SOFEMA
AVIATION SERVICES

Information & Cyber Security Workshop Presentation

6th Mar 2025 www.sassofia.com

Key Drivers

The aviation industry is a high-value target for cybercriminals, state actors, and hacktivists.

EASA is mandating Aviation Information and Cyber Security Regulations because cyber threats pose a significant risk to aviation safety, operational continuity, and compliance with international standards.

ICAO has mandated cyber resilience measures under Annex 17 (Security)

- **Why Information Security Matters for Part 145 Organizations**
- EASA Part 145 operations depend on the integrity, availability, and security of critical systems and data, including:
    - Maintenance management systems.
    - Digital maintenance records and operational data.
    - Communication systems used for real-time collaboration.

External Threats - Malware Attacks - Malicious software such as viruses, ransomware, and spyware designed to infiltrate systems, steal information, or disrupt operations.

Malware Examples in Part 145:

Infection of Maintenance Information Systems (MIS), leading to data corruption or system downtime.

Ransomware attacks locking critical maintenance data until a ransom is paid.

Impact: Delayed maintenance schedules, compromised data integrity, and operational disruptions.

Phishing Attacks - Fraudulent attempts to obtain sensitive information by disguising communication as trustworthy (e.g., emails or messages).

Examples in Part 145:

Phishing emails targeting maintenance staff to extract login credentials for critical systems.

Fake invoices sent to finance departments, resulting in unauthorized transactions.

Unauthorized access to systems, financial loss, and data breaches.

Systemic Vulnerabilities - Systemic vulnerabilities arise from inherent weaknesses in the organization's processes, systems, or technology.

Third-Party Software Vulnerabilities include - Weaknesses in software or tools provided by vendors include

- Diagnostic software containing hidden vulnerabilities exploited by attackers.
- Updates from vendors that inadvertently introduce malware.

Legacy IT Systems - Older IT systems that lack modern security features. Susceptible to easier exploitation by attackers, limited interoperability, and high operational risks.

Weak Authentication Mechanisms - Inadequate access controls, such as weak passwords or lack of multifactor authentication.

Supply Chain Threats - Part 145 organizations rely on various third-party vendors, contractors, and suppliers, which introduces vulnerabilities.

Supply Chain Attacks - Attacks targeting vendors to infiltrate the organization's systems.

- Exploits through third-party equipment or tools used for maintenance.
- Targeted breaches of data shared with external contractors.
- Loss of data integrity, operational inefficiencies, and regulatory consequences.

Emerging Threats - Compromised operations and system malfunctions.

Compromising Internet of Things (IoT) devices used in maintenance operations.

- Unauthorized access to IoT-enabled tools for remote diagnostics or data collection.
- Exploiting weak security in connected systems to disrupt maintenance operations.

- **General Introduction – Part 145 Information Security**

- The introduction of **Regulation (EU) 2023/203**, mandates the integration of information security requirements into aviation safety management.

  - For EASA Part 145 organizations, adopting robust information security practices demands a shift in how these organizations approach their operational, technical, and compliance frameworks.

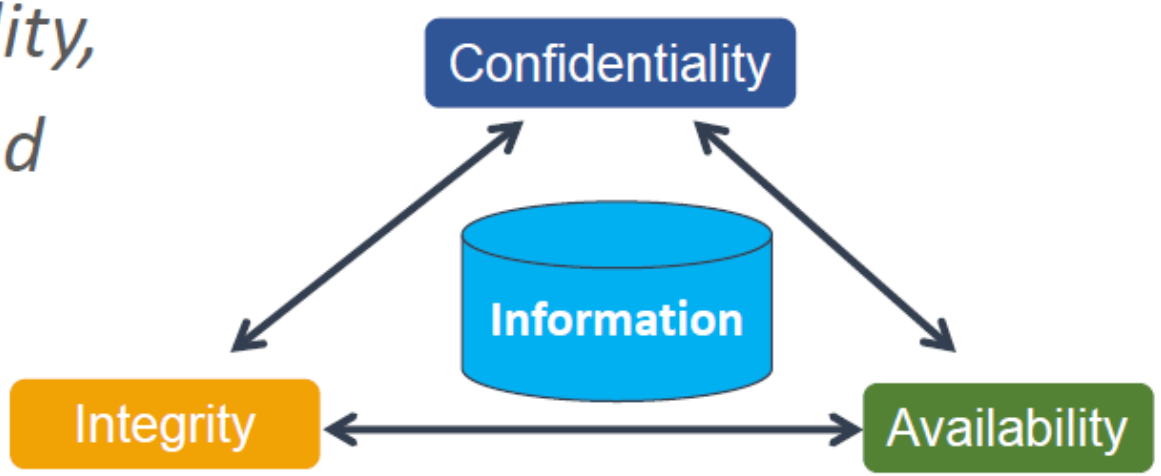
Regulation (EU) 2023/203 requirements are designed to:

