NIS Directive

Achieving Compliance & Maintaining Security

20th Feb, 2019

Applied Risk

NIS Directive

Achieving Compliance & Maintaining Security

Agenda.

- 1 I Introduction to EU NIS Directive
- 2 I Requirements for Operator of Essential Service
- 3 I Pitfalls and Challenges
- 4 I Journey to compliance
- 5 I Summary

Applied Risk

About Us

Applied Risk ensures the security of critical industrial infrastructure.

We provide critical infrastructure security at a global level without adversely impacting on production.

Our extensive engineering and cyber security knowledge of identifying vulnerabilities and risks is based on methodology honed over years of working in industrial environments.

Our offering includes a wealth of engineering and technical assurance services, combined with comprehensive security assessment.

These cover the full spectrum of our client's critical asset requirements while meeting international standards such as IEC 62443 and NIST 800-82.

Anne Klebsch

- ICS Security Consultant
- Over 9 years experience in IT and OT security
- Expertise in the areas of risk management, governance and regulatory compliance
- Worked with a wide range of major service providers in Oil & Gas, Tank Storage, FMCG, Pharmaceutical and Manufacturing
- Certified Industrial Cyber Security Professional (GICSP), Certified Information System Auditor (CISA), Certified Systems and Network Auditor (GSNA), M.Sc. Computer Security

Introduction NIS Directive

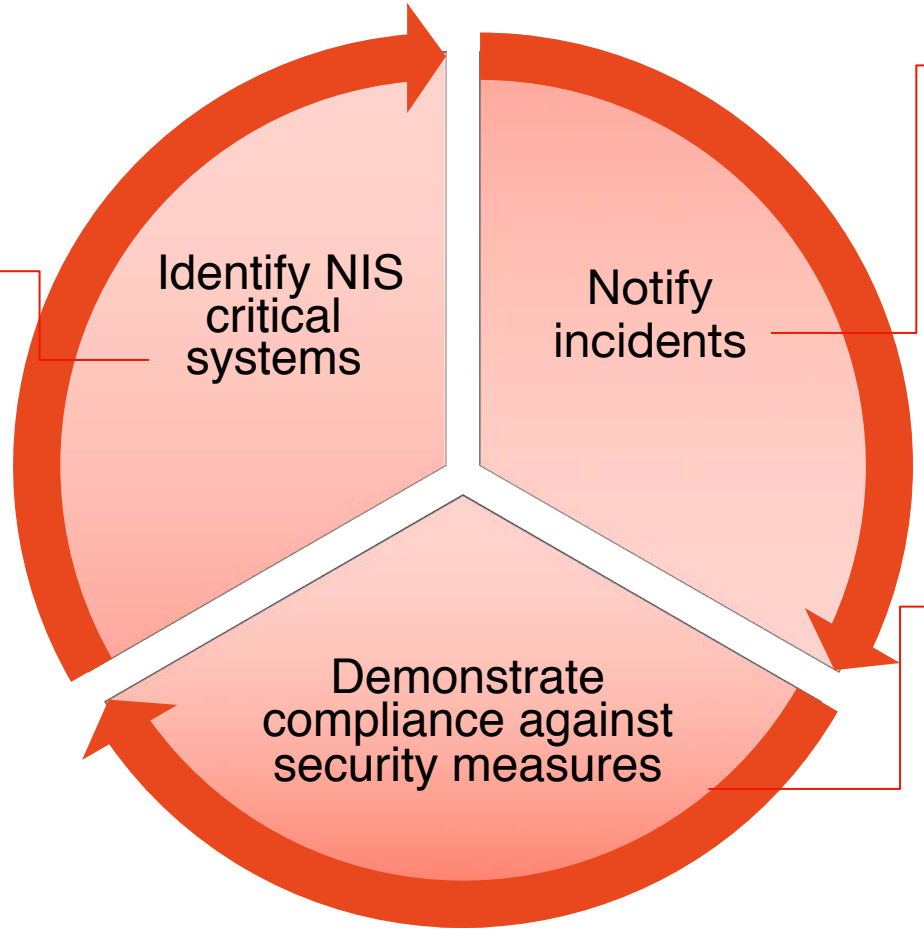
- Directive on security of network and information systems
- Adopted by the European Parliament in July 2016
- EU member states had been asked to transpose the Directive into national law in May 2018
- Objective: high common level of security of network and information systems across the Union

