The SHARE & DMP-SS Projects: secure private cloud for health research

Tito Castillo

Senior Information Systems Consultant, MRC Centre of Epidemiology for Child Health

With funding from:

JISC

Technology Strategy Board
Driving Innovation

Cloud computing

- Deliver computing as a set of services
- Shared networked resources
- Utility-based computing
- Flexible, scalable environment
- Information governance concerns
- ‘Private-clouds’

Information Security

Protection of **information** and **information systems** from unauthorised:

access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

- Confidentiality
- Integrity
- Availability

Information Security Management Systems

- International standard for information security
  - ISO-27001:2005
    - Describes requirements (i.e. what you 'shall' do)
    - Independently audited
- Associated code of practice
  - ISO-27002:2005
    - Provides guidance (i.e. what you 'should' do)
- An ISMS is dynamic

Context

- MRC Centre of Epidemiology for Child Health
  - 80 staff & students
  - Wide range of data management issues
  - Dedicated computer service (epiLab) since 2009
- epiLab
  - Virtual desktop (VDI) environment
    - SunRay (with smartcards)
    - Secure Global Desktop (browser-based)
  - VMware desktop/server virtualisation
  - Logical separation from UCL network services (ASA)

MRC Centre of Epidemiology for Child Health

UCL

The SHARE Project

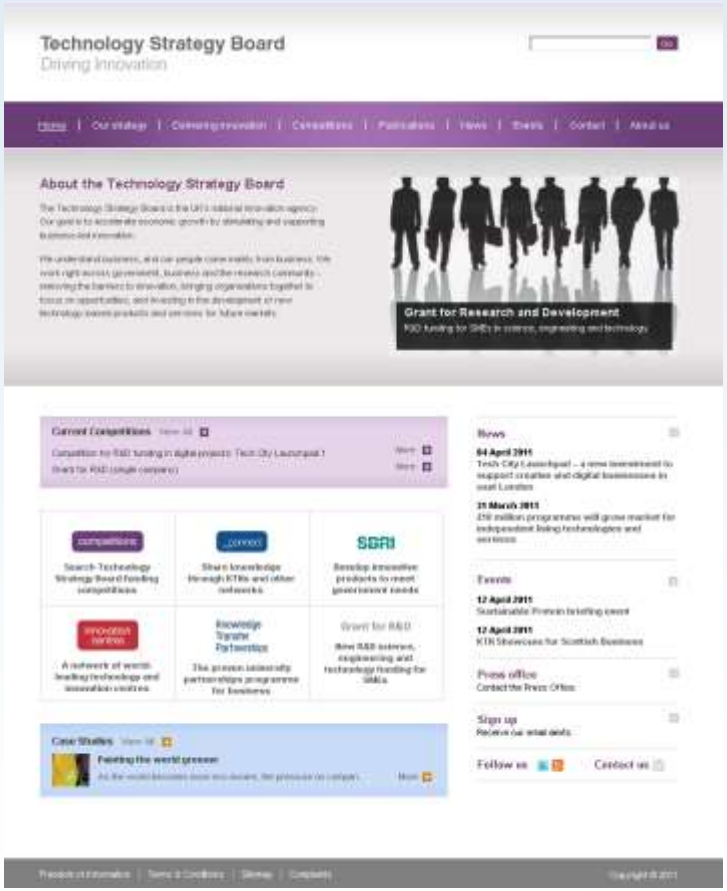
ja.net

JANET CSIRT Conference,
November 2011
London

AIMES GRID SERVICES

SHARE Project Background

- **Funded by the TSB**
  - UK national innovation agency
  - “Trusted Services” call
- **Uptake of digital services in areas**
  - trust a critical component of adoption
- **Fast-track projects funded over 12 months**
  - to create demonstrator
- **Adoption of cloud services in health care**
  - national priority area



SHARE Project Overview

- Funded in Sept 2010 for 12 months
- A collaboration between AIMES Grid Services and MRC Centre of Epidemiology for Child Health
- Total project value of 150k with 75k grant
- Methodology:
  - identify relevant use cases and to deploy these on SHARE

