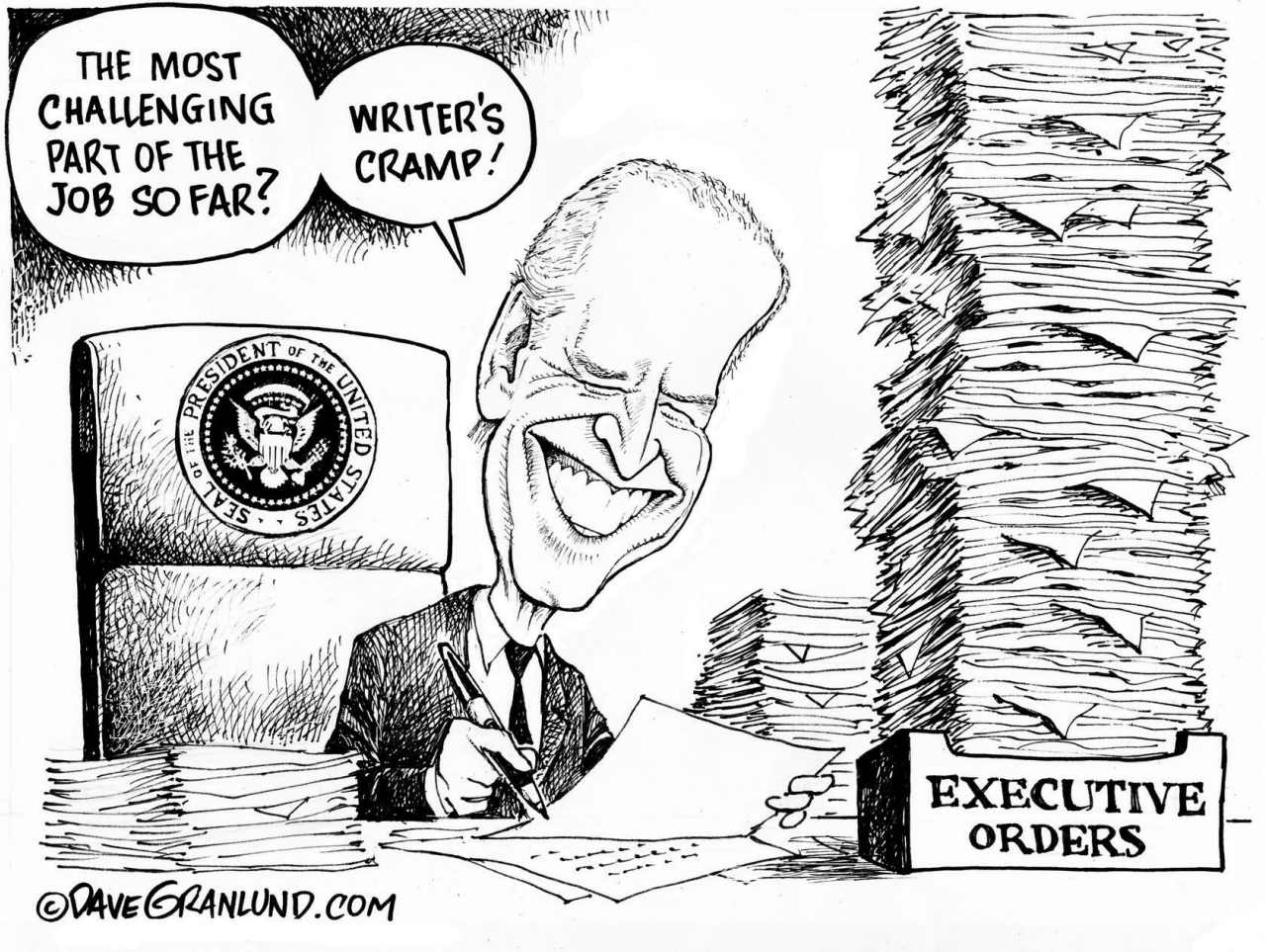
MASTER OF SCIENCE
IN ENGINEERING

TSM_SecIndOpT

Securing OT-relevant aspects of SCADA, DCS & ICS (II) Version: 1.2

Luca Haab | 02.03.2025 | Cours MSE


THE MOST CHALLENGING PART OF THE JOB SO FAR?
WRITER'S CRAMP!
SEAL OF THE PRESIDENT OF THE UNITED STATES
EXECUTIVE ORDERS
©DAVE GRANLUND.COM

The bigger picture: a “survival” policy

- As cybersecurity risks are becoming clearer, governments are introducing programs to counter those
- Those programs go beyond standardization as they request sensible information from suppliers of products or services. Examples are:
  - Full bill of material (HW and SW)
  - Full access to SW code
  - Localised production
  - Full access to personnel files
  - …

Trump's Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (2017)

ECONOMY NATIONAL SECURITY BUDGET IMMIGRATION ENERGY

EXECUTIVE ORDERS

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

INFRASTRUCTURE & TECHNOLOGY | Issued on: May 11, 2017

SHARE:

ALL NEWS

EXECUTIVE ORDER

_ _ _ _ _ _ _

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

Sources:
https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ and https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

