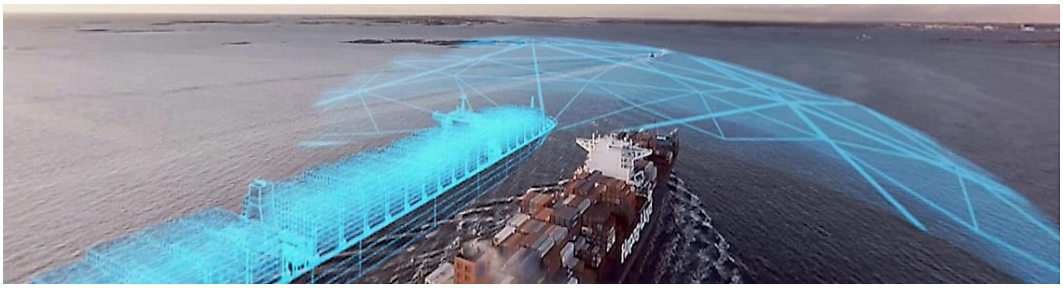
Information Systems Security in Shipping, according to ISO 27001



Stergios OIKONOMOU
Alexandros VOLIOTIS

About the presenters

Stergios Oikonomou

Stergios is a Lieutenant of Hellenic Air Force. His specialist is Communication & Electronic Technichian.

Stergios has in depth knowledge of Information Security and has worked for EU OHQ in Larissa.

Alexandros Voliotis

Alexandros is a 2nd Lieutenant of Hellenic Army. His specialist is Network Administrator.

Alexandros has in depth knowledge of Information System management and has worked for EU OHQ in Larissa.

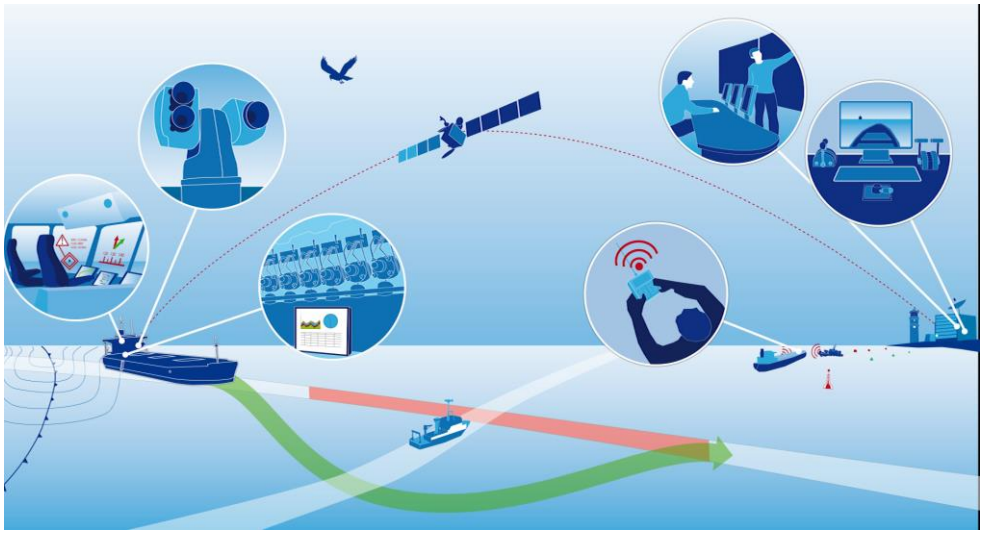
Stergios OIKONOMOU
Alexandros VOLIOTIS

ToC

- Shipping
- Information Systems
- Information Systems Security
- ISO 27001:2013
- Information Systems Security in Shipping, according to ISO 27001:2013
- Conclusions
- Questions

Shipping

Shipping



Stergios OIKONOMOU
Alexandros VOLIOTIS

Shipping

Stergios OIKONOMOU
Alexandros VOLIOTIS

Shipping

Container ships

carry most of the world's manufactured goods and products, usually through scheduled liner services.

Bulk carriers ships

transport raw materials such as iron ore and coal.

Tankers ships

transport crude oil, chemicals and petroleum products.

Cruise ships

perform short journeys for a mix of passengers, cars and commercial vehicles.

