



University
of Glasgow

RITICS

The NIS Directive and Supply Chain Resilience

Tania Wallis
Research Associate

Prof Chris Johnson
Head of Computing Science

tania.wallis@glasgow.ac.uk

christopher.johnson@glasgow.ac.uk

The NIS Directive and Supply Chain Resilience



Stakeholder assessment - to capture the needs of Operators, Suppliers, CA, BEIS, DCMS.

Industry challenges of supply chain mapping under NISD across different sectors: Transport, Energy, Water, Telecoms.

Develop operational metrics derived from NIS-D principles and NCSC supply chain guidance and apply to different sector supply chains.

Meta-metric assessment of measures applied to different sectors.



NCSC Supply Chain Principles

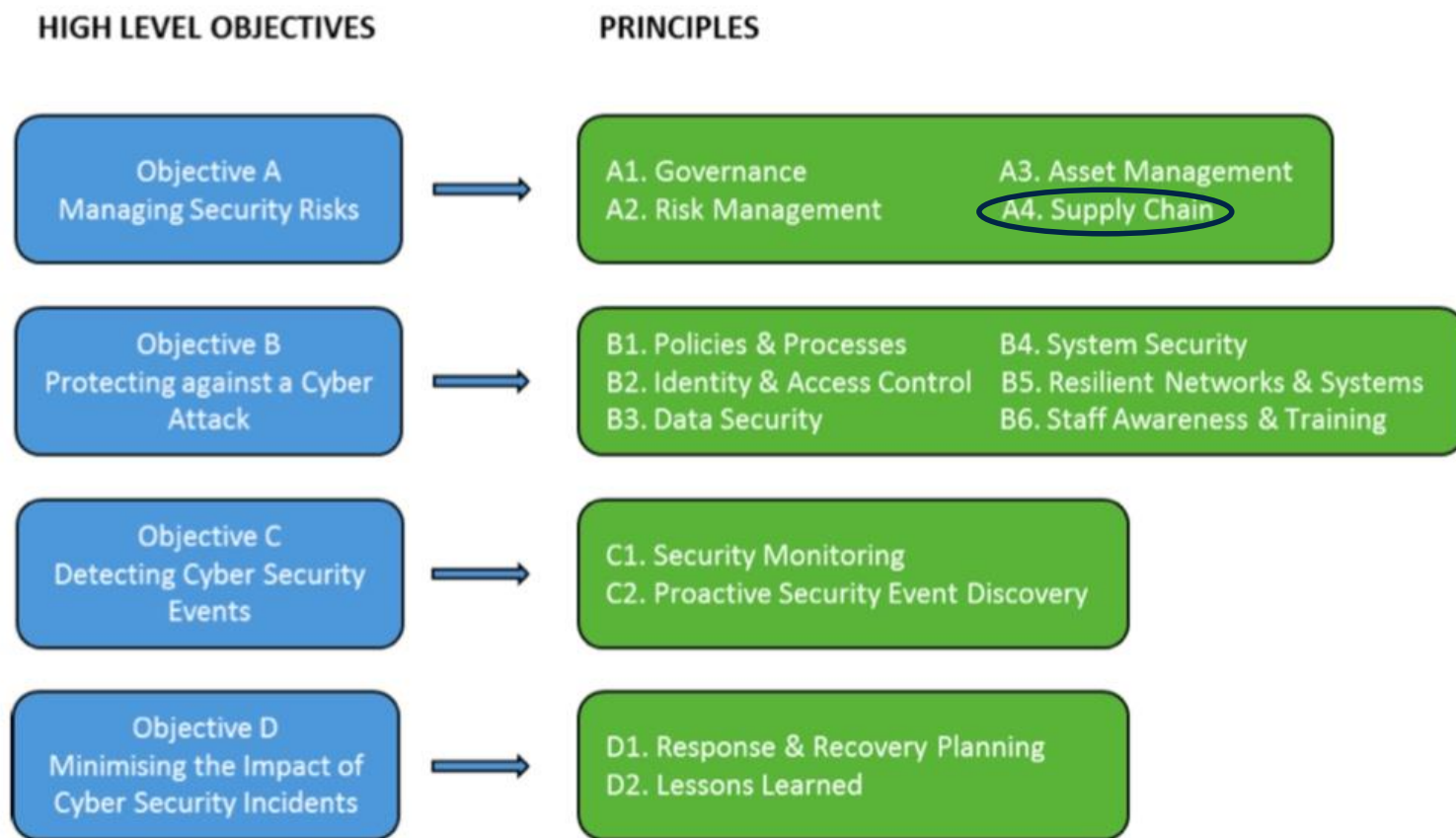
- I. Understand the Risks
- II. Establish Control
- III. Check your arrangements
- IV. Continuous Improvement