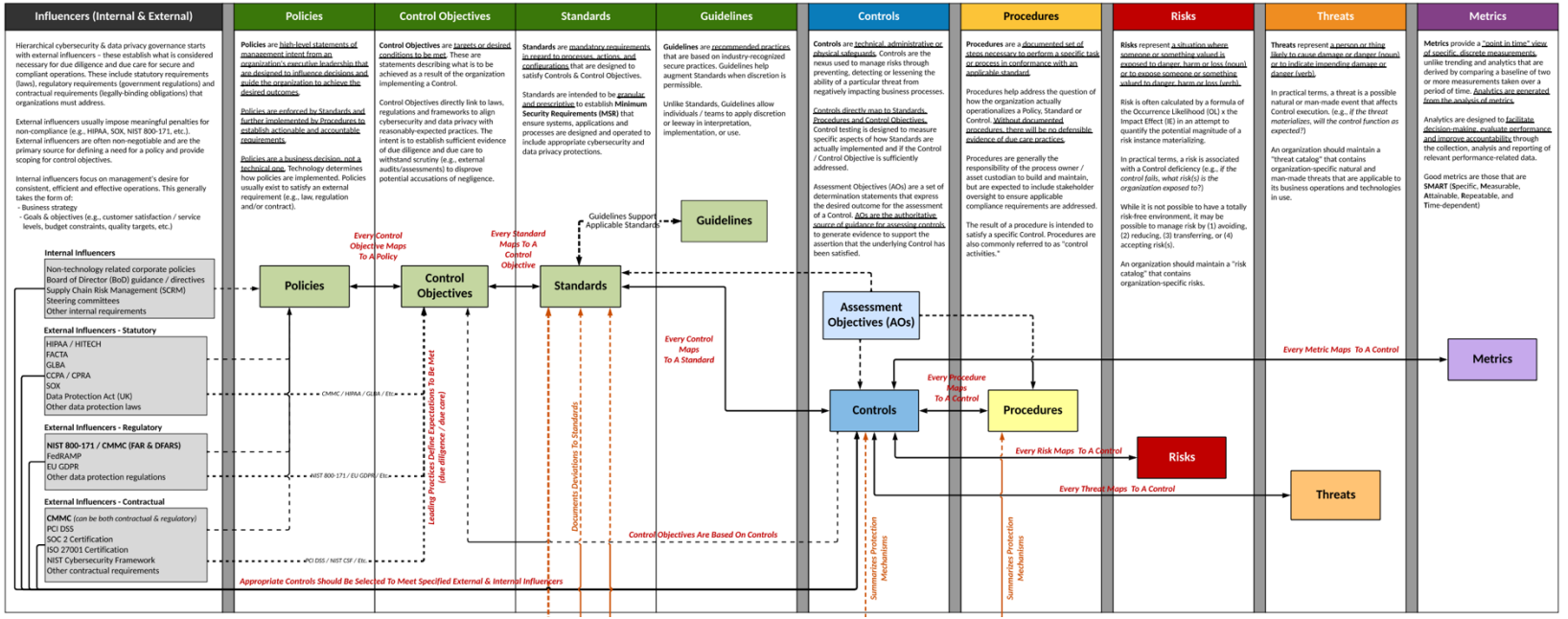
An example: Joe Biden's Executive Order "Improving the Nation's Cybersecurity" (2021)

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector
  - The EO ensures that IT Service Providers are able to share information with the government and requires them to share certain breach information.
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government
  - The EO helps move the Federal Government to secure cloud services and a zero-trust architecture, and mandates deployment of multifactor authentication and encryption within a specific time period.
- Improve Software Supply Chain Security
  - The EO will improve the security of software by establishing baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into their software and making security data publicly available.
  - It also creates a pilot program to create an "energy star" type of label so the government – and the public at large – can quickly determine whether software was developed securely.
- Establish a Cyber Safety Review Board
  - The EO establishes a Cyber Safety Review Board, co-chaired by government and private sector leads, with the authority to convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. This board is modeled after the National Transportation Safety Board, which is used after airplane accidents and other incidents.
- Create Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
  - The EO creates a standardized playbook and set of definitions for cyber vulnerability incident response by federal departments and agencies. The playbook will ensure all federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat and serve as a template for the private sector to use in coordinating response efforts.
  - Improve Detection of Cybersecurity Incidents on Federal Government Networks.
  - The EO improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response (EDR) system and improved information sharing within the Federal Government.
- Improve Investigative and Remediation Capabilities
  - The EO creates cybersecurity event log requirements for federal departments and agencies to improve an organization's ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact.

