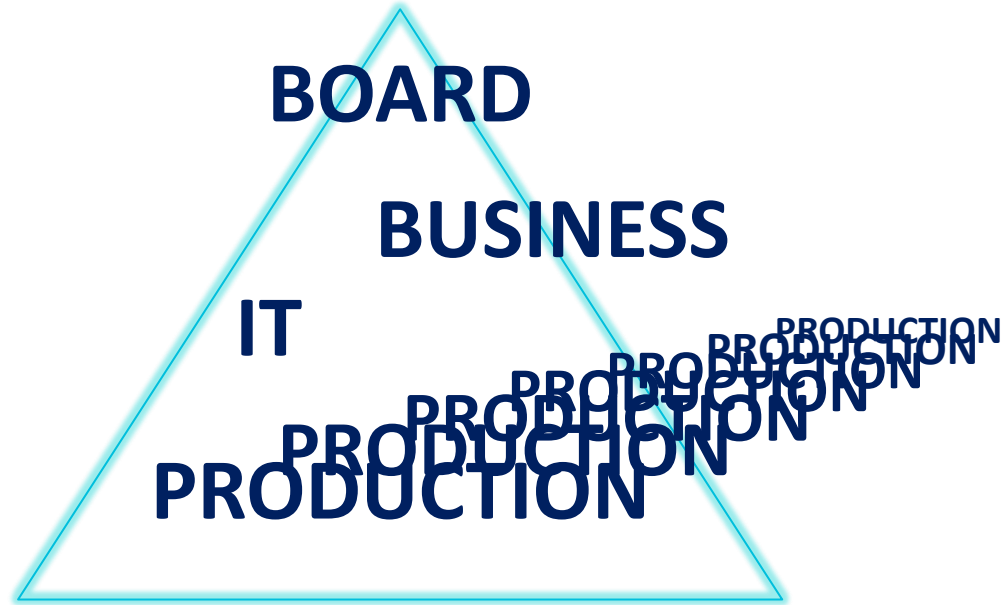
MATURITY

WHO IS RESPONSIBLE FOR OT CYBER RESILIENCE?