Introduction NIS Directive

- (a) It lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;
- (b) It creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
- (c) It creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
- (d) It establishes security and notification requirements for operators of essential services and for digital service providers;
- (e) It lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Requirements for Operators of Essential Service

- Identify those network & information systems that can impact business operations (essential services) in case of failure
- Can be in both physical, PCD and Office IT landscape
- Verify compliance with adequate security standard



- Implement & test procedure to notify incidents to regulator and CSIRTs
- Mandatory reporting for incidents that meet regulatory threshold (<72 hours)
- Voluntary reporting for all other incidents

- Identify country and asset NIS focal points
- Security measures cover of technical and non-technical areas (physical security, HR, supply chain, etc.)
- Provide information upon request
- Perform health check assessments
- Cooperate with regulatory audits

Applied Risk

Requirements for Operators of Essential Service

			
Thresholds for nomination as OES Factors considered when determining thresholds: • Number of users affected • Duration of the incident • Geographic spread of incident	• Train stations • Freight Yards • Shunting/ Marshalling Yards • Operators of rail tracks and signal boxes • Operation centers	• Rail was not nominated as different modes of transportation and detours would likely be available	• operator of a mainline railway • high speed rail services • metros, trams and other light rail services with more than 50 million annual passenger journeys • Operator of Channel Tunnel train or the infrastructure manager of the Channel Fixed Link
When to report to who?	• BSI and Federal Agency • Without undue delay	• Without undue delay	• without undue delay and no later than 72 hours after incident detection
Demonstrating compliance	• External audits • penalty up to €100,000.-	• External audits (government)	• CAF Self Assessment • Penalty 4% of the global turnover of the company

Case Study: Pitfalls and Challenges

- Based on our experience of advising OES that face NIS
- We present the most common:
  - Misconceptions
  - Challenges
  - Pitfalls encountered
- What should be done about them?

1. What are the requirements?

Challenge: Not clear what to do

If not yet, when is it EXPECTED?

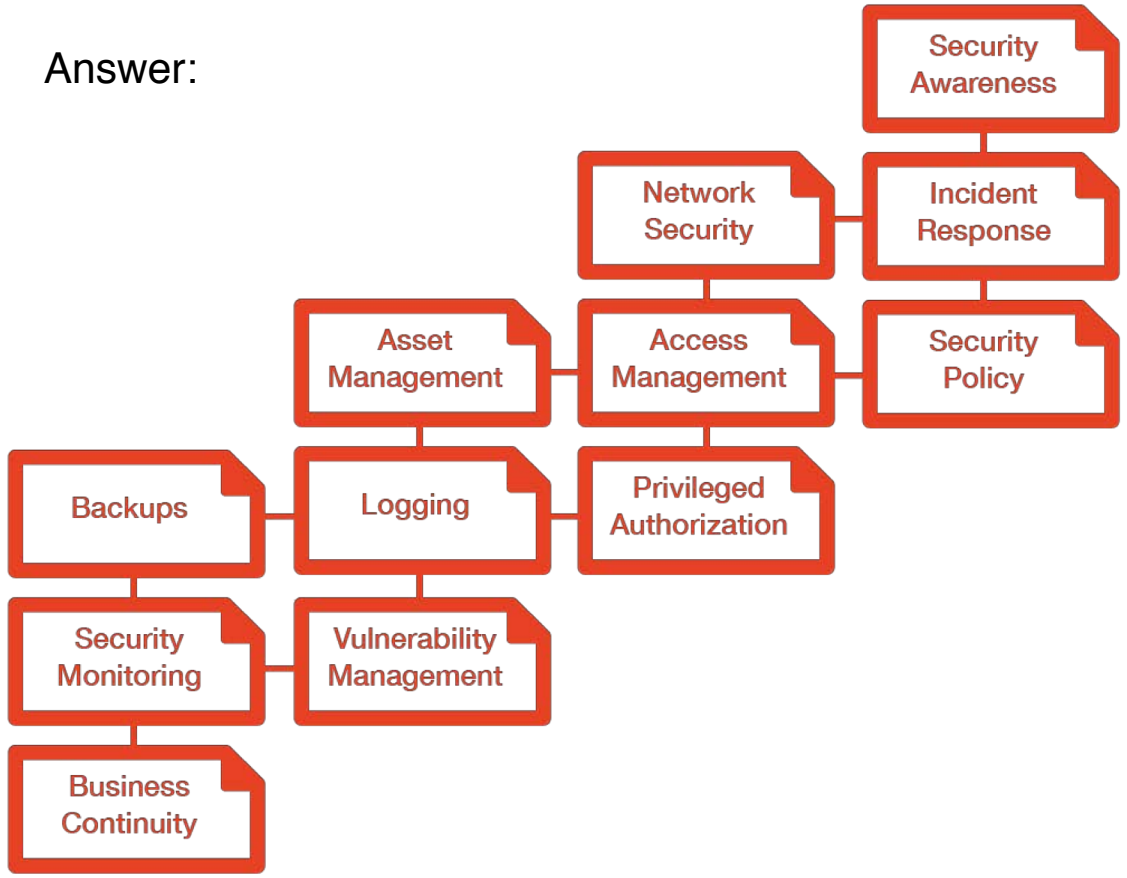
Has it been TRANSPOSED ?