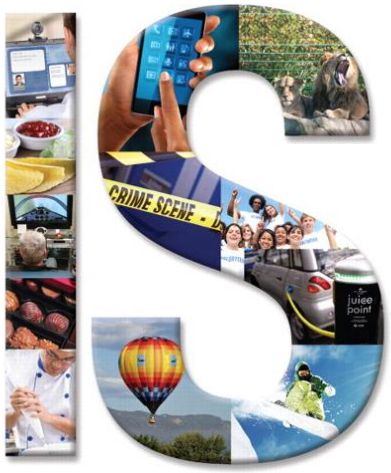
Shipping

- Over 90% of world trade is carried by the international shipping industry.
- Without shipping the import and export of goods would not be possible.

Information Systems (IS)

Definition of IS

"Information systems are interrelated components working together to collect, process, store, and disseminate information to support decision making, coordination, control, analysis, and visualization in an organization".

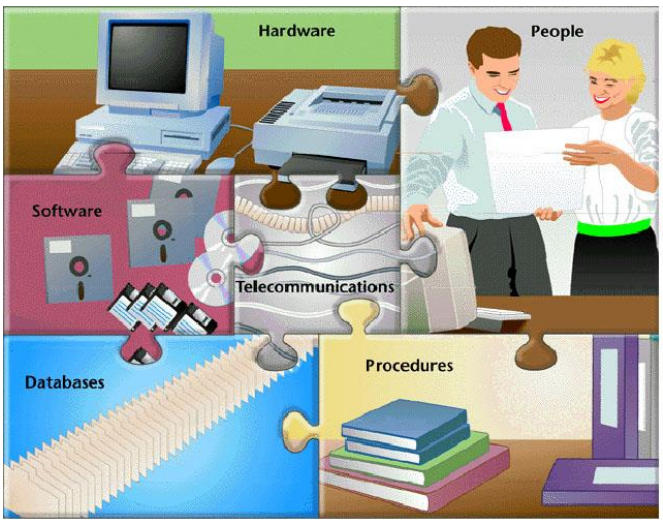


Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems (IS)

Component of IS

- Hardware
- Software
- Data
- Telecommunication - Network
- Procedures
- People



Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems (IS)

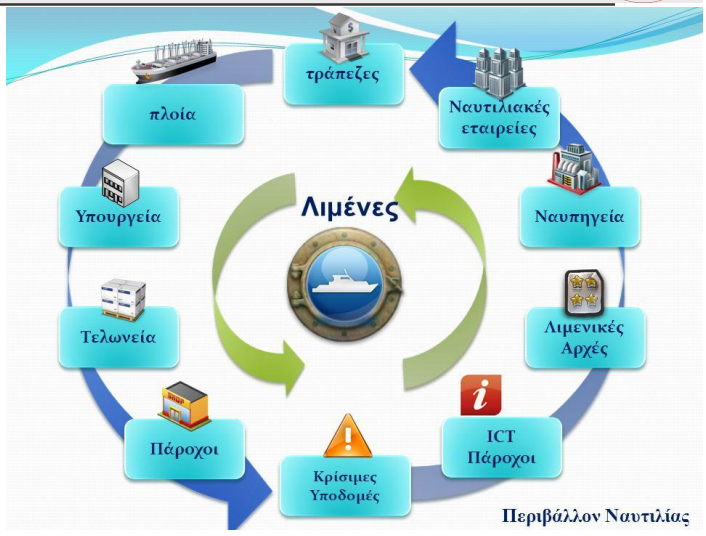
Types of IS

KMS (Knowledge Management Systems)
OAS (Office Automation Systems)
TPS (Transaction Processing Systems)
ESS (Executive Support Systems)
DSS (Decision Support Systems)
MIS (Management Information Systems)

Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems (IS)