Clear picture of supply chain risks.

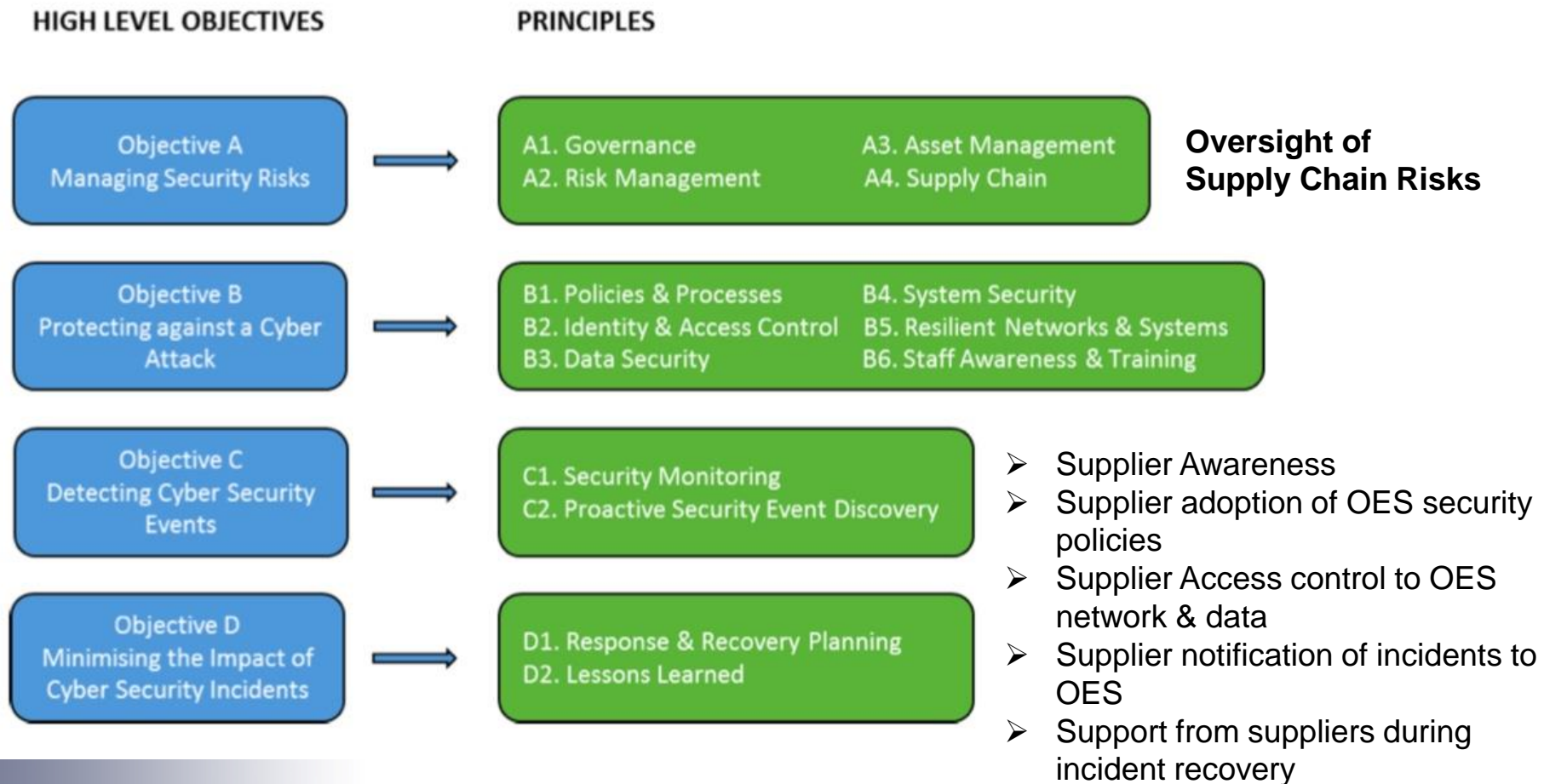
Minimum security requirements
Contracting processes