Is a draft being discussed?

Is a DRAFT available for COMMENTS?

What are DETAILS?

Answer:



Applied Risk

2. Is this only an IT Security topic

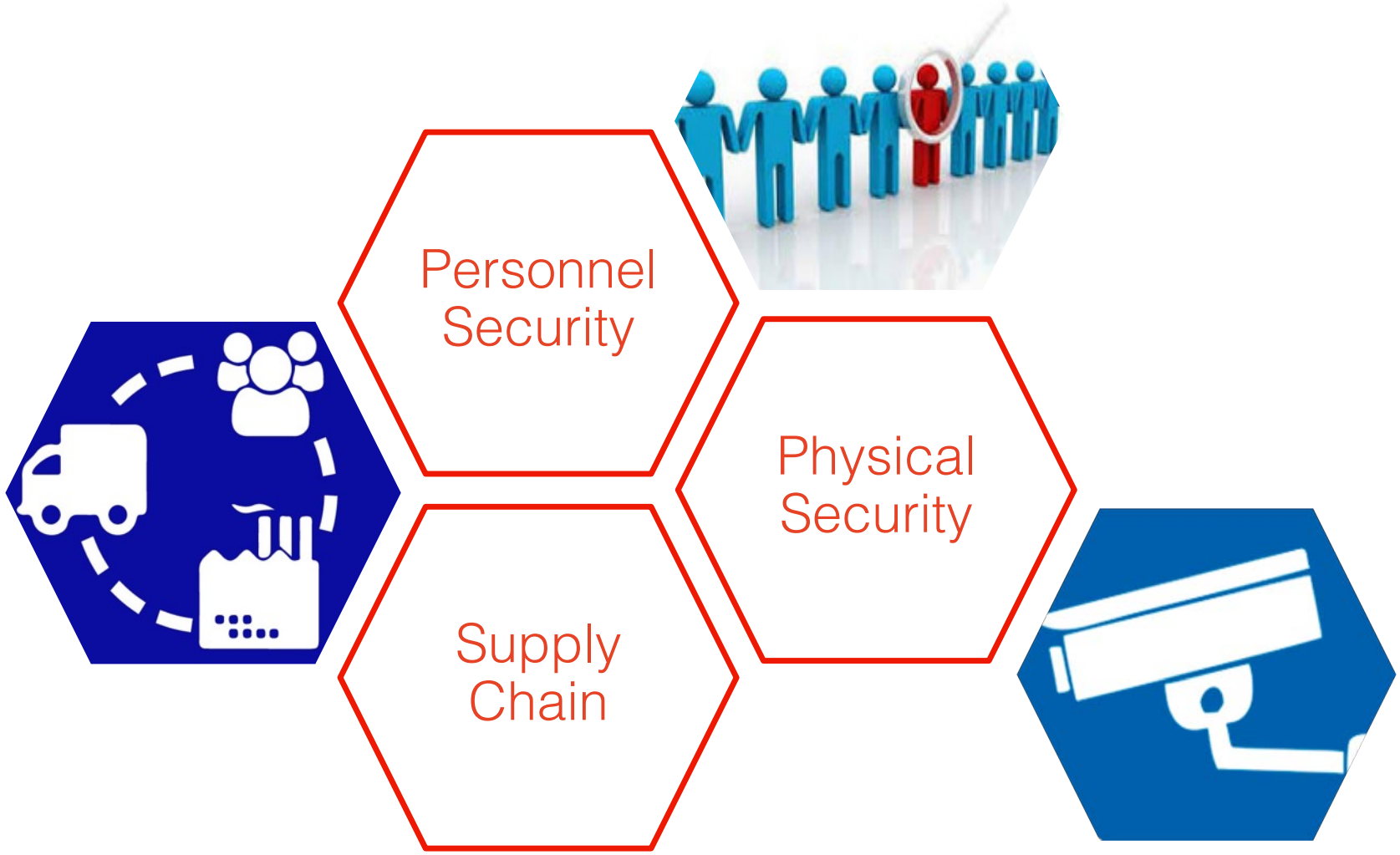
- Misconception 1:

It is not only about

Technical requirements

- Misconception 2:

It is not the same As GDPR



3. What is the journey to NIS compliance?

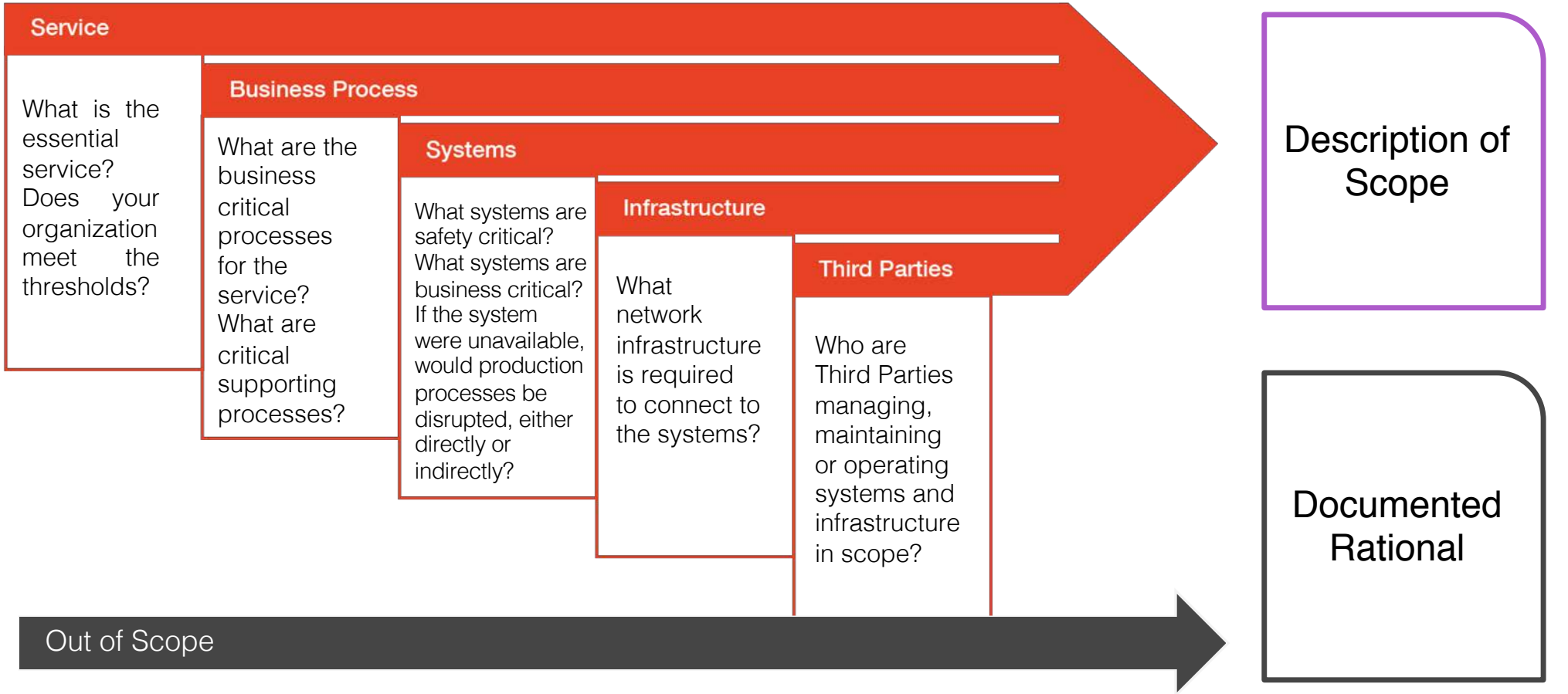
Challenge: With all those requirements it is not clear where to start