- Sources: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ and https://www.cisa.gov/executive-order-improving-nations-cybersecurity

USA are not alone…

Policies vs Standards vs Guidelines vs Procedures



Source: https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf

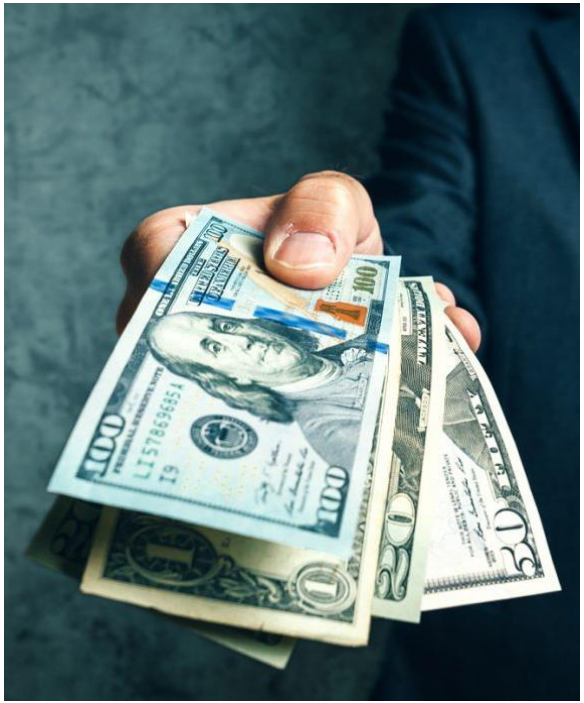
Standardization

Companies want standardization as it allows them to:

I. **maximize** the business benefits;

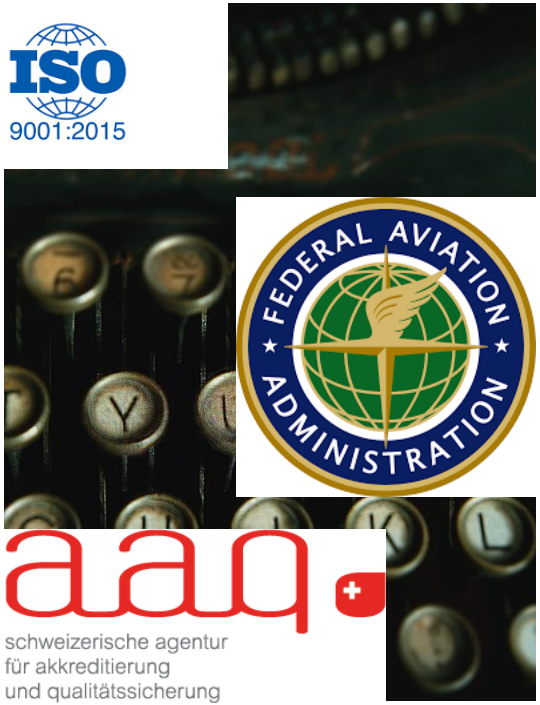
II. **institutionalize** the best practices in standards;

III. **be compliant** with contract obligations, national laws regulations & directives.



Standardization: Main Goals

Standardization != Certification



- Standard = formulae that describes the best way of doing something*
- Certification = provision by an independent body of written assurance (a certificate) that specific requirements are met

Source: https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_ISO.pdf

Standard Bodies

And the list is far from being complete

- International Electrotechnical Commission (IEC)
- National Institute of Standards and Technology (NIST)
- North American Electric Reliability Corporation (NERC)
- International Council on Large Electric Systems (CIGRE)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- American National Standards Institute (ANSI)
- International Society of Automation (ISA)
- Industrial Internet Consortium (IIC)
- OPC Foundation
- American Water Works Association (AWWA)
- DNP3 Users Group
- Modbus Organization
- European Telecommunications Standards Institute (ETSI)
- Underwriters Laboratories (UL)
- American Petroleum Institute (API)
- …

An example: Industrial Automation

International Electrotechnical Commission (IEC):
Specializes in standards for electrical and electronic technologies, including automation systems.

International Organization for Standardization (ISO):
Develops a broad range of standards covering quality, safety, and management practices.

American National Standards Institute (ANSI):
Oversees the creation of standards in the U.S., including industrial processes and safety guidelines.

European Norms (EN):
These are technical standards ratified by one of the three European Standards Organizations (ESO): European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), or European Telecommunications Standards Institute (ETSI)

Source: https://eltra-trade.com/blog/essential-standards-in-industrial-automation

An example: Industrial Automation

- Safety
- Communication
- Programming
- Quality Management
- Environmental and Energy Efficiency
- Cybersecurity

An example: Industrial Automation

IEC	Purpose	Scope	Benefits
60950-1	Safety requirements for information technology equipment	Applies to electrical equipment designed for connection to mains supply	Ensures safety and reduces electrical hazards
61010-2-201	Safety requirements for electrical equipment for measurement, control, and laboratory use	Covers safety requirements for electrical equipment used in these environments	Enhances safety and reliability in measurement and control environments
61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	Applies to all safety-related systems that use electrical/electronic/programmable electronic technologies	Ensures functional safety and reduces risk of failures
62061	Functional safety of safety-related electrical, electronic, and programmable electronic control systems	Specific to machinery applications	Improves safety in machinery operations
61511	Functional safety – Safety instrumented systems for the process industry sector	Applies to safety instrumented systems in the process industry	Ensures reliable operation of safety systems in process industries
62443	Security for industrial automation and control systems	Covers cybersecurity aspects of industrial automation systems	Protects against cyber threats and enhances system security

