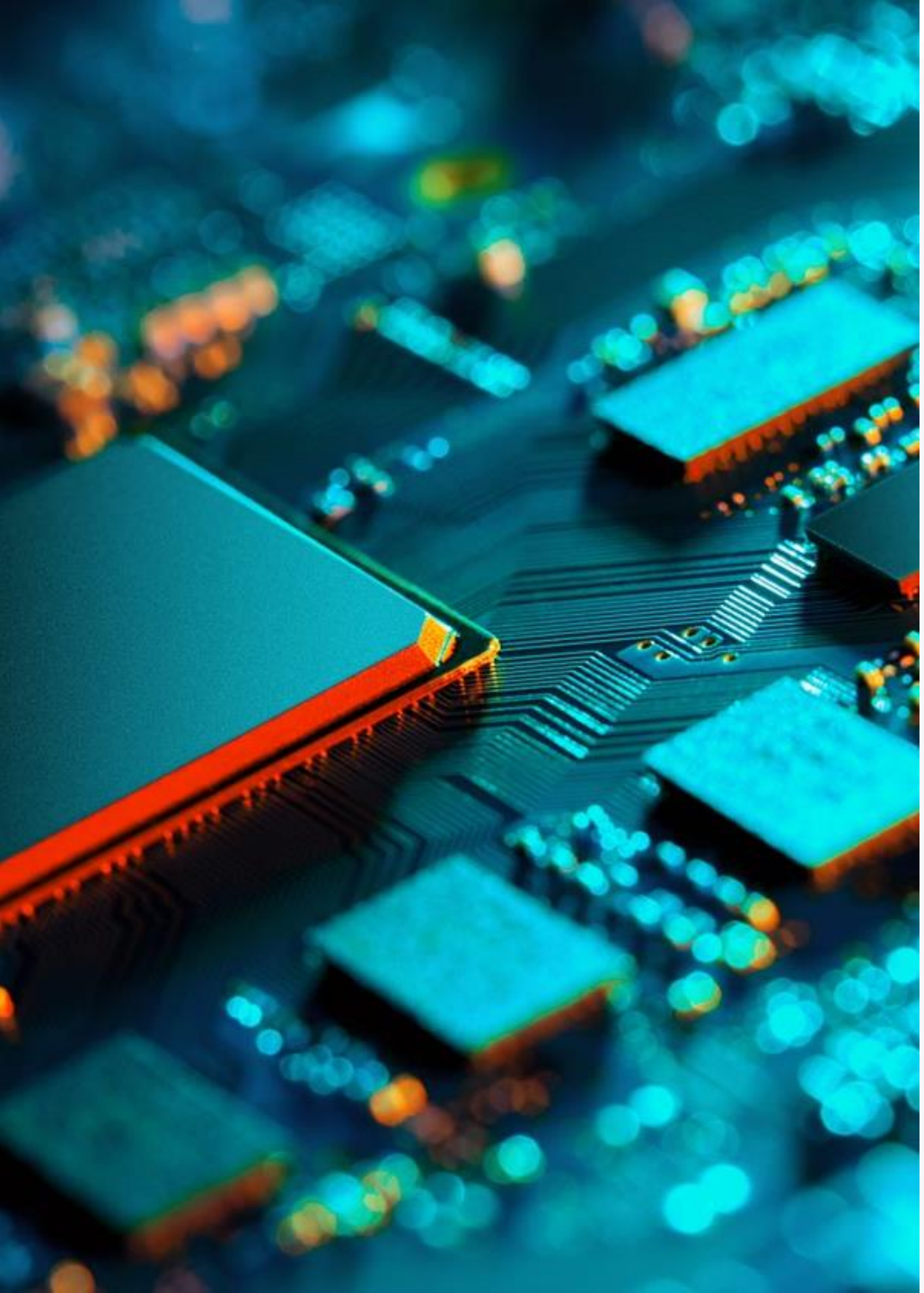


WEBINAR APRIL 2024

NIS2 DIRECTIVE

CYBERSECURITY IN THE PTX INDUSTRY

BUREAU VERITAS

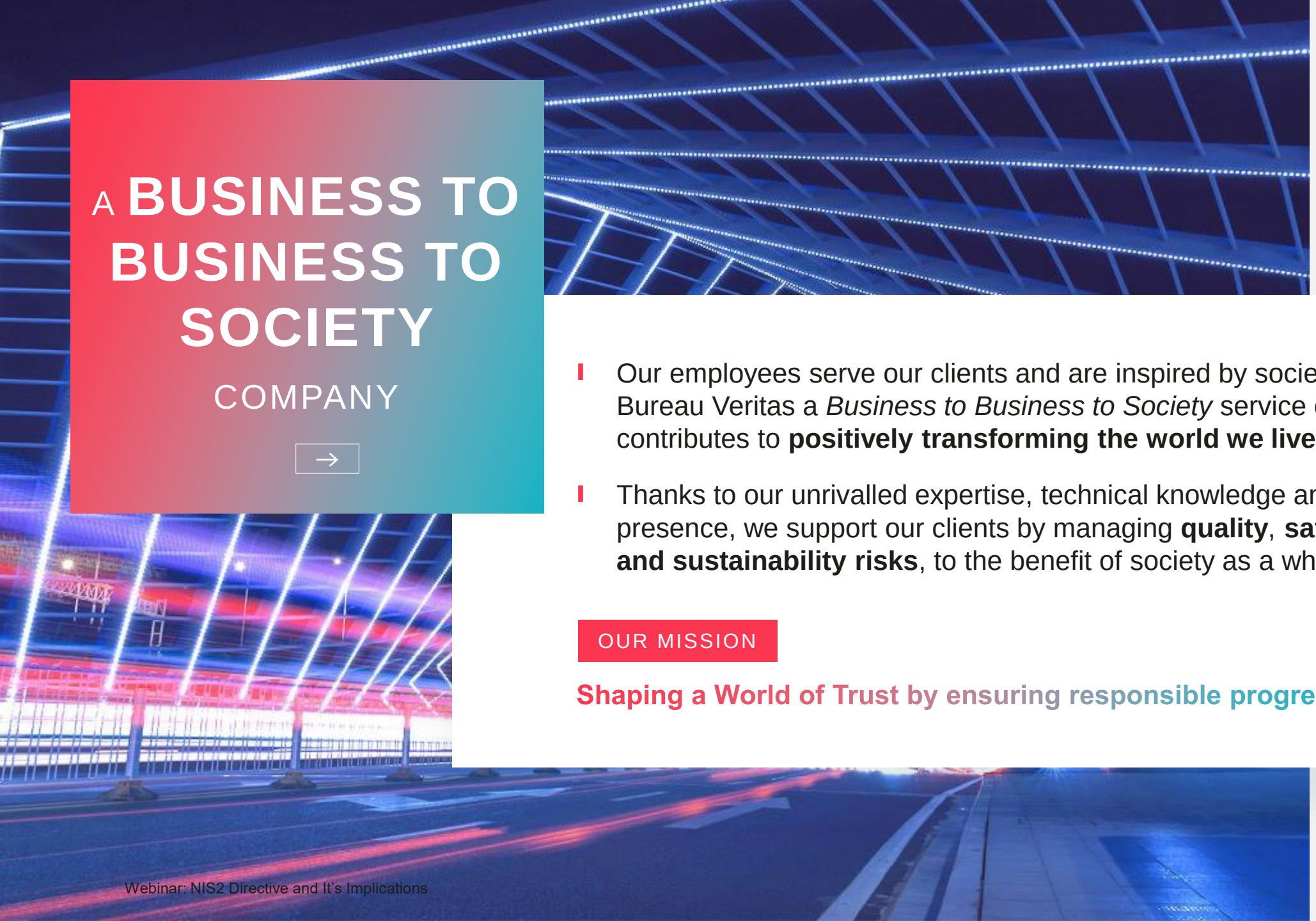
JENS BERTELSEN

Business Developer & Lead Auditor

- 40+ year in sales and ICT industry
- Certified lead implementer, certified lead auditor in ISO 9001 and ISO 27001
- Thorough knowledge of quality and information security, ISO 27001, IEC 62443 and cybersecurity in critical sectors
- Based in both private and public companies, I have a broad experience in quality, security, management systems, GDPR and data infrastructure
- Passionated about delivering inspiring teaching, where high professionalism is combined with practical experience and insight

KEY TAKEAWAYS

- Short about Bureau Veritas
- Summary of the NIS2 Directive and Its Implications for European Businesses
- Essential Provisions and Mandates of NIS2 Applicable to Organizations Across Diverse Sectors
- Practical Advice for Navigating NIS2 Compliance, Covering Risk Management and Incident Response Planning



A BUSINESS TO BUSINESS TO SOCIETY COMPANY

- Our employees serve our clients and are inspired by society; they make Bureau Veritas a *Business to Business to Society* service company that contributes to **positively transforming the world we live in**.
- Thanks to our unrivalled expertise, technical knowledge and worldwide presence, we support our clients by managing **quality**, **safety**, **health and sustainability risks**, to the benefit of society as a whole.