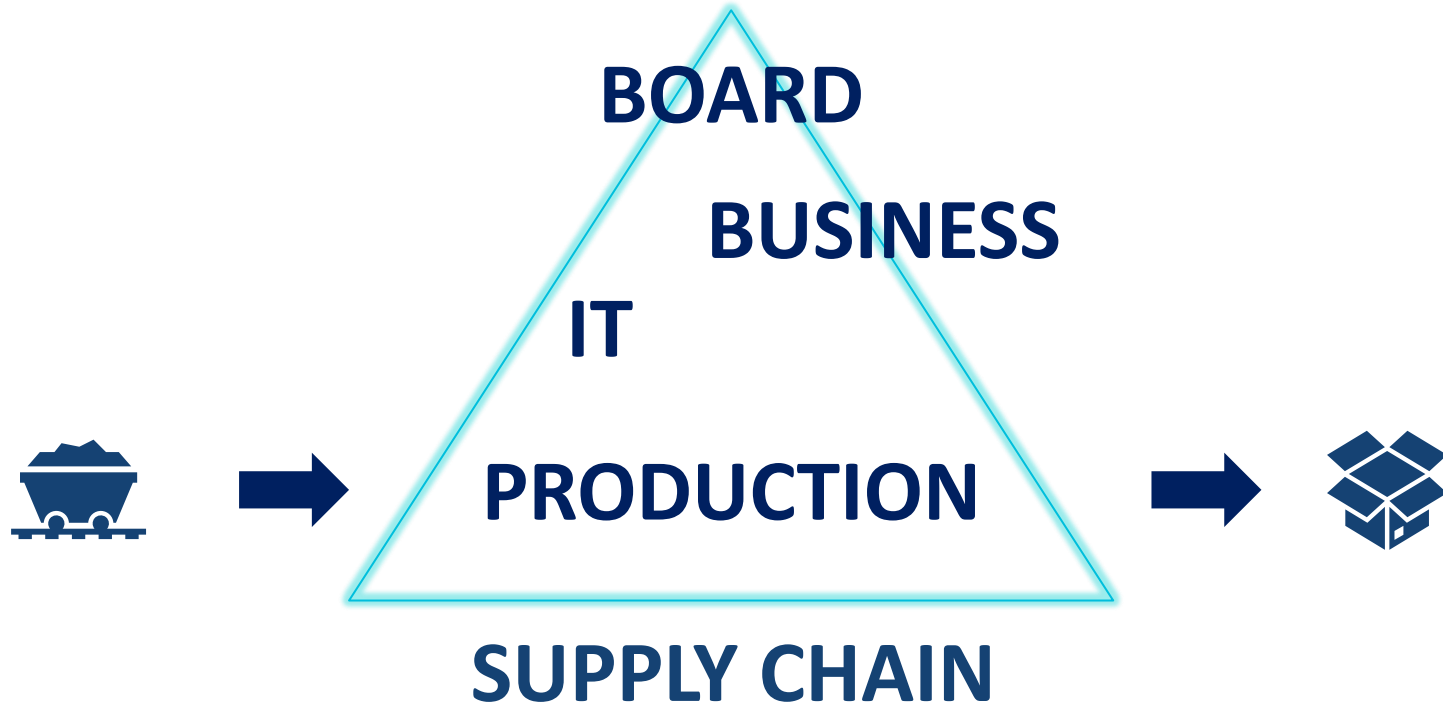
The general picture of organizations



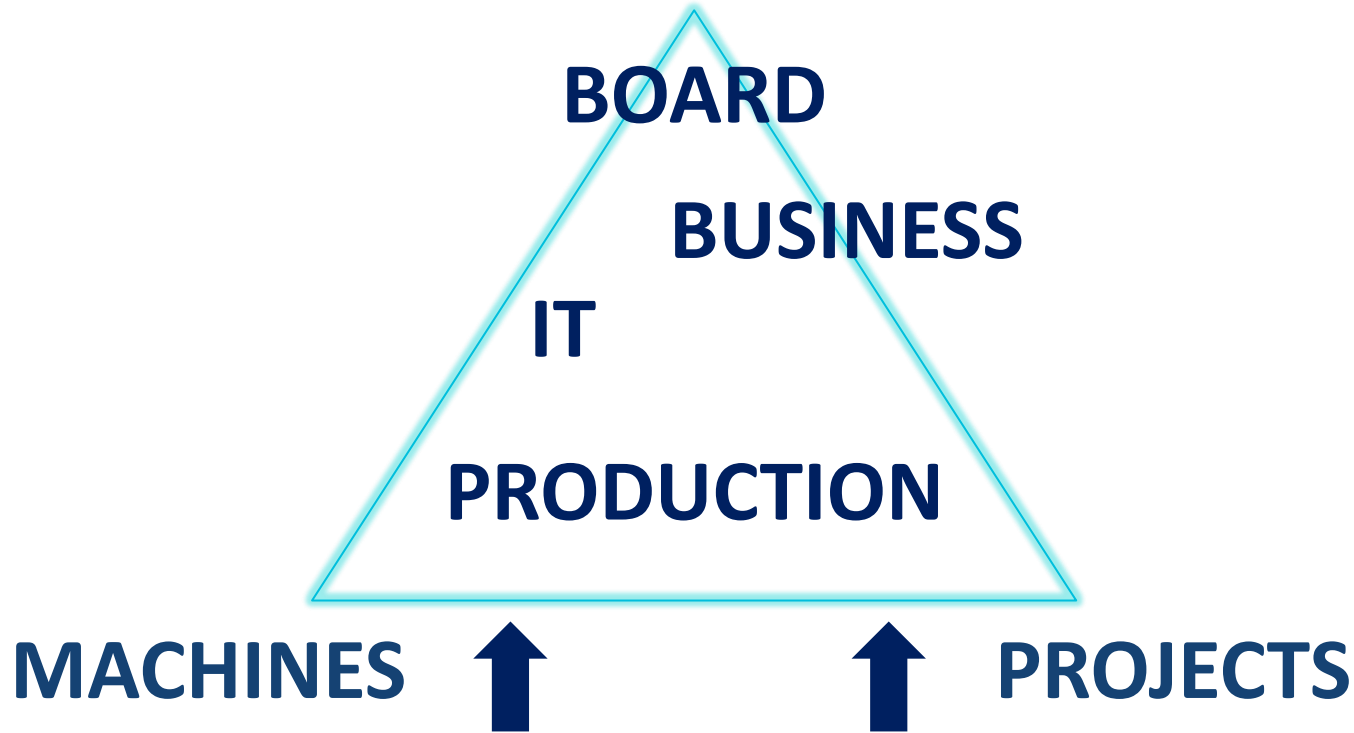
Production facilities have local Profit & Loss responsibility



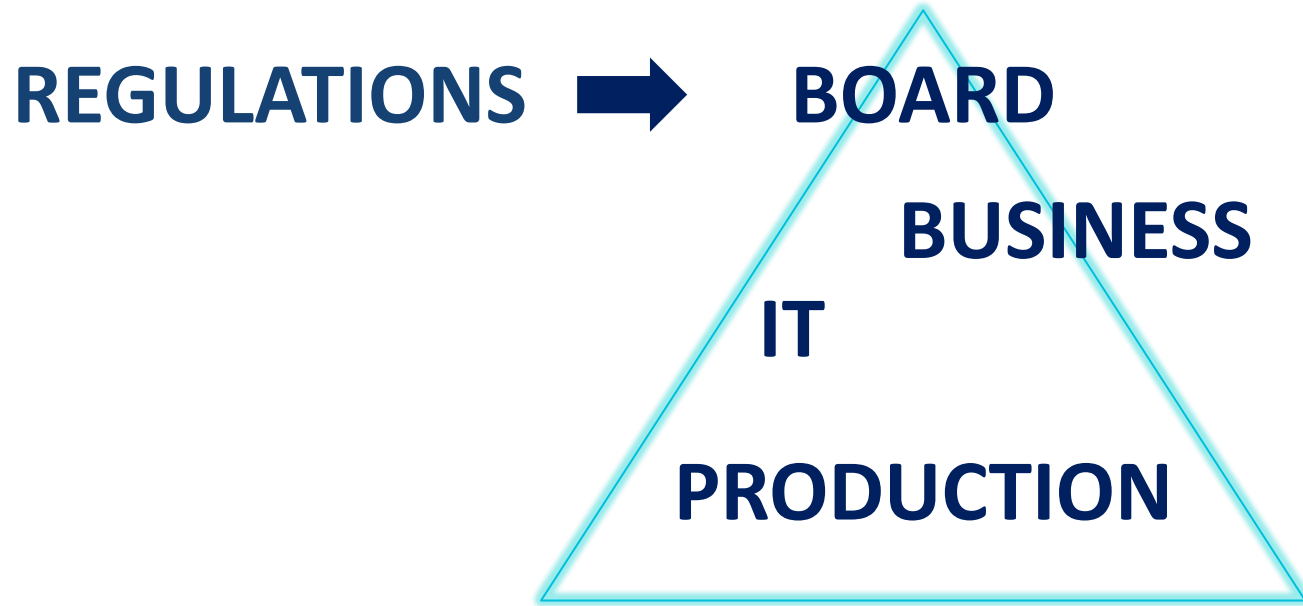
Production is part of a larger supply chain out of organization boundaries



