Cybersecurity Risk Management and Governance

CSP003_C_E

PRESENTATION BY:

PROF. DR. SHAREEFUL ISLAM
CHATZOPOULOU ARGYRO

Cybersecurity Risk Management and Governance

01. Goals: Who-What-Why you need to take this training

02. Training logistics: When-Where-How

03. Learning outcomes

04. Training outlines

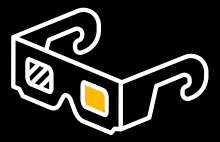
05. Exercises details

06. Practical information and requirements

07. Registration information and contacts

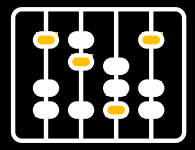
Goals: Who-What-Why you need to take this training

WHO



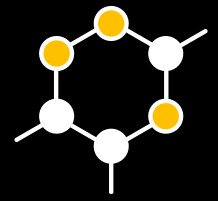
WHO can attend the training modules and profiles of the attendees

WHAT



basic concepts regarding Cybersecurity Risk Management and Governance as seen and applied within the Energy domain

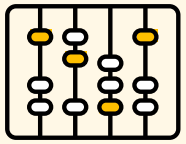
WHY



Equipping participants with the knowledge and skills necessary to implement concepts of governance within an organization

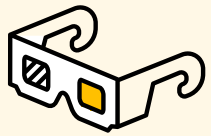
CSP Training Logistic: When-Where-How

WHEN



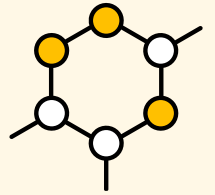
Time schedule: …..

WHERE



ONLINE-ONSITE-Location Information

HOW



Delivery Method

Value Propositions

Benefits to Participants

- Level of Training Module: Advanced
- Cybersecurity Professional Training
- Hands-on and Practical Skills Development
- Rooted with European Cybersecurity Skills Framework
- Cutting-edge insights from industry-academic experts
- Specialized information on the energy sector
- Certificate of the completion
- Helps with skills development and career advancement

WHO

Profile of Training Participants

- IT professional
- Security professionals
- Business leaders

and any other professionals that need or want to understand the basic concepts related to Cybersecurity risk management and Governance.

WHO

Prof. Dr. Shareeful Islam

Highly motivated and committed cyber security and risk management professional with experience in research, training and consultancy.

Consultant for managing cyber security risks and information security management system to develop risks management framework following ISO 27001:2013, ISO31000:2018, NIST-CSF, STIX threat modelling, CIS_CSC and other relevant standards in various business environments.

Certified Management of Risks (MoR), PRINCE 2 practitioner and a subject matter expert in Risk Management

Over 90 peer reviewed publications with top journals and conference

https://scholar.google.com/citations?user=IAxS1IsAAAAJ&hl=en

WHO

Chatzopoulou Argyro (Iro)

Experienced Lead Auditor and Trainer with a demonstrated history of working in the services industry. Skilled in all kinds of audits including ISO 27001, Information Systems, IT Service Management, Privacy, Quality and Business Continuity.

A person with strong communication and management skills honed through conducting more than 1500 audits, delivering more than 500 training courses and managing teams nationally or internationally.

- Member of CEN/CLC/JTC 13 "Cybersecurity & Data Protection“
- Member of the ISO/IEC JTC1 SC27 "Information Security, Cybersecurity & Data Privacy“
- Member to the Ad-Hoc Working Group on the European Cybersecurity Skills Framework

WHAT

Training Topics

- Cyber security in energy sector
- Risk Management framework Governance processes
- Role, responsibilities and authorities
- Security controls and industry specific standards related to security management and governance

WHY

Learning Outcomes

- Demonstrate an in-depth understanding of cyber security risk management framework in energy sector;
- Recognize the significant cybersecurity governance structures and processes in the energy sector;
- Critically assess and report security risk and suggest suitable mitigation strategies in professional manner
- Critically develop and evaluate security policy and select controls by following ISO 27019 for security governance.

Background Knowledge and Prerequisites

Background knowledge:

Basic understanding of computers and networking (IT)

Basic understanding of cybersecurity concepts

Prerequisites:

None

Registration: How to register and other practical information

The specific registration process for the Cybersecurity Risk Management and Governance training may vary depending on the training provider or institution. However, the general steps are typically straightforward and can be completed online or in person.

1. Online Registration
2. In-Person Registration
3. Additional Practical Information

Evaluation method

Evaluation Element	How	Notes
Coursework portfolio	Learner needs to produce a 3000-word portfolio at the end of the module by performing a list of tasks to demonstrate the learning outcomes are achieved.	(80%) Summative assessment
Presentation	Learners need to present the outcomes of the portfolio to demonstrate their understanding	(20%) Summative assessment
Group discussion	During the seminar	

Training Outline:
Part 1

Topic-1: Cyber security in energy sector

Cyber security fundamentals

Cyber security context in energy sector

Topic-2: Risk Management framework

Risk management Basics

Principles of risk management and processes

Cybersecurity threats and vulnerability management in the energy sector

Examples and exercises

Course progress

01. Cyber security in energy sector

02. Risk Management framework

03. Security controls and standards of the specific domain

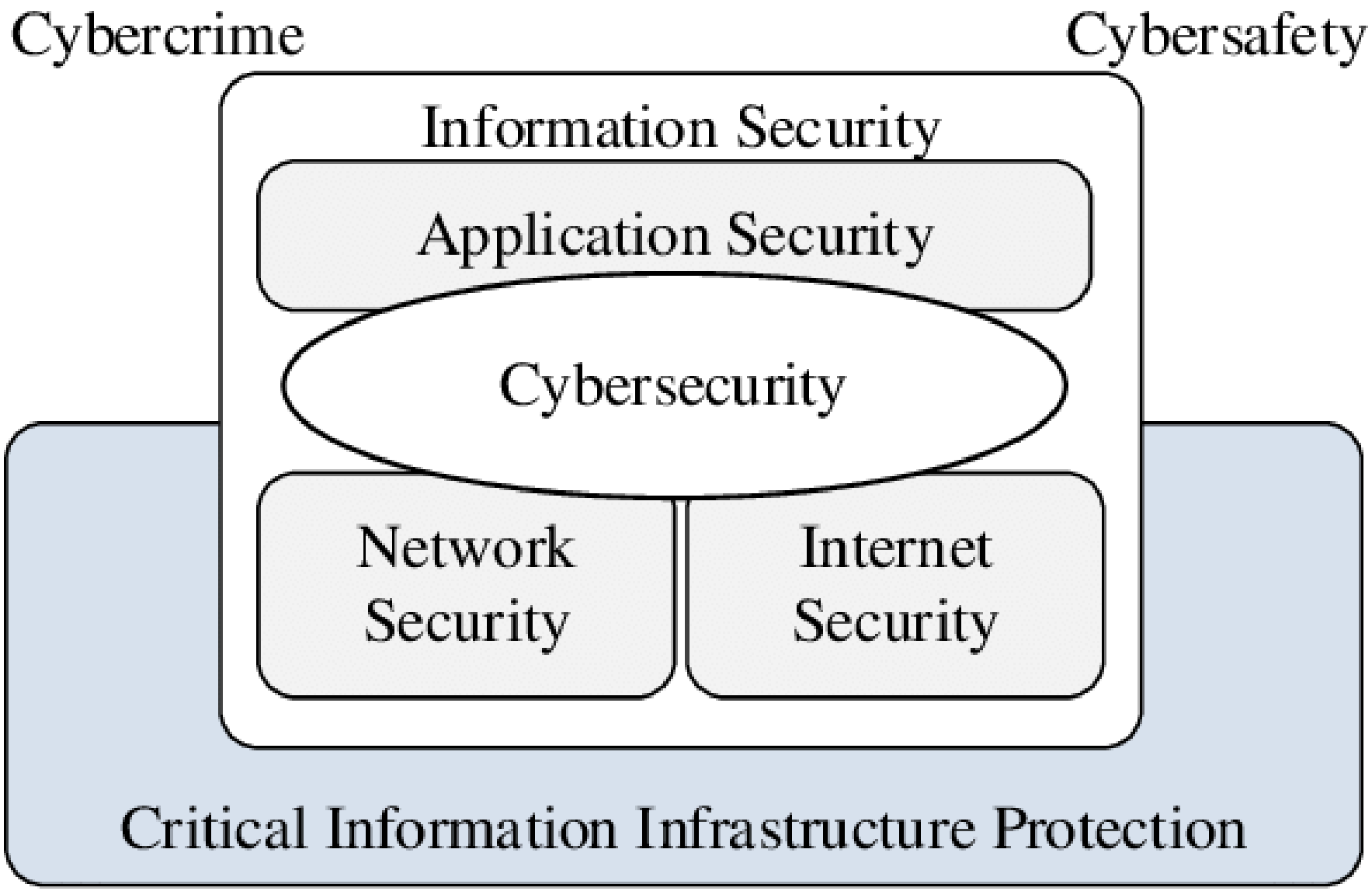
Information Security Vs. Cyber Security

Information security

- Protecting information and information systems from unauthorized use, assess, modification or removal.
- Two sub-categories
  - Physical environment by ensuring the premises is secure
  - No one can access information electronically
- Concerned with making sure data in any form is kept secure and is a bit more broad than cybersecurity

Cyber Security

- How individuals and organisations reduce the risk of cyber attack.
- Cyber security is the practice of protecting information and data from outside sources on the Internet.
- cyber security focuses on digital information but also, it deals with other things as well: Cyber crimes, cyber attacks, cyber frauds, law enforcement.