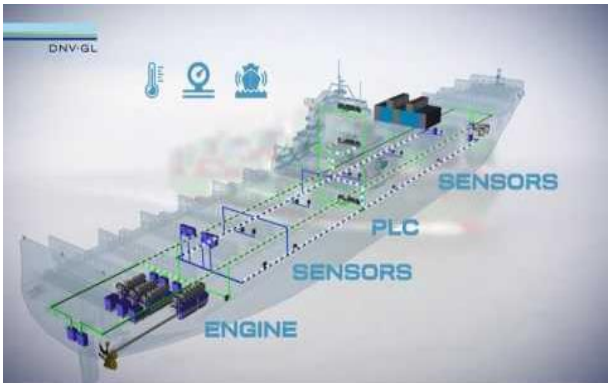
Use of IS



Stergios OIKONOMOU
Alexandros VOLIOTIS

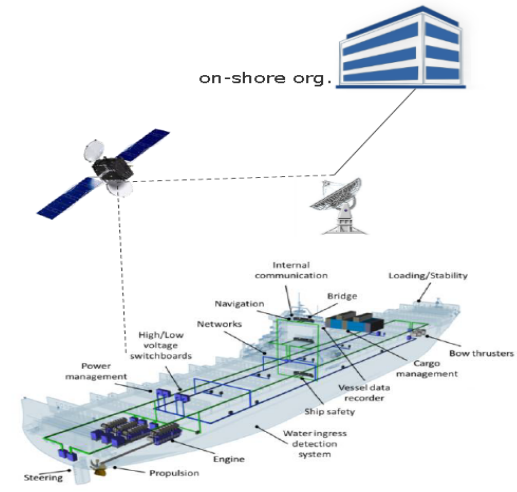
Information Systems (IS)

IS in Shipping



Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems (IS)



Information Technology (IT)

- IT networks
- E-mail
- Administration, accounts, crew lists, …
- Planned Maintenance
- Spares management and requisitioning
- Electronic manuals
- Electronic certificates
- Permits to work
- Charter party, notice of readiness, bill of lading…

At risk: Mainly finance and reputation

Operation Technology (OT)

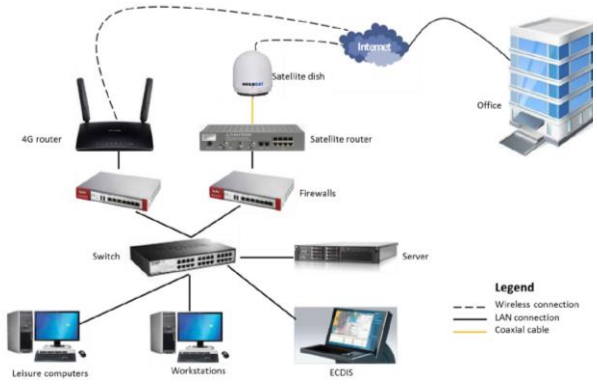
- PLCs
- SCADA
- On-board measurement and control
- ECDIS
- GPS
- Remote support for engines
- Data loggers
- Engine & Cargo control
- Dynamic positioning, …

At risk: Life, property and environment + all of the above

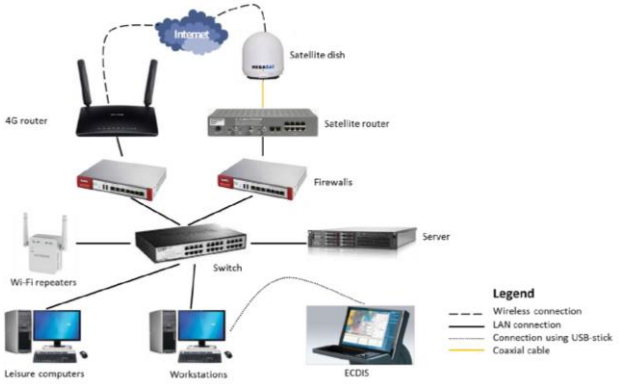
Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems (IS)