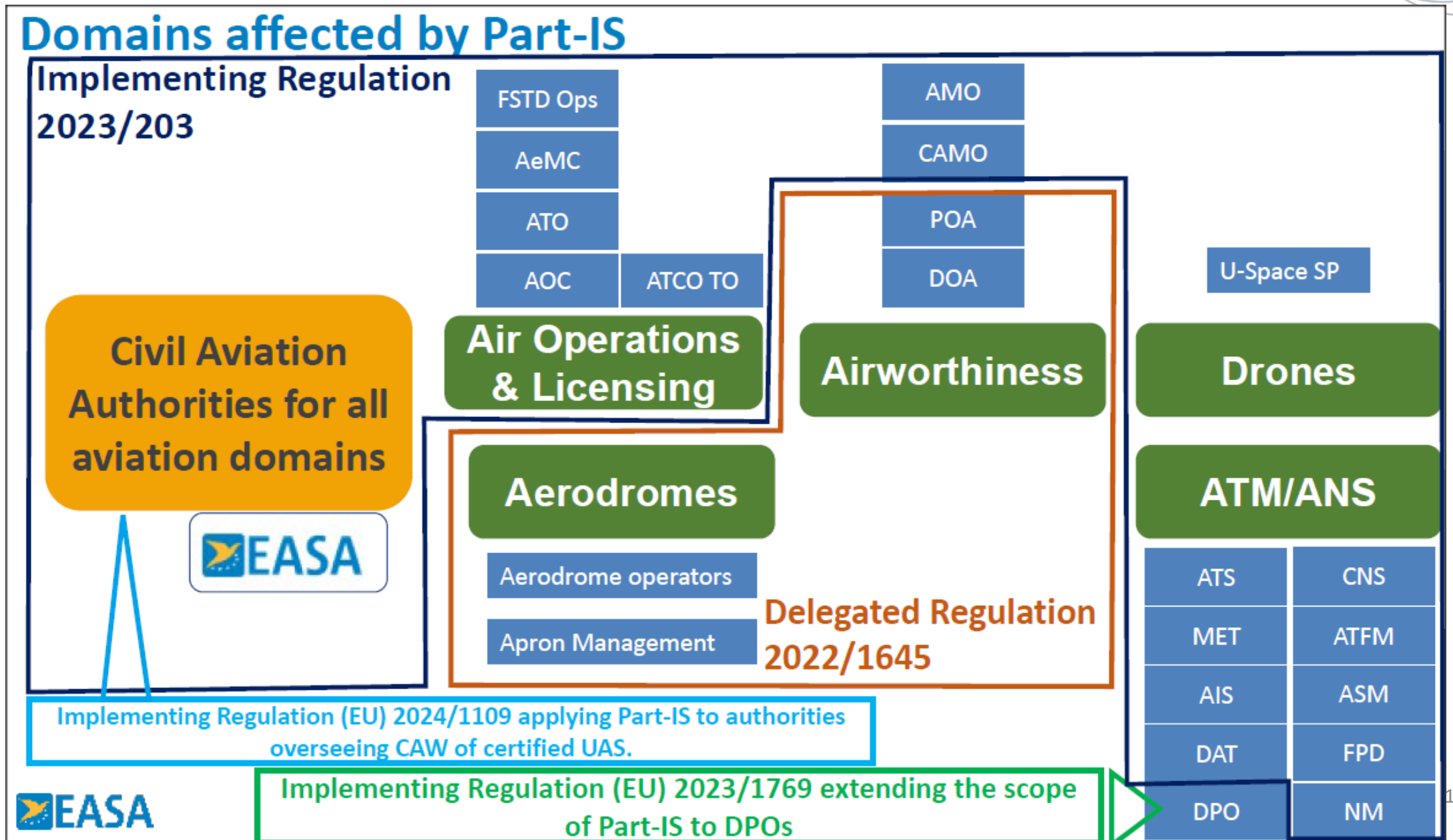
- Integrate **Information Security Management Systems (ISMS)** into the overall management system.
- Identify, assess, and mitigate risks arising from information security threats.
- Align with international standards like ISO 27001, while addressing aviation-specific needs.
- Establish reporting mechanisms for cybersecurity incidents to relevant competent authorities.