Performance of supply chain security

Achieve improvement plans
Effectiveness of security measures



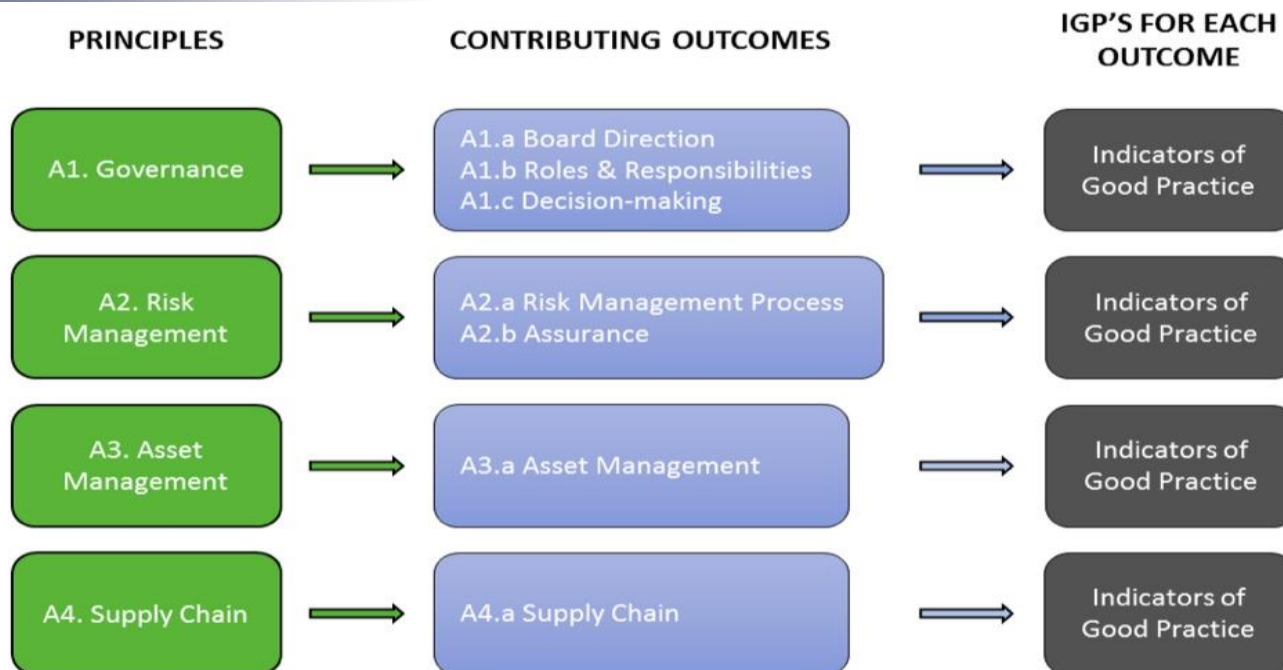
NIS-D Objectives



Supply Chain expectations under NIS-D

CAF Profile - expectations for each sector to achieve.

