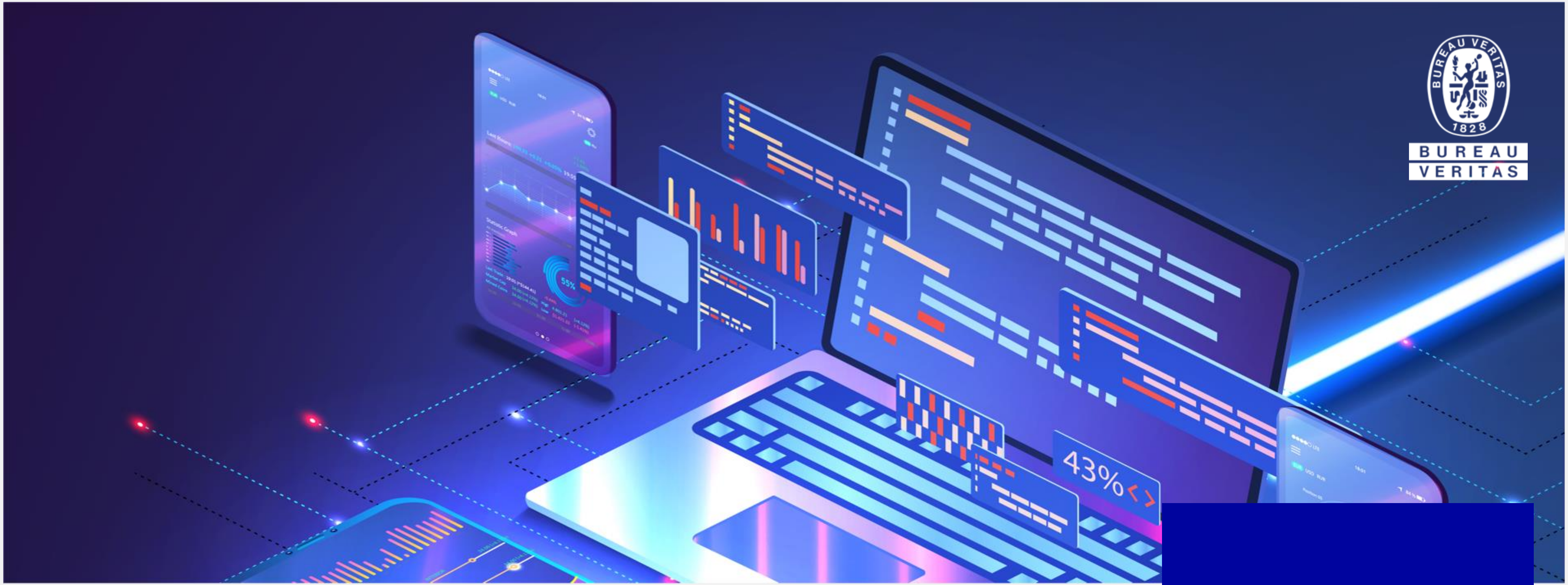


No Process Safety without Cybersecurity

Process Safety Congres – Dordrecht 14 May 2025

Dirk Jan van den Heuvel & Klaas-Otto Ykema

BUREAU VERITAS

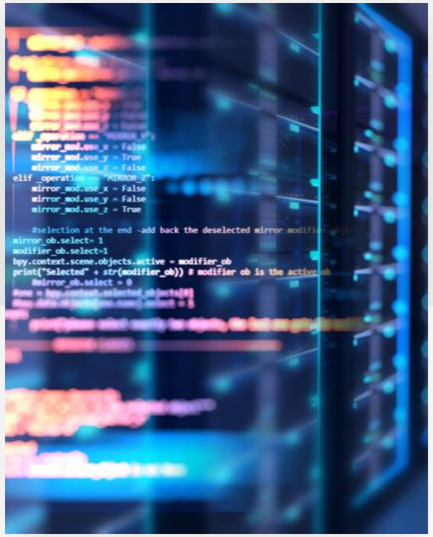
Topics to address

01

Intro

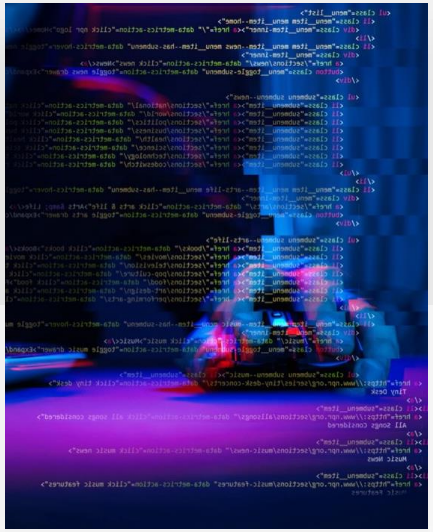
02

Safety & Cybersecurity



03

What to do to protect OT?