OUR MISSION

Shaping a World of Trust by ensuring responsible progress.

BUREAU VERITAS

KEY FIGURES

€5.7

billion

REVENUE IN 2022

c.84,000

employees*

400,000

clients

~1,600

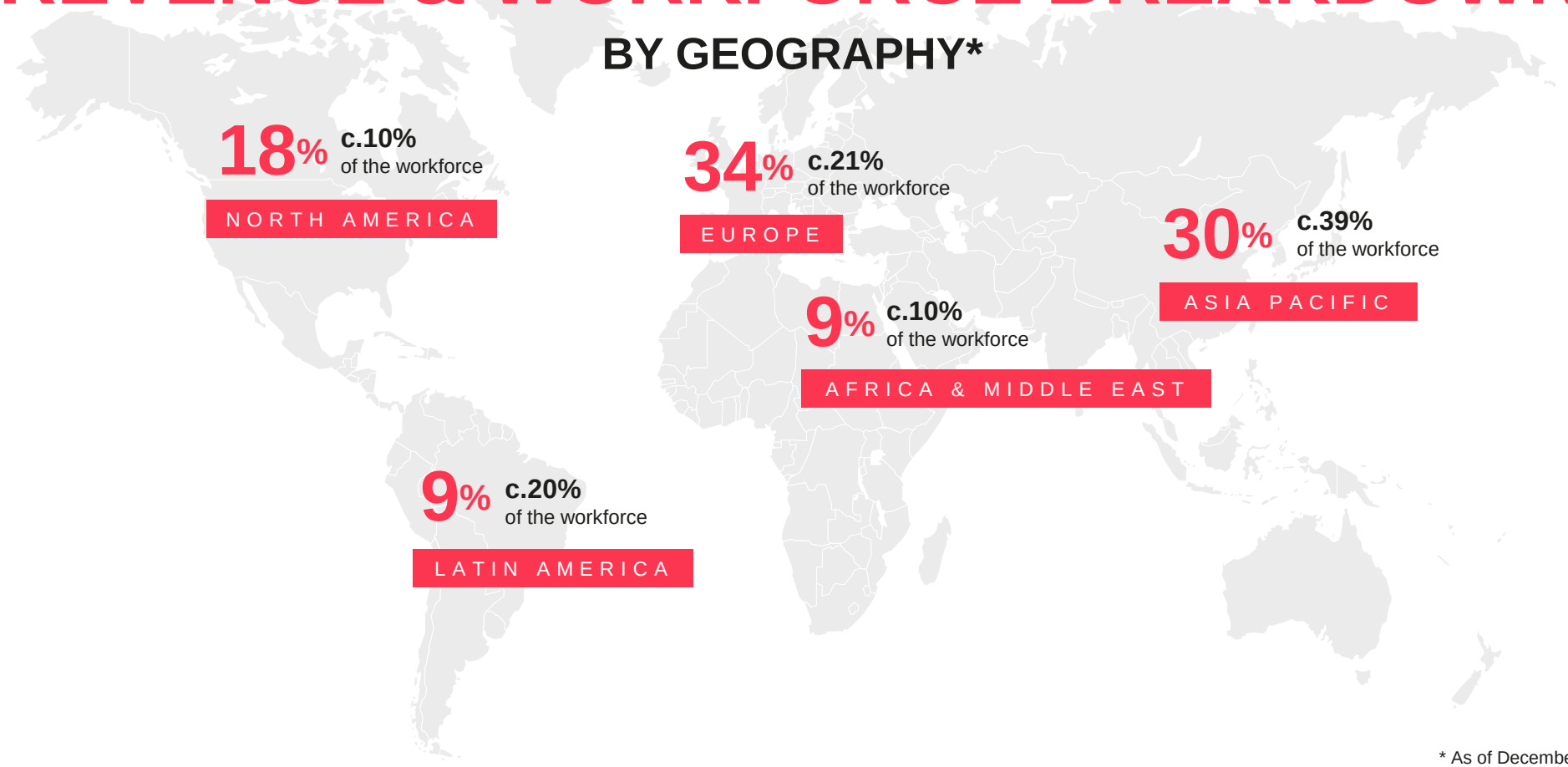
offices & laboratories

IN 140 COUNTRIES

* As of July 26, 2023

REVENUE & WORKFORCE BREAKDOWN

BY GEOGRAPHY*



18% c.10% of the workforce

NORTH AMERICA

34% c.21% of the workforce

EUROPE

30% c.39% of the workforce

ASIA PACIFIC

9% c.10% of the workforce

AFRICA & MIDDLE EAST

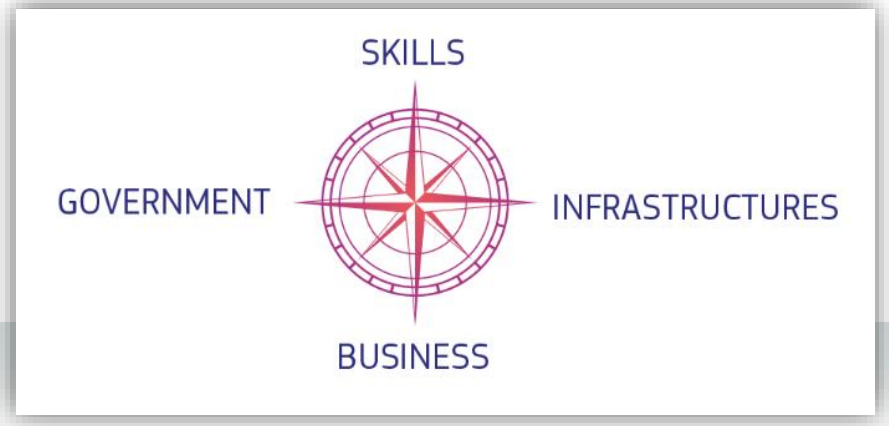
9% c.20% of the workforce

LATIN AMERICA

* As of December 31, 2022

EUROPE'S DIGITAL DECADE

- The EU's digital strategy aims to make the digital transformation work for citizens and businesses, while contributing **to achieving the goal of a climate-neutral Europe by 2050**.
- On 9 March 2021, the European Commission presented a vision and the way forward for **Europe's digital transformation by 2030**. The Commission is now phasing in a Digital Compass for the EU's Digital Decade, which revolves around four key points.



https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

EUROPE'S DIGITAL ÅRTI

2030 DIGITAL TARGETS

The European Commission adopted the Digital Decade programme in March 2021. It sets up four target areas:

- **Digital infrastructure and capacity by 2030:**
  - Gigabit for everyone, 5G everywhere
  - Europe wants its first computer with quantum acceleration, so Europe can be at the forefront of quantum capabilities by 2030
  - 10,000 climate-neutral secure edge node points
  - Doubling EU-based production of breakthrough and sustainable semiconductors

- **Digital education and skills by 2030:**
  - 20 million ICT specialists employed in the EU on gender convergence