Project deliverables

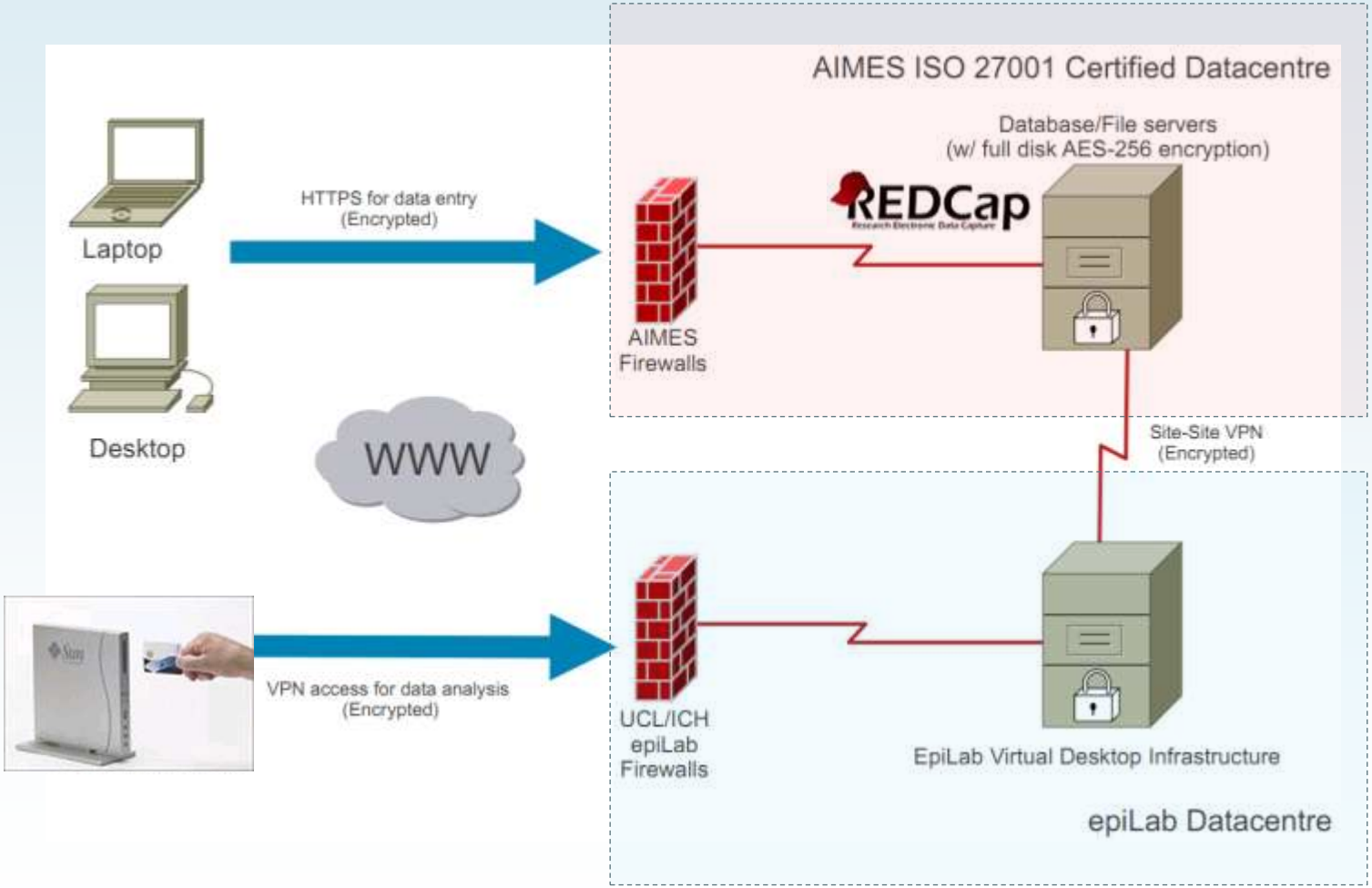
- **Infrastructure**
  - Secure VPN
  - Virtualised desktop/server/storage
  - N3 connection (NHS secure file transfer & email)
  - Full ISO-27001 system / service audit / Penetration testing
- **Contractual framework**
  - Template contractual document for provision of cloud services for healthcare
  - Literature review, historical / jurisdictional perspective (US-UK-EU)
- **Authentication**
  - 2 factor authentication (NHS compatible smartcards)
  - Incident management / Monitoring (Issue tracking & Delivery portals)
- **Case study**
  - UK surveillance study of congenital hypothyroidism in children

Outcomes: Infrastructure

AIMES

- Virtualisation using vCentre Server
  - Initial proof of concept
    - Windows 7 desktops (user authentication)
    - Encrypted file & database Storage
- **MRC Centre**
  - Virtual Desktop ‘broker’
    - Sun Ray server (smart card authentication)

Outcomes: Infrastructure Schematic



Outcomes: Contractual framework

- Main areas of concern often overlooked:
  - **Compliance with DPA and FOI Act**
    - ISO 27001 UK based hosting,
  - **Criminal investigation relating to data holdings**
    - Legal Investigative access and appropriate user permissions and monitoring (ISO 27001)
  - **Demarcation of networks:**
    - Clear contract that identifies obligation and right of both parties;
  - **Supplier falls below agreed service level**
    - Robust SLA that provides a high uptime and quality of service standard that incentivises supplier to rectify problems.
  - **Ownership of data and access rights**
    - Ownership and responsibility for content should remain with the user
    - Any processing or manipulation would be done by license.

