CYRIS360

GRC services

April 2024 – Version 1.1

Unleashing Cyber Resilience in Every Direction.

In this Presentation

Overview

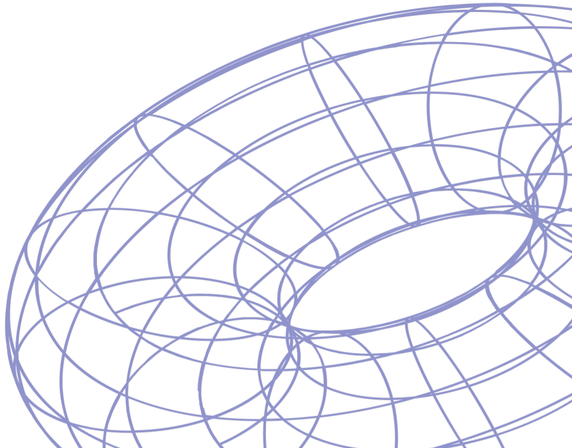
1. ISO/IEC 27001 Overview & Benefits

Online shopping can change the way we do business.

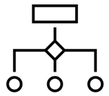
Reduce the risks related to information security

Earn customer's trust

Increase your competitive advantage



The ISO/IEC 27001 Controls

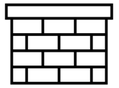


Organizational

37 controls related to the ISMS documentation such as general policies and processes.

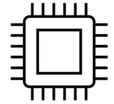
People

8 controls related to managing your staff such as onboarding and offboarding processes.



Physical

14 controls related to the organization's premises such as employee access to secure areas.

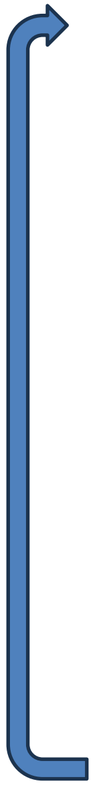


Technological

34 controls related to systems, cryptography, software and network to protect the assets.

The ISO High Level Structure

(aka: Annex L)



Step 1

Plan

4-Context of the organization
5-Leadership
6-Planning

Step 2

Do

7-Support
8-Operation

Step 3

Check

9-Performance Evaluation

Step 4

Act

10-Improvement

2.1 ISO 27035

ISO/IEC 27035-1:2023 presents basic concepts, principles, and processes with key activities of information security incident management.

Incident response process:

- Plan & Prepare
- Detect & Report
- Assess & Decide
- Respond
- Learn lessons

- **Part 1**: Principle and process.
- **Part 2**: Guidelines to plan and prepare for incident response.
- **Part 3**: Guidelines for ICT Incident response operations.

2.2 ISO 22301

Relevant if Business Continuity is important for you/your customers

Certifiable standard – can be implemented independently or in combination with ISO27001

Examples:

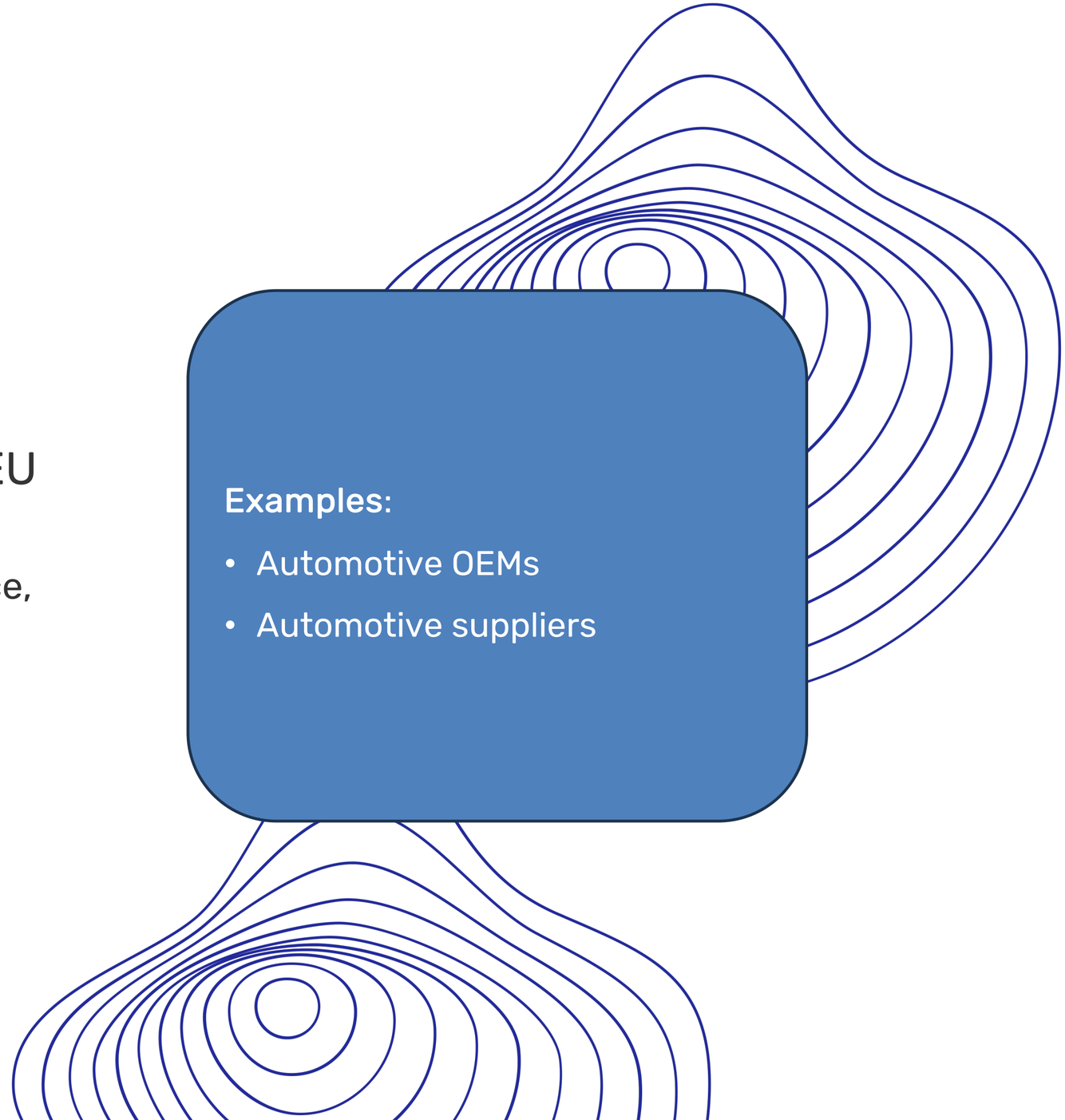
- Energy & Utilities
- Telecom service providers
- Mobility solutions providers
- Banking, Payment and FinTech

2.3 TISAX ISA

Relevant for Automotive industry in EU

Extends ISO27001 with topic-specific guidance, and include 6 maturity levels:

- Incomplete
- Performed
- Managed
- Established
- Predictable
- Optimized



3. Information Security Governance

Infrastructure

We help our clients protect their digital infrastructure (On-prem & Cloud) by reducing the attack surface and implementing secure communication (Including TLS configuration)

IAM

We help our clients implement Identity and access management (IAM) best practices, such as multifactor authentication, least privilege, and separation of duties.

DLP

We help our clients protect their data by implementing Data Loss Prevention (DLP).

SOC

We help our client detect and respond to unusual & suspicious activities by implementing a Security Operation Center (SOC)

4. Relevant EU Regulations

4.1 NIS2

NIS2 regulation apply to entities that operates in certain (critical) sectors, if these are qualified as important or essential entities.

- Information security policy
- Incident handling
- Business continuity
- Supply chain security
- Network security
- Risk management
- Cyber hygiene & Training
- Use of cryptography

4.2 DORA

DORA relates explicitly to EU financial services, focusing on maintaining cybersecurity resilience.

- ICT Risk Management Framework
- Incident Management and Reporting
- Compliance Management and Reporting
- Operational Resilience
- Supply chain security

Do you have any questions?

Let us know: we are happy to help!

info@cyris360.com

www.cyris360.com

CYRIS360