04

Critical infra / OT Regulation

05

Q & A

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

01.

Intro

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

ABOUT BUREAU VERITAS

ABOUT VERSATEC

INDEPENDENT EXPERT COMPANY

- ✓ Founded in 1993 in the Netherlands
- ✓ 40 FTE staff + flexible layer
- ✓ Part of Bureau Veritas Group since 2024

INTEGRATED SERVICES

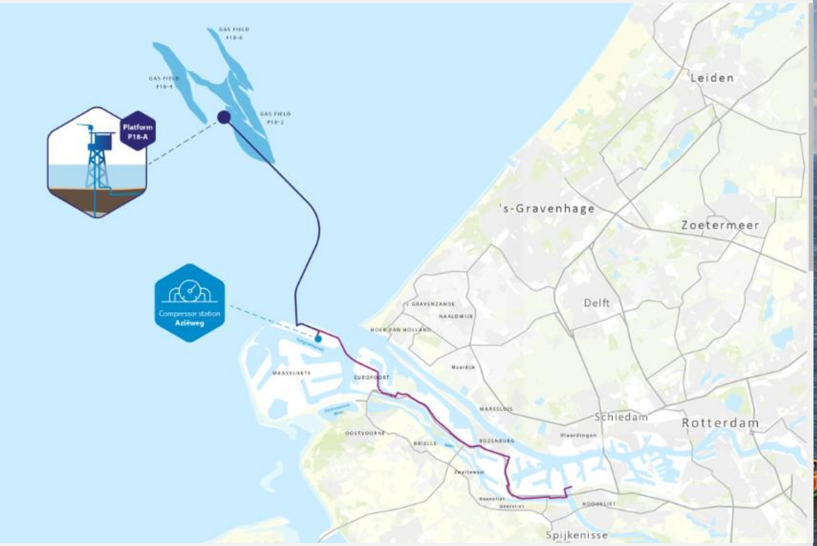
- ✓ Health Safety & Environment
- ✓ Operational Excellence
- ✓ Quality & Technical Compliance
- ✓ Technical Documentation & Training (E-learning)
- ✓ Digital Smart Solutions

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

TECHNICAL CONSULTANCY

- ✓ Technical consultancy in the offshore and energy industry
- ✓ To deliver safe and efficient operations and sustainable future in the energy mix
- ✓ Reduce project and operational risks, as well as reduce operational cost in asset life cycle



ABOUT SECURA / BV CYBER

INDEPENDENT EXPERT COMPANY

- ✓ Founded in 2000 in the Netherlands
- ✓ 200+ staff in NL / Europe
- ✓ Part of Bureau Veritas Group since 2021

INTEGRATED APPROACH

- ✓ People, process and technology
- ✓ IT, OT, IoT
- ✓ Using (international) standards, metrics and certification
- ✓ Assess & address