Ship A's Network



Ship B's Network



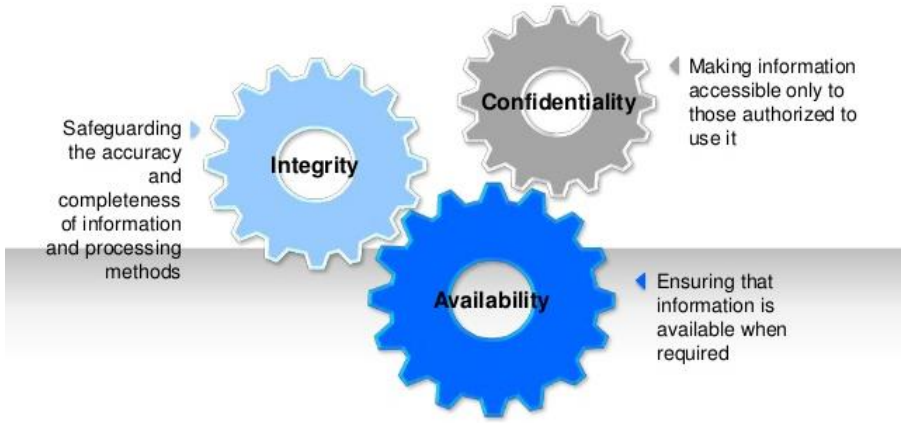
Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems Security