  - Basic digital skills for at least 80% of the population

EUROPE'S DIGITAL DECADE

2030 DIGITAL TARGETS

- **Digital transformation of business by 2030:**
  - 75% of European companies have embraced cloud, AI, big data and artificial intelligence
  - More than 90% of European SMEs with at least a basic level of digital maturity

- **Digital government by 2030:**
  - 100% online delivery of essential public services
  - 100% of European citizens have access to medical records (e-records)
  - 80% of citizens use digital ID solutions

The European Parliament has launched more than 110 legislative proposals and actionplans to achieve these goals. They are expected to be adopted and implemented in the member states towards 2030 – including NIS2 from 2024

https://www.europarl.europa.eu/legislative-train/schedule

SOME KEY CYBER-RELATED INITIATIVES

- Digital Services Act (DSA)
- Digital Markets Act (DMA)
- European Chips Act
- European Digital Identity
- Artificial Intelligence (AI)
- European Data Strategy
- European Industrial Strategy
- Space Initiatives
- EU-US Trade and Technology Council
- Critical Entities Resilience Directive (CER Directive)
- Cyber Resilience Act
- Digital Operational Resilience Act (DORA)
- EU policy on Cyber Defence
- Proposal for the Cyber Solidarity Act
- Cyber diplomacy toolbox
- ….

NIS2 DIRECTIVE OVERVIEW

- NIS2 is the new version of the Net and Information Security Directive.
- NIS2 aims to enhance cybersecurity and information security across the EU by setting binding legal requirements.
- NIS2 significantly expands the scope of organizations covered.
- NIS2 imposes stricter cybersecurity requirements on organizations.
- NIS2 places responsibility on organizational leadership.
- NIS2 also covers public authorities.