Outcomes: Authentication

- Use of two factor authentication
  - Password plus smartcard
    - Something you know and something you have
  - Oracle Sun Ray thin clients
  - Compatible with NHS smartcards
  - Independent of desktop operating system

Outcomes: case study

- UK surveillance study of congenital hypothyroidism in children
  - June 2011 - June 2014
  - Paediatricians provide information about children newly diagnosed with hypothyroidism
  - Secure data collection (within SHARE environment) using online questionnaire

- Information governance
  - Research Ethics Committee (REC) approval
    - Prerequisite for research studies involving NHS patients
  - National Information Governance Board (NIGB) Section 251 approval
    - Approval to collect patient data without seeking individual consent (NHS Act 2006)
    - Minimal identifiers collected to allow matching of duplicate cases by paediatricians
    - System Level Security Policy: clarifying researcher responsibilities for data handling, archiving and eventual anonymisation within the secure environment

Outcomes: research data

- Data entry
  - Primary route: REDCap (Vanderbilt University)
    - Online questionnaires for individual records
  - Secondary route: NHS Secure File Transfer Service
    - Specialist centres requirement for bulk upload of multiple patient records
    - Requires N3 connection

- Data analysis
  - Virtual Desktop Infrastructure (VDI)
    - Oracle SunRay ultra-thin clients (Smartcards + password)
    - VPN connection to ISO-27001 environment
    - No data held locally

Issues

- Information governance of patient research data
  - Identifiable data
  - Individual patient consent
  - Researcher responsibilities for secure data processes
- N3 sponsorship arrangements
  - Delays in NHS organisations approval process
- Local ISO-27001 certification
  - Define small-scope ISMS
  - Include domain-specific risk treatment plan
- Software license considerations
  - Some software licensing models not suited to the cloud
- Service demarcation
  - Domain-specific vs Domain-neutral

MRC Centre of Epidemiology for Child Health

UCL

The DMP-SS Project

ja.net

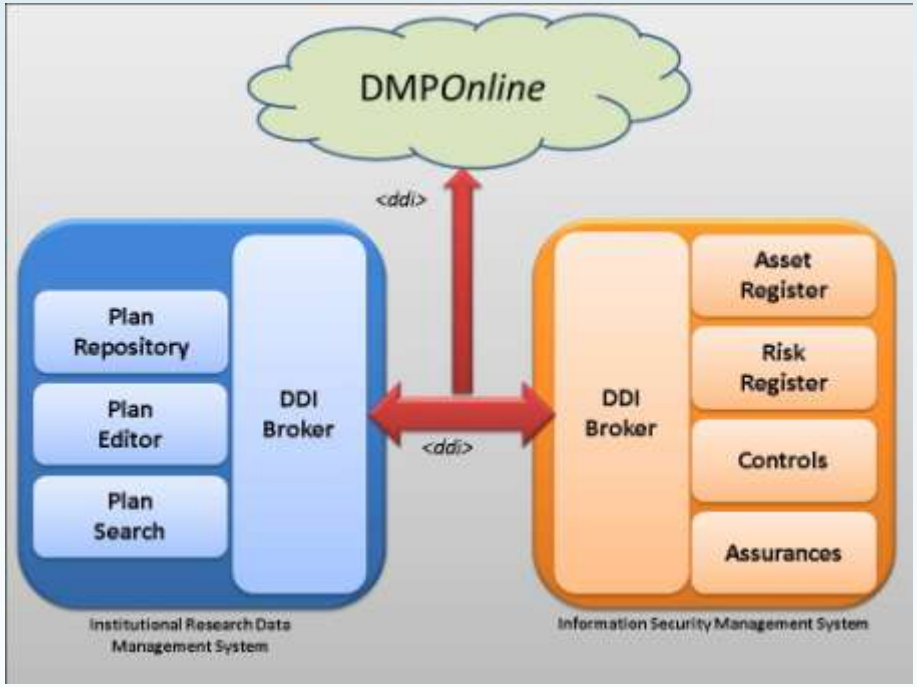
JANET CSIRT Conference,
November 2011
London

