File 20090313.1100: Notes from meeting with Dr Martin this morning at 10:00 a.m.:

Who's got a handle on risk averseness *vs* risk avoidance?

Why are things the way they are (in C&A) and do they still need to be? Are they converging on civilian best practices, or are they leading, or otherwise?

Why do we do C&A of high-value systems? Because in the 1970s, the quality of engineering was low. Things like CM and rigorous test plans did not exist much yet.

Question: are other governments doing the same thing about Protection Profiles (PP)—official or unofficial?

- Write a paper about it?

Anecdotally, CESG seems to be more risk-averse than NSA.

- True?
- Why?

US and UK security classifications: UK

- TS
- S
- Classified
- Restricted
- U

US and UK security classifications: US

- Top Secret
- Secret
- Confidential
- Unclassified

Draw a chart of C&A standards.

Go visit Dr Ian Levy and invite him here [to comlab].

For next week's meeting:

- Reply to infosec show email.
- Report that I have contacted Dr Ian Levy by email.
- Chart of C&A standards.
- Point to a place in the chart.

Next meeting is 19th March 2009 at 10:00 a.m.

References