SECTORS COVERED

Essential entities	Important entities
Energy (Electricity*, **EV charging**, **district heating**, oil, gas, **hydrogen**)	**Postal and courier services**
Transport (**air**, rail, water, road)	**Waste management**
Banking	**Chemicals** (**Manufacture, production, distribution**)
Financial marked infrast.	**Food** (**Manufacture, production, distribution**)
Health (Healthcare, **EU laboratories, product research and development, pharmaceutical products, manufacturing medical devices**)	**Manufacturing** **Medical devices, computer, electronic and optical products, electrical equipment, machinery and equipment, motor vehicles, trailers and semi-trailers and other transport equipment;** **(EFT L31 & Grp 26, 27, 28, 28, 29, 30 in NACE**)
Drinking water	Digital providers (online marketplaces, search engines, **social networking services platform**)
Waste water	
Digital infrastructure (IXP, DNS, TDL, Cloud, **Datacenters, Communication, Trust providers**)	
Public admin.	
Space and ground services	

MEASURES*

NIS2 art.	Demand
Article 3 -3 + 4	Entities shall **establish a point of contact** and provide at least the following information
Article 20, -1	Management bodies must approve risk and mitigating measures
Article 20, -1	Management shall supervise the implementation of mitigating measures
Article 20, -2	Members of management bodies must follow cybersecurity risk management training
Article 20, -2	Management bodies shall provide equivalent training to their employees
Article 21, -1	**The risks of societal and economic impact on the recipients of services must be mitigated**
Article 21, -2, a)	Risk analysis and information system security policies must be established
Article 21, -2, b)	Incidents must be handled and assessed
Article 21, -2, c)	Business continuity must be established, such as backup management and restoration
Article 21, -2, d)	Supply chain security needs to be identified and established, including direct supplier aspects
Article 21, -2, e)	Security shall be ensured in the acquisition, development and maintenance of network and information systems
Article 21, -2, f)	Policies and procedures shall be established to assess the effectiveness of cybersecurity risk management measures
Article 21, -2, g)	Basic cyber hygiene practices and cybersecurity training need to be established
Article 21, -2, h)	Policies and procedures regarding the use of cryptography and, where appropriate, encryption shall be established
Article 21, -2, i)	Establish staff security, access control policies and asset management
Article 21, -2, j)	Measures must be put in place to protect voice, video and text communications and to establish emergency communications
Article 23, -1)	Notification to the CSIRT of **any incident having a significant impact** on the provision of services shall be established

*) Note; The authorities may make further demands over the coming years

REPORTING OBLIGATIONS

Essential entities – Annex I	Other critical sectors – Annex II
a) on-the-spot checks and external supervision, including sample checks, to be carried out by trained professionals;	a) on-the-spot checks and external ex-post inspections carried out by trained professionals;
b) regular and targeted safety audits carried out by a qualified independent body or competent authority;	b) targeted safety audits carried out by a qualified independent body or competent authority;
c) ad hoc audits, including where justified by a significant incident or an infringement of this Directive by the essential entity;	-
d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary in cooperation with the affected entity;	c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary in cooperation with the affected entity;
e) requests for information necessary to assess the cybersecurity risk management measures put in place by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to provide information to the competent authorities pursuant to Article 27;	d) requests for information necessary to assess ex post the cybersecurity risk management measures put in place by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to provide information to the competent authorities pursuant to Article 27;
f) requests for access to data, documents and information necessary for the performance of their supervisory tasks;	e) requests for access to data, documents and information necessary for the performance of their supervisory tasks;
g) requests for evidence of the implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying documentation;	f) requests for evidence of the implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying documentation;