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

SECURA SERVICE OFFERING

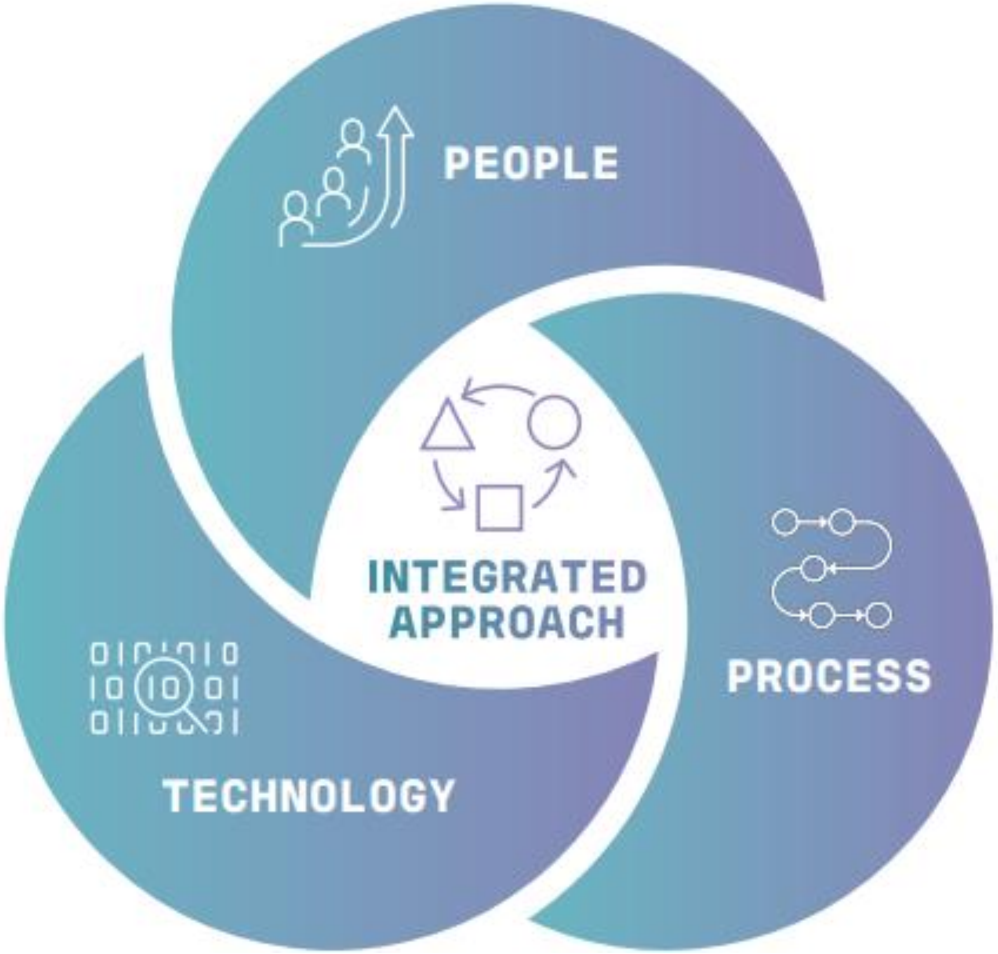
TECHNOLOGY

IT

- ❑ Pentesting Services
- ❑ Design Review
- ❑ Threat Modeling
- ❑ SIEM / SOC Testing

OT

- ❑ Site Assessment
- ❑ NIS2 Services
- ❑ Threat Modeling
- ❑ OT Cyber FAT / SAT



PEOPLE

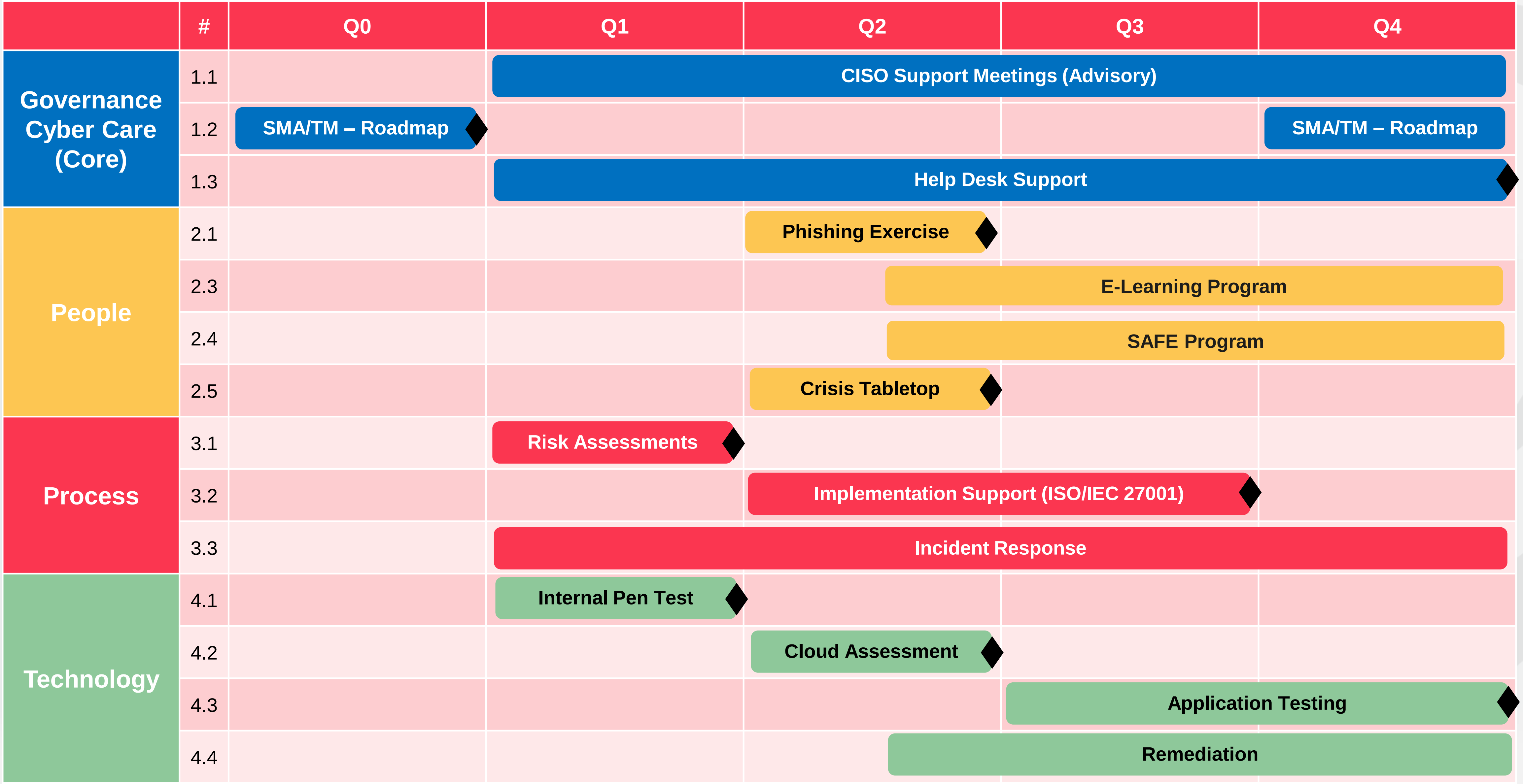
- ❑ Phishing
- ❑ Social Engineering
- ❑ E-learning
- ❑ Training Courses
- ❑ SAFE Program (Behavior)
- ❑ Security Behavior Review
- ❑ Tabletop Crisis Management