Delegated Regulation (EU) 2022/1645 – published 26.9.2022
DOA, POA, Aerodrome operators, Apron Mgt Services operators
16.10.2025
Implementing Regulation (EU) 2023/1769 extending the scope
Implementing Regulation (EU) 2023/203 – published 2.2.2023
Civil Aviation Authorities, EASA and all other types of approved org's
22.2.2026
Implementing Regulation (EU) 2024/1109 extending the scope
EDD 2023/008/R, 2023/009/R, 2023/010/R – published 12.7.2023
Acceptable Means of Compliance and Guidance Material

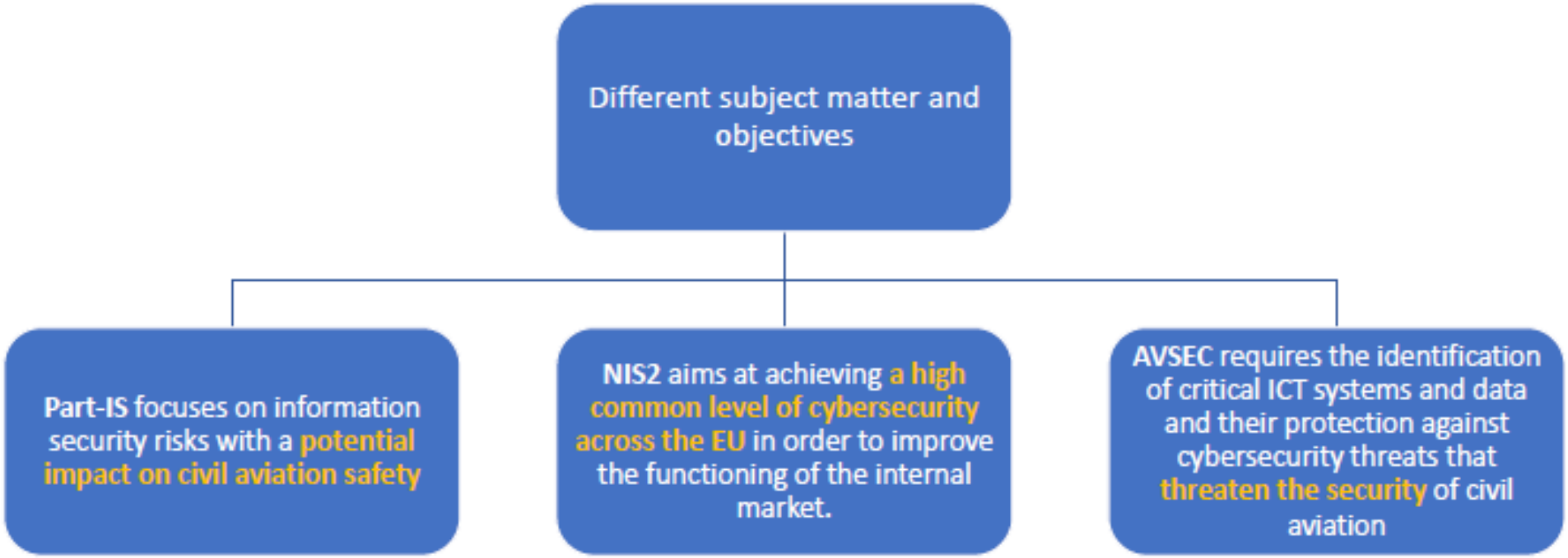
What is Information Security Management?

