Jisc

16/09/16

Setting the scope for your ISMS

James Davis

Background

Background

- Jisc is not just an NREN
- Approximately 500 employees
- Eight offices across the UK
- Company is split into units called directorates
  - Jisc Technologies runs the Janet network
  - Other directorates provide HR, IT etc.
  - Jisc Technologies has ISO 9001 certification

Background

- As part of a larger security programme we were given three years of funding to establish a certified ISO 27001 ISMS within Jisc Technologies
- Project documentation was clear that this was to be a pilot ISMS to develop capability, before expanding it to the entire directorate
- Project had clear sponsorship by our executive team and by what would become the ISMS's top management

- Budget, time and resources provide limits on success
- We decided from the outset to only put forward a limited number of services for the certification scope

- This was clearly supported by the project documentation and senior management
- Clear emphasis on this only being the start of our ISO 27001 journey, and a commitment to further development

Developing the context

Context

"4.1 The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system"

Context

- Possible inputs
  - Project paperwork
  - Corporate strategy and objectives
  - Directorate Operating Plan
  - Personal knowledge
  - ~~SWOT analysis~~

Context

- The context doesn't need to be documented. A good idea to do so.

- Improvements we made
  - Listing external and internal issues under separate headings
  - Greatly expanding on internal issues
  - Adding explicit mention of our operating plan, the the pilot project, interested parties, legal, regulatory and contractual requirements
  - Making the context an internally published document

Interested parties

Initial Attempt

- We reviewed the contracts, laws and regulations that we thought were within scope and from this identified interested parties and their requirements
- Also included our funders
- This was easy and well understood – we're thorough with our legal and financial paperwork ☺

- But not good enough for the external auditor ☹
- In hindsight we focused too much on the NOTE under section 4.2 "The requirements of interested parties may include legal and regulatory requirements and contractual obligations."

- A limited scope presents interesting challenges in terms of interested parties
- Are teams outside of scope interested parties?
- It helps to better define what you think an interested party actually is

- 27001:2013 says:
  - *"The organization shall determine: a) interested parties that are relevant to the information security management system"*

- What does it mean to be relevant to the ISMS?

- ISO 9000:2015 says:
  - *"The relevant interested parties are those that provide significant risk to organizational sustainability if their needs and expectations are not met"*

- We reestablished our understanding of what it means to be an interested party within our context documentation:

"In determining which interested parties are relevant to the ISMS we have looked at those that provide significant risk to organizational sustainability if their needs and expectations are not met."

- Resulted in adding new parties such as:
  - Security guard company
  - Cleaning company
  - Fire and Alarm company
  - Building access company
  - Campus management company
  - Jisc Board
  - Employee Representation Forum

- None of these have contracts directly within the in-scope services, but do impact on the ISMS

It doesn't stop here

- Now you have defined your interested parties, you need to show you are doing something about them

- Perhaps through:
  - Communications and awareness activities
  - Selection of controls
  - Risk management activities

- Explicitly documenting the link between these activities and your identification of interested parties is helpful

- We excluded companies like
  - Secure shredding company
  - Hardware disposal company
  - Microsoft (Office 365)

- In these cases we felt that the risks to the ISMS weren't inherent in the services being provided

Developing the scope

On the Certificate

The provision of Information Security related to Trust and Identity services defined as:

1) Janet Certificate Service
2) Eduroam (UK)
3) UK Access Management Federation
4) Assent

» Defining the scope is not this simple

Defining the scope

- You need to be able to justify the certification scope to your auditor
- The scope needs to be meaningful to your customers
- You need to demonstrate that you've taken the context, external and internal issues, the needs of interested parties, and dependencies on others into account

- You don't need to document any of this, but it helps
- Certification scope may differ from the ISMS scope

What we did at Jisc

- Set the ISMS scope to be the entire directorate – minimizes updates to key documents, helps manage boundaries.
- Certification scope is documented separately
  - Largely a document intended for the external auditor