Cybercrime
Cybersafety
Information Security
Application Security
Cybersecurity
Network Security
Internet Security
Critical Information Infrastructure Protection

Security Target

The desired levels of security and assurance varies between organization, industries, even departments

There is not single approach applies to every one

Three main security goals

- Confidentiality(C)
- Integrity(I)
- Availability(A)

Three security services necessary to support the CIA

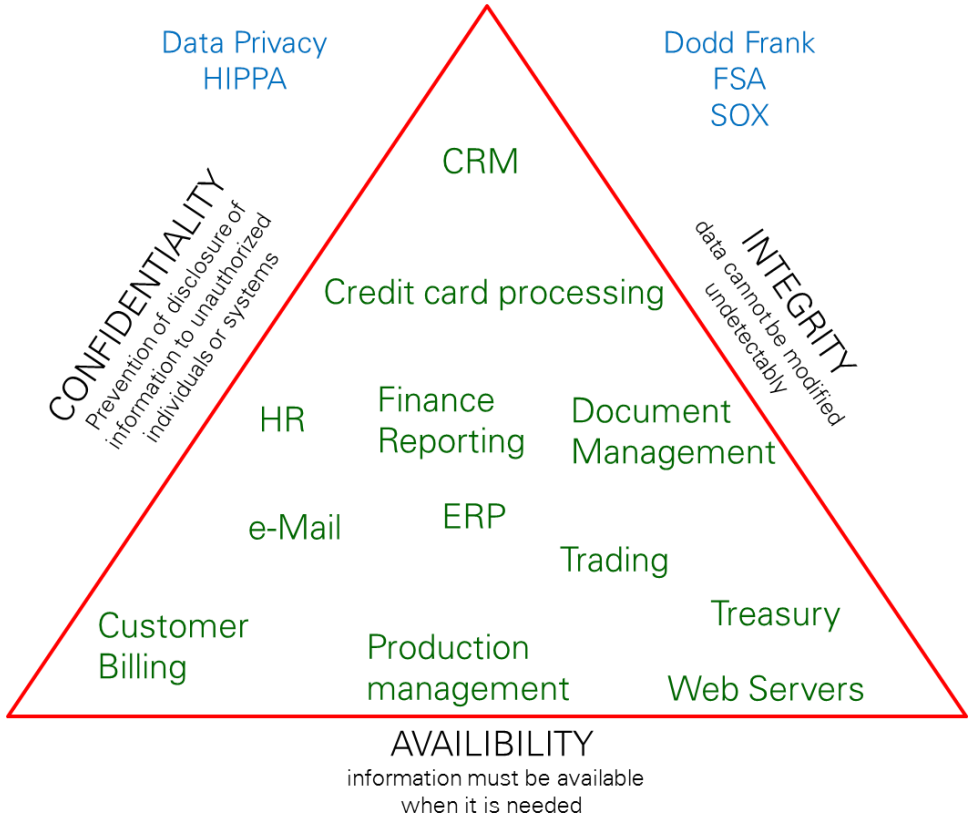
- Identification
- Authentication
- Authorization

CIA

Ability to control or restrict access so that only authorized individuals can view sensitive information. Classification's may include

- Secret
- Confidential
- Internal &
- Public

Typical risks: Loss of privacy, unauthorised access to information, Identity theft, etc.



Information is accurate and reliable and has not been tampered or changed in an unauthorized way. Integrity controls ensure that the information is authentic, accurate and reliable.

Typical risks: Fraudulent activities, manufacturing defects, inaccurate financial reporting, etc.

Data is available to the users when needed

Typical risks: Business disruption, loss of customer confidence, loss of revenue, etc.

Key Information Security Concepts

Access - a subject or object's ability to use, manipulate, modify, or affect another subject or object.

Asset – anything that has value to an individual, an organization or a government

Cyber Space- interconnected digital environment of networks, services, systems, and processes

Threat: potential cause of an unwanted incident, which may result in harm to a system, individual or organization

Vulnerability: weakness of an asset or control that can be exploited by a threat

Cyber incident- cyber event that involves a loss of information security or impacts business operations

Key Information Security Concepts

Attack - an act that is an intentional or unintentional attempt to cause damage or compromise to the information and/or the systems that support it.

Control countermeasure- means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature

Exploit - to take advantage of weaknesses or vulnerability in a system.

Exposure - a single instance of being open to damage.

Malicious contents- applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

Risk - the probability that something can happen.

Cyber security in energy sector

- Energy sector is one of the key critical infrastructures for any country /economy
- A reliable and secure energy supply is vital for a functioning economy and society, and is a key aim of policy
- cybersecurity is an evolving security challenge for the electricity sub-sector
- persistent threat to the electricity sub-sector and can cause severe physical and economic harm
- A single compromised manufacturer or poorly secured component for Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), or software management systems, when broadly distributed across the electricity subsector, could compromise utility systems

Cyber security in energy sector

- A cyber breach of an energy utility could result in blackouts and a loss of trust from utility customers.
- Ethernet (TCP/IP) based communication protocols to industrial automation and control systems.
  - e.g. IEC60870-5-104-designed for the remote control in electric substations.
    - Interoperability among different vendors
    - Data and measures from Controlled Stations to Master Station
  - IEC 62351(GOOSE Protocol) a secure version of IEC60870-5-104
    - Generic Object-Oriented Substation Events (GOOSE), which is a widely used communication protocol defined in IEC 61850, provides reliable and fast transmission of events for the electrical substation system
    - Mutual Authentication (User/Device Certificates)/ Authenticity/ Integrity/ Role Based Access Control/ Public Key Infrastructure

Cyber security in energy sector

- ModBus-RTU/ ModBus-TCP/IP Master & Slave
  - used for transmitting information between electronic devices
  - lacks strong authentication mechanisms
  - All MODBUS messages are transmitted in clear text across the transmission media.
  - no integrity checks built into the MODBUS application protocol, and as a result it depends on lower layer protocols to preserve integrity

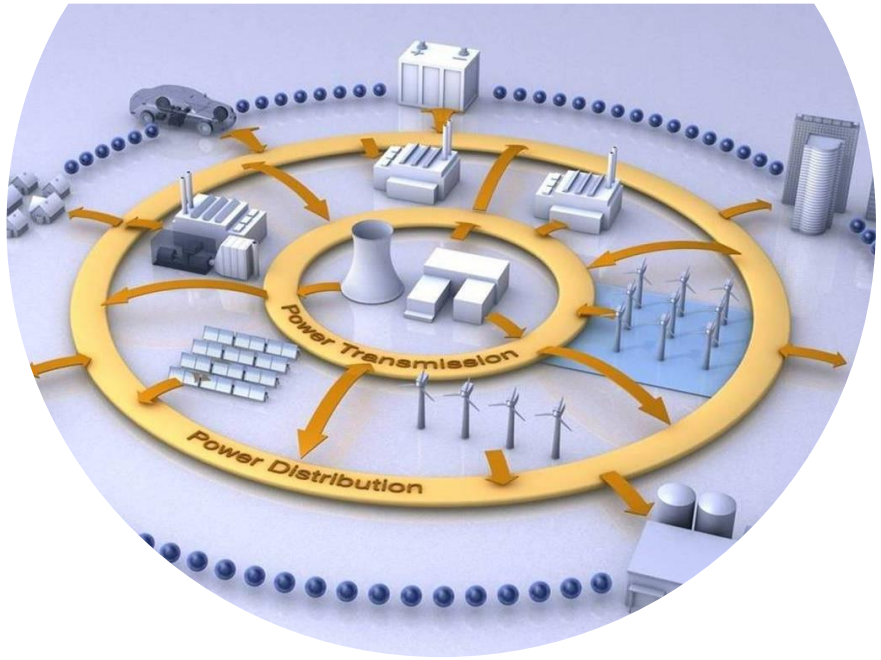
Smart Grid

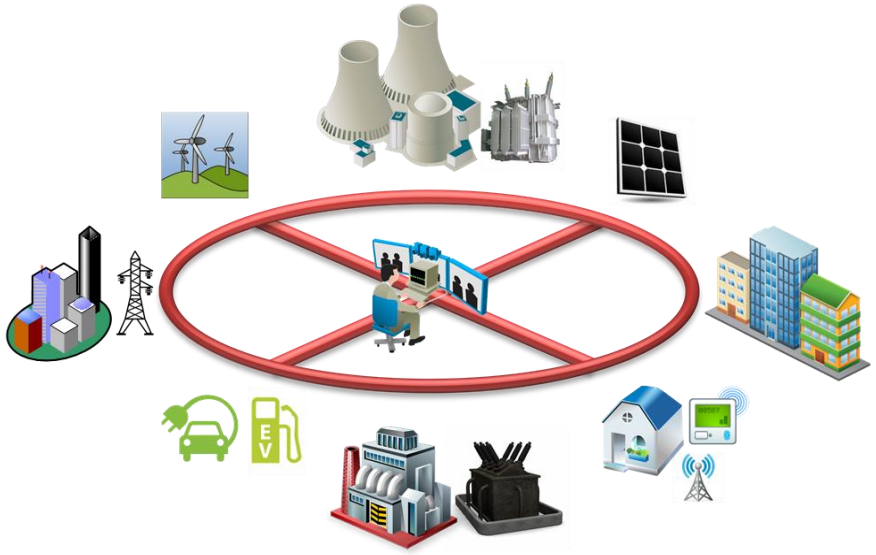
- Smart Grid, also known as the next generation of the power grid, is considered as a power grid infrastructure with advanced information and communication technologies (ICT) that will enhance the efficiency, availability, and reliability of power systems.
- Various devices are required in SG for monitoring, analyzing and controlling the power grid.
- The ICT innovations such as IoT play major roles in Smart Grid to be enable to enhance the efficiency, availability, and reliability of power systems by supporting various network functions throughout the generation, transmission, distribution, and consumption of the electric power
- Smart Grid is an essential part of sustainable smart cities in ensuring reliability, availability, and efficiency of the power grid. Smart Grid is the next generation of power grid in which the management and distribution of electricity are performed in advanced bi-directional communication systems.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094.