IEC	Purpose	Scope	Benefits
61800-5-1	Adjustable speed electrical power drive systems – Safety requirements	Applies to adjustable speed electrical power drive systems	Promotes energy efficiency and safe operation
61000	Electromagnetic compatibility (EMC) standards	Covers EMC requirements for electrical and electronic equipment	Ensures equipment does not interfere with other devices
61131	Programmable controllers	Defines standards for programmable controllers, including programming languages	Enhances interoperability and standardization in control systems
61499	Function blocks for industrial-process measurement and control systems	Applies to function blocks used in industrial process control	Promotes reusability and interoperability of control system components
61512	Batch control	Provides guidelines for batch control processes	Ensures consistent and reliable batch processing
60204-1	Safety of machinery – Electrical equipment of machines	Covers safety requirements for electrical equipment used in machinery	Enhances safety and compliance in machinery operations
13849	Safety of machinery – Safety-related parts of control systems	Applies to the design and integration of safety-related parts of control systems	Improves safety and reliability of machinery control systems
60947	Low-voltage switchgear and controlgear	Specifies standards for low-voltage switchgear and controlgear	Ensures reliable operation and safety in industrial environments

ISO	Purpose	Scope	Benefits
9001	Quality management systems – Requirements	Applies to any organization, regardless of size or industry	Improves quality management, enhances customer satisfaction
14001	Environmental management systems – Requirements with guidance for use	Applicable to any organization seeking to manage its environmental responsibilities	Reduces environmental impact, improves sustainability
45001	Occupational health and safety management systems – Requirements	Designed for organizations to improve employee safety, reduce workplace risks	Enhances workplace safety, reduces accidents and illnesses
ISO/IEC 27001	Information security management systems – Requirements	Applicable to any organization managing sensitive information	Protects information assets, enhances data security
22000	Food safety management systems – Requirements for any organization in the food chain	Covers all organizations in the food chain, from farm to fork	Ensures food safety, improves consumer confidence
13485	Medical devices – Quality management systems – Requirements for regulatory purposes	Specific to organizations involved in the design, production, installation, and servicing of medical devices	Ensures quality and safety of medical devices, meets regulatory requirements

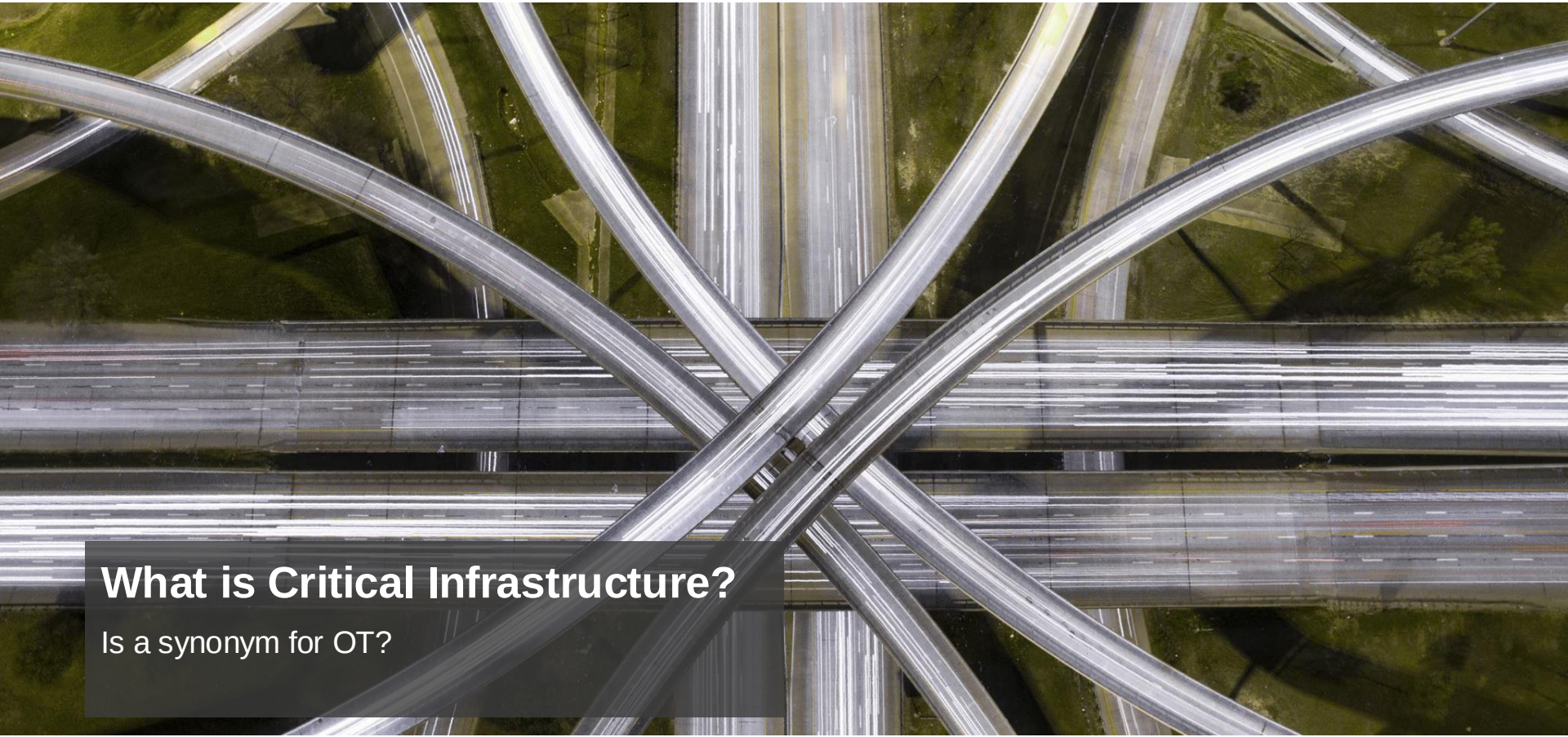
ANSI	Purpose	Scope	Benefits
ANSI/ASME B31	Code for Pressure Piping	Covers design, materials, construction, and testing of piping systems	Ensures safety and reliability of piping systems
ANSI/IEEE C2	National Electrical Safety Code	Covers safety standards for the installation, operation, and maintenance of electrical supply and communication lines	Ensures electrical safety, reduces risk of electrical hazards
ANSI/NFPA 70	National Electrical Code	Provides guidelines for safe electrical design, installation, and inspection	Enhances electrical safety, reduces risk of fire and electrical accidents
ANSI/ISEA Z87.1	Occupational and Educational Personal Eye and Face Protection Devices	Specifies requirements for eye and face protection devices	Improves safety, reduces risk of eye and face injuries
ANSI/ISO 14001	Environmental Management Systems	Applicable to any organization seeking to manage its environmental responsibilities	Reduces environmental impact, improves sustainability
ANSI/ISO 9001	Quality Management Systems	Applies to any organization, regardless of size or industry	Improves quality management, enhances customer satisfaction
ANSI/ASQ Z1.4	Sampling Procedures and Tables for Inspection by Attributes	Provides sampling procedures for inspection by attributes	Ensures consistent quality control, reduces inspection costs
ANSI/ASHRAE 90.1	Energy Standard for Buildings Except Low-Rise Residential Buildings	Specifies minimum energy efficiency requirements for buildings	Improves energy efficiency, reduces energy consumption and costs
ANSI/ISA-88	Batch Control	Provides guidelines for batch control processes	Ensures consistent and reliable batch processing