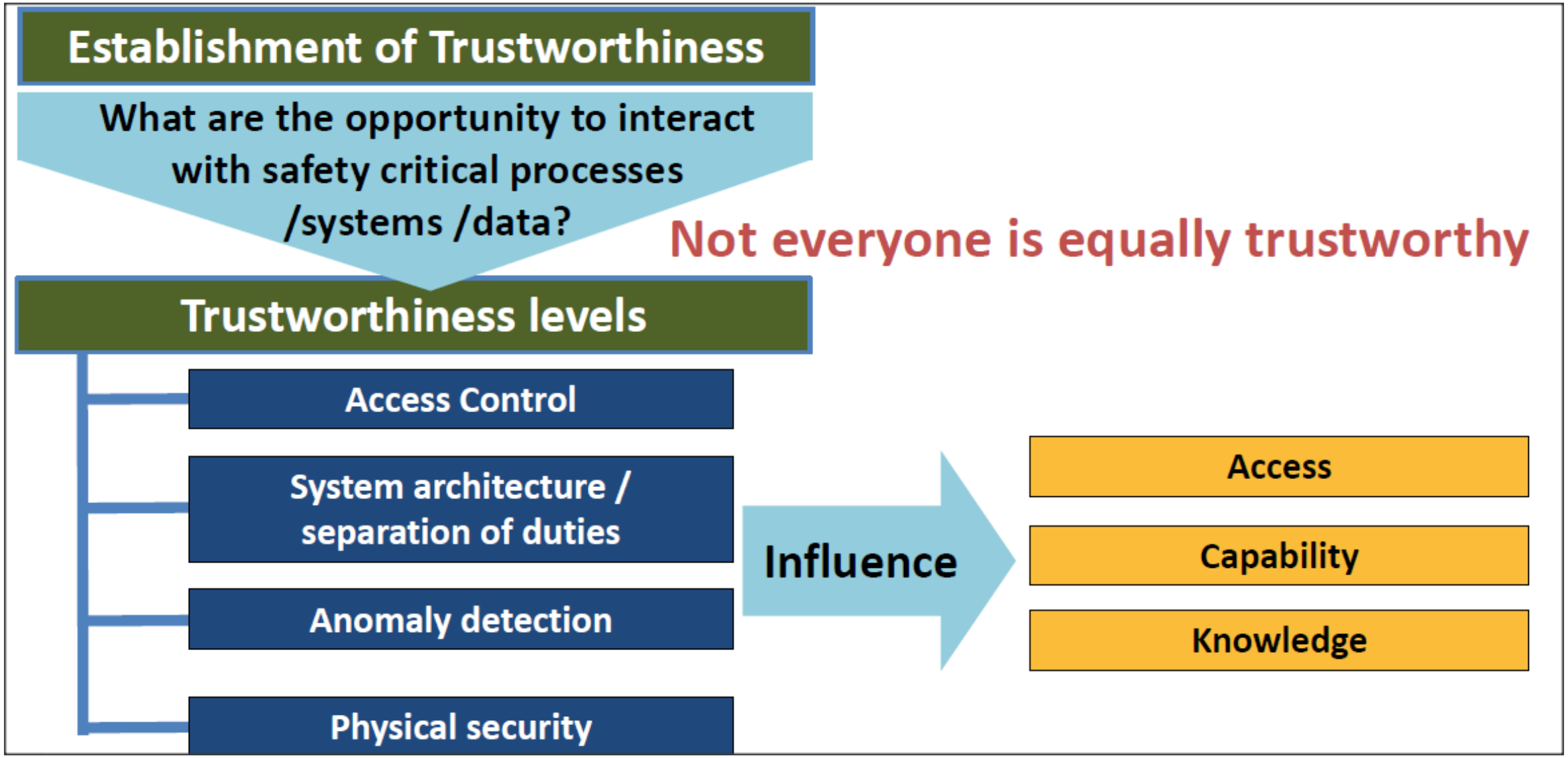
- ISO 27000 states that ***Information Security Management*** *is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their*
  - *Confidentiality,*
  - *Integrity, and*
  - *Availability.*