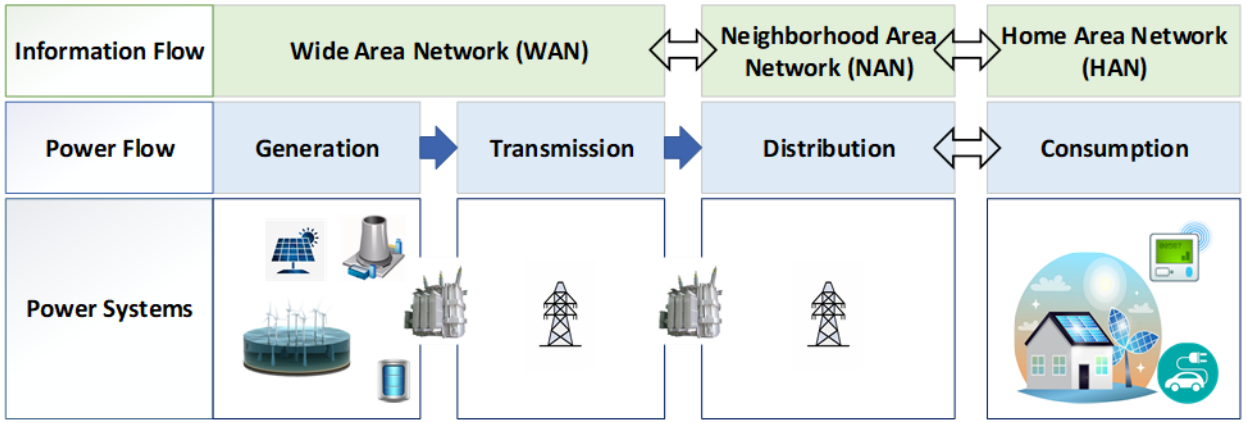
ICS/SCADA Around Us

- ICS: Industrial Control System
- SCADA: Supervisory Control and Data Acquisition





Smart Grid Architecture



Course progress

01. Cyber security in energy sector

02. Risk Management framework

03. Security controls and standards of the specific domain

What is Risk?

An uncertain event or a set of events that should it occur will have an effect on the achievement of objectives

- Energy sector organizations those concern with programs or projects will encounter uncertain events when trying to achieve their objectives
  - These events may arise inside or outside of the organization
  - Threat: an uncertain event that would have a negative impact on the objectives if it occurred
  - Opportunity: an uncertain event that would have a positive impact on the objective if it occurred

What is Cyber Security Risk?

The expected loss of confidentiality, Integrity,

Availability or Accountability

,

The probable frequency and probable magnitude of future loss of confidentiality, integrity

The goal of risk management is to maximize the output of the organization in terms of services, product and revenue while minimizing the chance of unexpected negative outcomes

Risk Management framework

- RM commonly comprises of two general phases
  - Risk assessment
    - Risk identification
      - List of risk items which threat in a specific context
    - Risk analysis
      - Transform raw risks into decision enabling knowledge
      - Severity of the identified risks
    - Risk prioritization
      - Identified and analyzed risks are ranked by relevant weight
  - Risk control
    - Risk management plan
      - How to address the prioritized risks?
      - Which risks are acceptable
      - Contingency plan
    - Risk control
      - Implement the risk control action
    - Risk monitor
      - Check the effectiveness of the implemented control action
      - Identify new risks
    - Risk resource repository
      - Risk data based for future project

ISO 31000:Risk Management

Assist the organization in integrating risk management into significant activities and functions

The effectiveness of risk management will depend on its integration into the governance of the organization, including decision-making

- support from stakeholders, particularly top management

When designing the framework for managing risk, the organization should examine and understand its external and internal context

External Context

- cultural, political, legal, regulatory, financial, technological, economic and environmental factors
- contractual relationships and commitments;

Internal Context

- vision, mission and values;
- data, information systems and information flows;
- standards, guidelines and models adopted by the organization;

  — capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);

Risk Management Activity

- Identify the assets
- Identify the threats to those assets
- Identify the vulnerabilities that might be exploited by the threats
- Identify the impacts that losses of CIAA may have on those assets

  - Assets are resources or information to be protected
  - Goal
    - Pro-actively gather all necessary information about an organization's assets
      - Monitor identified assets to become aware of attacks
        - Take necessary actions
  - Importance
    - Most organizations do not know of compromises
      - 92% of all information security incidents in 2011 identified by third parties
        - E.g. law enforcement, other ISPs
      - Often attacks have acted for weeks or months

Asset types

- General
  - Assets found in most organizations
  - E.g. email
  - Industry-wide checklists possible
- Idiosyncratic
  - Distinct to an organization
    - E.g. student transcripts
  - Correct identification difficult
  - requires determination of the processes, procedures and activities in the organization
    - Considerable effort and attention to detail necessary

•Two approaches

•Bottom up

•Talking to co-workers/ Learning curve

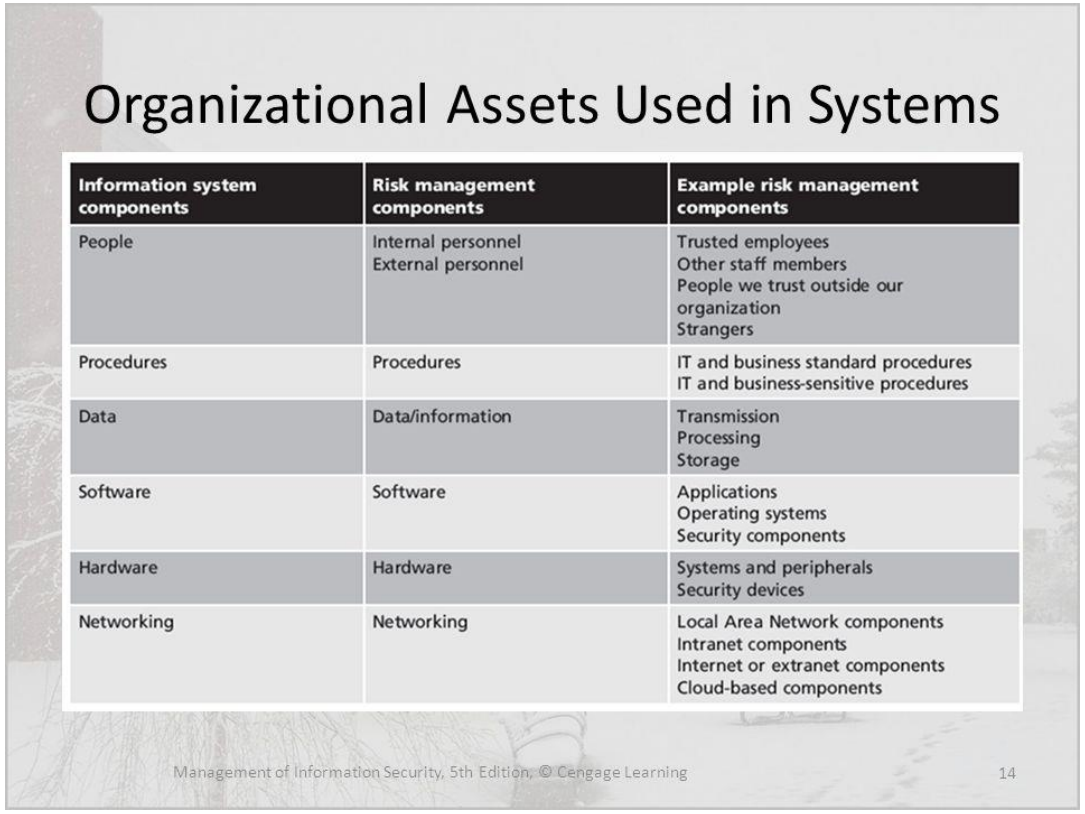
•Learn the inner workings of the company/ Employee knowledge

•Top down

•"About us" on website/ Annual reports

•Vision statement/ Mission statement

Organizational Assets



Asset	Asset Type	Sensitivity	Criticality
Laptop	Hardware Asset	Restricted	Required
Student Grades	Informational Asset	Restricted	Essential
Smith Richard- - Security Analyst	Personnel Asset	Restricted	Required
Microsoft Office Suite/moodle	Software Asset	Unrestricted	Deferrable
Microsoft Office License	Legal Asset	Unrestricted	Required

Asset Inventory

Asset Name	Category	DETAILS	POSSIBLE OWNER	Acceptable use	Required Protection	Sensitivity/ Criticality
				Read Write Edit Distribution Delete	C=H/M/L I=H/M/L A=H/M/L	

Threat Identification related to the Assets

- Capabilities, intentions and attack methods of adversaries to exploit or cause harm to assets
  - NIST definition
    - Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure or modification of information, and/ or denial of service

Goal

- Once assets are identified, identify threats for optimal information security investments
  - No defense necessary if no harm anticipated

Threats

- Threats sources
  - Deliberate actions by people – This group includes people inside and outside your organization who might take deliberate action against your assets.
  - Accidental actions by people – This group includes people inside and outside your organization who might accidentally harm your assets.
  - System problems – These are problems with your information technology (IT) systems. Examples include hardware defects, software defects, unavailability of related systems, viruses, malicious code, and other system-related problems.
  - Other problems – These are problems that are outside of your control. These can include natural disasters (e.g., floods and earthquakes) that can affect your organization's IT systems, unavailability of systems maintained by other organizations, and interdependency issues. Interdependency issues include problems with infrastructure services, such as power outages, broken water pipes, and telecommunication outages.