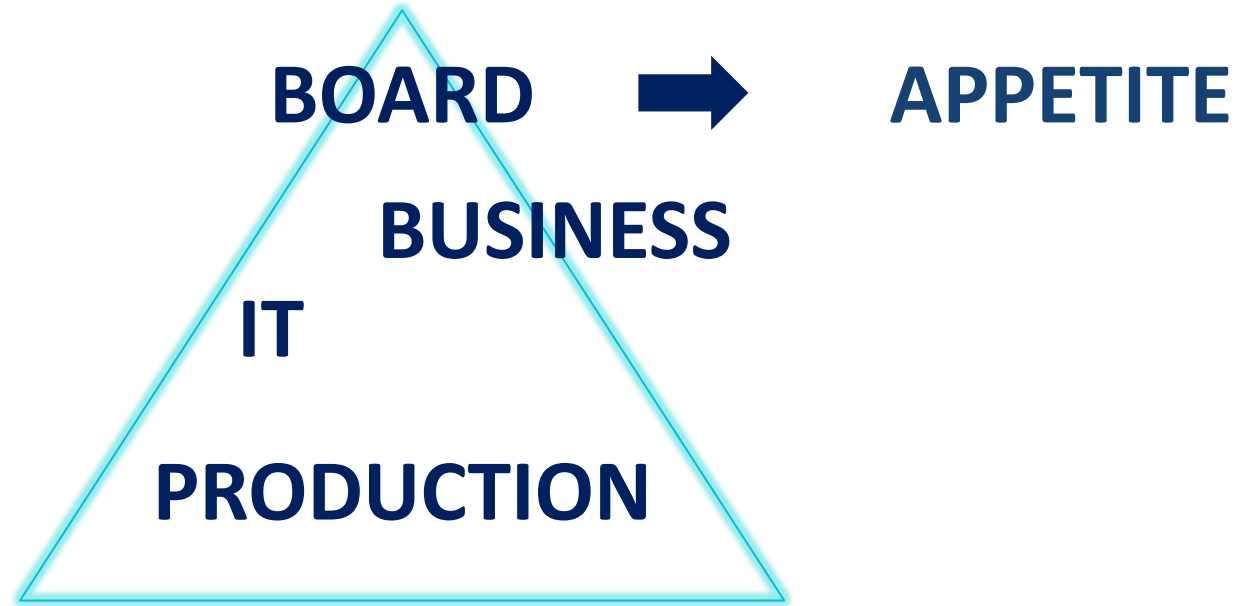
Production is depending on external cooperation partners



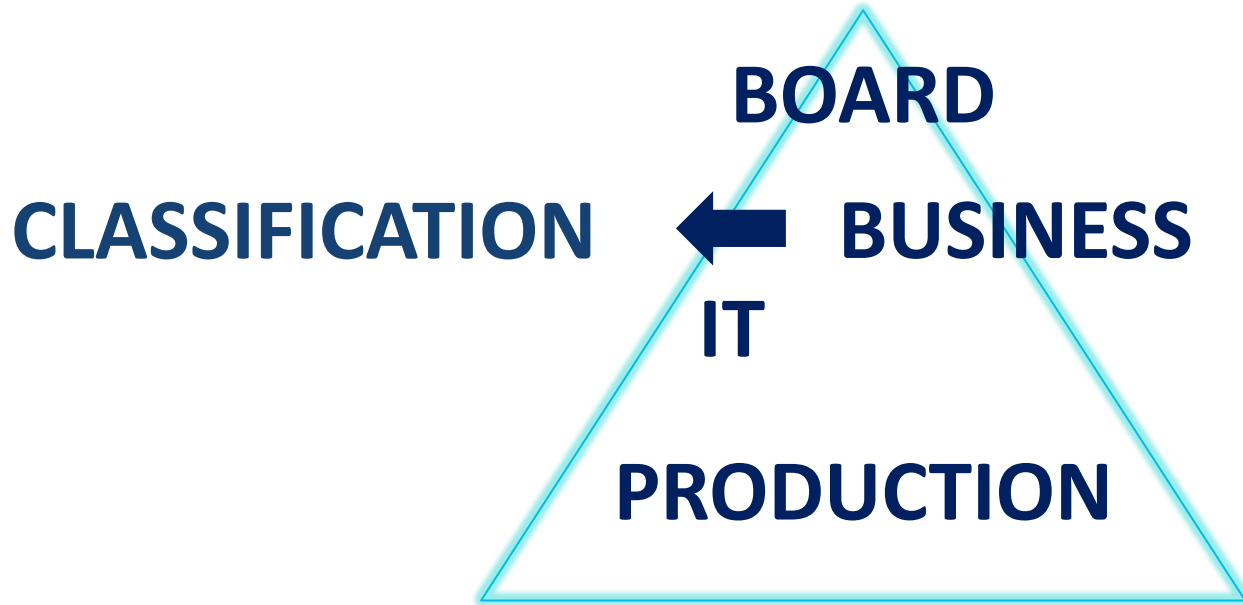
The board needs to comply to regulations