PROCESS

- ❑ Security Maturity Assessment
- ❑ Security Management Implementation
- ❑ NIS2 / DORA Services
- ❑ Audit & Assurance
- ❑ Crisis Management
- ❑ IT / OT Assessment
- ❑ Supply Chain Security

Secura A BUREAU VERITAS COMPANY versatec A BUREAU VERITAS COMPANY

EXAMPLE INTEGRATED APPROACH



	#	Q0	Q1	Q2	Q3	Q4
Governance Cyber Care (Core)	1.1		CISO Support Meetings (Advisory)			
	1.2	SMA/TM – Roadmap ◆				SMA/TM – Roadmap
	1.3		Help Desk Support ◆			
People	2.1			Phishing Exercise ◆		
	2.3			E-Learning Program		
	2.4			SAFE Program		
	2.5			Crisis Tabletop ◆		
Process	3.1		Risk Assessments ◆			
	3.2			Implementation Support (ISO/IEC 27001) ◆		
	3.3		Incident Response			
Technology	4.1		Internal Pen Test ◆			
	4.2			Cloud Assessment ◆		
	4.3				Application Testing ◆	
	4.4			Remediation		

02.

No Safety without Cybersecurity

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

```
        mirror_mod.use_y = True
        mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
        #mirror_ob.select = 0
```

Cyber-Physical Systems (CyPhy)

Operational Technology (OT)

Industrial Control Systems (ICS)