Vulnerabilities

Weaknesses in information systems that gives threats the opportunity to compromise assets

Relationship with threats

- Vulnerability is not a risk without a threat exploiting it
- Threat is not a risk without a vulnerability to be exploited

Risk Analysis

Once the risks are identified we need to know how severe are the risks

Risk analysis estimate and prioritise the risks

- the likelihood or probability that the risk is real
- the consequences of the problems associated with the risk, should it occur.

- Well-informed decisions about which risks need to be addressed and to what degree it is appropriate to mitigate the risks

Very challenging tasks

Probability becomes truly subjective when a trust value does not exist

Risk Analysis

Defining likelihood

- Rating of both the probability that a threat will successfully exploit a vulnerability as well as how often that might occur
- Criteria
  - Size of the threat universe(scope of the user community that can access a vulnerability)
  - Motivation of the threat actor
  - Sophistication of attack or skill level required
  - Knowledge of organization
  - Level of controls in place to deter or impede exploit
  - Attractiveness of the target

Impact definition

- LOW impact: implies risk has a limited adverse effect on the business and CIAA
- Medium impact: implies risk has a serious adverse effect on the business and CIAA
- High impact: implies risk has a severe adverse effect on the business and CIAA

Risk Analysis

Risk level

- Low risk: implies that it is recommended to develop a corrective measure and contingency plan.
- Critical risk: implies the risk has a serious adverse affect on the organization and correctives actions are needed and contingency plan should be developed and execute within a specific period of time.
- Highly critical risk: implies the identified control measures for the risk mitigation need to be implemented immediately within a short duration through a plan.

Risk Analysis

- Estimate the probability of occurrence
- Probability is the overall rating—often a numerical value on a defined scale (such as 0.1 – 1.0)—of the probability that a specific vulnerability will be exploited
- Estimate the impact on the project on a scale of 1 to 5, where
  - 1 = low impact
  - 5 = catastrophic impact

– Risk Level

  – In case of quantitative assessment

Ri=P(Ri) X I(Ri)

=.55 X . 8 [Assume P(Ri)=.55 and I(Ri)=.8]

=.44

Risk Analysis

In case of qualitative assessment

- Ri=P(Ri) X I(Ri)
- Ri=Medium X High
- Ri=??

Likelihood	impact		
	high	medium	low
High	H	H/M	Extreme
Medium	H/M	M	M/L
Low	**Extreme**	**M/L**	**L**

Risk level determines the priority of the risks

- it is not possible to look at all the identified risks
- Risk that requires immediate attention

Risk Control

- To gain control of the risks as early as possible
- Initially focus on the top prioritized risk events and factors
- Once possible countermeasure is identified then you need to select the most potential ones to control the risks
  - Cost, technical expertise, assets
- Without a true sense of the cost of the controls over time and impact to the organization to support them, hard to make the right decision
- Risk threshold
  - Specific level up to which a risk can be accepted
- Its all about making decision and balancing the cost
- Total expense of the controls should never cost more than the asset is worth

Risk Control Strategy

- Avoid
  - Changing some aspect of the project so that threats either can no longer have an impact or can no longer happen
  - Ex: rearrange skype meeting instead of physical meeting

Reduce
  - Reduce likelihood/impact of the risk
  - Ex: more user training to reduce the low usability of product

Fallback
  - A fallback plan if the risk occurs to reduce the impact of the risk
  - Reactive
  - Ex: Hire extra developers if schedule overruns

Transfer
  - A third party takes on responsibility for the financial impact of the risk
  - Ex: insurance

Risk Control Strategy

Accept Do nothing
- Keep the risk as it is more economical
- Risk need adequate monitoring
- Ex: competitor launch new product

Share (can be an opportunity)
- Pain/gain formula
- Risk sharing principles with third party
- Ex: customer/supplier agree to share the cost of price

Enhance (Opportunity)
- Enhance the probability of event occur
- Enhance the impact of the event
- Ex: delay product release

Reject (Opportunity)
- A conscious and deliberate decision is taken not to exploit/enhance the opportunity
- needs continuous monitoring
- Ex: Not take advantage of early release

Smart Grid Vulnerabilities

Legacy SCADA systems

Lack of cyber security controls

- Specified for specific domains – bulk power distribution, metering

Vulnerabilities might allow an attacker to

- Penetrate a network,
- Gain access to control software, or
- Alter load conditions to destabilize the grid in unpredictable ways

Even unintentional errors could result in destabilization of the grid

- Inherent complexity
  - exposure to potential attackers and unintentional errors
  - Interdependent networks introduce common vulnerabilities

Increased number of entry points and paths

Compromise of data confidentiality or customer privacy

Attack Vectors Reaching the ICS/SCADA Network

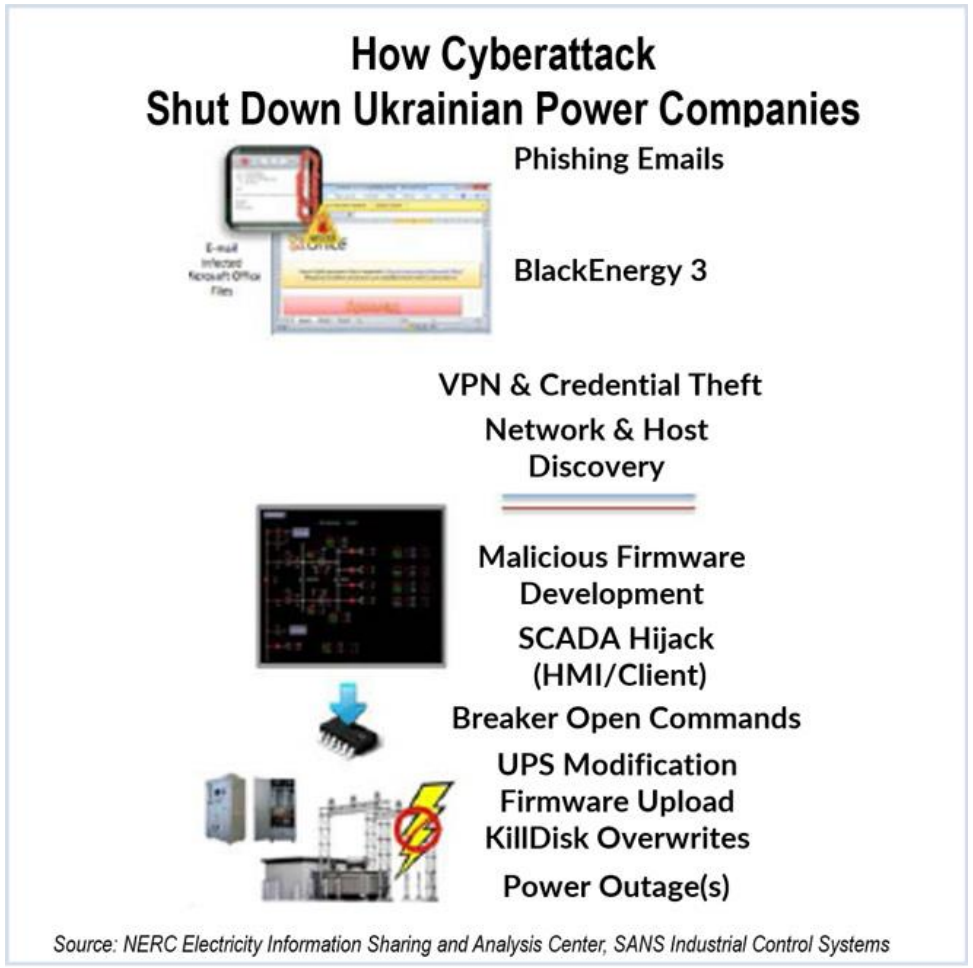
Removable Media

Phishing

Software Vulnerabilities

Cyber Attack on Ukrainian Power Grid December 2015

BlackEnergy malware a cyber-attack on supervisory control and data acquisition (SCADA) system at power Grid in Ivano-Frankvisk city in Ukraine was able to cut electricity for more than 6 hours and affected more than 100k people



Attack Sequence

Attackers entered the SCADA network through hijacked VPNs

↓

Issued commands to disable UPS

↓

Initiated Telephone DoS

↓

Overwrote firmware on sub-station serial-to-Ethernet converters, preventing remote M&C