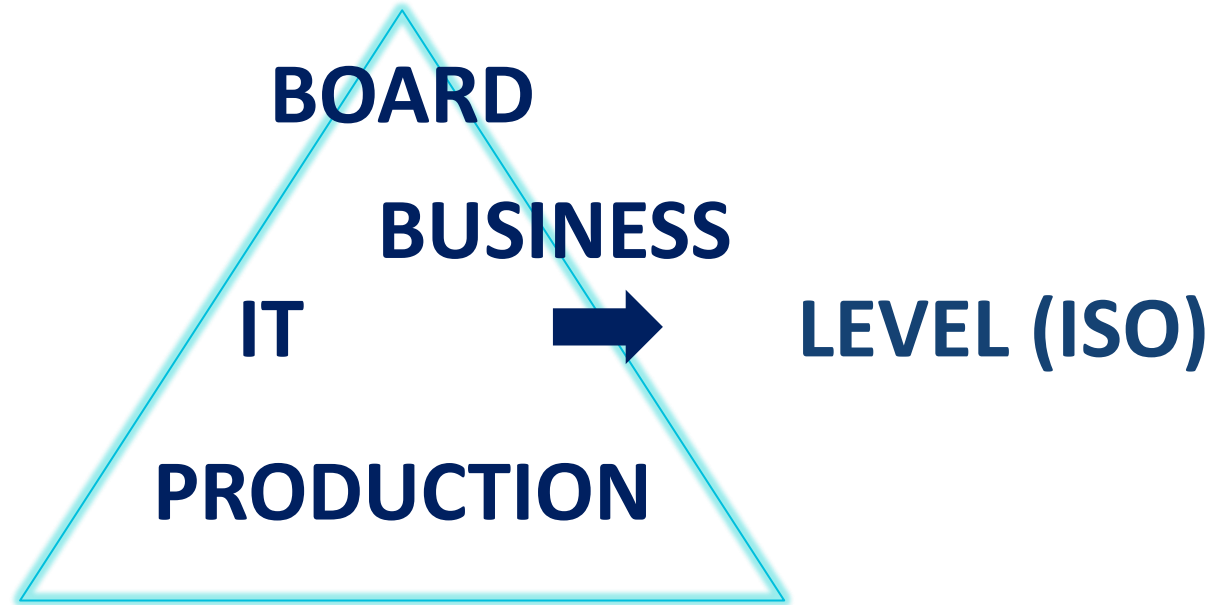
The board can define the overall risk appetite



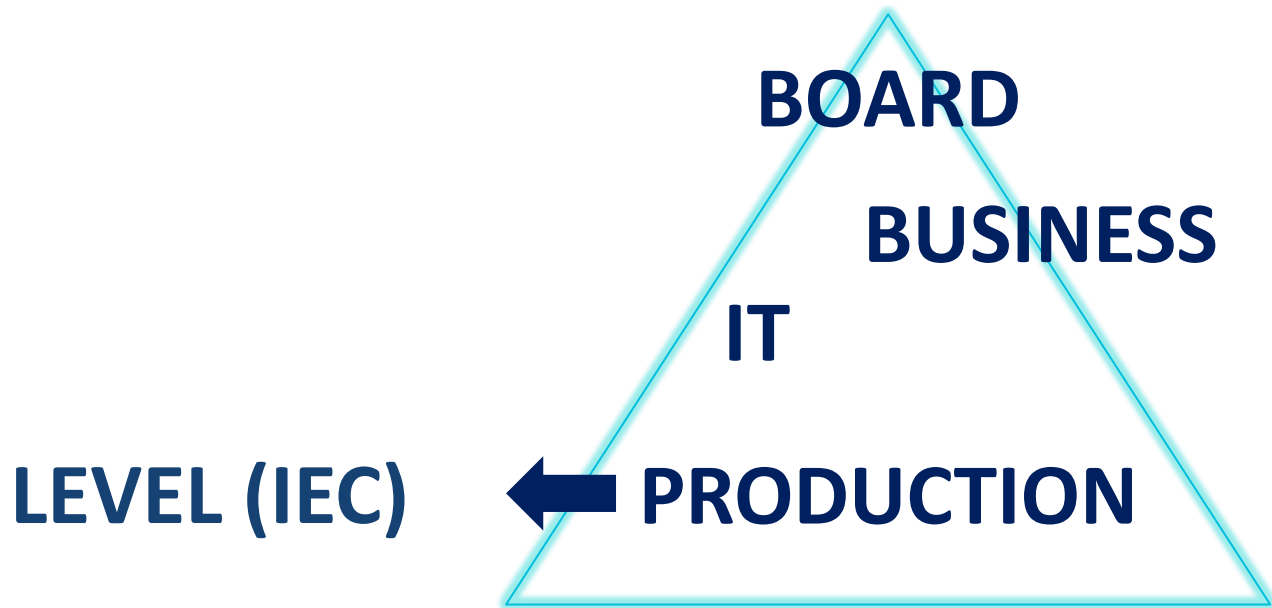
The business “owns” the production facilities and can classify the criticality