A4a Supply Chain expects “**Partially Achieved**”.



A4a Supply Chain

Contributing outcomes predominantly either **Partially Achieved** or **Not Achieved** among OES.

- Proactively manage procurement, 3rd parties and the wider supply chain.
 - Know exactly who you are interacting with, and why.
 - Actively ensure 3rd parties comply with your cybersecurity policies - ensure contract management enforce compliance.
 - Ensure 3rd parties are aware of the need to notify you of breaches and cyber security issues within agreed SLAs.
 - Ensure contract staff receive adequate cybersecurity training and awareness.
- [Water]
-
- Deep understanding of supply chain wider risks including sub-contractors.
 - Security requirements of suppliers are mutually understood, specified in contracts, with shared-responsibility model clearly documented.
 - Effective management of network connections and data sharing with 3rd parties.
 - Mutual support with suppliers during incident response.
 - Management of risk includes risk to essential services of supply chain being impacted by “capable and well-resourced attackers”.

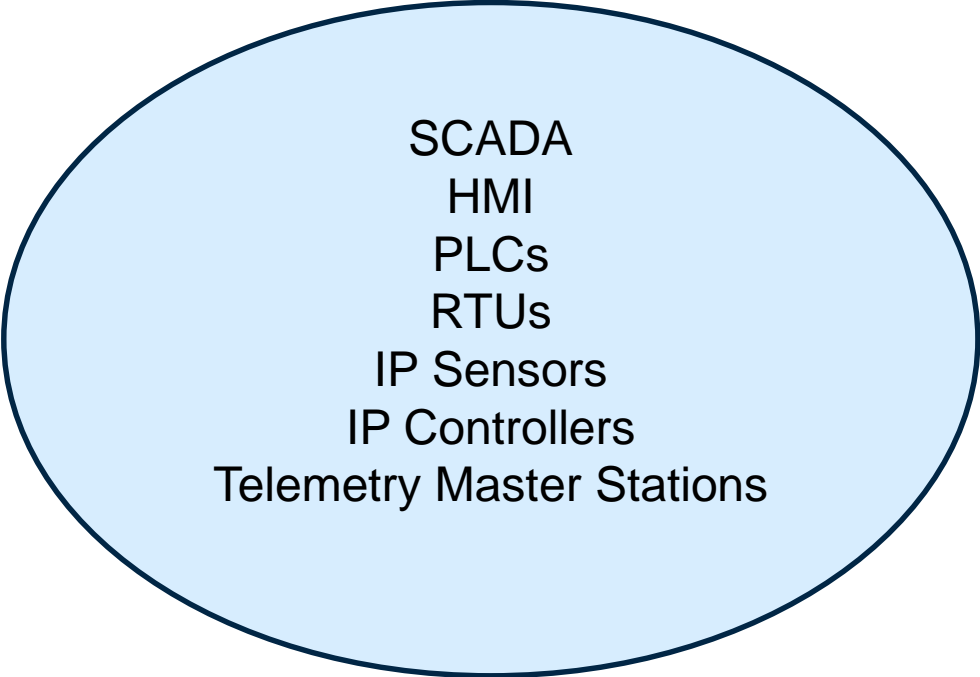
[Aviation]

NIS-D Scope - defining critical assets

Any system that includes a direct impact on delivering essential services.

Supply chain can impact beyond scoping boundary required by NIS-D i.e. consequences of intrusion to corporate or supplier systems requires a broader awareness.