AIMES GRID SERVICES

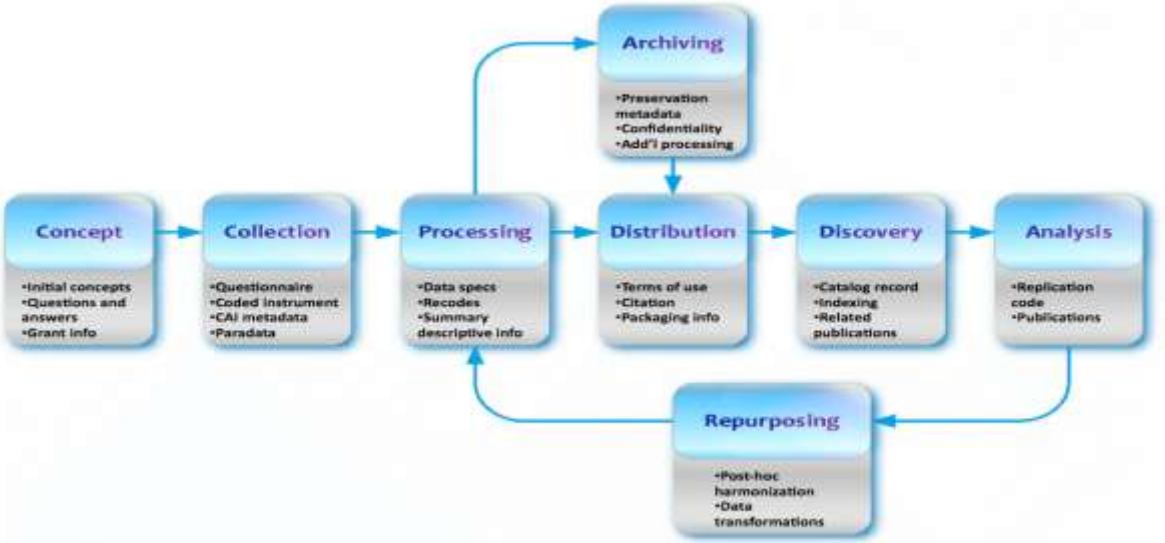
DMP-SS Project Background

Data Management Planning for Secure Services

- **Funded by the JISC**
  - Managing Research Data programme
  - Collaboration with Digital Curation Centre
- **Objective**
  - Build central metadata registry of data management plans (DMP)
  - Link Data Management Plans with an ISMS
- **Question**
  - Can Data Management Plans be integrated into an ISO-27001 certified ISMS?



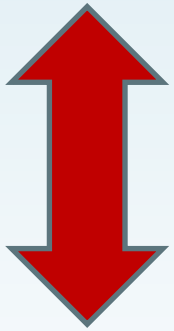
Why DMP-SS?



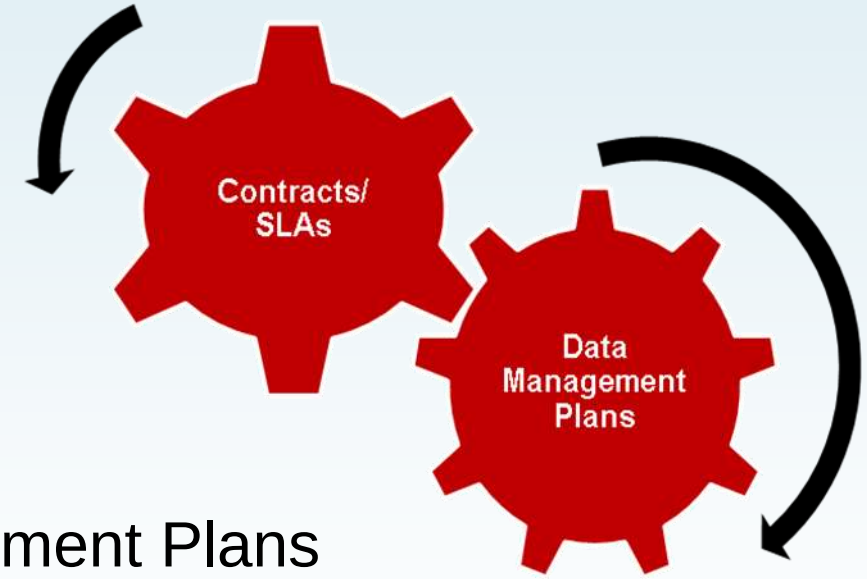
- Need to ‘embed ‘ information security best-practice in research data management
- Research data management planning is already required by major UK funding agencies
- Reduce administrative burden
- Use a language that researchers can understand