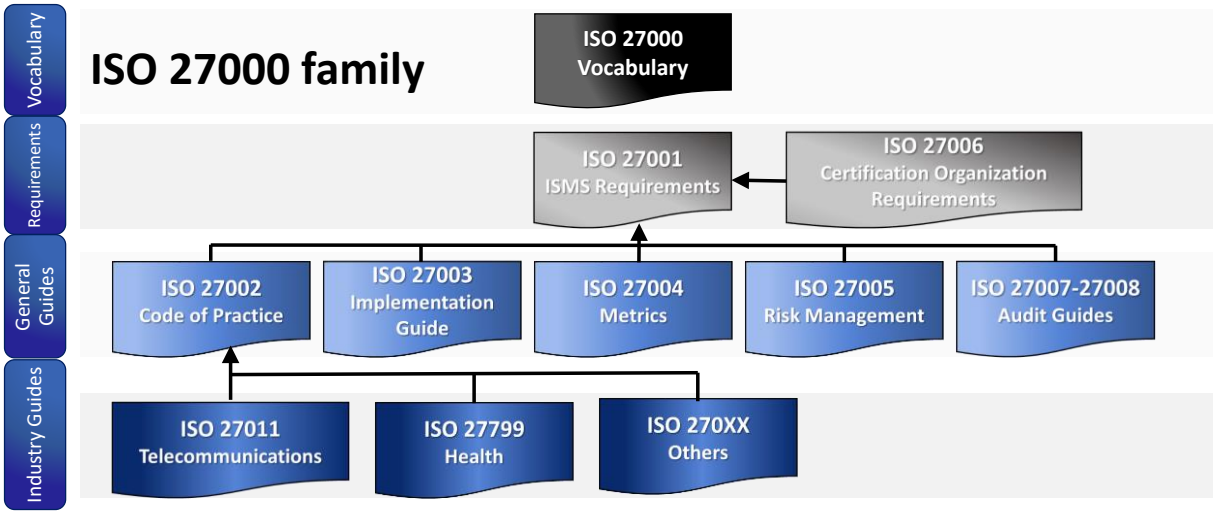
Stergios OIKONOMOU
Alexandros VOLIOTIS

Information Systems Security

Components of Information Security

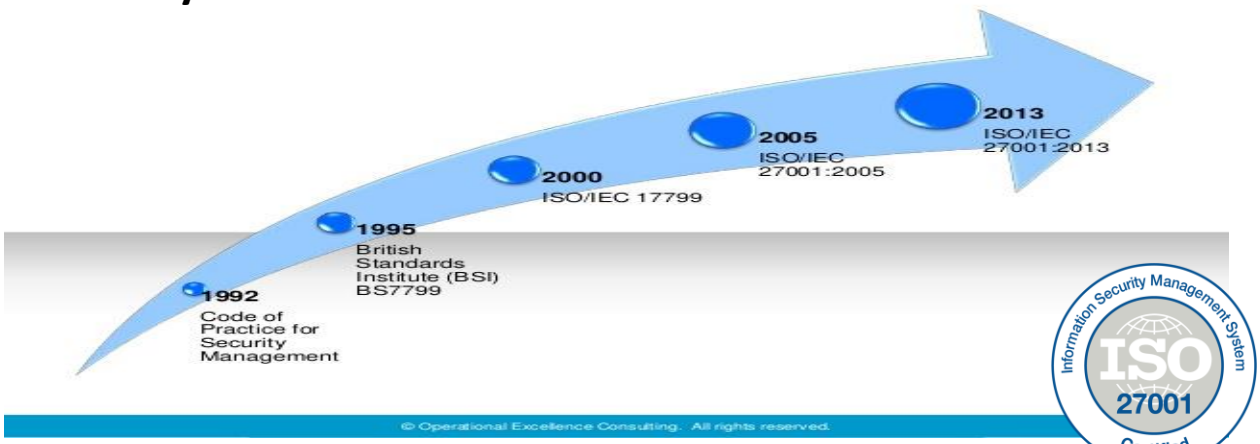


ISO 27001:2013



ISO 27001:2013

History of ISO 27001:2013



Stergios OIKONOMOU
Alexandros VOLIOTIS

ISO 27001:2013

ISO 27001 Structure

0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
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
  - 6.1.1 General
  - 6.1.2 Information security risk assessment
  - 6.1.3 Information security risk treatment
- 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
  - 7.5.1 General
  - 7.5.2 Creating and updating
  - 7.5.3 Control of documented information

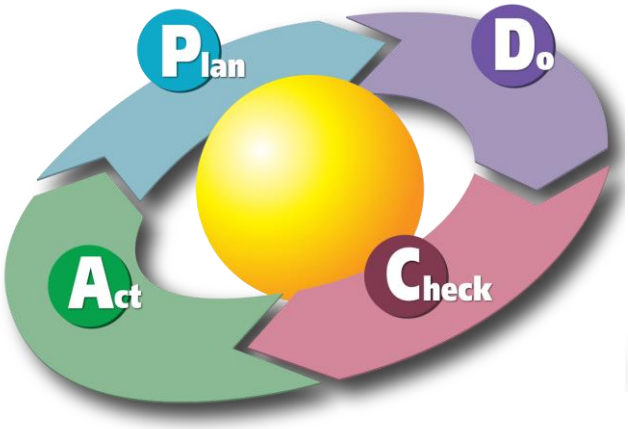
8 Operation
- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

9 Performance evaluation
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10 Improvement
- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