↓

Began opening breakers on the system and took substations off

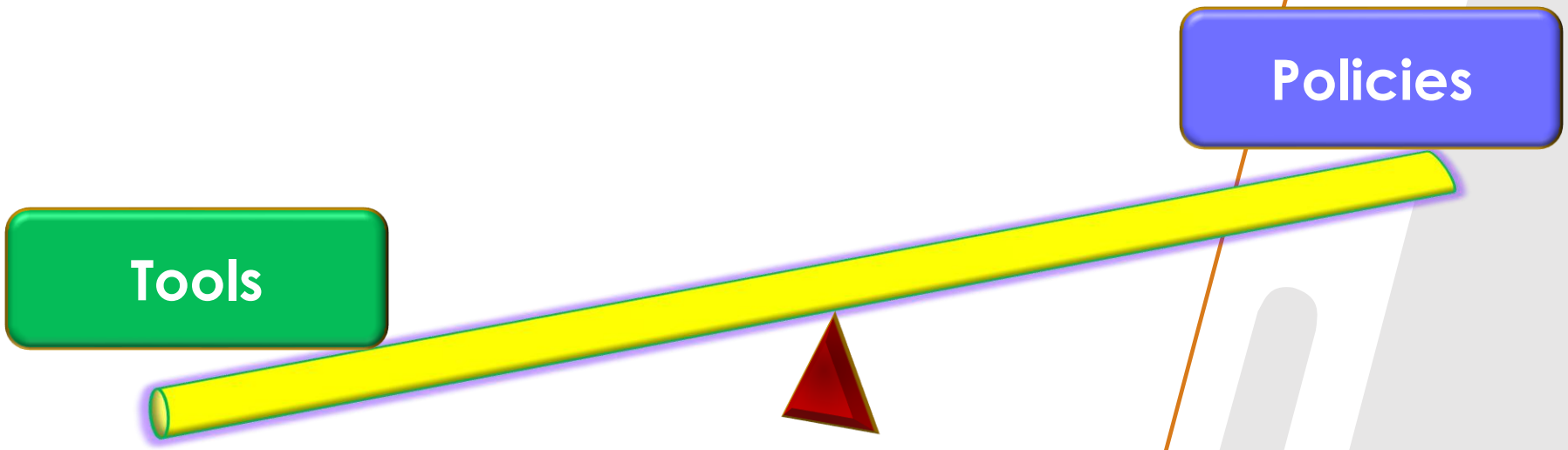
↓

Used KillDisk Malware to wipe files from operator stations at around 5 pm

Threats and risks in Smart Grid

- unauthorized access can disrupt energy supply networks, leading to power outages and other damages.
- DoS, ransomware attacks, insider threats, and attacks targeting Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems
- Risks
  - Disruption of the service delivery
  - Blackout
  - erc

Controls



Controls

- Access controls
- Encryption
- Authentication
- Regular security patches and updates
- Physical security
- Intrusion Detection Systems (IDS)
- Blockchain

Training Outline:
Part 2

Topic-3: Security controls and standards of the specific domain.

Introduction to ISO/IEC 27001, status, versions, structure (Clauses 1-4 and Annex A).

ISO 27001:2022 / ISO/IEC 27002:2022 control themes

Terms and definitions of ISO 27000 adapted to the energy utility domain

Guidance on the controls of ISO/IEC 27002:2022 adapted to the energy utility domain.

Energy specific controls as proposed by ISO/IEC 27019 (DIS).

Topic-3: Security controls and standards of the specific domain.

We will cover these skills

- Gain basic knowledge on the structure, status and versions of ISO/IEC 27001
- Gain knowledge on the themes of ISO/IEC 27002:2022
- Get acquainted with basic terms and their definitions as used by ISO/IEC 27002
- Get acquainted with how these basic terms are adapted to fit the energy utility sector.
- Critically develop and evaluate security policy and select controls by following ISO 27019 for security governance.

Course progress

01. Cyber security in energy sector

02. Risk Management framework

03. Security controls and standards of the specific domain

Resources: Books and Reference Materials

1. ISO/IEC 27000:2018, Information technology. Security techniques. Information security management systems. Overview and vocabulary, https://www.iso.org/standard/73906.html
2. ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. Information security management systems. Requirements. https://www.iso.org/standard/27001
3. ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection. Information security controls. https://www.iso.org/standard/75652.html
4. ISO/IEC 27019:2017, Information technology. Security techniques. Information security controls for the energy utility industry. https://www.iso.org/standard/68091.html
5. ISO/IEC DIS 27019, Information technology. Security techniques. Information security controls for the energy utility industry. https://www.iso.org/standard/85056.html
6. ISO/IEC 27001:2013, Information technology. Security techniques. Information security management systems. Requirements. https://www.iso.org/contents/data/standard/05/45/54534.html
7. ISO/IEC 27002:2013, Information technology. Security techniques. Code of practice for information security controls. https://www.iso.org/standard/54533.html