OT/ICS IS EVERYWHERE

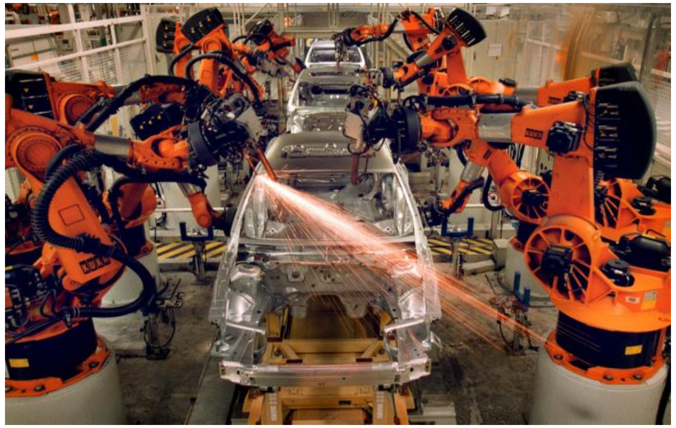
Electric

Oil & Gas

Water

Mining

Nuclear

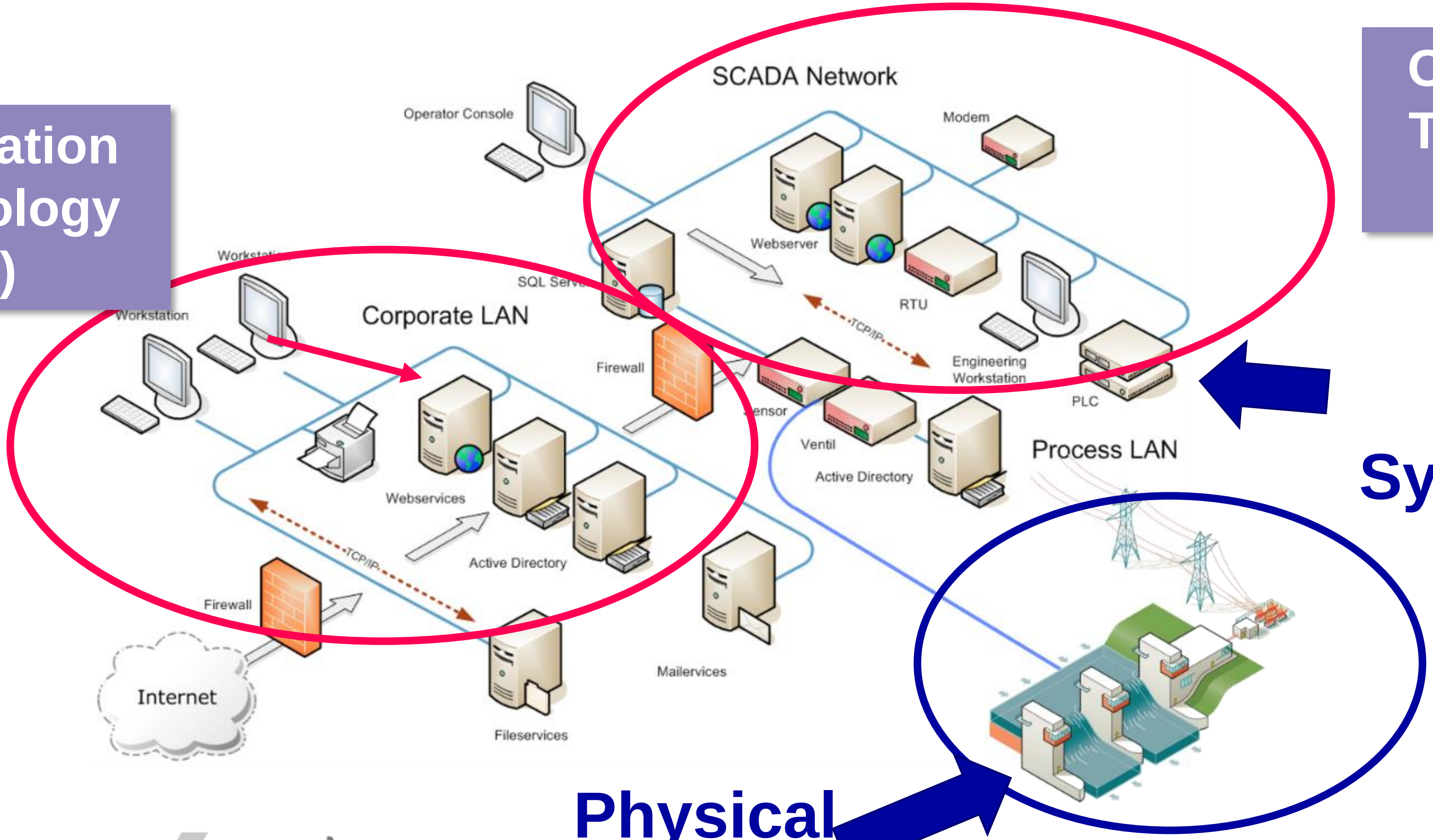


Manufacturing

INDUSTRIAL CONTROL SYSTEMS (ICS)

Information Technology (IT)

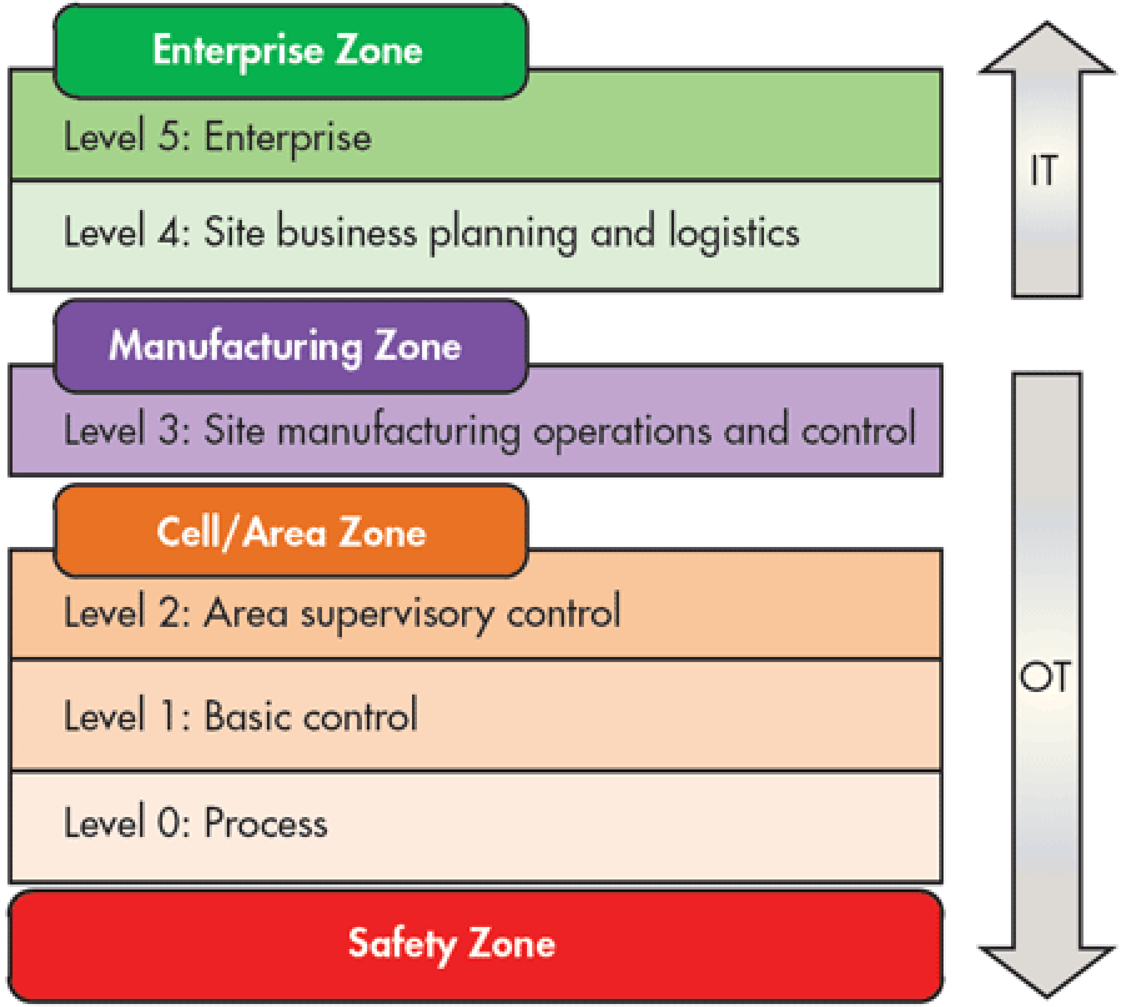
Operational Technology (OT)