Identify	Collect documentation of existing control framework	Template to document applicable controls	Library of control evidence
Map	Match control framework to requirements to determine completeness	Mapping between international standards & NIS requirements	Documentation how NIS requirements are met
Assess	Test effectiveness of controls	Assessment Methodology	Insights into effectiveness of security measures
Remediate	Create action plan to address any gaps identified	/	Remediation plan

Applied Risk

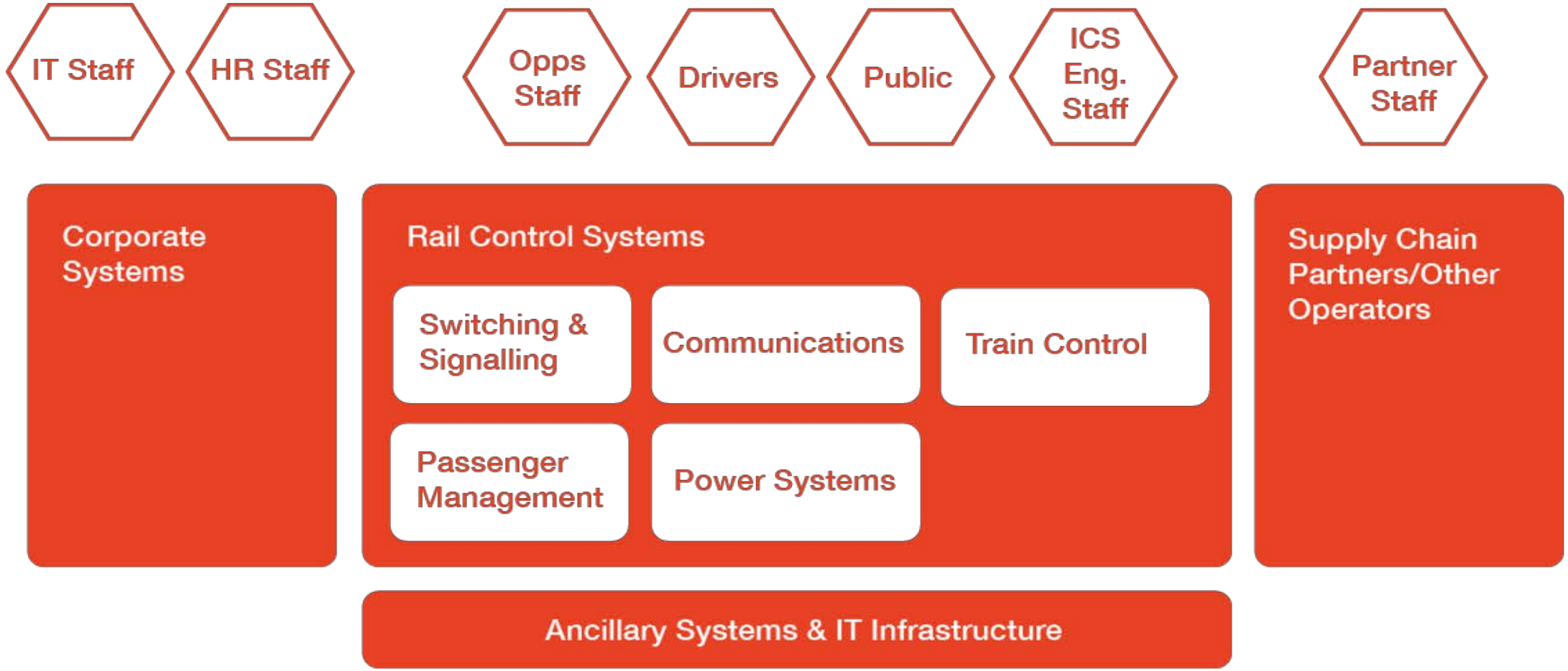
4. What is affected by NIS?

Pitfall: The scope was not directly identified / Not relevant parts of the organization get assessed while vital systems and Third Parties are overlooked



Applied Risk

What is affected by NIS? - Example



5. What does it take to demonstrate Compliance

Misconception: Compliance is treated as a checkmark exercise of a set of activities that occurs once.