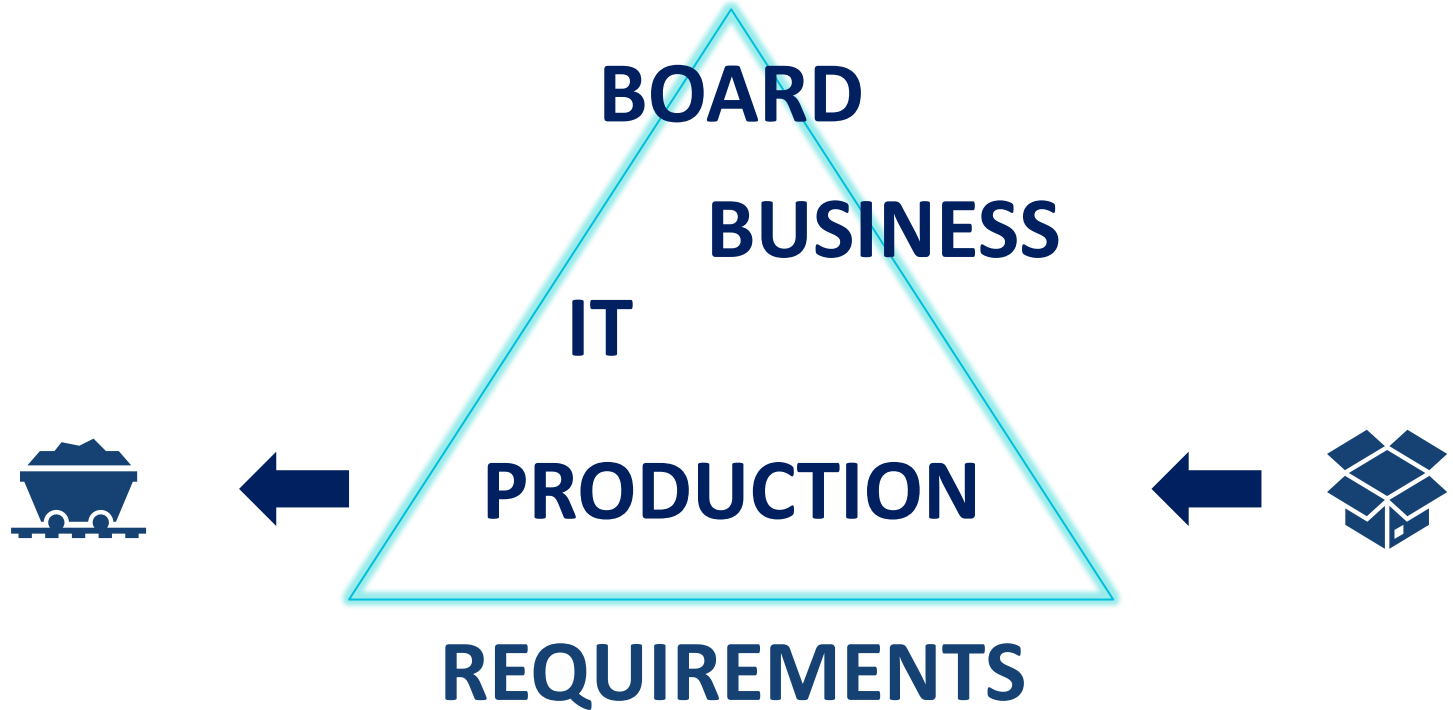
IT covers information security risks based on ISO27000



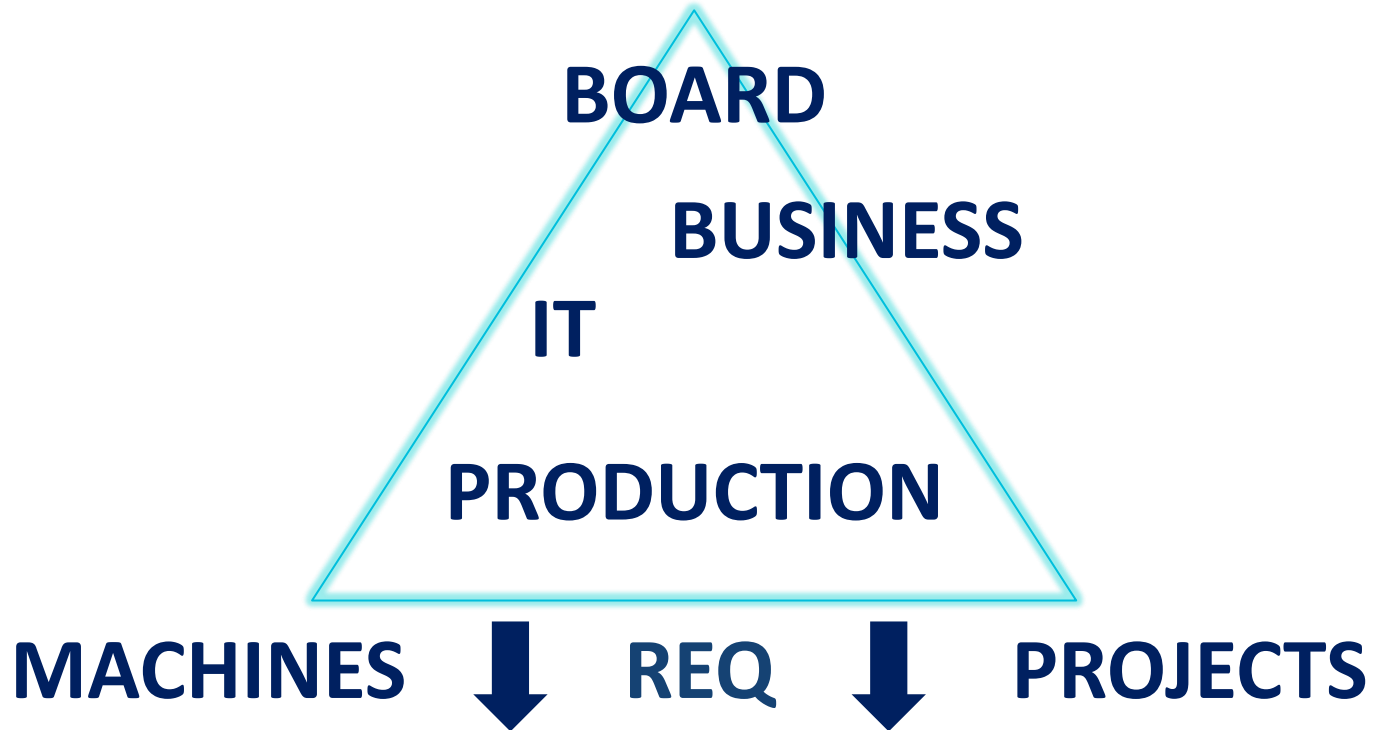
Production covers HSEQ risks based on IEC62443, facing legacy installed base



Asset Owners need to set requirements to suppliers



Asset Owners need to set requirements to suppliers



Start by defining roles and responsibilities before implementing technology

CHANGE



FrieslandCampina nir
nourishing by nature



FrieslandCampina – What makes OT
Complex in our Dairy Supply Chain?