EN	Purpose	Scope	Benefits
EN 1	Flued oil stoves with vaporizing burners	Applies to oil stoves with vaporizing burners	Ensures safety and performance of oil stoves
EN 54	Fire detection and fire alarm systems	Covers components and systems for fire detection and alarm	Improves fire safety, ensures reliable detection and alarm systems
EN 115	Safety of escalators and moving walks	Specifies safety requirements for escalators and moving walks	Improves safety, reduces risk of accidents
EN 166	Personal eye protection	Specifies requirements for eye protection devices	Enhances safety, reduces risk of eye injuries
EN 286	Simple unfired pressure vessels designed to contain air or nitrogen	Applies to pressure vessels for air and nitrogen	Ensures safety and reliability of pressure vessels
EN 60204-1	Safety of machinery – Electrical equipment of machines	Covers safety requirements for electrical equipment used in machinery	Enhances safety and compliance in machinery operations
EN 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems	Applies to safety-related systems using electrical/electronic/programmable technologies	Ensures functional safety, reduces risk of failures
EN 62061	Functional safety of safety-related electrical, electronic, and programmable electronic control systems	Specific to machinery applications	Improves safety in machinery operations
EN 62443	Security for industrial automation and control systems	Covers cybersecurity aspects of industrial automation systems	Protects against cyber threats, enhances system security

Standards/Certification: always an obligation?