Domains affected by Part-IS
Implementing Regulation 2023/203
FSTD Ops
AeMC
ATO
AOC
ATCO TO
AMO
CAMO
POA
DOA
U-Space SP
Civil Aviation Authorities for all aviation domains
EASA
Air Operations & Licensing
Airworthiness
Drones
Aerodromes
Aerodrome operators
Apron Management
Delegated Regulation 2022/1645
ATM/ANS
ATS
CNS
MET
ATFM
AIS
ASM
DAT
FPD
DPO
NM
Implementing Regulation (EU) 2024/1109 applying Part-IS to authorities overseeing CAW of certified UAS.
EASA
Implementing Regulation (EU) 2023/1769 extending the scope of Part-IS to DPOs

Three different set of rules




Establishment of Trustworthiness
What are the opportunity to interact with safety critical processes /systems /data?
Not everyone is equally trustworthy
Trustworthiness levels
Access Control
System architecture / separation of duties
Anomaly detection
Physical security
Influence
Access
Capability
Knowledge

Organisation	Certificate	Part-IS	NIS 2	AvSec	Remarks
Commercial air carriers	AOC	Y	Y	Y	only Large (> 250 employee) or Medium 50 to 249 employees*
Airports	ADR Management	Y	Y	Y	only Large (> 250 employee) or Medium 50 to 249 employees*
Air traffic control [ATC]	ANSP	Y	Y	(Y)	only Large (> 250 employee) or Medium 50 to 249 employees*
Aircraft Manufacturers	POA, DOA	Y	Y / (Y)		To be determined by the Member State
Equipment Manufacturers	POA, DOA	Y	Y / (Y)		To be determined by the Member State
Maintenance organisations	MOA	Y	(Y)	(Y)	To be determined by the Member State
Maintenance management	CAMO	Y	(Y)	(Y)	To be determined by the Member State

What are the Key Ingredients for Part-IS?

Basic Regulation

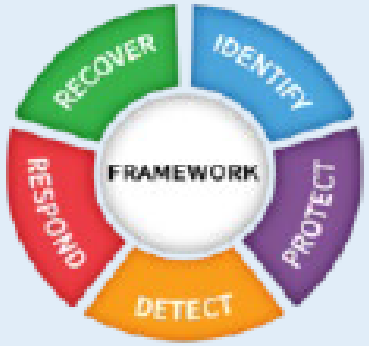
- Acceptable Safety Risks
- Record-keeping
- Personnel Requirements

ISO 2700x

- Information Security Management System (ISMS)
- Information Security Risk Assessment
- Continuous Improvement

NIST Cyber Security Framework

- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery



Reporting Regulation

- Information Security External Reporting Scheme

[Applicable from 22 February 2026 – Regulation (EU) 2023/203]

1. Establishment of an Information Security Management System (ISMS)

- The organization must set up, implement, and maintain an ISMS to manage information security risks with potential impacts on aviation safety (Annex II, IS.I.OR.200).
- The ISMS must:
  - Define a policy on information security risks.
  - Identify, assess, and manage information security risks (IS.I.OR.205).

- Implement measures for risk treatment, detection, response, and recovery (IS.I.OR.210, IS.I.OR.220).
- Ensure continuous improvement of the ISMS (IS.I.OR.260).

2. Internal and External Reporting

- An internal reporting scheme must be established for collecting and evaluating information security events (IS.I.OR.215).
- An external reporting scheme must be implemented for notifying competent authorities about information security incidents that could pose significant risks to aviation safety (IS.I.OR.230).
  - Reports must include initial notifications (as soon as the condition is identified) and detailed follow-up reports within 72 hours.

3. Risk Management

- The organization must identify and assess risks related to its activities, facilities, systems, and interfaces with other organizations (IS.I.OR.205).
- Risk treatment must ensure measures are taken to avoid, control, or mitigate unacceptable risks without introducing new safety risks (IS.I.OR.210).