ISO/IEC-standards

New EU-legislation

The company's management system

QMS/ISMS
IT/OT Security Management System

STANDARDS ARE STAKEHOLDERS

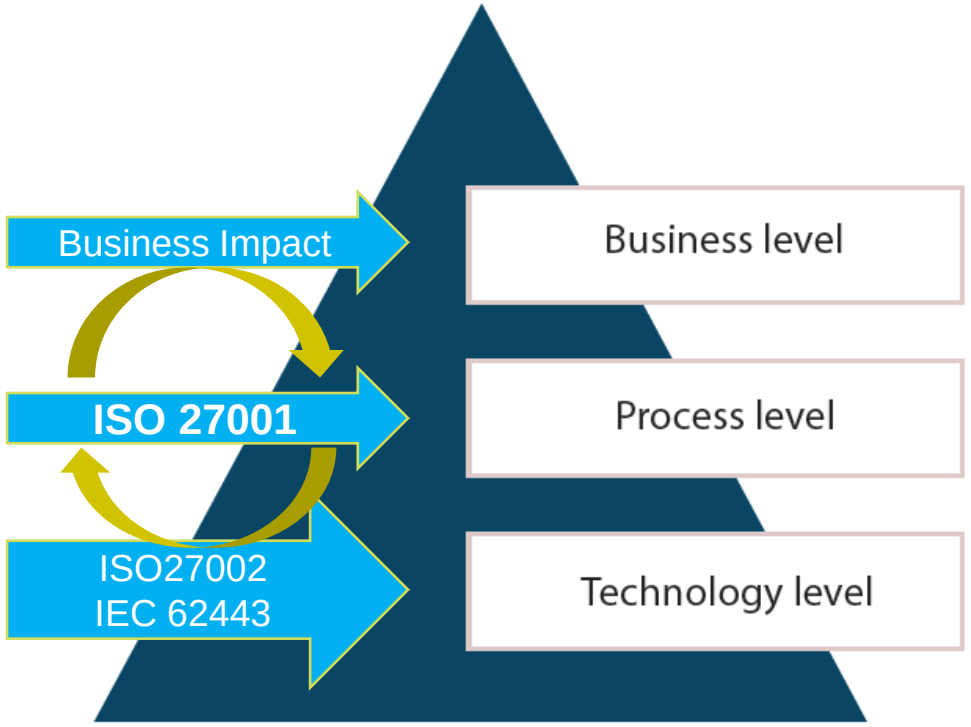
- ***ISO/IEC 27001****: An international standard for information security management systems (ISMS) that can be customized to meet the security needs of IT, OT, and IoT environments*
- ***ISO 22301****: ISO 22301 is an international standard for business continuity management (BCMS). It provides guidelines for establishing, implementing, monitoring, maintaining and improving an effective business continuity system*
- ***IEC 62443****: This series of standards focuses on safety in industrial automation and control systems (IACS).*
- ***ISO/IEC 15408*** *(Common Criteria): An international standard for evaluating the security of IT, OT and IoT products and systems.*
  NIST Cybersecurity Framework*: NIST SP 800-82 Rev. 2. This guidance from the National Institute of Standards and Technology (NIST) provides guidelines for improving the cybersecurity of industrial control systems.*
- ***IEEE 802.1X****: A standard for port-based access control for networks that may be relevant for ensuring access to OT and IoT devices on the network.*

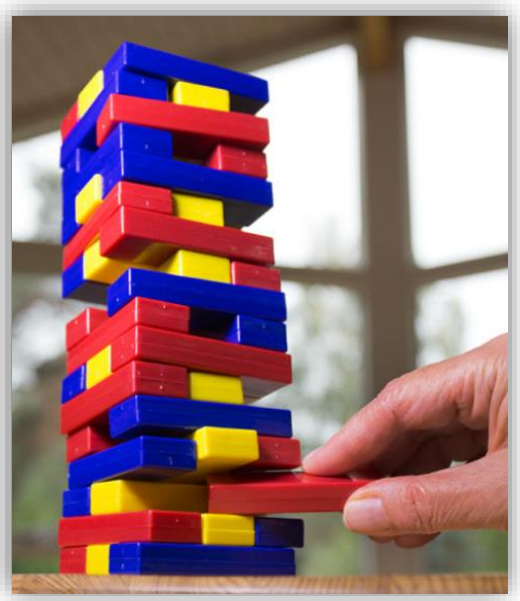
UNDERSTAND FIRST THE PROCESS

How do we earn money? Which value propositions do we offer?

Which processes do we have?

Specific technologies within IT / OT

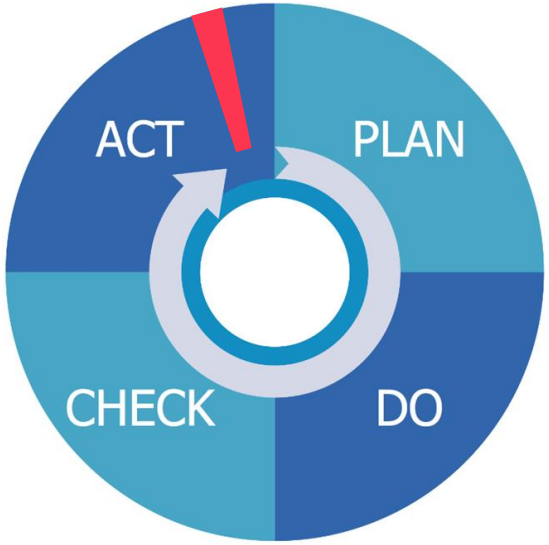




PLAN DO CHECK ACT

10) Continuous improvement
10a) Accredited certification (option)