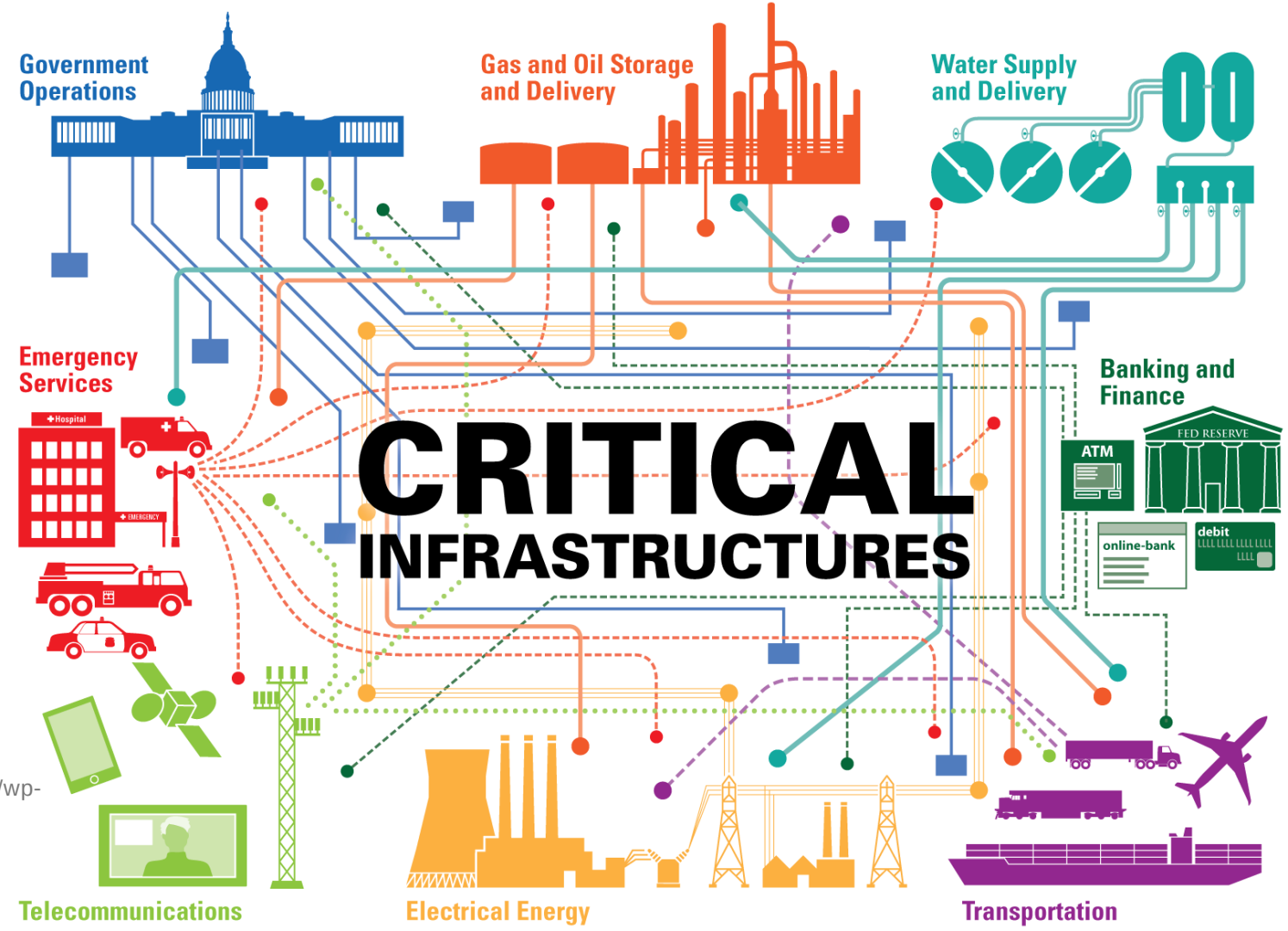
- Ensures fulfillment of necessary quality
- Allow preferred access to market
- Defines obligations and gives guarantees

More information: https://cytrics.inl.gov/cytrics/



What is Critical Infrastructure?

Is a synonym for OT?



Source: https://privacy108.com.au/wp-content/uploads/2020/12/critical-infrastructure-01.png

C(H)ritical Infrastructure

Energy (natural gas supply, oil supply, power supply, district and process heating)

Finances (financial and insurance services)

Information & communication
(information technologies, media, postal service, telecommunications)

Public administration (teaching and research, cultural assets, parliament, government, justice, administration)

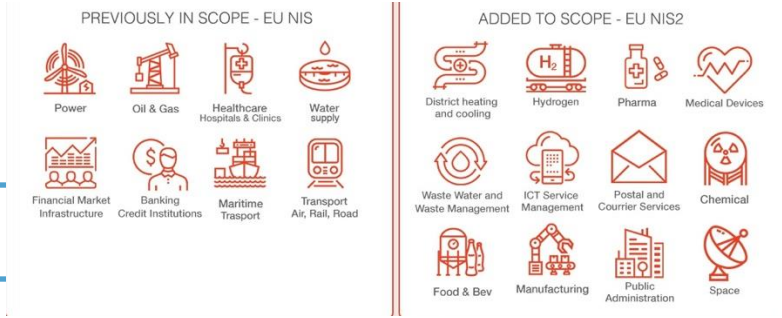
Public health (medical care, laboratory services)

Public safety (armed forces, emergency services, civil defence)

Transport (air transport, rail transport, road transport, water transport)

Food and water (food supply, water supply)

Waste disposal (refuse, sewage)



Source: https://applied-risk.com/resources/valentines-day-industrial-tech-talk-the-eu-nis2-directive-and-cyber-security

Source: https://www.babs.admin.ch/en/critical-infrastructures

Critical Infrastructure Priorities

Sektoren	Teilsektoren (Branchen)
Behörden	Forschung und Lehre
	Kulturgüter
	Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung
	Erdölversorgung
	Fern- und Prozesswärme
	Stromversorgung
Entsorgung	Abfälle
	Abwasser
Finanzen	Finanzdienstleistungen
	Versicherungsdienstleistungen
Gesundheit	Medizinische Versorgung
	Labordienstleistungen
	Chemie und Heilmittel
Information und Kommunikation	IT-Dienstleistungen
	Telekommunikation
	Medien
	Postdienste
Nahrung	Lebensmittelversorgung
	Wasserversorgung
Öffentliche Sicherheit	Armee
	Blaulichtorganisationen
	Zivilschutz
Verkehr	Luftverkehr
	Schienenverkehr
	Schiffsverkehr
	Strassenverkehr

Sehr grosse Kritikalität*

Grosse Kritikalität*

Erhebliche Kritikalität*

★► Die Kritikalität steht für die relative Bedeutung des Teilsektors bezüglich möglicher Auswirkungen eines Ausfalls des Teilsektors von wenigen Tagen bis Wochen auf die Bevölkerung und die Wirtschaft.

