Resources for Chapter 4 – Scoping

RESOURCES

- **Scope definition for a data safe haven – UCL, case study**

Scope definition for a data safe haven – UCL, case study

The purpose of the UCL Data Safe Haven is to enable researchers to access and use sensitive identifiable data in a secure manner. It was created by the Information Services Division on behalf of the School of Life and Medical Sciences (SLMS), but a few research studies outside SLMS who need to handle sensitive identifiable data also use it.

In 2013, a decision was made to achieve certification to ISO/IEC 27001 for this environment. Work began in early 2014, and we passed our first certification audit in May 2014.

Multiple scopes

Certification of the whole of UCL was not appropriate or feasible, so we had to think very carefully about how to define our scope: what were we controlling, what would be audited and what would be certified?

In the end, we decided that we actually had four different scopes:

- The scope of the Data Safe Haven, which we called the "organisation", to match the term used in 27001. This was a challenging term to use, as it had to be clear that we did not mean the whole of UCL when we used the word "organisation" in project meetings
- The scope of the ISMS
- The scope of audit
- The scope for certification

We agreed that the staff of the organisation should be defined as follows:

- Staff who manage and administer the environment (physically and logically)
- Staff who use the environment for research
- Top management who make executive decisions

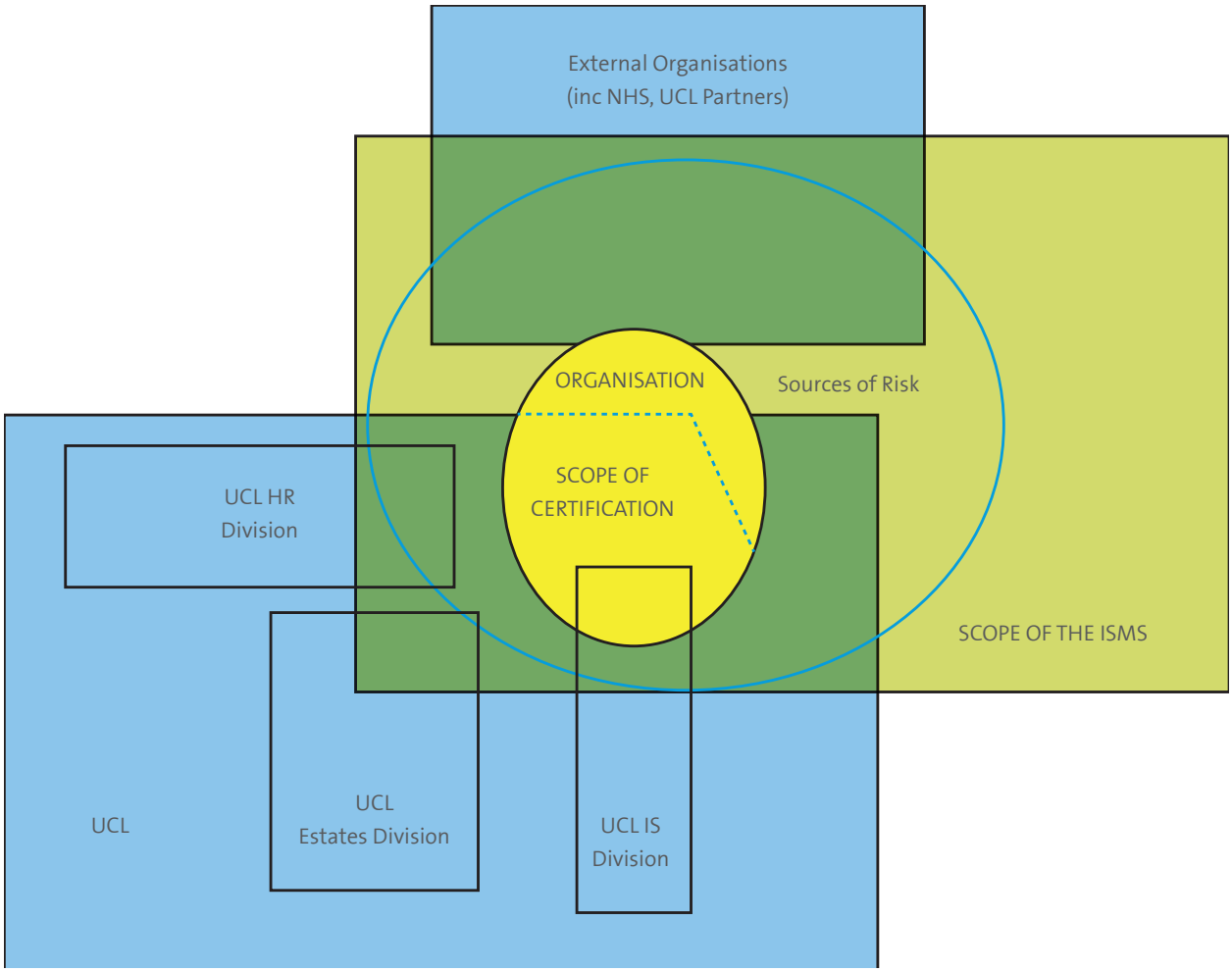

Figure 1: Scope diagram for UCL's Data Safe Haven

As can be seen in Figure 1, the scope for certification is a subset of the scope of the organisation, which is itself a subset of the scope of the ISMS. The scope of the audit was effectively the same as the scope of the ISMS, so anything within the ISMS could have been audited, but only those items within the scope for certification could have been certified.

Understanding our scope

In order to get to this point, we had to work through a number of difficult issues.

The first problem which we had to solve was how internal third parties, such as HR and Estates, would fit into the picture. HR defines contracts and pre-employment checks, as well as carrying out some checks at the request of research units, while Estates controls physical security (e.g. card access to server rooms, and physical access to researcher offices).

It was decided that UCL parties which were outside our organisation should be treated:

- as sources of risk;
- as providers of controls.

We considered the options and agreed that the controls they carried out were within the ISMS, but external to the organisation. This was arrived at through externally facilitated workshops with members of the core project team, focusing on specific areas of risk.

What about external third parties? We could have managed service providers through contracts - but thankfully we had no external service providers. We did, however, have external entities which needed to pass data into the environment. We treated them as external potential sources of risk, rather than as part of our scope for certification.

Finally, how should we handle researchers? Most researchers were included within the scope of certification. However, one research study from another faculty was agreed to be part of the organisation, but was being treated as a "customer", and was hence excluded from the scope of certification. This is shown in the illustration as the diagonal part of the dotted line inside the "golden egg".

The scope statement

Our official scope statement for our certificate was short and sweet: "The provision of the "Data Safe Haven" environment for the processing and storage of personal identifiable information in accordance with the Statement of Applicability version 1 dated 6th May 2014." In contrast, our detailed scope document runs to seven pages, with five diagrams. This is due to be extended by adding in explicit references to external legislative, statutory and contractual requirements, at the recommendation of our external auditors.

Learning points

- There are likely to be a number of different ideas about what scope means. At the beginning of your compliance work, put more effort than you think is necessary into clarifying the terms used, and reinforce the definitions for your chosen scopes regularly, to keep everyone on track.
- Identify your external parties and decide early on whether they are within your scope for compliance or outside it, and how you will handle the issue at audit time
- Specify all of your external drivers explicitly, so that you can justify any controls which they require, and so that their impact on your decisions about scope can be understood.