A culture of compliance

- Funding & Resourcing
- Monitoring
- Performance targets
- Consequence management
- Training

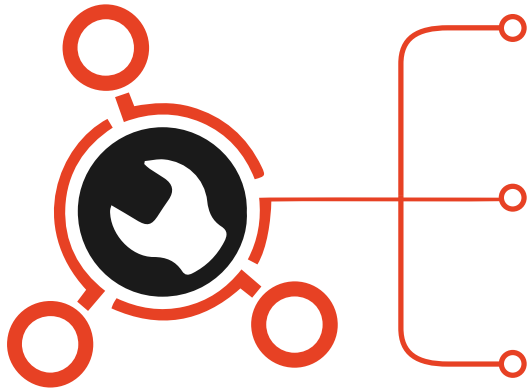
Policy evidence requirements

- Consistent
- Enforced to users
- Current,
- Version control

Controls

- ensure compliance with policies
- Review
- Performance assessment
- Compliance assessment
- Technical & Organizational Controls

Compliance activities are threefold:



1. Identifying NIS relevant systems (once)
2. Reporting incidents (incidentally)
3. Demonstrating compliance (when auditec

Applied Risk

6. What if requirements are not met?

Misconception: all requirements of the referenced standard have to be assessed as all fully met

- That itself does not lead to incompliance to the NIS Directive as long as gaps are known and being addressed.
- Regulators are seeking evidence of constant evaluation and improvement of security measures.

7. How should one prepare for an external audit or inspection

Keep Evidence checklist

- What: Overview of to be gathered or prepared evidences needed to demonstrate compliance
- Why: During an audit evidence will have to be provided on short notice. Too often findings are caused by documents not being provided in time
- How: Keep an overview or register of file names and links per requirements

Company-wide evidences

- relevant for the test of design during audits
- Includes all documents (policies, procedures etc.) that are relevant to demonstrate how your companies Control Framework in design meets NIS requirement

Evidences specific from NIS Compliance

- Documentation of the agreed scope
- Mapping of the controls to NIS requirements
- Design and Implementation of the Incident Notification procedure

Local evidences ready

- Documentation to demonstrate operating effectiveness of controls including:
- Asset management
- Disaster Recovery
- User reviews and access controls
- Physical security of the asset

Evidences as result of improvement

- Improvement plan plus regular communication on the status of activities (i.e. in form of meeting minutes/ ppt)
- Evidence for completed quick-wins (easy to fix improvements)

Existing Compliance and Assurance evidence

- Internal peer reviews (LoD 2)
- Internal Audit reports (LoD 3)
- External assessments by third party
- Assurance reports for suppliers

8. What has to be done for Incident Notification

Misconception: Incident notification is just a form that has to be added to existing incident management process

NIS transposition will define

- what has to be reported,
- how it has to be reported,
- how quick it has to be reported to them.

It is up to critical infrastructures to embed those requirements into their existing incident management processes

- Timely identify when an incident becomes applicable to be reported
- Understand when an incident has to reported and what information should be included in reporting
- Appoint key contact to submit notification in case of an incident
- Adjust existing incident management processes
- Execute exercises to practice

An example journey to NIS compliance

1. Understand local transposition of NIS legislation and what are requirements
2. Create awareness in organization and identify relevant stakeholders
3. Assign responsibility of NIS requirements
4. Identify Scope of processes and systems that are NIS relevant
5. Identify current controls of the organization and map them to Security requirements of NIS
6. Address any gaps in the control design and procedures and prepare assessment methodology
7. Identify relevant Third Parties
8. Investigate if contracts with Third Parties are fit for purpose or start process to update them
9. Create NIS Incident Notification Procedures
10. Create scenarios for potential incident and train staff
11 Run simulation of incident notification and evaluate lessons learned
12. Execute internal assessment (self-assessment or via third party)
13. Collect relevant documentation or evidence to support assessment
14. Create improvement plan for any gaps identified
15. Embed improvements into organization

External Audit or Inspection

Applied Risk

Summary

1. Get involved

- OES should inform themselves on the status of the NIS Directive in the country they operate in. This also applies if the legislation is still in draft. The earlier an OES gets insights into what the NIS Directive will mean for them, the more time there is to prepare.

2. Understand the scope

- OES should, based on the critical processes within the sites that deliver the essential services, clearly define systems, applications and infrastructures that fall under the scope of the Directive.

3. Document & check existing controls

- OES should assemble an overview of all security measures currently in place. The existing security measures can be compared to standards such as IEC 62443 or ISO 27001 to verify completeness. Requirements should be mapped against the requirements defined by the Competent Authority of the country.

4. Establish Incident notification

- EU member states will define what has to be reported and how it has to be reported. It is up to OES to embed those requirements into their existing processes.

Questions?

Applied Risk

Anne Klebsch
aklebsch@applied-risk.com
www.applied-risk.com