► Die Gewichtung macht keine Aussagen über die Kritikalität von einzelnen Objekten.

► Die Gewichtung orientiert sich an einer normalen Gefährdungslage. Bei Katastrophen und Notlagen kann sich die Kritikalität der Teilsektoren ändern.

Settori	Sottosettori
Autorità	Ricerca e insegnamento
	Beni culturali
	Parlamento, governo, giustizia, Amministrazione
Energia	Approvvigionamento di gas
	Approvvigionamento di petrolio
	Teleriscaldamento e calore di processo
	Approvvigionamento di elettricità
Smaltimento	Rifiuti
	Acque reflue
Finanze	Servizi finanziari
	Servizi assicurativi
Sanità pubblica	Prestazioni mediche
	Servizi di laboratorio
	Chimica e agenti terapeutici
Informazione e comunicazione	Servizi informatici
	Telecomunicazioni
	Media
	Servizi postali
Alimentazione	Approvvigionamento alimentare
	Approvvigionamento idrico
Sicurezza pubblica	Esercito
	Organizzazioni di pronto intervento
	Protezione civile
Trasporti	Traffico aereo
	Traffico ferroviario
	Traffico navale
	Traffico stradale

Criticità molto elevata*

Criticità elevata *

Criticità marcata*

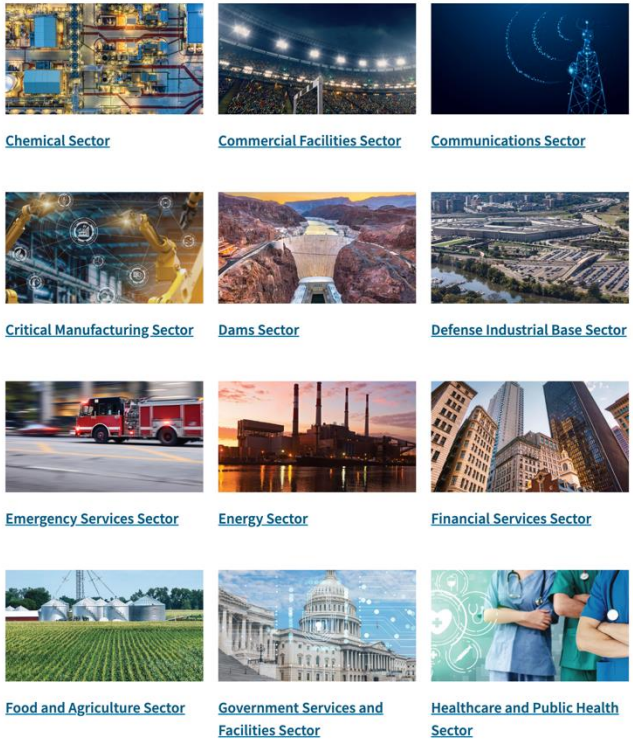
★► Per criticità s'intende l'importanza relativa del sottosettore in relazione a possibili conseguenze di una sua interruzione di pochi giorni fino a settimane.

► Dalla ponderazione non si possono trarre conclusioni sulla criticità di singoli oggetti.

► La ponderazione si basa su una situazione di minaccia normale. In caso di catastrofi e situazioni d'emergenza, la criticità dei sottosettori può cambiare.

Source: https://www.babs.admin.ch/en/publications-on-critical-infrastructure-protection

swissuniversities



Source: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Source: https://www.ey.com/en_ie/are-you-ready-for-nis2-how-will-it-impact-your-organisation-are-you-prepared

Flags, source: https://en.wikipedia.org/

Obligations (as per NIS2*)

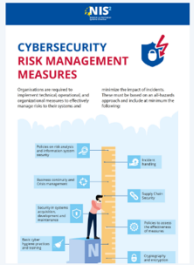
Policies on risk analysis and information system security
Incident handling
Business continuity, including backup management, disaster recovery, and crisis management
Supply chain security
Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
Policies and procedures to assess the effectiveness of cyber security risk-management measures
Basic cyber hygiene practices and cyber security training
Policies and procedures regarding the use of cryptography and encryption
Human resources security, access control policy, and asset management
The use of Multi-Factor Authentication (MFA) and secured emergency communications
A coordinated vulnerability disclosure policy

Source: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
*: Network and Information Systems 2 (NIS2) is active since 10/2024

Topic 1: What You Need to Know
Infographic / Video

Topic 2: What's new in NIS2

Topic 3: Sectors in Scope



Topic 4: Risk Management Measures

Topic 5: Incident Reporting Obligations

Topic 6: EU-Level Collaboration

For more information about NIS2

- The European Union Agency for Cybersecurity - NIS 2 https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2
- The legal text https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Do not mix with DORA (Directive 2022/2554 financial entities to improve their digital resilience) and CER (Directive 2022/2557, overarching framework addressing resilience of critical entities)

swissuniversities

Consequence

– Chapter 8 Criminal Provisions

– Art. 60 Violation of obligations to provide access and information or to cooperate

– Art. 2

[1] The controlle [1] On complaint, a fine not exceeding 250,000 francs shall be imposed on private persons who:

subject's personality or fundamental rights as quickly as possible.

