ISO 27005 Risk Management

I.G.Batten@bham.ac.uk

27005 supports 27001

- On Thursday we will start reading 27001, because we will understand all of it from other things we have done
- 27005 is a later, supporting standard but worth reading first (it’s a lot clearer, for a start off)
- Although it has its flaws, following 27005 is beneficial

Purpose

- Not a method, “guidelines” … “support” … “assist” (p. 1)
- Provides a vocabulary and talking points for designing your own risk management system
- Draws heavily on ISO 31000
- Linked to older version of 27001 (“Plan Do Check Act”) rather than 2013 revision (which permits 6 Sigma and others)

Intention

- Provides a means to check that a risk management strategy is broadly sensible
    - Enterprises can ensure their in-house method is compliant
    - Auditors can check that a scheme is sensible
    - You can’t sensibly get a 27005 certificate in isolation

Section 3: Vocabulary

- Should be clear definitions of often-used terms.
- What do you think?
    - Consider 3.7 “likelihood”
    - Consider 3.18 “stakeholder”
- Definitions might require tightening in your system.

Sections 4–6

- 4: Structure
- 5: Background
- 6: Overview
  - Table 1 is a very good summary of an ISMS process

Section 7: Context Establishment

- 7.2 is roughly equivalent to writing IS1 impact levels etc from scratch!
- 7.3 is determining the scope / focus of interest
- 7.4 is again re-writing parts of IS1

So why not use IS1?

- Aimed at government and organisations that need to protect government-classified data
- Emphasis is on protecting labelled material of high classification in clear environments against well-resourced, well-motivated, capable threat actors
- As we found in the exercise, “real” enterprises are all at IL2
- If we pretend that our most sensitive data is IL5, we get absurd risk outcomes

Section 8: Risk Assessment

- Note: “A risk is a **combination** of the consequences…and the likelihood” (my emphasis)
- 8.2.2 asset register, 8.2.3 threat actors (sort of), 8.2.4 and 8.2.5 existing position, 8.2.6 will produce impact levels for CIA.
- 8.3 is an IS1 activity, but done against the backdrop of your own criteria
- The “combination” bit is up to you, rather than coming from IS1’s matrices.

Section 9: Risk Treatment

- Slightly different taxonomy:
  - Modification, Retention, Avoidance, Sharing
- Still leading to residual risk
- Note p.21 where paragraph 2 is concerned with cost while paragraph 3 is much more wide-ranging.

9.2 Risk Modification

- Combines risk **reduction** and risk **mitigation**

9.3 Risk Retention

- aka Risk **Acceptance**
- Note that it superficially implies simply accepting risk, when in fact what it means is reducing the risk under 9.2 and then accepting what is left
- Note also how short the section is

9.4 Risk Avoidance

- Combines risk **transfer** amongst other things
- Would include both “do credit card processing with PayPal” and “stop accepting credit cards”.
- Again, note how short it is.

9.5 Risk Sharing

- Also covers amongst other things risk transfer
- 9.2 > (9.3 + 9.4 + 9.5)
- Very clear the assumption is the main controls you use are about risk modification (reduction and mitigation)

10 Risk Acceptance

- Again, residual risk statement needs to be formally signed off (later we will read 27001!)

11 Communication and Consultation

- Motherhood and apple pie
- Covers training, governance and discussion
- But very important

12 Monitoring and Review

- 12.1: is the environment changing?
- 12.2: is the ISMS working within the environment?

Annex A: Scoping

- Picks up things you might not have thought of
- Note focus on regulation and legislation

Annex B: Assets, Impacts

- Very similar to IS1
- But covers much wider range of situations

Annex C: Example Threats

- Starting point, not finishing point

Annex D: Compromise Methods

- Again, a starting point

Annex E: Approaches

- Very similar to IS1 (I think I heard it came from the same people)

Annex F: Constraints

- Side effects and costs

Tentative