Introduction to ISO/IEC 27001

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

https://www.iso.org/standard/27001

ISO/IEC 27001 Revision history

More previously

Withdrawn
ISO/IEC 27001:2005

Previously

Withdrawn
ISO/IEC 27001:2013

Withdrawn
ISO/IEC 27001:2013/Cor 1:2014

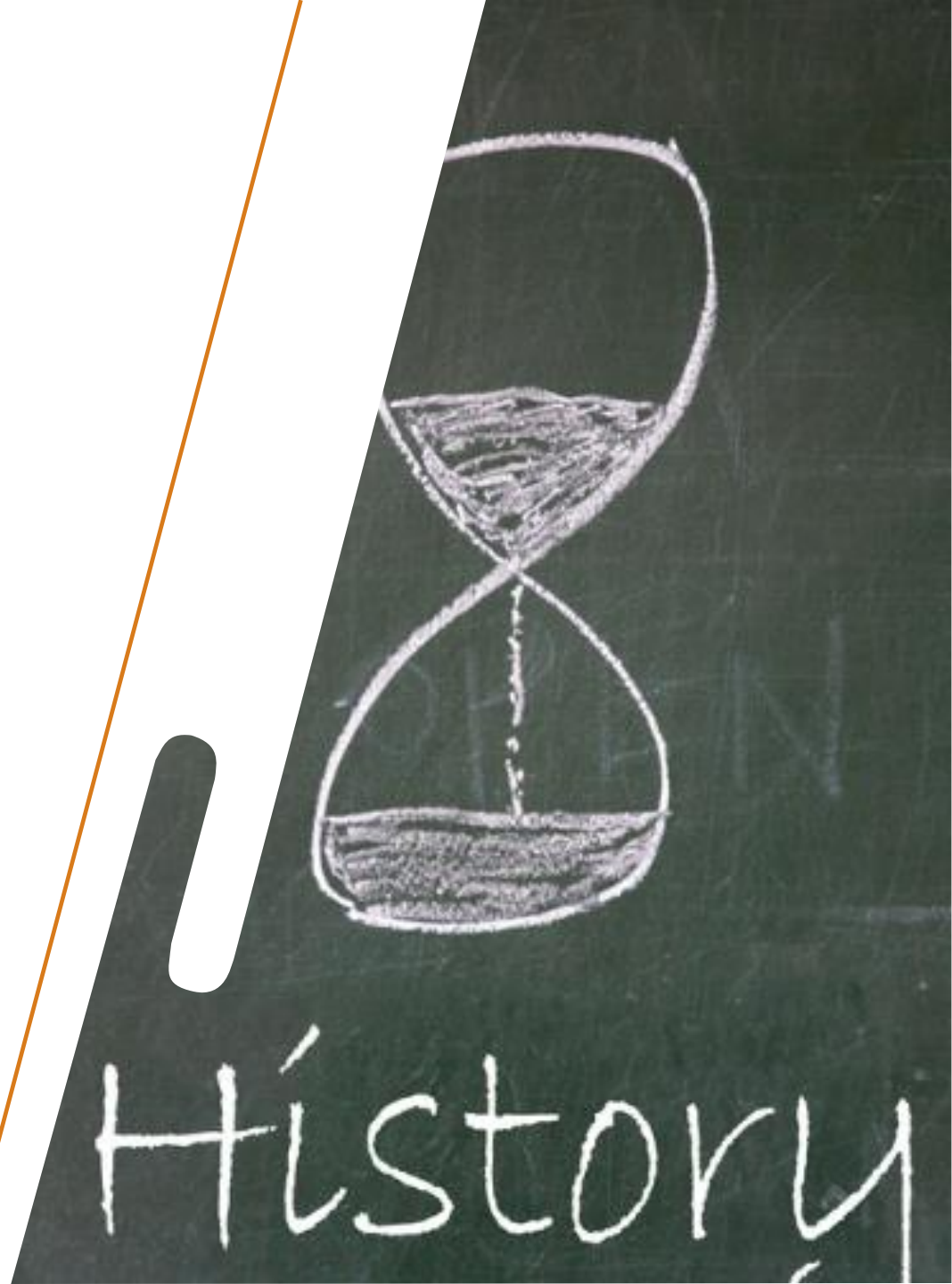
Withdrawn
ISO/IEC 27001:2013/Cor 2:2015

Now

Published
ISO/IEC 27001:2022
Stage: 60.60

Corrigenda / Amendments

Under development
ISO/IEC 27001:2022/Amd 1



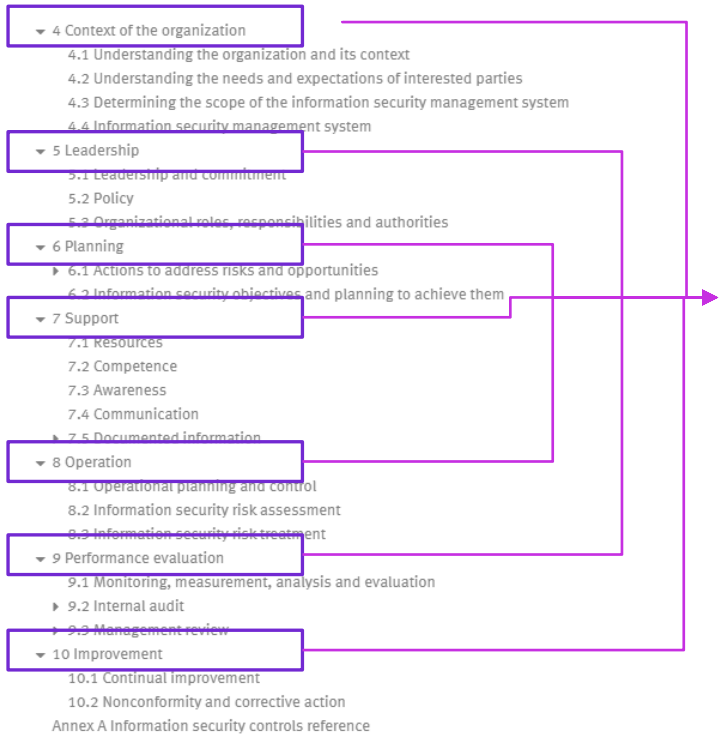
ISO/IEC 27001 Structure

- 4 Context of the organization
  - 4.1 Understanding the organization and its context
  - 4.2 Understanding the needs and expectations of interested parties
  - 4.3 Determining the scope of the information security management system
  - 4.4 Information security management system
- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities and authorities
- 6 Planning
  - 6.1 Actions to address risks and opportunities
  - 6.2 Information security objectives and planning to achieve them
- 7 Support
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- 8 Operation
  - 8.1 Operational planning and control
  - 8.2 Information security risk assessment
  - 8.3 Information security risk treatment
- 9 Performance evaluation
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.2 Internal audit
  - 9.3 Management review
- 10 Improvement
  - 10.1 Continual improvement
  - 10.2 Nonconformity and corrective action

Annex A Information security controls reference

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

ISO/IEC 27001 Structure



Clauses

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

ISO/IEC 27001 Clauses

4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

ISO/IEC 27001 Clauses

4. Context of the organization	→	Scope of the system and an analysis of issues and interested parties.
5. Leadership	→	Information Security Policy , Roles, responsibilities and authorities
6. Planning	→	Risk management methodology, risk assessment, risk register, risk treatment plans, Objectives and plans
7. Support	→	Competencies, Document management procedures, Communication procedures
8. Operation	→	Change Management procedure
9. Performance Evaluation	→	KPIs, Internal audit procedure, Internal audits, Management review
10. Improvement	→	Corrective actions procedure

ISO 27001 – Annex A

ISO 27001 in clauses 4-10, does not prescribe a set of measures / controls to be applied by organizations.

ISO 27001 mandates the design and implementation of a risk management process, that allows the organization to

- identify it's own criteria for risk acceptance,

- consider the possible risks taking into account measures already in place (existing measures) and

- identity risks that do not fulfill them.

For these risks, the organization needs to propose (proposed measures) and implement suitable risk treatment plans.

ISO 27001 – Annex A

After this process, organizations are asked to compare the existing and proposed measures against a list of Information Security controls that can be used as reference, in order to see if something needed has been omitted.

A control is defined as a measure that modifies or maintains risk. Some of the controls are controls that modify risk, while others maintain risk.

An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts.

[definition of control by ISO/IEC 27002:2022]

Structure of the controls

Organizational Controls

37 controls

People Controls

if they concern people

8 controls

Physical Controls

if they concern physical objects

14 controls

Technological Controls

if they concern technology

34 controls

ISO/IEC 27002:2022

The standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations.

The guidance is generic and can be used by organizations of all types and sizes (including public and private sector, commercial and non-profit) who create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

ISO/IEC 27002:2022 - Attributes

Control Type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
# preventive # detective # corrective	# confidentiality # integrity # availability	# identify # protect # detect # respond # recover	# governance # asset management # information protection # human resource security # physical security # system and network security # application security ….	# governance and ecosystem # protection # defense # resilience

Standard IT environments VS Process control systems used by energy utilities and energy suppliers

Information technology (IT) is the development, management, and application of computer equipment, networks, software, and systems.

IT is crucial to modern business operations because it enables people and machines to communicate and exchange information.

IT Operations focus on the day-to-day management of IT departments, which includes managing devices, maintaining networks, testing the security of applications and systems, and providing technical support.

Infrastructure maintenance focuses on the process of setting up and maintaining infrastructure equipment, such as cabling, laptops, phones and phone systems, and physical servers.

IT Governance focuses on the process of ensuring that IT policies and services align with the needs and demands of the organization.*

VS

Process control systems collect process data and monitor the status of the physical processes using sensors.

The systems then process this data and generate control outputs that regulate actions using actuators.

The control and regulation are automatic but manual intervention by operating personnel is also possible.

Information and information processing systems are therefore an essential part of operational processes within energy utilities.

Process control systems in the energy utility sector are increasingly interconnected to form complex systems.

* https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity

Criteria for a secure energy supply and delivery

01. Impairment of the security of energy supply.
02. Restriction of energy flow.
03. Affected share of population.
04. Danger of physical injury.
05. Effects on other critical infrastructures.
06. Effects on information privacy.
07. Financial impacts.

ISO/IEC 27002:2022 and ISO/IEC DIS 27019

ISO/IEC DIS 27019 provides guidance based on ISO/IEC 27002:2022 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes.

Examples include:
central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterization devices;
digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements;
all further supporting information systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving, historian logging, reporting and documentation purposes;
communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology;
Advanced Metering Infrastructure (AMI) components, e.g. smart meters;
measurement devices, e.g. for emission values;
and others
BUT not the process control domain of nuclear facilities. This domain is covered by IEC 63096.

Energy management system

equipment/infrastructure used to monitor, measure and control the energy consumption in private households, residential buildings or industrial customer installations

Note 1 to entry: The term “energy management system” is also commonly used to refer to a set of applications used by operators of transmission power grid to monitor, control, and optimize the performance of the generation and/or transmission system.

Attention: ISO 50001:2018, Energy management systems, Requirements with guidance for use, refers to energy management system to establish an energy policy, objectives, energy targets, action plans and process(es) to achieve the objectives and energy targets.

Process control system

system that serves to control and monitor the generation, production, transmission, storage and distribution of electric power, gas, oil and heat, including the control of associated supporting processes.

Note 1 to entry: Process control systems are often referred to more generally as industrial control systems. In this document, the terms process control system and industrial control system are restricted to technologies and components used in the energy utility industry.

Basic Terms

blackout

widespread electrical power outage

critical asset

asset which can have a direct impact on production or generation, transmission, storage and distribution of electric power, gas, oil and heat

distribution system

distribution grid for the transport of electrical energy using a high, medium or low voltage grid, or a local or regional distribution network for the transport of gas, oil or heat

Basic Terms

Energy supply

process of generation, production or storage of energy for delivery to customers and the operation of an energy supply network

energy utility

legal body or a person that supplies energy in form of electricity, gas, oil or heat to other parties, to an energy distribution network or to a storage complex

maintenance

measures used in the field of energy supply that are normally related to inspection, fault clearance and improvement

Basic Terms

supervisory control and data acquisition (SCADA)

process control system generally used to control dispersed assets using centralized data acquisition and supervisory controls

smart grid

electric power system that utilizes information exchange and control technologies, distributed computing and associated sensors and actuators

transmission system

transmission grid for the transport of electrical energy using a high voltage or ultra-high voltage grid or a gas transmission network for the transport of natural gas using a high-pressure pipeline network

Organizational controls with no additional guidance

A.5.1	Policies for information security - No additional guidance
A.5.3	Segregation of duties - No additional guidance
A.5.4	Management responsibilities - No additional guidance
A.5.7	Threat intelligence
A.5.10	Acceptable use of information and other associated assets
A.5.11	Return of assets
A.5.13	Labelling of information
A.5.14	Information transfer

Organizational controls with no additional guidance

A.5.18	Access rights
A.5.21	"Managing information security in the information and communication technology (ICT) supply-chain"
A.5.22	Monitoring, review and change management of supplier services
A.5.23	Information security for use of cloud services
A.5.24	Information security incident management planning and preparation
A.5.25	Assessment and decision on information security events
A.5.27	Learning from information security incidents
A.5.29	Information security during disruption

Organizational controls with no additional guidance

A.5.30	ICT readiness for business continuity
A.5.32	Intellectual property rights
A.5.33	Protection of records
A.5.34	Privacy and protection of personal identifiable information (PII)
A.5.35	Independent review of information security
A.5.36	Compliance with policies, rules and standards for information security

Organizational controls with limited additional guidance

A.5.2	Information security roles and responsibilities
A.5.6	Contact with special interest groups
A.5.8	Information security in project management
A.5.16	Identity management
A.5.19	Information security in supplier relationships
A.5.26	Response to information security incidents
A.5.28	Collection of evidence
A.5.37	Documented operating procedures

Organizational controls with additional guidance

A.5.5	Contact with authorities
A.5.9	Inventory of information and other associated assets
A.5.12	Classification of information
A.5.15	Access control
A.5.17	Authentication information
A.5.20	Addressing information security within supplier agreements
A.5.31	Legal, statutory, regulatory and contractual requirements

New organizational controls for the energy utility industry

A.5.38 Identification of risks related to external business partners

Control: The risks to the organization's information and information processing facilities resulting from relationships with external business partners should be identified and appropriate controls implemented before granting access.