[2] In the notification, it shall as a minimum specify the nature of the breach of data security, its consequences and the measures taken or planned.

[3] The processor shall notify the controller of any breach of data security as quickly as possible.

[4] The controller shall inform the data subject if this is required for their protection or if the FDPIC so requests.

[5] It may limit, delay or dispense with the provision of information to the data subject if:

a. there is a reason for doing so pursuant to Article 26 paragraph 1 letter b or paragraph 2 letter b or the provision of information is prohibited by a statutory duty of confidentiality;
b. the provision of information is impossible or requires disproportionate effort; or
c. the provision of information to the data subject is equally guaranteed by making a public announcement.

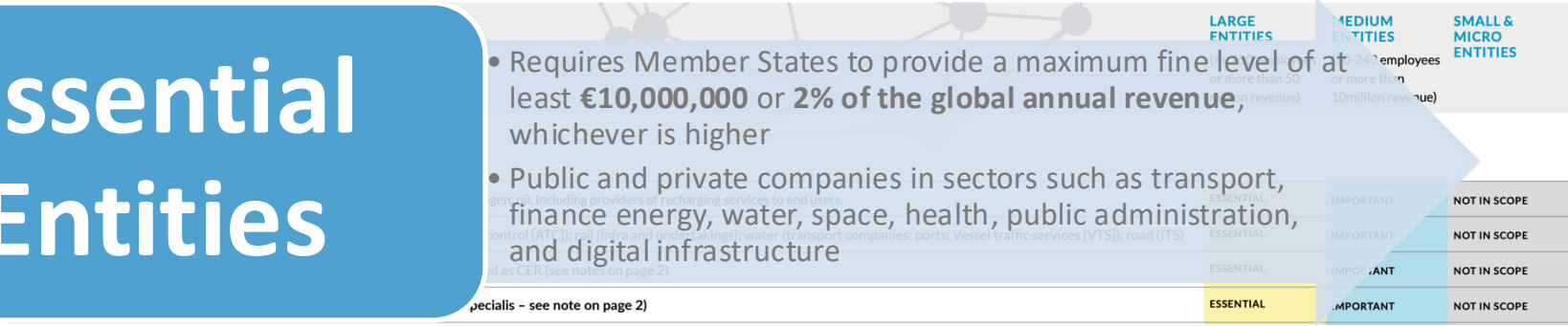
[6] A notification made pursuant to this Article may only be used against the person required to notify in criminal proceedings with that person's consent.

Federal Act on Data Protection (01.09.2023) - https://www.fedlex.admin.ch/eli/cc/2022/491/en

Consequence (II) - EU

Essential Entities

- Requires Member States to provide a maximum fine level of at least **€10,000,000** or **2% of the global annual revenue**, whichever is higher
- Public and private companies in sectors such as transport, finance energy, water, space, health, public administration, and digital infrastructure



Important Entities

- Requires Member States to fine for a maximum of at least **€7,000,000** or **1,4% of the global annual revenue**, whichever is higher
- Public and private companies in sectors such as foods, digital providers, chemicals, postal services, waste management, research, manufacturing

For definition of entities: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_2_ENTITIES.pdf

Other consequences

- Article of the Swiss Criminal Code*
  - Data theft (Art. 143)
  - Unauthorised access to a data processing system (Art. 143bis)
  - Data damage (Art. 144)
  - Computer fraud (Art. 147)
  - Obtaining personal data without authorisation (Art. 179)
  - Disclosure of personal data to a third country or an international body (Art. 349c)
- Information Security Act (Informationssicherheitsgesetz, ISG** / Legge sulla sicurezza delle informazioni, LSIn***)
- …

*: https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en
**: https://www.fedlex.admin.ch/eli/oc/2024/257/de
***: https://www.fedlex.admin.ch/eli/oc/2024/257/it


Some light at the end of the tunnel

Assess your maturity

- SME Quick Check: https://itsec4kmu.ch/cyber-check-landingpage
- ENISA CSIRT Assessment tool: https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity

Food for thoughts

- 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION

(reading for a lengthy coffee break as it entails way more than OT)

References

- https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf
- https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_ISO.pdf
- https://www.cencenelec.eu/european-standardization/international-policy/iso-and-iec/
- https://www.isa.org/standards-and-publications/isa-standards
- https://www.babs.admin.ch/en/publications-on-critical-infrastructure-protection
- https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2
- https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_2_ENTITIES.pdf
- https://itsec4kmu.ch/cyber-check-landingpage
- https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity
- https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ics.html