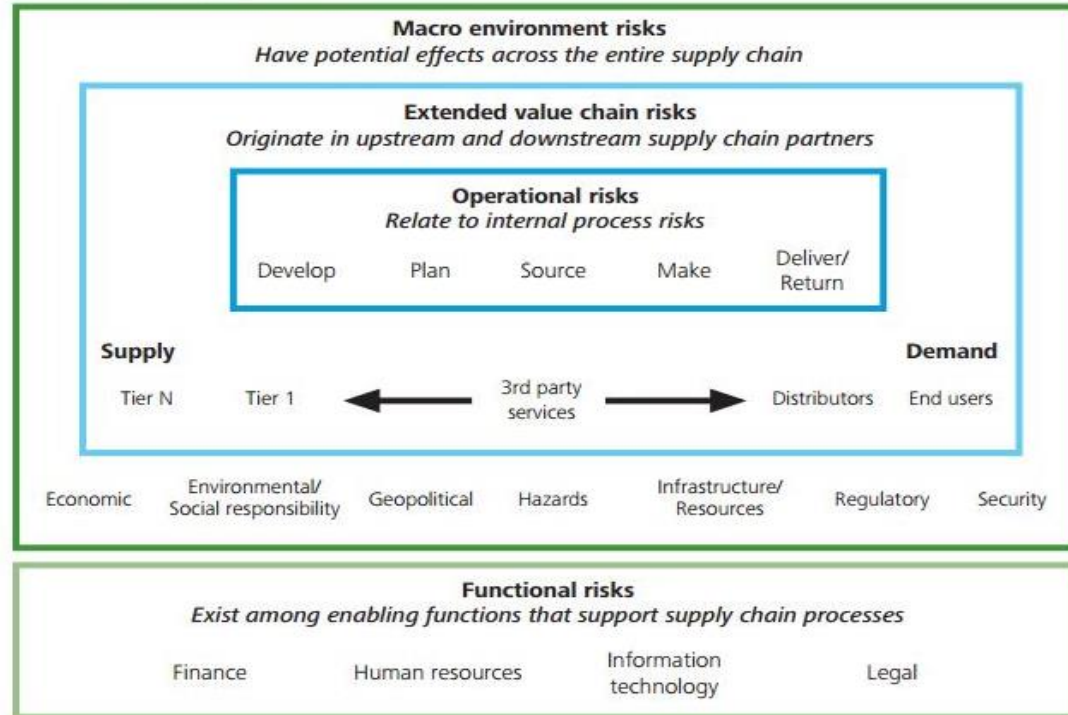
The process for identifying critical assets needs to include supply chain dependencies.



SCADA
HMI
PLCs
RTUs
IP Sensors
IP Controllers
Telemetry Master Stations

Systems in scope are included in the company's cyber assessment framework (CAF).

Visibility of Supply Chain Risks



[Ref Deloitte]

Clear oversight of supply chain risk:

- Which suppliers to audit
- Where to focus improvements.

NIS-D as a tool for change

Obligations under NIS-D and the CAF:

“have given us a strong focus to improve security”.

“is helping us to create a security culture”.

- Levers & Contractual Arrangements.
- Sharing security responsibility with suppliers.
- Questionnaires, self-assessments.
- Interviews, audits.
- Formal agreements, contracts, SLAs, OLAs.
- Sharing information, notifications from suppliers.



Addressing Supply Chain Risks

Focus on procurement stage - assessing risk to OES:



- Checklist of questions - supplier risk rating.
- Scoring matrix during procurement but least cost is primary goal.
- Risks arising during procurement logged in risk register.

Ongoing contract management - through-life assurance:



- 3rd party connection agreements for access to OES network
- Supplier notification process
- Audit and inspection but insufficient resources to audit them all

Improvements in progress

Different methods depending on the level of importance of supplier to OES:

- Provide information on cyber security expectations and requirements.
- Build trust with face-to-face meeting to assess their cyber security capability.
- Work together with critical suppliers on security improvements.

Managing suppliers with access to OT:

- Authorisation for specific tasks.
- Cybersecurity briefings/training appropriate to the task.
- Compliance of engineer laptops.
- Reporting of security incidents.