Detailed Discussion: Risk Management in EASA Part 145 Organizations

Risk management is a cornerstone of ensuring aviation safety, particularly as it pertains to information and cyber security risks.

Under the Requirements of REGULATION (EU) 2023/203, Organizations must adopt a Systematic Approach to Identifying, Assessing, Treating, and Managing Risks that may arise from Information Security Threats.

3. Risk Management

- The organization must identify and assess risks related to its activities, facilities, systems, and interfaces with other organizations (IS.I.OR.205).
- Risk treatment must ensure measures are taken to avoid, control, or mitigate unacceptable risks without introducing new safety risks (IS.I.OR.210).

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Identify Potential Cybersecurity Risks - Key Actions:

For each identified activity, facility, and resource, list potential cybersecurity vulnerabilities. Include risks such as:

- Unauthorized access to maintenance systems.
- Compromised calibration data for critical tools.
- Ransomware attacks on maintenance records.
- Conduct brainstorming sessions or use established to identify vulnerabilities.
- Include risks posed by external entities (e.g., third-party contractors with IT access).

Assess Interfaces with Other Organizations - Key Actions:

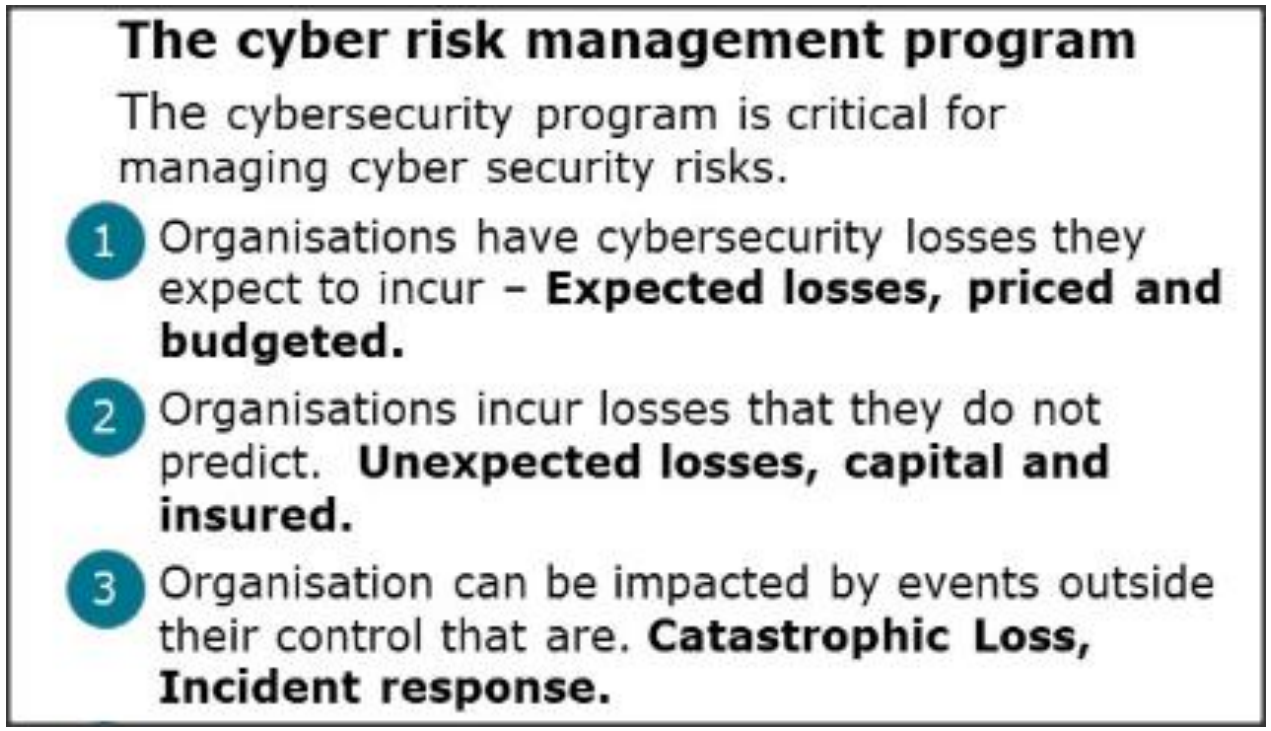
Document interfaces with external organizations that could introduce cybersecurity risks.