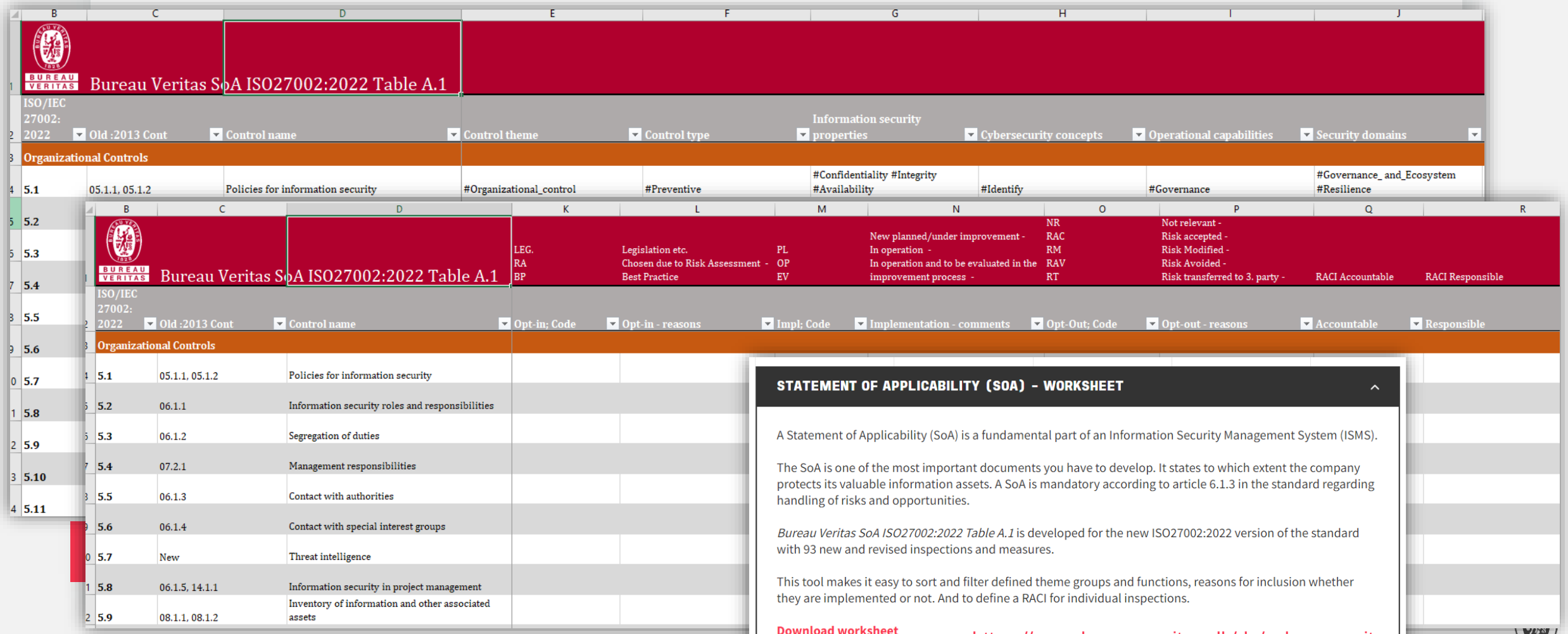
8) Internal Testing and Audit Program
9) Management review



1) Understand terms and requirements
2) Business Impact (BIA)
3) Risk management
4) Business Case
5) Policies and objectives

6) Process- and control implementation
7) Statement of Applicability

IMPLEMENTATION



STATEMENT OF APPLICABILITY (SOA) - WORKSHEET

A Statement of Applicability (SoA) is a fundamental part of an Information Security Management System (ISMS).

The SoA is one of the most important documents you have to develop. It states to which extent the company protects its valuable information assets. A SoA is mandatory according to article 6.1.3 in the standard regarding handling of risks and opportunities.

Bureau Veritas SoA ISO27002:2022 Table A.1 is developed for the new ISO27002:2022 version of the standard with 93 new and revised inspections and measures.

This tool makes it easy to sort and filter defined theme groups and functions, reasons for inclusion whether they are implemented or not. And to define a RACI for individual inspections.