Introduction and Why:

Our Food Industry is essential for the millions of people that depend on us.

Let OT help to protect our critical industry



Mark Schut
BG OT Manager
Food and Campina

Business Groups:

- Ingredients + Specialized Nutrition

Previous roles:

- OT Manager Borculo
- Maintenance Manager Borculo
- Asset Management Consultant [Stork]

Education:

MSc Industrial Engineering & Management - University of Twente

25 m
& active
consumers



20%

of all medicine
tablets worldwide

LACTOSE



30+

different biological drugs and
vaccines for treatment of a
wide range of diseases

hydrolysates



Veghel

The Netherlands



Borculo

The Netherlands



Workum

The Netherlands



Bedum

The Netherlands



Delhi

North America



Beilen/Zwolle

The Netherlands



Wageningen

The Netherlands



FrieslandCampina 

nourishing by nature

19,576

Employees

30

Countries of operation

12.9B

Revenue

50

Factories



From B2B to B2C, from FMCG to Pharma – our product affect millions of consumers every day.

Using our 7 Business Groups we export to over 100 countries 



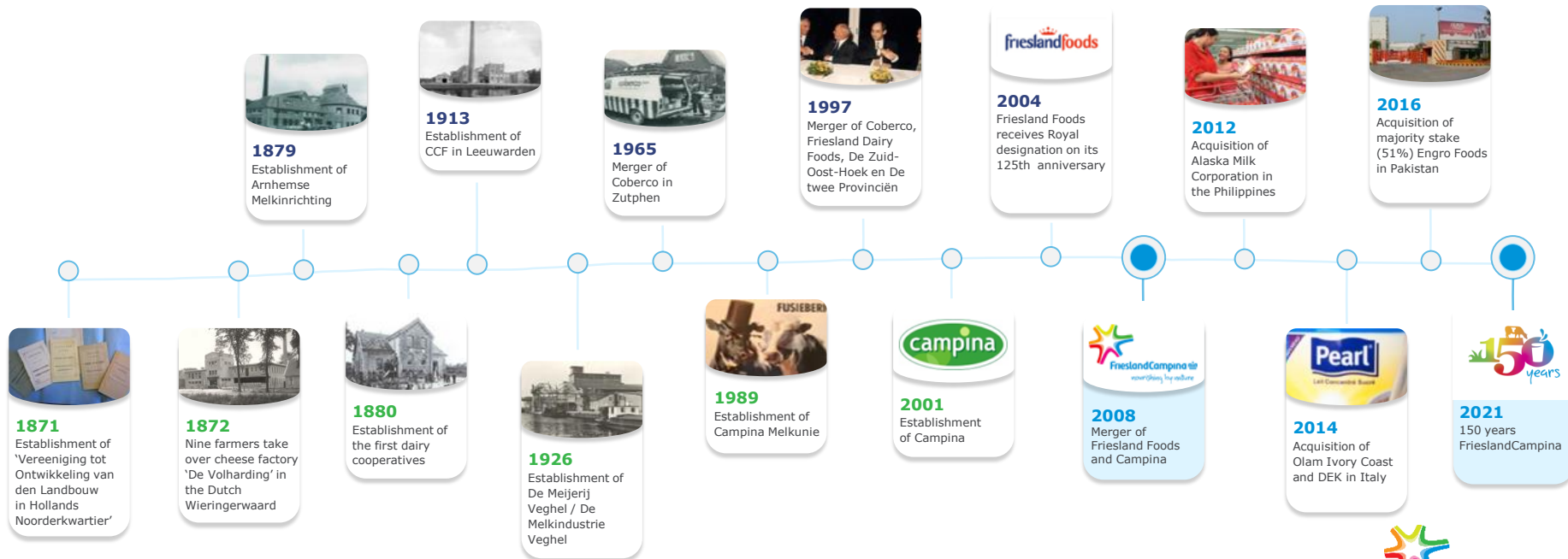
FrieslandCampina
nourishing by nature

Our History: 150+ years of dairy expertise



Our company of today is the result of a long journey of **mergers and acquisitions**. We evolved from a **local for local** supply chain to a **global** dairy supply chain.