- Examples include connections with suppliers, CAMOs, or design organizations.
- Use a data flow analysis to visualize all data exchange points.
- Assess the cybersecurity measures of external parties, ensuring they align with your standards.

Detailed Discussion: Risk Management in EASA Part 145 Organizations

Risk management is a cornerstone of ensuring aviation safety, particularly as it pertains to information and cyber security risks.

Under the requirements of COMMISSION IMPLEMENTING REGULATION (EU) 2023/203, organizations must adopt a systematic approach to identifying, assessing, treating, and managing risks that may arise from information security threats.



THE 12 CYBERSECURITY PROFILES

Chief Information Security Officer (CISO)

Cyber Incident Responder

Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator

Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

Penetration Tester

Each role is considered in the context of regulatory compliance, focusing on practical implementation, continuous improvement, and measurable outcomes aligned with IS.I.OR.240.

Accountable Manager - Cybersecurity Duties:

Holds overall corporate authority to ensure the implementation and financing of the Information Security Management System (ISMS).

- Establishes and promotes the **information security policy**, ensuring its alignment with organizational objectives and regulatory requirements (IS.I.OR.200(a)(1)).
- Ensures adequate resourcing for cybersecurity measures, including personnel, tools, and training (IS.I.OR.240(a)).

Accountable Manager Information Security Obligations

Oversees implementation and financing of the ISMS.

Aligns information security policy with organizational objectives.

Ensures resources for cybersecurity: personnel, tools, and training.

Monitors ISMS compliance and drives improvements.

Understands cybersecurity regulations and their impact on aviation safety.

- Monitors compliance of the ISMS through regular feedback and improvement measures (IS.I.OR.260).
- Demonstrates a basic understanding of cybersecurity regulations and their impact on aviation safety.

Accountable Manager - Cybersecurity Performance Measurement:

- Implementation and promotion of an effective **information security policy**.
- Availability of resources to address cybersecurity risks and compliance with ISMS requirements.
- Incident response performance, including adherence to reporting timelines and corrective actions.
- Continuous improvement of the ISMS, evidenced through successful audits and risk assessments.

Nominated Post Holder - Cybersecurity Duties:

Oversees the implementation of cybersecurity controls within their operational area.

Ensures compliance with risk assessment processes to identify and address information security risks (IS.I.OR.205).

Monitors cybersecurity activities, such as internal reporting schemes (IS.I.OR.215) and risk treatment measures (IS.I.OR.210).

Coordinates with other stakeholders to ensure consistent application of cybersecurity policies and practices across interfaces.

Nominated Post Holder - Cybersecurity Performance Measurement:

- Completion of risk assessments and implementation of risk treatment plans.
- Timely and accurate reporting of cybersecurity events to internal and external stakeholders (IS.I.OR.230).
- Effective integration of cybersecurity controls into daily operations.
- Reduction in vulnerabilities and alignment with safety objectives.

Business Area Manager - Cybersecurity Duties:

Ensures cybersecurity risk management processes are effectively implemented within their department.

Oversees training and awareness programs for employees to minimize cybersecurity risks (IS.I.OR.240(g)).

Coordinates the reporting of cybersecurity events and incidents within their area of responsibility (IS.I.OR.215).

Allocates resources to ensure compliance with cybersecurity requirements for systems, data, and infrastructure.

Business Area Manager - Cybersecurity Performance Measurement:

- Departmental compliance with cybersecurity regulations, as verified through internal and external audits.
- Participation in cybersecurity incident detection and response activities (IS.I.OR.220).
- Staff competency in identifying and mitigating cybersecurity risks.
- Integration of cybersecurity practices into operational workflows.

Compliance & Safety Manager - Cybersecurity Duties:

Develops and oversees the **Information Security Risk Assessment** process, ensuring risks are identified, classified, and treated effectively (IS.I.OR.205 and IS.I.OR.210).