ISO 27001:2013

Models

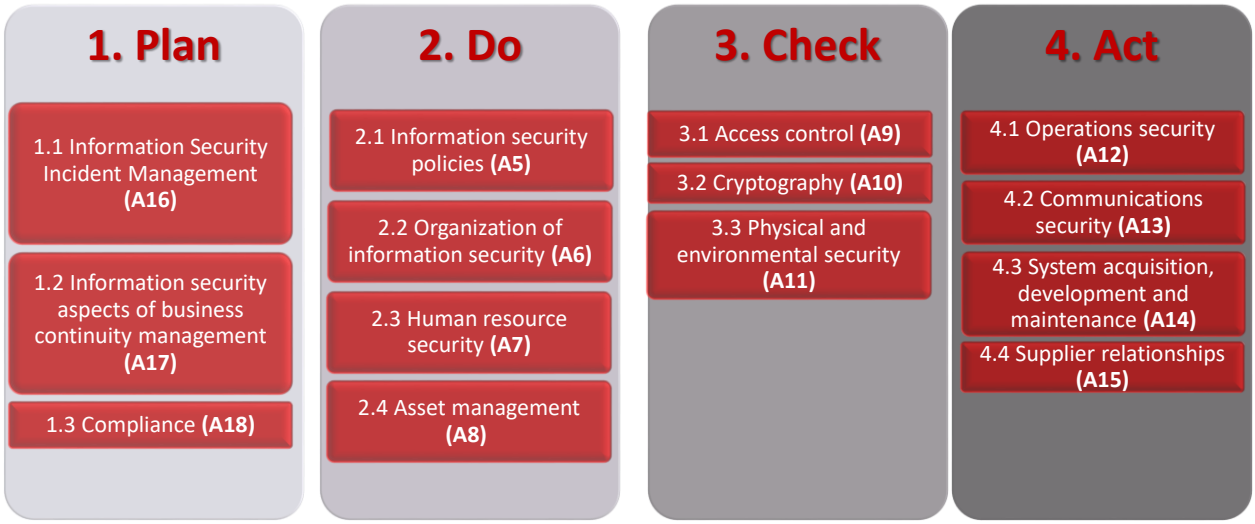


ISO 27001:2013

PDCA Model

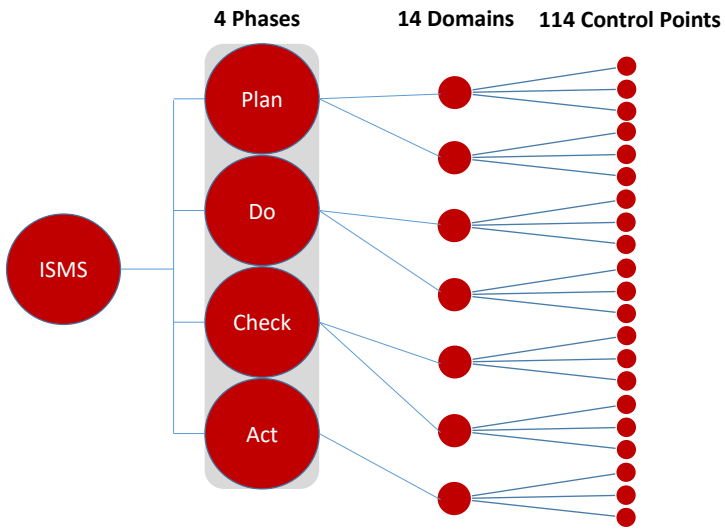
- Plan (establish the ISMS)
  - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Do (implement and operate the ISMS)
  - Implement and operate the ISMS policy, controls, processes and procedures.
- Check (monitor and review the ISMS)
  - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Act (maintain and improve the ISMS)
  - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

ISO 27001.2013



Stergios OIKONOMOU
Alexandros VOLIOTIS

ISO 27001:2013



Stergios OIKONOMOU
Alexandros VOLIOTIS

ISO 27001:2013

Continual Improvement of ISMS

The organization shall continually improve the effectiveness of the ISMS through the use of:

- The information security policy;
- Information security objectives;
- Audit results;
- Analysis of monitored events;
- Corrective and preventive actions;
- Management review.

ISO 27001:2013

Benefits of ISO 27001:2013

- **It improves enterprise security**
- **It is an independent, unbiased measurement of the actual information security state**
- **It reduces customer and supply chain audit**
- **Increased legislative and regulatory compliance**
- **Keeps Confidential information secure**
- **Gives confidence to customers and stakeholders on how you manage risk**
- **Secure exchange of information**
- **Minimizes risk exposure**
- **Builds a culture of security**
- **Protects the Organization assets, shareholders and customers**
- **Provide Competitive advantage**
- **Enhanced Costumer Satisfaction**

Information Systems Security in Shipping, according to ISO 27001:2013

7.2.2 ***Information security awareness, education, and training***

The organisation must provide the following training to its staff and that of suppliers involved in the operational management of the digitisation or archiving processes performed by the organisation:

- awareness training
- continuous training

Example

awareness posters, briefings, slide decks for seminars and courses, guidelines, tests and quizzes

Keep

- awareness diary
- rolling plan
- employee training records (updated)

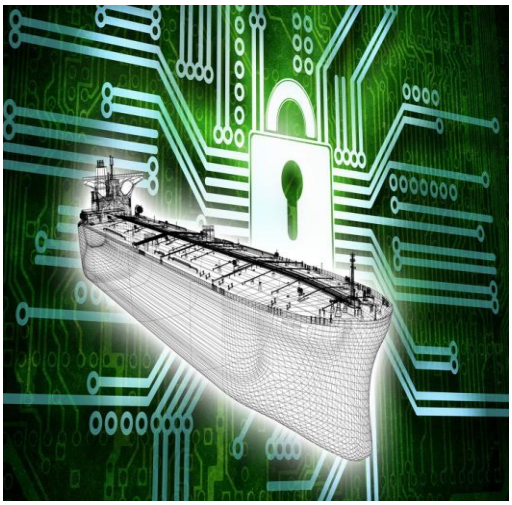
Information Systems Security in Shipping, according to ISO 27001:2013

8.2.1 ***Information classification***

Classification levels and guidelines must be defined and implemented by the organisation specifically for clients' digital files and documents managed by the organisation as part of the digitisation or archiving processes.