Download worksheet

https://www.bureauveritas.dk/da/cybersecurity

CERTIFICATION

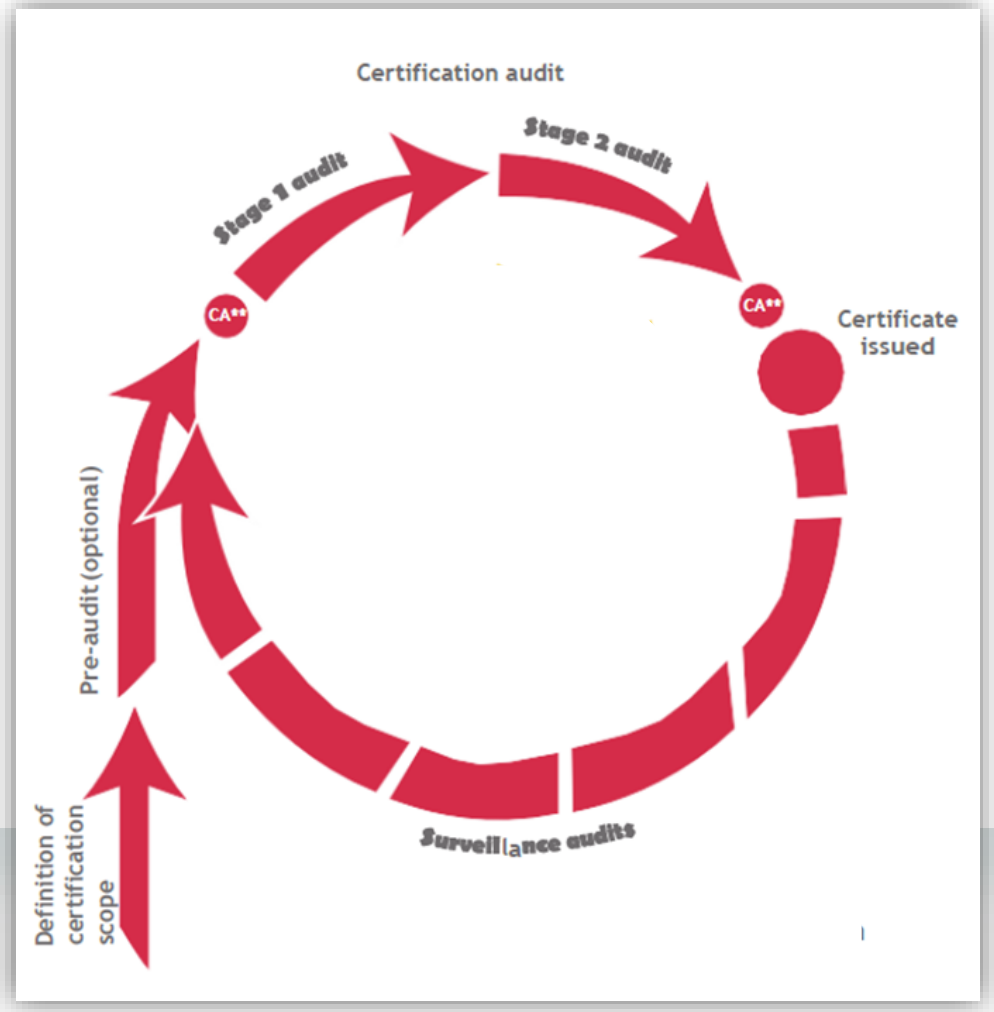
- Certification is the process by which an independent third-party organization evaluates and certifies that a device, product, process, or organization meets certain standards or requirements.

- The certification is a kind of quality stamp that shows that the certified device – by random sampling – meets the established standards and requirements.

- Certification has several purposes
  - *Quality stamp*
  - *Trust and credibility*
  - *Compliance with rules and regulations*
  - *Continuous improvement*

ACCREDITED CERTIFICATION

- Definition of certification Scope
- Preliminary inspection
- Main control — year 1
- Corrective actions and certification
- Maintenance Visits – Years 2 and 3
- Recertification



NEXT STEP

How to proceed?

01 Sign up for our free webinar regarding ISO 27001 certification I May 15th
https://www.bureauveritas.dk/da/events-og-downloads (In Danish)

02 Read more about ISO 27001 certification
https://www.bureauveritas.dk/en/needs/iso-27001-certification

03 Training: Introduction to NIS2 (In Danish)
https://www.bureauveritas.dk/da/kurser/class-intro-til-nis2-hvad-er-det-hvad-betyder-det-og-hvordan-kommer-vi-i-gang

04 Training: ISO 27001 Internal Auditor (In English & Danish)
https://www.bureauveritas.dk/da/kurser/class-iso-27001-internal-auditor-english

QUESTIONS

WWW.BUREAUVERITAS.DK