Monitors and evaluates the organization's compliance with cybersecurity regulations (IS.I.OR.225).

Implements and manages the **internal reporting scheme** for cybersecurity events, including detection, analysis, and follow-up (IS.I.OR.215).

Ensures regular updates and reviews of the ISMS based on lessons learned from incidents and evolving threats (IS.I.OR.260).

Compliance & Safety Manager - Cybersecurity Performance Measurement:

- Timely identification and resolution of cybersecurity incidents.
- Regular and comprehensive updates to the ISMS based on performance indicators and incident reviews.
- Quality and thoroughness of safety and cybersecurity training initiatives.
- Reduced exposure to information security risks across the organization.

Common Responsible Person - Cybersecurity Duties:

- Coordinates cybersecurity policies, procedures, and responsibilities across shared organizational structures (IS.I.OR.240(d)).
- Establishes procedures for managing **shared information security risks**, ensuring adequate integration across all entities (IS.I.OR.205(b)).
- Oversees implementation and continuous improvement of cybersecurity practices within shared resources and infrastructure (IS.I.OR.260).
- Maintains a collaborative relationship with all stakeholders to ensure consistent compliance with cybersecurity objectives.

Refer to BASIC Checklist - Basic Check List for ISO 27001 Cyber Security Information System (Sofema Library)

Gaps Identified:

- Insufficient integration of systemic vulnerability assessments.
- Lack of a structured process to evaluate supply chain cybersecurity risks.

Recommendations:

1. Conduct detailed risk assessments in line with IS.I.OR.205.
2. Utilize AMC1 IS.I.OR.200 to develop a framework for emerging threat identification.

Gaps Identified:

- Missing or incomplete ISMM documentation.
- Lack of a defined amendment process for ISMS.

Recommendations:

1. Update ISMM following AMC1 IS.I.OR.250 requirements.
1. Implement structured amendments per GM1 IS.I.OR.250

Gaps Identified:

- Undefined competency requirements for ISMS roles.
- Limited cybersecurity training for contractors and third-party vendors.

Recommendations:

Enhance training programs based on AMC1 IS.I.OR.240(e).

Ensure role-specific training, referencing GM1 IS.I.OR.240

Gaps Identified:

- Inadequate deployment of automated vulnerability detection tools.
- Weak multifactor authentication protocols.

Recommendations:

1. Strengthen encryption measures following AMC1 IS.I.OR.200(c).
2. Regularly test IT systems as outlined in GM1 IS.I.OR.200(d)

Gaps Identified:

- Lack of scenario-based testing for incident response.
- Inconsistent external reporting mechanisms.

Recommendations:

1. Conduct scenario-based exercises as detailed in AMC1 IS.I.OR.220(b).
2. Establish reporting protocols using IS.I.OR.230 guidelines

Gaps Identified:

- Limited audit integration into cybersecurity management.
- Insufficient monitoring of third-party compliance.

Recommendations:

1. Expand audit programs per AMC1 IS.I.OR.235(b).
1. Use findings to refine ISMS continuously, as outlined in GM1 IS.I.OR.260

Gaps Identified:

- Inadequate documentation of improvement initiatives.
- Emerging threats are not consistently reassessed.

Recommendations:

Conduct comprehensive reviews following GM1 IS.I.OR.260(a).

Update security controls to address newly identified vulnerabilities

Gaps Identified:

- Insufficient oversight mechanisms for contractors.
- Lack of consistent audit schedules for third-party compliance.

Recommendations:

Strengthen contractor oversight with regular audits as per GM1 IS.I.OR.235.

Develop clear compliance requirements for all third-party activities

Gaps Identified:

- Incomplete records of cybersecurity incidents.
- Weak cross-referencing between records and ISMS protocols.

Recommendations:

Maintain comprehensive records following AMC1 IS.I.OR.245.

Ensure clarity and accessibility of all documentation

Thank you for attending this Workshop

I hope very much you found it useful and informative

Any Questions?

Here is the Discount Code for the 145 Cyber Course on SOL

CYBER20