**Security – technical considerations**

High Level:

- ensure that there is a documented set of technical ontrols mandated

- ensure that there is audit process against those controls

Many government audit processes assume a microsoft environment. You might need to do additional work to ensure linux machines and applications are adequately covered.

Example controls are in resources directory. They can be taken and customised.

TopTen for rapid assessment

1. Operating system is a LTS (long term service edition)
2. There is an automatic process for applying OS security patches
3. Host based firewall configured allowing minimal access
4. Access is via ssh according to agreed policy - keys, no root access etc
5. DHIS2 version is not more than 3 versions behind latest release. Process exists to apply patch releases regularly.
6. Automated backup system is in place and regularly tested, including offsite.
7. Postgresql database accesss controls allow minimal access
8. Web-proxy server is properly (ssllabs test A+) configured with SSL
9. Database data is on separate data partition (allowing encryption at rest, performance settings)
10. Monitoring and alerting system is in place (wide range of options depending on environment. eg. boombox might be fine with email + logwatch + munin )

Every system must have a document data owner and responsible administrator!!