Man-in-the-middle service model

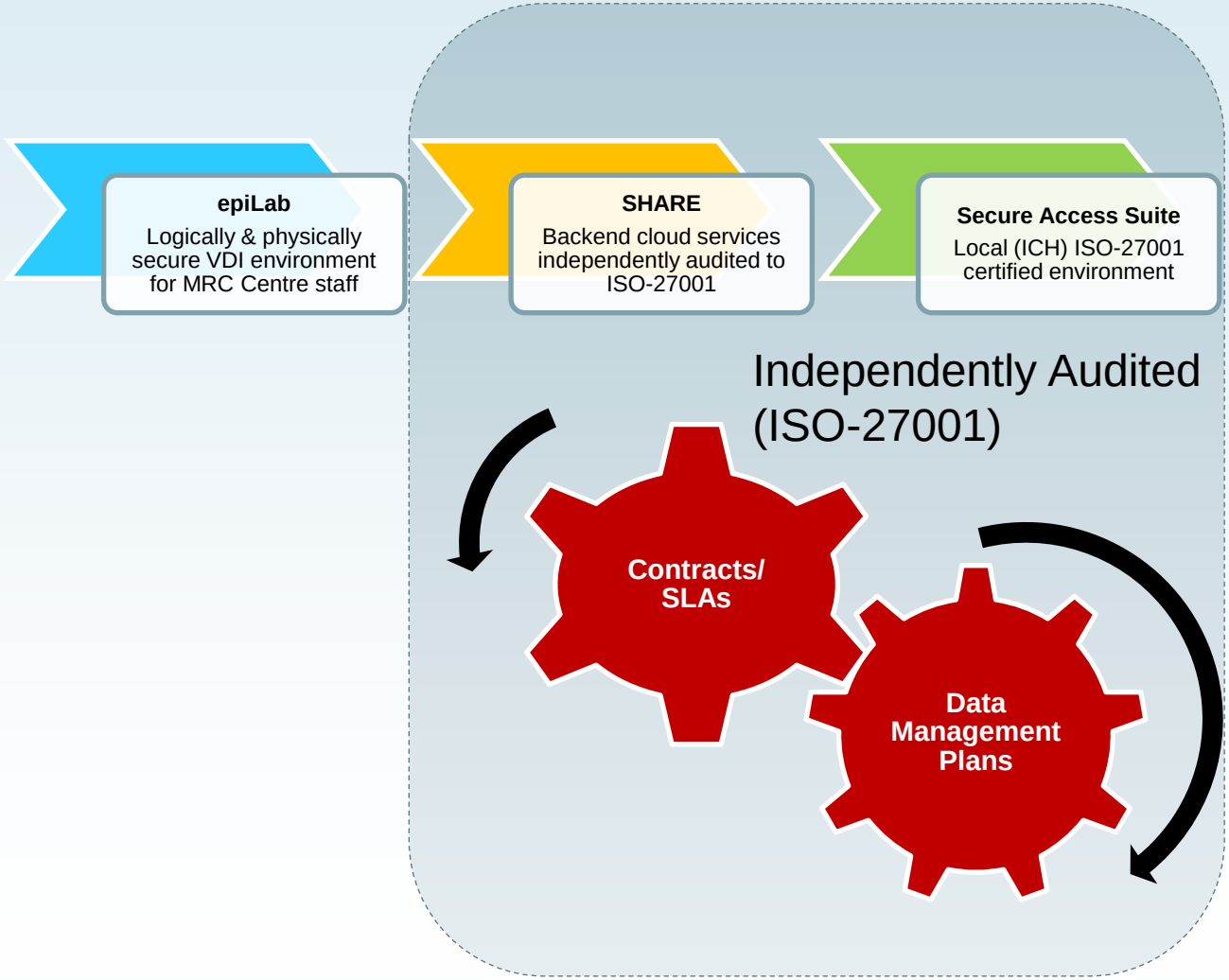
- Cloud provider
  - Contracts & SLAs



- Researcher
  - Approved Data Management Plans



Security Maturity Chronology



Conclusions

- User engagement is critically important
- Cloud doesn't mean
  - large-scale
  - international
- Work out lines of demarcation (takes time)
- Need agile approach to contracts/SLAs