Industrial Control Systems (ICS)

Physical process

PURDUE MODEL



Enterprise Zone

Level 5: Enterprise

Level 4: Site business planning and logistics

Manufacturing Zone

Level 3: Site manufacturing operations and control

Cell/Area Zone

Level 2: Area supervisory control

Level 1: Basic control

Level 0: Process

Safety Zone

IT

OT

Purdue Model for Control Hierarchy logical framework

Information Technology

- Enterprise domains—Levels 4 and 5
- Concerned with securing data
- Typically managing servers, workstations, email systems, databases, and applications

Operations Technology

- Plant domains—Levels 3 through 0
- Concerned with safety and availability of their physical and cyber assets because disruption could cause human harm or disruption to production and processes
- Typically maintaining production, process automation, and equipment spread throughout wide geographies such as transmission substations or water-pump stations

BRIEF TIMELINE OF ATTACKS TARGETING OT

MAROOCHY
Australia, 2000

STUXNET
Iran, 2010

BLACKENERGY
Urkaine, 2015

INDUSTROYER
Ukraine, 2016

TRITON
Saudi Arabia, 2017

WATER UTILITIES
Israel, 2020

PORT, GAS STATIONS, RAILWAYS*
Iran, 2020-2021

ЧЕРНІВЦІОБЛЕНЕРГО

UKRENERGO
State enterprise | National power company

بتــرورابــغ
Petro Rabigh

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

* Despite major operational disruptions, it seems IT systems of OT-heavy organisations were targeted

RANSOMWARE ATTACKS AGAINST OT ORGANIZATIONS

MAERSK
Global, Logistics, 2017

NORSK HYDRO
NO, Metal & Energy, 2019

WATER UTILITIES
Global, 2018-2020

ENERGY FIRMS
Global, 2020

COLONIAL PIPELINE
US, Oil & Gas, 2020

NEW COOPERATIVE
US, Agriculture, 2020

JBS
BR, Food, 2021

TRANSNET
ZA, Logistics, 2021

VDL
NL, Manufacturing, 2021

03.

How to protect OT systems against cyber risks?

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

RULE 1. ESTABLISH THE BASELINE

You Can’t Protect What You Don’t Know

What Should Be Mapped in a Cybersecurity Baseline?

- ➢All IT & OT Assets
- ➢User & Access Controls
- ➢Third-Party Risks
- ➢Regulatory & Compliance Status
- ➢ Known Vulnerabilities

RULE 2. ADOPT & IMPLEMENT A HOLISTIC DEFENSE STRATEGY

PEOPLE: THE FIRST LINE OF DEFENSE

80% of breaches start with human error – employee awareness is crucial.

Phishing simulations & cybersecurity training reduce social engineering risks.

Access control & multi-factor authentication (MFA) minimize unauthorized entry.

PROCESS: THE SECURITY BACKBONE

Cyber security governance and policies are a must.

Incident Response & Crisis management – Rapid response limits damage.

Regulatory and Standards Compliance prevents legal risks and strengthens overall resilience

TECHNOLOGY: ENHANCING PROTECTION

Segmentation

Usage of technologies in line with actual threats to counter attacks.

Data Encryption & Backup Strategies ensure business continuity.