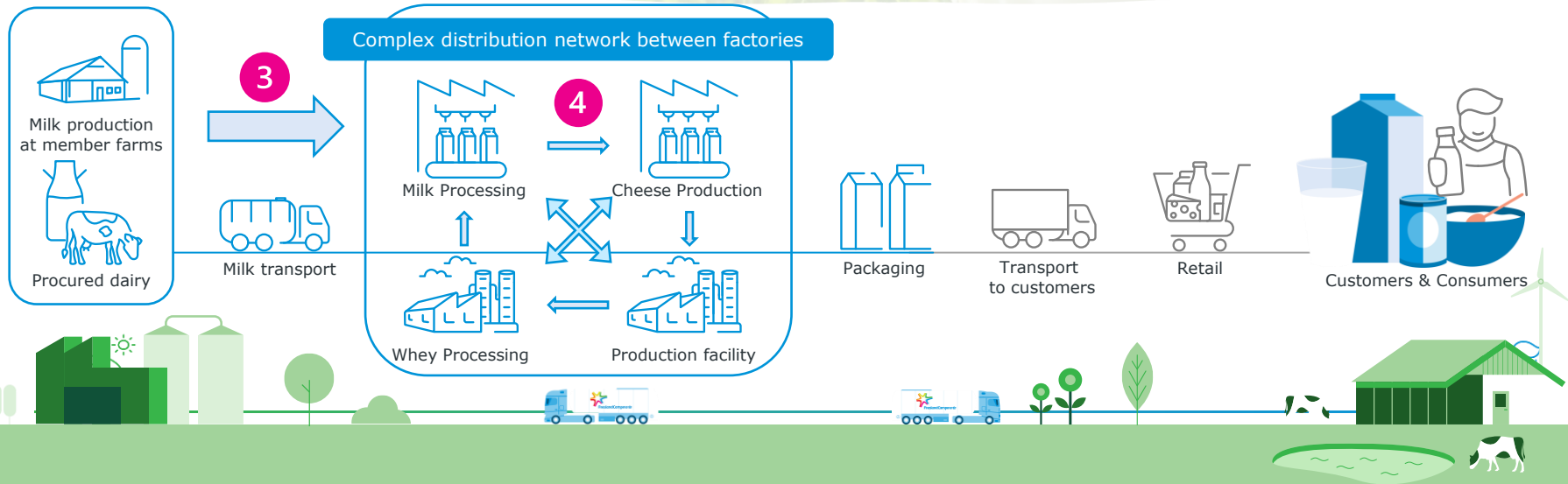
1




From Grass to Glass

2

Responsibility over the entire Supply Chain





Looking back:
Challenges and
successes from
2019 till now.

#1 Laying the foundation: Ownership & Organization

The **Global and Local design** of the OT Operating Model are expected to **deliver the following benefits:**



Foster OT Talent, Build Capability

Foster OT talent and capability building, providing **improved growth opportunities** in FC OT



Accelerate OT System Standardisation

Organise and accelerate standardisation of **Global OT technology landscape to reduce cost**



Deliver Fit-for-purpose OT

Develop cost efficient, fit-for-purpose OT organisation with **OT Clusters formalised** supplementing Local OT



Maintain Local Ownership

Maintain local ownership for **day-to-day OT operations and maintenance** given criticality to production



Enhance FC Competitiveness

Enable OT to enable better **market competitiveness**



Improve OT Cybersecurity

Build tailored OT cyber capabilities with **dedicated OT security specialists** to set guardrails, monitor risks and drive compliance, safeguarding business continuity



Drive OT **Improve budgeting** to support OT in efficient decision making for budget allocation

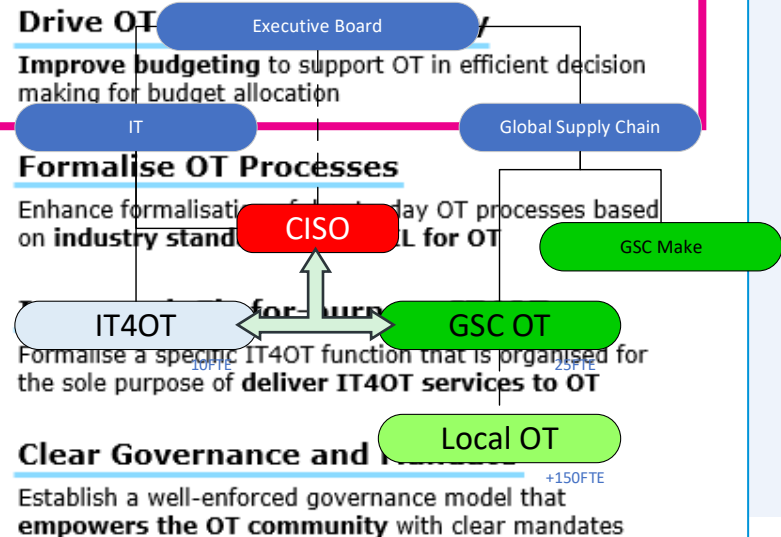
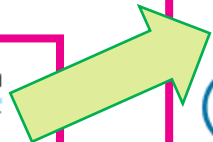


Formalise OT Processes

Enhance formalisation of **day-to-day OT processes based on industry standards** for OT



Clear Governance and Empowerment
Establish a well-enforced governance model that **empowers the OT community** with clear mandates



#2 The sharp increase of cyber threats:

1st awareness campaign that kicked started our journey

Standalone program 2019-2023 within Business Group Ingredients.


Overall objectives:

1. To raise *the digital resilience* of the different production locations
2. Acquire insights on the OT Maturity of production location and to what extend vulnerabilities do occur within OT.
3. Use retrieved information to develop strategies and procedures for incidents and to train Local OT.

Key take outs:

- A. Mature OT organization also underestimate the risk Cyber poses
- B. Having the right tooling is key to be successful on topics like: B&R, PAM, NSM.