Control Type: Preventive

Purpose: To maintain an agreed level of information security in external business partners relationships.

New organizational controls for the energy utility industry

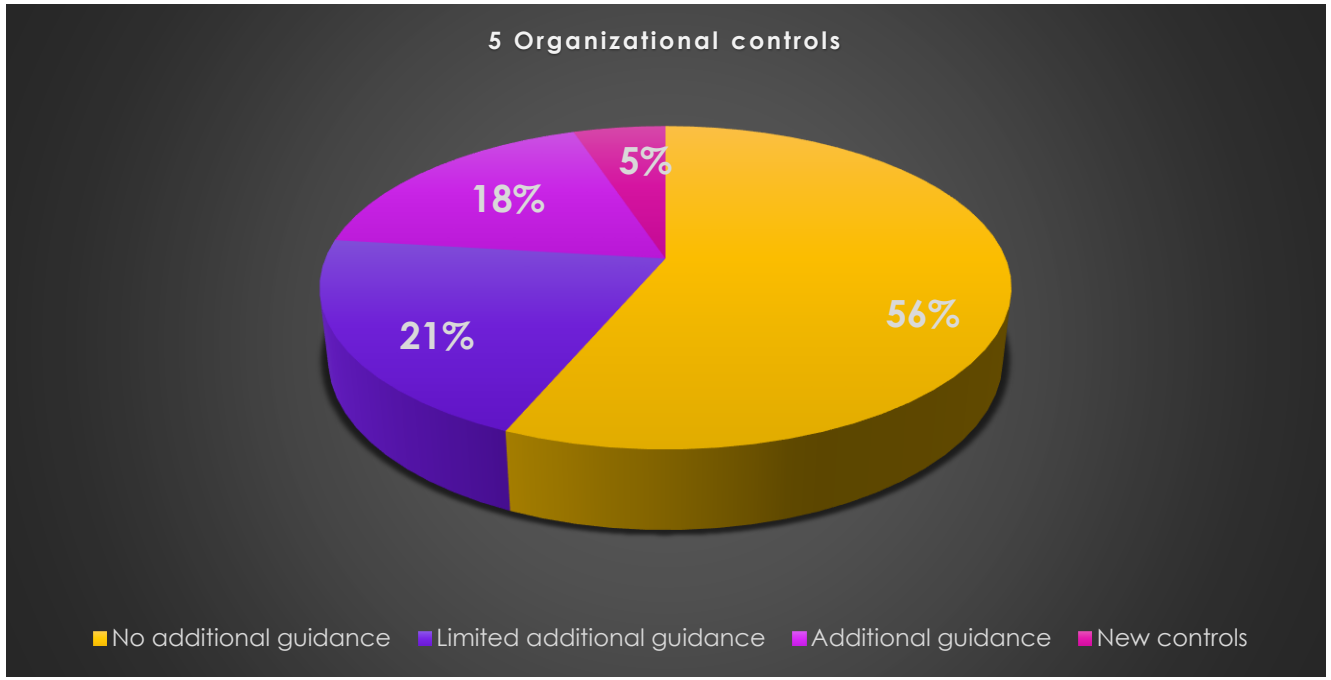
A.5.39 Addressing security when dealing with customers

Control: All identified security requirements should be addressed before giving customers access to the organization's information or assets.

Control Type: Preventive

Purpose: To protect information and other associated assets from unauthorized access of customers.

5 Organizational controls summary



People controls with no additional guidance

A.6.4 Disciplinary process

A.6.5 Responsibilities after termination or change of employment

A.6.6 Confidentiality or non-disclosure agreements

A.6.8 Information security event reporting

People controls with limited additional guidance

A.6.1 Screening

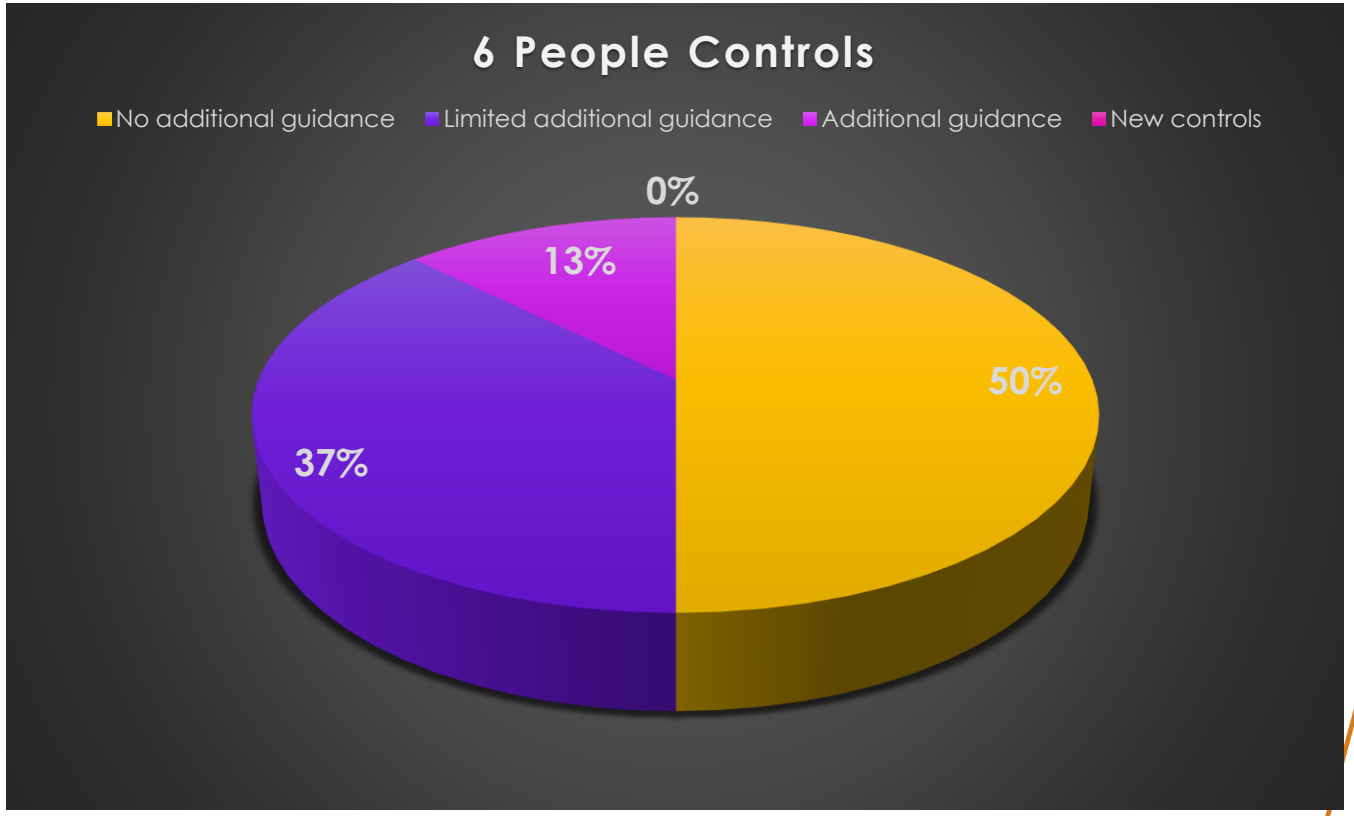
A.6.2 Terms and conditions of employment

A.6.3 Information security awareness, education and training

People controls with additional guidance

A.6.7 Remote working

6 People controls summary



Physical controls with no additional guidance

A.7.3 Securing offices, rooms and facilities

A.7.4 Physical security monitoring

A.7.5 Protecting against physical and environmental threats

A.7.6 Working in secure areas

A.7.13 Equipment maintenance

A.7.14 Secure disposal or re-use of equipment

Physical controls with limited additional guidance

A.7.1 Physical security perimeters

A.7.2 Physical entry

A.7.7 Clear desk and clear screen

A.7.8 Equipment siting and protection

A.7.10 Storage media

A.7.11 Supporting utilities

A.7.12 Cabling security

Physical controls with additional guidance

A.7.9 Security of assets off-premises

New physical controls for the energy utility industry

A.7.15 Securing control centres

Control: Measures to ensure the physical security of control centres, e.g. where control system servers, HMI and supporting systems are housed, should be designed, developed and applied.

Control Type: Preventive

Purpose: To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in control centres.

New physical controls for the energy utility industry

A.7.16 Securing equipment rooms

Control: Measures to ensure the physical security of equipment rooms where control system facilities used by energy utilities are located, should be designed, developed and implemented.

Control Type: Preventive

Purpose: To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in equipment rooms.

New physical controls for the energy utility industry

A.7.17 Securing peripheral sites

Control: Physical security controls should be designed, developed and implemented or appropriate countermeasures applied to protect peripheral sites.

Control Type: Preventive

Purpose: To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in peripheral sites.