Regular security assessments and tests to verify implemented measures

RULE 3. CHECK, DOUBLE CHECK

What to do?

- Security Maturity Assessments
- VAPT (Vulnerability Assessment & Penetration Testing)
- Red Teaming
- Crisis Simulation & Tabletop Exercises
- Ransomware Resilience

Why auditing, testing matters?

Without testing is no security

Most weaknesses detected too late

Train incident response teams

Building confidence

04.

Cybersecurity Regulation

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

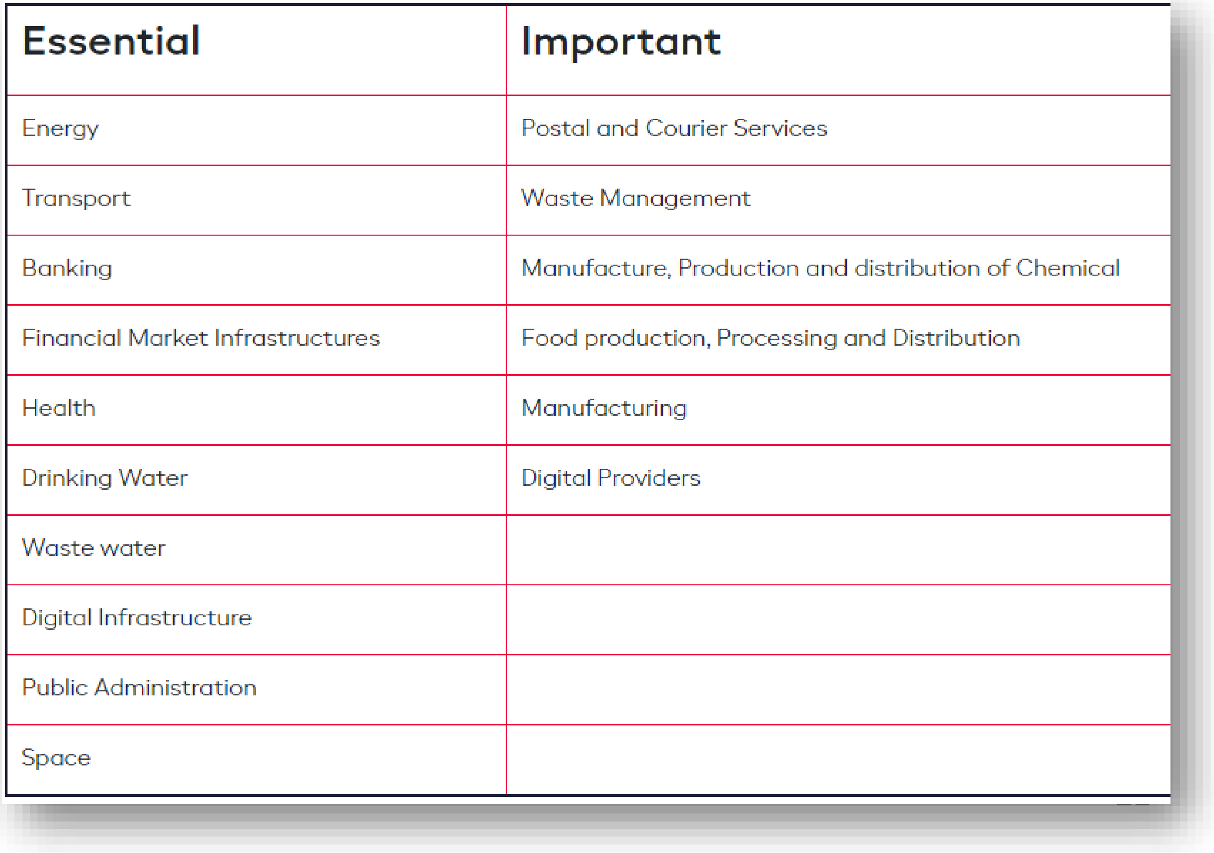
NIS2

Extension to NIS1 and applicable to more sectors

- Essential & Important sectors
- Personal accountability (directors)
- Much more…

National legislation effective from 2024/2025 onwards

- National law may be more restrictive than the EU directive.
- NL will implement this in Q3 2025