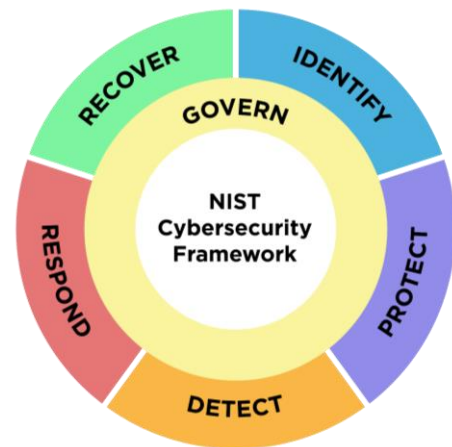
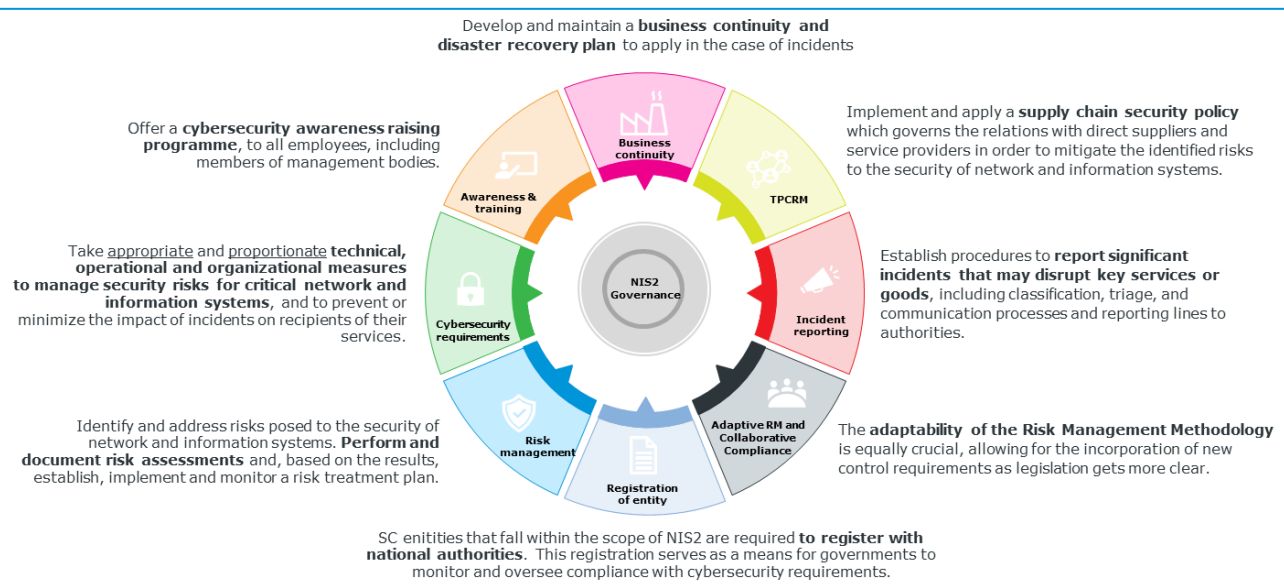




Moving forward:
Our current roadmap
for NIS2 to provide
inspiration for your
organization

Our approach to NIS2: Key activities from NIS2 Directive

Our strategy: **Map the key requirements** onto our **NIST Security Framework**. Then based on the GAP between the existing performance and required output – define a program to **enhance** our overall **Cyber Resilience**.



Our approach to NIS2: Examples OT initiatives

Multiple OT Global programs are already in progress to address requirements and some need to be accelerated. Some additional activities need to be updated/be started due to latest insights NIS2



To be continued



To be accelerated



To be updated/started

<ul style="list-style-type: none">• OT Data Center hosting• Privileged Access Management• OT Backup and version control• OT Control assessments• Security policies• OT ITIL Handbook	<ul style="list-style-type: none">• Network Security Monitoring• Automated OT asset discovery• IT-OT network split• Incident response procedures	<ul style="list-style-type: none">• Business Impact Assessment• Third party risk management• Business continuity plan• Incident reporting• Cyber Awareness Program
---	---	--

Challenges to be aware of during rollouts

Resourcing projects • Availability of knowledge & resources per site • Required downtime • Embedding implemented solutions • Preventing previous behaviour.

Our approach to NIS2: Accelerate Cyber Resilience

Protect FrieslandCampina Supply Chain "From Grass to Glass"

Why:

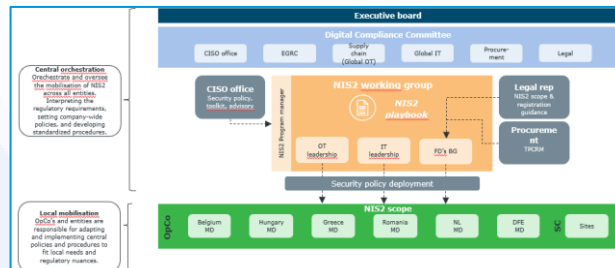
- In response to evolving cyber threats and regulatory mandates such as NIS2, FC is committed to significantly enhancing our cybersecurity resilience.
- Cyberattacks in the retail and consumer goods sector, including FMCG, surged by 30% in Q2 2024 compared to the same period in 2023 — highlighting the urgent need to accelerate our efforts.
- While we've made steady progress over the past two years, we are convinced that we can further improve our maturity level.

Target:

Reduce risk and ensure that a potentially business-halting **cyberattack becomes a contained incident** — prevented from spreading across sites or environments and effectively managed with acceptable disruption.

How:

Creating **One Joined Program** – support by the board - between **IT, OT and IRS** to accelerate individual initiatives and reducing the impacts factory downtime & resources.



Key take outs

- IT & OT are not converging – but to realize success collaboration between all disciplines is needed;
- Clearly define your future IT&OT organizations and ensure endorsement from Top Management;
- Ownership is key to success -> include your Supply Chain;
- Standards drive efficiency – Governance ensures alignment;
- Tooling will help you to succeed– but it does require preparation time.

Thank you for your time!



Q&A