New physical controls for the energy utility industry

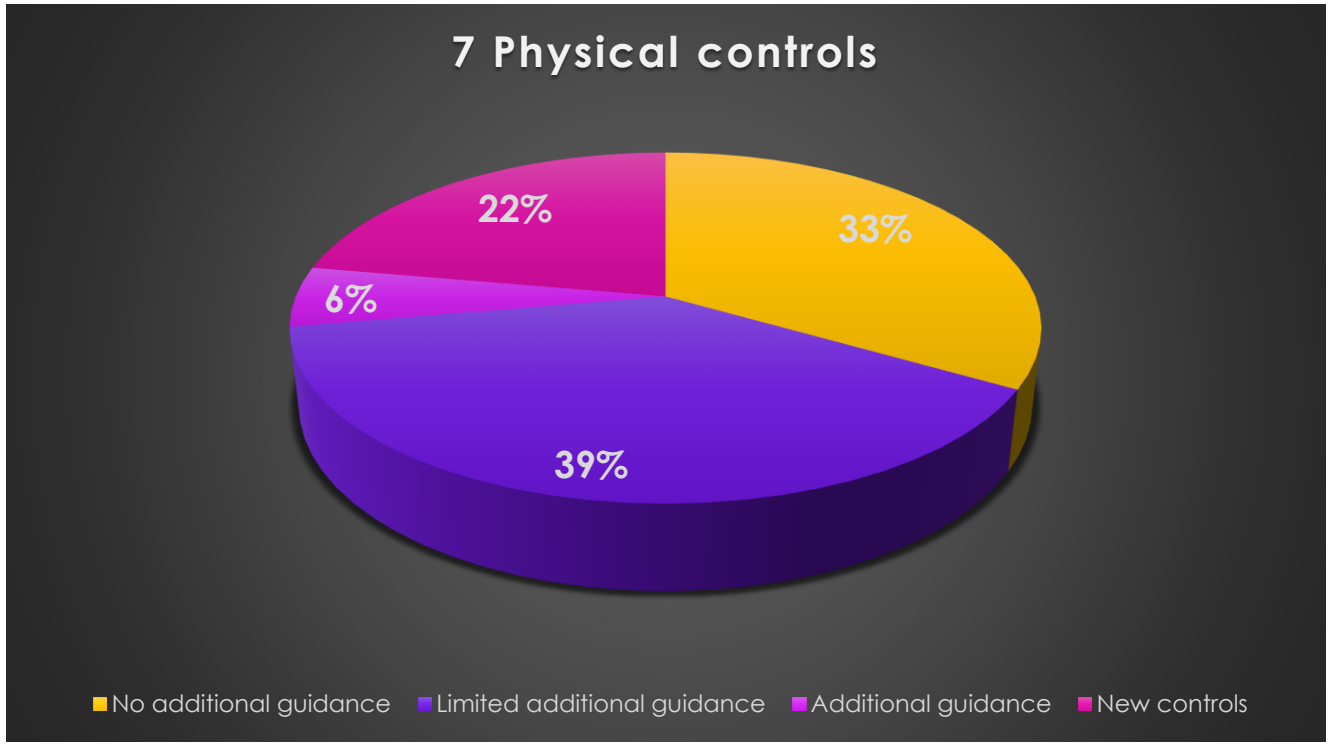
A.7.18 Interconnected control and communication systems

Control: For interconnected control and communication systems, responsibilities and interfaces with external parties should be clearly defined in order to be able to disconnect and isolate each organization from the others within an appropriate period of time in case of security incidents.

Control Type: Preventive

Purpose: To protect interconnected control systems and related communication lines from interference and compromise over the interconnection.

7 Physical controls summary



Technological controls with no additional guidance

A.8.2	Privileged access rights
A.8.3	Information access restriction
A.8.6	Capacity management
A.8.9	Configuration management
A.8.10	Information deletion
A.8.11	Data masking
A.8.12	Data leakage prevention
A.8.13	Information backup
A.8.16	Monitoring activities

Technological controls with no additional guidance

A.8.18 Use of privileged utility programs

A.8.20 Networks security

A.8.21 Security of network services

A.8.23 Web filtering

A.8.25 Secure development life cycle

A.8.26 Application security requirements

A.8.27 Secure system architecture and engineering principles

Technological controls with no additional guidance

A.8.28 Secure coding

A.8.29 Security testing in development and acceptance

A.8.30 Outsourced development

A.8.33 Test information

A.8.34 Protection of information systems during audit testing

Technological controls with limited additional guidance

A.8.4	Access to source code
A.8.5	Secure authentication
A.8.8	Management of technical vulnerabilities
A.8.14	Redundancy of information processing facilities
A.8.19	Installation of software on operational systems
A.8.22	Segregation of networks
A.8.32	Change management

Technological controls with additional guidance

A.8.1 User end point devices

A.8.7 Protection against malware

A.8.17 Clock synchronization

A.8.24 Use of cryptography

A.8.31 Separation of development, test and production environments

New technological controls for the energy utility industry

A.8.35 Treatment of legacy systems

Control: The energy utility should ensure that all legacy systems are identified along with their potential information security vulnerabilities and that appropriate controls are implemented.

Control Type: Preventive

Purpose: To reduce the risks from the use of legacy systems

New technological controls for the energy utility industry

A.8.36 Integrity and availability of safety functions

Control: The integrity and availability of information, assets, systems, components and functions that are required to ensure safety functions should be protected in accordance with sector-specific standards and legal requirements.

Control Type: Preventive

Purpose: To protect the integrity and availability of safety functions against failure, interference and manipulation.

New technological controls for the energy utility industry

A.8.37 Securing process control data communication

Control: Security measures to ensure the security requirements of internal and external process control data communication should be designed, developed and implemented.

Control Type: Preventive, Detective

Purpose: To protect information transmitted via process control data communication from compromise.

New technological controls for the energy utility industry

A.8.38 Logical connection of external process control systems

Control: The energy utility organization should ensure that risks resulting from process control systems' connection to external parties are assessed and that only authorized communications and information flows can be exchanged.

Control Type: Preventive, Detective

Purpose: To protect control systems from interference, manipulation and compromise over logical connections with external parties.

New technological controls for the energy utility industry

A.8.39 Least functionality

Control: Process control systems should be designed, configured, operated, and maintained to provide only required functions.

Control Type: Preventive

Purpose: To reduce the risks originating from unnecessary functionalities.

New technological controls for the energy utility industry

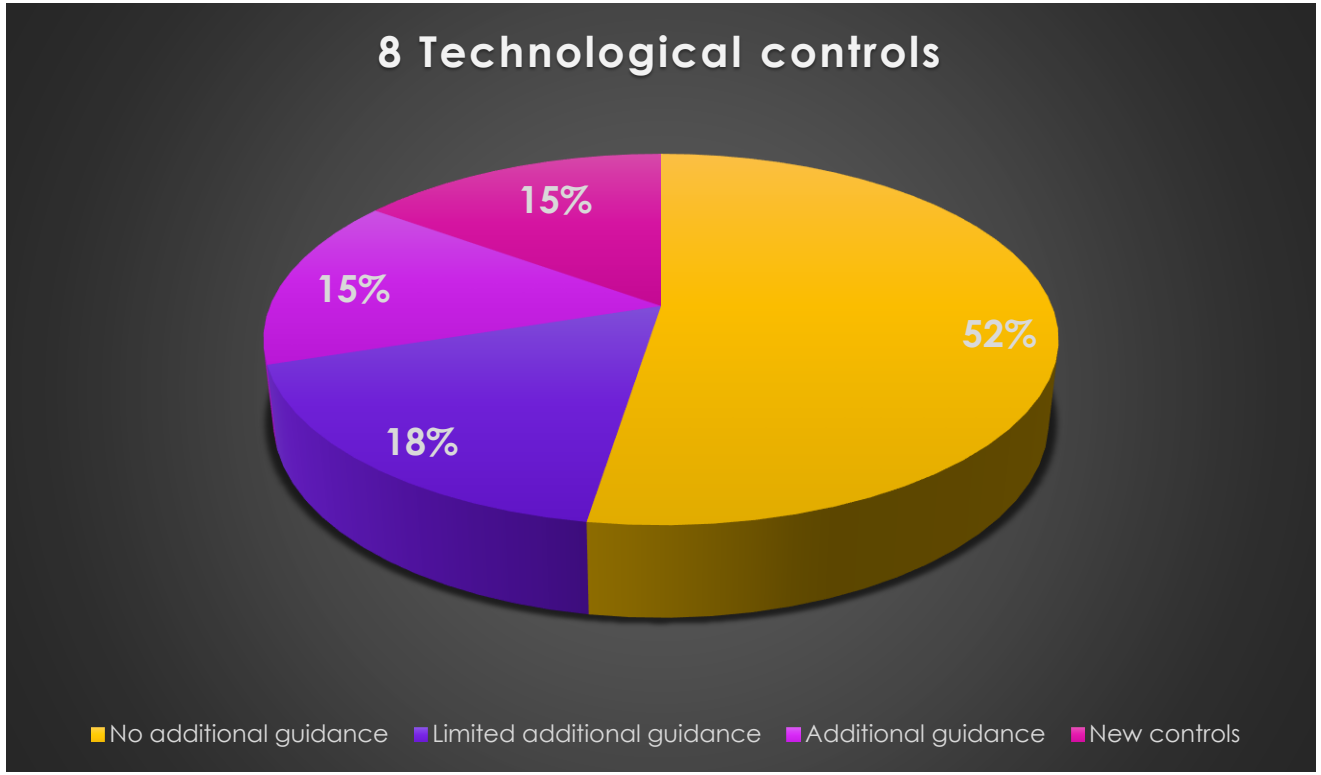
A.8.40 Emergency communication

Control: Essential communication links should be maintained in case of emergencies.

Control Type: Preventive, Detective

Purpose: To ensure essential communication is possible even under adverse conditions.

8 Technological controls summary



Thank you

Please send all questions to:

shareeful@gmail.com
ac@apiroplus.solutions