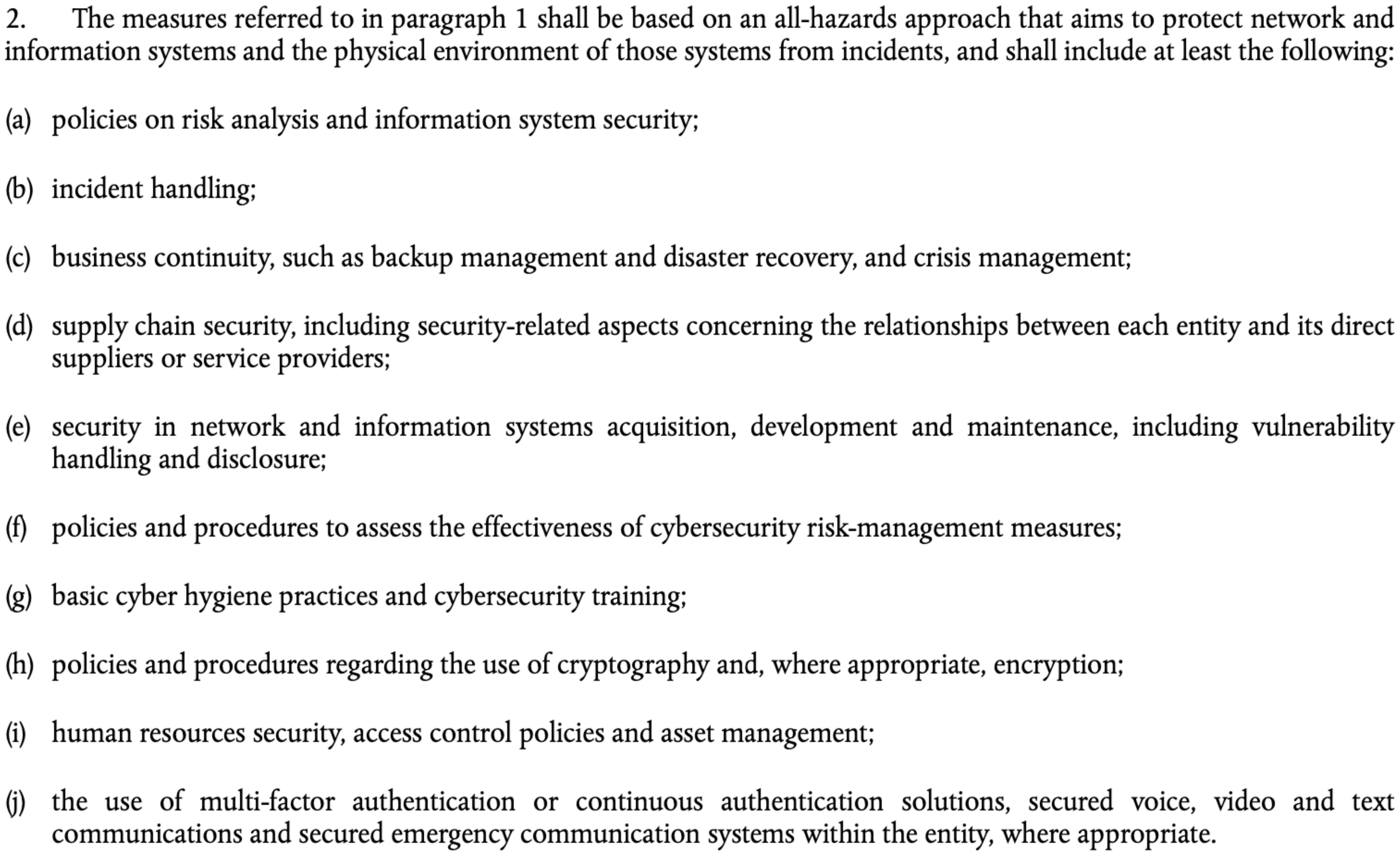


Essential	Important
Energy	Postal and Courier Services
Transport	Waste Management
Banking	Manufacture, Production and distribution of Chemical
Financial Market Infrastructures	Food production, Processing and Distribution
Health	Manufacturing
Drinking Water	Digital Providers
Waste water	
Digital Infrastructure	
Public Administration	
Space	

Secura A BUREAU VERITAS COMPANY versatec A BUREAU VERITAS COMPANY

NIS2

Article 21



2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

SUMMARY

- Operation Technology is critical in society
- There are severe risks for these systems
- These are different from risks in IT
- A holistic, structured approach is needed to protest these systems
- This requires a lot of competencies & expertise
- Regulations are in place for critical infrastructure

05.

Q&A

Secura
A BUREAU VERITAS COMPANY

versatec
A BUREAU VERITAS COMPANY

Secura

A BUREAU VERITAS COMPANY

versatec

A BUREAU VERITAS COMPANY

WWW.SECURA.COM

WWW.VERSATEC.NL

LEGISLATIVE ACTIVITIES IN EUROPE

2022

UNECE R155 & R156

New regulation for automotive sector - cars and supply chain

2023

CYBER SKILLS ACADEMY

EU wide program for closing the cyber skills gap

2024

NIS 2

Essential & Important Entities **must reinforce cyber measures and supply chain**

2025

DORA

Traditional and non-traditional financial institutes must implement cyber measures

2026 & BEYOND

CRA

All connected products must demonstrate cyber conformity

MPR

Machinery must account for AI and Cybersecurity for safety

RED

Radio devices must reinforce cybersecurity