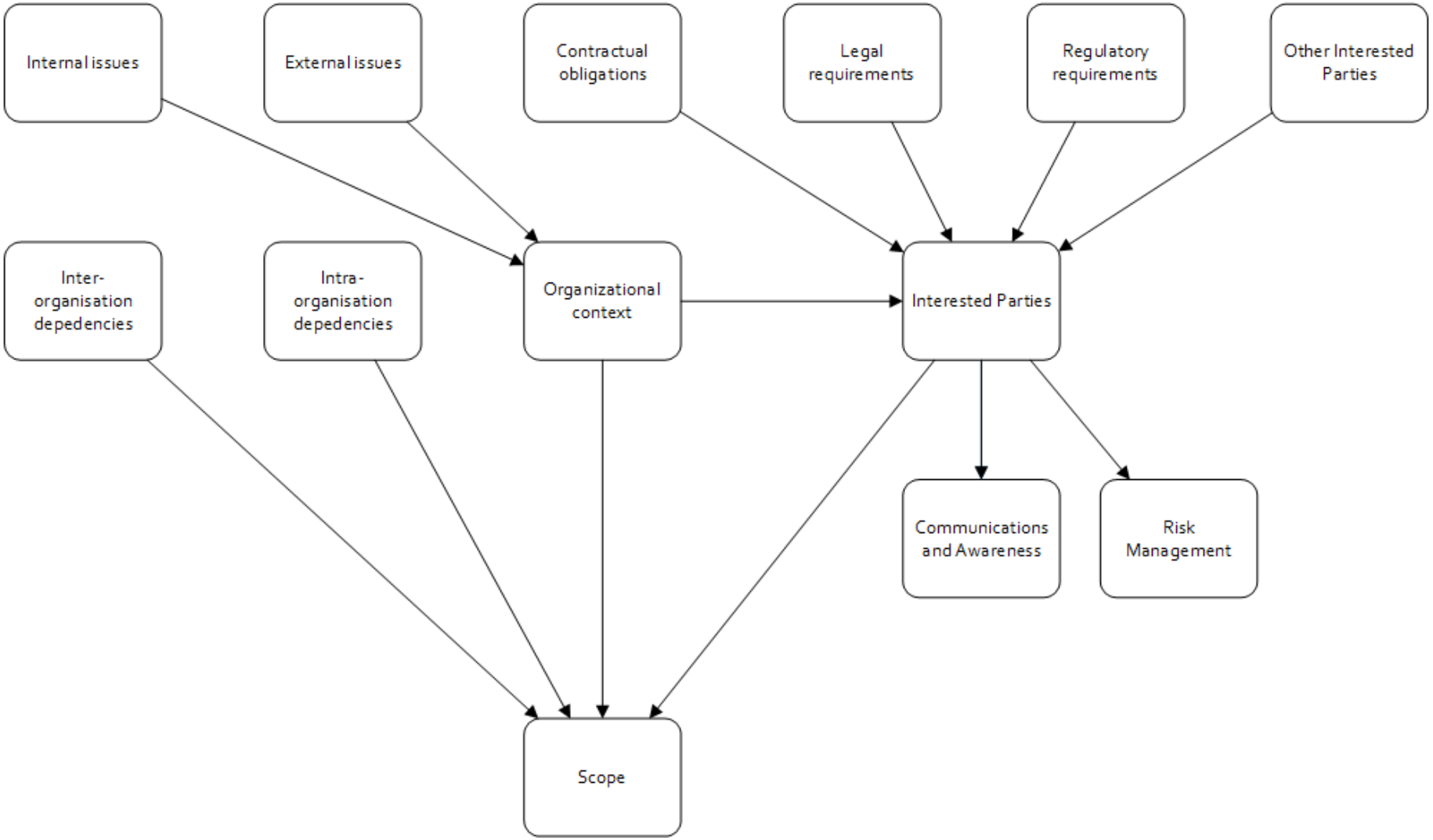
Documenting the scope

Within the scoping document

- Explanation of the structure of Jisc
- Logical description of the services in scope
- Geographic locations of the scope
- Links to the physical boundaries of those locations
- High level network diagrams
- Organogram showing staff in scope, and their place in Jisc's structure
- Key organisations considered to be out of scope

Summary

The complete picture



Find out more…

James Davis
Information Security Manager

james.davis@jisc.ac.uk