epiLab-SS
An ISO 27001-certified cloud-hosted environment for research

Tito Castillo, Rich Hutchinson, Anthony Thomas, Luke Romanowski, Stelios Alexandrakis, Christiana McMahon, Jenny Towsey

MRC Centre of Epidemiology for Child Health, UCL Institute of Child Health
epiLab-SS: a suite of trusted and managed information security services to research staff at the UCL Institute of Child Health (ICH). These services are hosted at AIMES Grid Services, a secure ISO-27001 data centre and accessed via thin-client devices using two-factor authentication at secure locations within the ICH.

Key Technologies/products used:

• Oracle VDI (incorporating Sun Ray Server Software)
• Sun Ray Thin Clients + smartcards
• Windows 2008 Server R2 / Windows 7 Enterprise
MRC Centre of Epidemiology for Child Health

• Largest research unit in the ICH
• ~75 members of permanent staff – computing facility requirements equal to 100+ desktops
• Wide range of projects involving analysis of identifiable and de-identified data:
   Disease Surveillance Projects
• Project lead for largest ever UK-wide birth cohort study – Life Study
   ~100,000 babies and their mothers tracked from pregnancy to birth and beyond – pilot phase beginning in 2013
  http://www.lifestudy.ac.uk
A common problem: The “server” in the corner

- Shared PC disconnected from any network running Windows XP – the “server”
- Used for storage of data from cohort study participants
- Data backed up to removable hard drive
- Lack of centrally-supported policy/procedure-led client/server/domain architecture
- Lack of formalised information governance and data management planning arrangements
- Users generally left to their own devices to manage their data
Generic requirements

- Secure data enclave
- Secure endpoints
- General-purpose desktop environment
- Scalable architecture
- Standard technology
- Minimal bespoke software
epiLab

- Locally Managed Secure Computing Facility for the Centre
- Mixed environment – Solaris, Windows, Linux
- Provides secure authentication, storage and access to research data and software
- Virtual Desktops and Servers
- Private network with our own ASA 5510 failover pair – (external DNS managed by ISD/UCL). Routes public IP addresses on the main ICH network with NAT to/from internal
- Running since the tail end of 2009
epiLab Feature Breakdown

- Internal AD domain (Server 2008 R2) provides SSO to all epiLab services – also includes internal DHCP, DNS, local CA etc.
- 2FA for users/services using smartcard “tokens” and AD auth.
- VDI – desktops cloned from “golden” templates - highly flexible and customisable – pool-based automatic provisioning/recycling – individual assignments
- ~20Tb of SMB/CIFS RAID-6 (SATA) storage with on-disk snapshots for study/user-generated data
- ~9.5Tb of iSCSI RAID-50 (SAS) for VM storage
- Nightly tape backups – with weekly off-site storage rotation
- Remote replication of select user data + a MySQL slave hosted in an ISO 27001-certified datacentre – Linux VMs using full-disk encrypted LVM and/or eCryptfs
- Virtual computation servers for low-impact statistical/genetic analysis software
- SCP file transfer into/out of epiLab – using SSH/pam_mount/CIFS
- Web, Application and database servers – Kerberized against our internal AD domain – incl. Wiki, REDCap (secure online survey/data collection tool), NADA (Study metadata catalogue), Redmine, LimeSurvey, web-based large file transfer with CAPTCHA and e-mail verification (Zend.To)
- Mandatory encryption of all data in transit to clients (VPN and/or HTTPS)
epiLab
The ISO 27001 Journey Starts

• September 2010 – award of ~£70k from TSB following a call for “Trusted Services”
• Fast-tracked projects funded over 12 months with a view to creating demonstrators for new trusted services
• SHARE (Shared-Services Health Applications and Resources Environment) – co-application with AIMES Grid Services CIC Ltd. ISO 27001 certified since 2007. (IaaS Tier 3 provider. Registered on the UK government’s G-Cloud catalogue.)
• Initial deployment of basic remote desktops to analyse data collected with REDCap (also hosted at AIMES)
SHARE

Laptop

Desktop

WWW

Ultra Thin Client

HTTPS for data entry (Encrypted)

VPN access for data analysis (Encrypted)

AIMES ISO 27001 Certified Datacentre

Database/File servers (w/ full disk AES-256 encryption)

Windows Virtual Desktops

Site-Site VPN (Encrypted)

AIMES Firewalls

Auth/Sun Ray Server/Token Management

UCL/ICH epiLab Firewalls

epiLab Datacentre

Janet CSIRT Conference, November 2012
epiLab-SS architecture
The ISO 27001 Standard

• Originally developed from British Standard BS 7799 (which the UCISA Toolkit is based upon)

• International standard for information security: ISO-27001:2005
  ❖ Describes requirements (i.e. what you ‘shall’ do)

• 11 security control clauses collectively containing a total of 39 main security categories plus an introductory mandatory clause introducing risk assessment and treatment. 139 controls in Annex A.

  e.g. A.11.2.2 (Privilege management) - The allocation and use of privileges shall be restricted and controlled.