Supply chain “a huge problem for us”

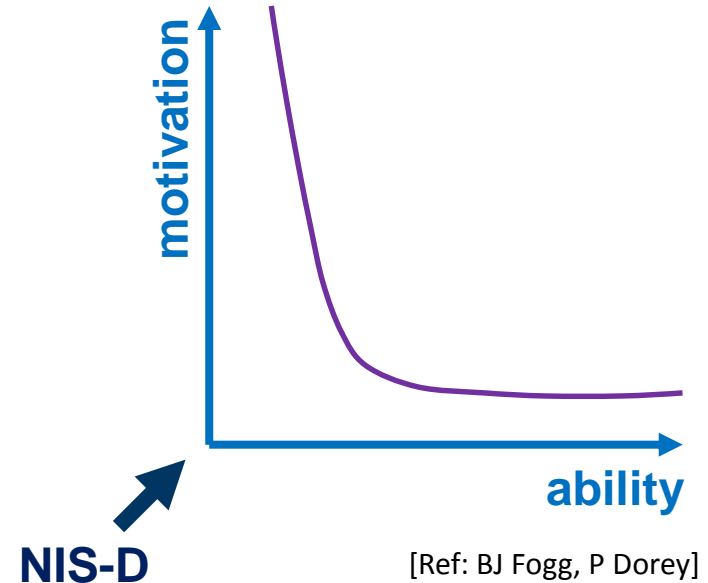
- Established contracts do not include security requirements.
- Limited ability to negotiate security requirements.
- Supply chain incidents may not be notified to the OES.
- Visibility of sub-contractors very limited.
- Broad reach of supply chain, beyond Europe.
- Suppliers using NIS-D as a selling point but little evidence of their security.
- Lack of choice in selecting suppliers – low cybersecurity maturity among available suppliers.
- Deployment of new sites – outsourced without cyber security requirements and expectations.
- Uncertainties over shared responsibilities in operations, complex dependencies.

Elements required to change supplier behaviour:

TRIGGER – expectations from NIS-D, security requirements of OES

MOTIVATION – CA Emphasis, contractual obligations from OES. Improvement relative to peers. Minimum standards to supply to OES.

ABILITY – cybersecurity maturity of supplier, OES carrying risk because too costly to resolve.



Highly motivated suppliers using the CAF.

OES lack negotiating power with some suppliers:

- dependency on single supplier to deliver essential product
- large supplier – single security offering, specific requirements not possible.



**Clear
Accountability**

Single point of accountability for an organisation's supply chain:

- To improve supply chain visibility and collaboration.
- To achieve an integrated view of supply chain risks.
- Assess and manage risks with a multi-faceted approach.

Significant investment effort to secure supply chain
– could combined approaches leverage improvements more effectively?

- OES & DSP dependencies.
- OES supplying to each other.
- Dependencies on Comms.
- Common requirements with key suppliers could give more emphasis on the security needs of OES?
- Establish standards for supplying to an OES?

Establishing a record of good practice:

- Water UK NIS-D Working Group
- Energy E3CC



Metrics...What should we measure?

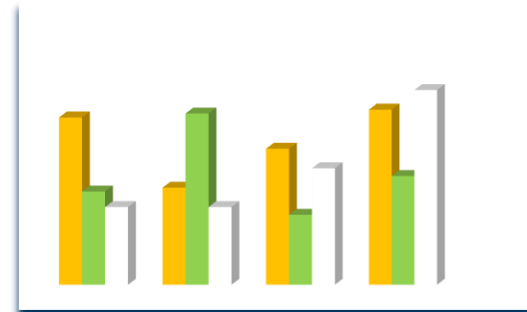


Next Steps:

- Further interviews with OES
- Aim to develop metrics to assess uptake of NIS-D Recommendations & NCSC supply chain principles
- Apply metrics in different sectors.

Quantitative oversight of supply chain risk:

- To inform supply chain improvements
- Measure effectiveness of process to achieve NIS-D outcomes.





University
of Glasgow

RITICS

Tania Wallis

Research Associate

tania.wallis@glasgow.ac.uk

Prof Chris Johnson

Head of Computing Science

christopher.johnson@glasgow.ac.uk