The organisation must:

- **Define** classification levels and guidelines for the following elements:
  - client collected documents (analogue and digital).
  - digital documents generated by scanning clients' analogue documents.
  - clients' digital files.
- **Ensure** that these classification levels and guidelines are reviewed by the person responsible for the digitisation or archiving processes regularly (at least once a year)



Information Systems Security in Shipping, according to ISO 27001:2013

11.1.2 *Physical access controls*

The organisation must take into account the following directives:

- All visitors to the organisation:
  - **Must** be accompanied by a member of the organisation permanently authorised to circulate in the areas accessed by the visitors, even if they have already been authorised to access such areas.
  - **Must** be excluded from areas associated with the digitisation process
- Third parties with permanent authorisation to access secure areas of the organisation must not be able to access the technical assets
- The technical digitisation or archiving system must be protected against unauthorised access:
  - In the event of evacuation of the areas hosting these assets.
  - If they are located in multi-occupant sites

Information Systems Security in Shipping, according to ISO 27001:2013

15.1.2 *Security within supplier agreements (1/3)*

The organisation must include the following conditions in the contractual document drawn up with the supplier supporting the digitisation or archiving processes performed by the organisation:

- Provisions concerning ownership of the products and services,
- Provisions concerning the continuous provision of the products and services provided by the supplier, including in the event of disaster.
- Observance of the organisation's digitisation or archiving policy.

Information Systems Security in Shipping, according to ISO 27001:2013

15.1.2 *Security within supplier agreements (2/3)*

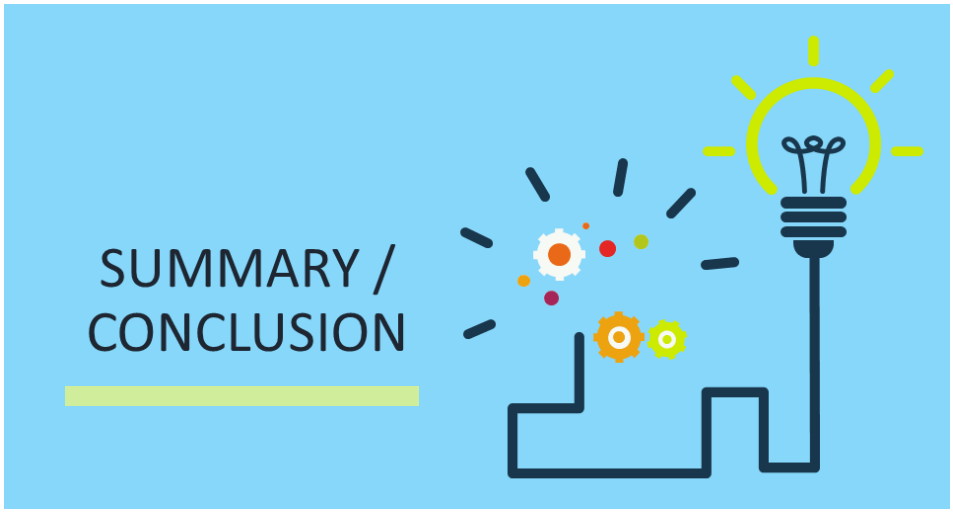
- Measures guaranteeing:
  - The swiftest possible notification of any security changes applied to the assets of the supplier and their suppliers that could affect the digitisation or archiving processes performed by the organisation.
  - That the information belonging to the organisation that is accessed by the supplier and their suppliers is used exclusively for the purposes for which it was made available to the supplier and their suppliers.
  - That changes affecting the supplier's suppliers involved in the digitisation or archiving processes performed by the organisation are approved in advance by the organisation.

Information Systems Security in Shipping, according to ISO 27001:2013

15.1.2 *Security within supplier agreements (3/3)*

- The commitment of the supplier to cooperate with the organisation in any investigations undertaken by the organisation to resolve incidents that could affect the services or products provided to the organisation by the supplier, that are assumed or shown not to be attributable to the supplier or their suppliers.
- The right to audit the supplier and their suppliers equally, in consideration of their involvement in the digitisation or archiving processes performed by the organisation.

Conclusion



Questions