• Independently audited
Swiss Cheese Model

Reason’s model of incident causation

“When an adverse event occurs, the important issue is not who blundered, but how and why the defences failed.” Reason, J (2000)
Accompanying code of practice

- ISO-27002:2005
  Provides guidance (i.e. what you ‘should’ do)

A.11.2.2 - Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process. The following steps should be considered:

a) the access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should be identified;

b) privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (11.1.1), i.e. the minimum requirement for their functional role only when needed;

c) an authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete;

d) the development and use of system routines should be promoted to avoid the need to grant privileges to users;

e) the development and use of programs which avoid the need to run with privileges should be promoted;

f) privileges should be assigned to a different user ID from those used for normal business use.
Information Security Management System (ISMS) Development

**PLAN**
- Management Support
- Define ISMS Scope
- Create Asset Register
- Risk Assessment
- Risk Treatment Plan
- Statement of Applicability

**DO**
- Create ISMS
- ISMS Implementation Programme
  - Compliance Review
  - Stage 1 Audit
  - Stage 2 Audit
  - ISO-27001 Certification

**CHECK**
- Corrective Action
  - Corrective Action Procedure
Scoping, Risk Assessment and Treatment

June-October 2011

Initial asset register generation and accompanying risk assessment

1. Identify the information assets that need to be protected along with their owners (Data, software, hardware, people, services, locations etc.)
   e.g. power supplies or other utilities at ICH (UCL Estates and Facilities are owners)

2. Identify any vulnerabilities that relate to these assets
   e.g. Lack of Business Continuity Procedure or Disaster Recovery Plan

3. Identify threats that need to be guarded against.
   e.g. loss through fire/flood etc.

4. Estimate the likelihood of threats exploiting vulnerabilities (otherwise known as risks)
Risk Assessment and Treatment Method

• Decide a threshold level of “acceptable risk” above which controls need to be applied to mitigate residual risk
  
ed.g. all of section A.14 (BCP) and A.9.1.4 (Protecting against external and environmental threats)

• Assign scores (1-10) for vuln. + likelihood + impact = Risk Exposure

• If the sum >8, then a treatment is required -> select controls from Annex A -> SoA.

• Re-score after treatment applied -> Managed Risk Exposure
Policy Document Generation

October 2011 – present

• Despite the small scope, we chose NOT to employ only 14 out of a possible 139 controls
  • Off-site equipment
  • Removable media
  • E-Commerce
  • Mobile computing

• MS Sharepoint used for document control, versioning and tasks

• Our ISMS currently has 69 policy documents. We use bookmarks in footers to allow us to programmatically track which documents refer to which controls
Project Registration and Data Management Planning

- Data Management Plans are a mandatory part of admission onto our service
- Helps demonstrate that the ISMS design has been adapted to meet the needs of our researchers
- Assures engagement of researchers with the ISMS
- Using the MRC’s template as a model
- 3-page document with simple to answer questions for the PI
  - Data description
  - Method of collection
  - Management/documentation/curation
  - Confidentiality
  - Sharing and external consumption

http://blogs.ucl.ac.uk/dmp-ss/
Internal Audit

May 2012
- Team members underwent 1-day internal auditor training with ISO 27001 consultant

June 2012
- Internal audit carried out over 1 week – all adopted controls split up between the team
- Checklist sheet used to score coverage of controls

<table>
<thead>
<tr>
<th>Reference</th>
<th>Audit area, objective and question</th>
<th>Findings</th>
<th>Status (%)</th>
<th>Control Owner</th>
<th>Assigned Auditor</th>
<th>Action following Audit</th>
<th>Action Performed</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4.4</td>
<td>Remote diagnostic and configuration point protection</td>
<td>Is this applicable? (RH mentions it is covered by the Access Control policy - CH-E001)</td>
<td>75</td>
<td>RH</td>
<td>SA</td>
<td>Make more explicit mention in Access Control and Operating Procedure of the “diagnostic points”</td>
<td>Updated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.4.5</td>
<td>Segregation in networks</td>
<td>Segregation of Duties document mentions it but not elaborate - is it required?</td>
<td>75</td>
<td>RH</td>
<td>SA</td>
<td>Check documents again.</td>
<td>Segregation of Duties has been updated to cover this. Furthermore, MTP/Network Usage Policy has also been updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
External Audit

Stage 1: July 2012

• 1 day – Found no major non-conformities – recommendation for Stage 2
• Corrective procedures to any minor non-conformities and observations worked through in preparation for:

Stage 2: September 2012

• 2 days – included interviews with UCL CERT, Records Office (DP issues), Estates/Facilities etc. Found no minor or major non-conformities
• ISO 27001 accreditation awarded on September 28th.
Key Points to Takeaway

• Management support
• Take your time with the risk assessment/treatment
• Start with a small scope – an existing ISMS can be refactored or repurposed if there are common components
• A closely-knit team cannot be underestimated