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

NHS-HE Forum, November 2012

Information Security & Information Governance

- **Information security** is relates to the application of one or more controls
  - ➢ designed to reduce risk of information incidents
- **Information Governance** is the formal application of information security within an organisation
  - ➢ designed to support the business needs of the organisation.

NHS Information Governance Toolkit

- 10 years old - based on BS7799 which became ISO27001
- The “HORUS model”
  - **Holding** information securely and confidentially;
  - **Obtaining** information fairly and efficiently;
  - **Recording** information accurately and reliably;
  - **Using** informaiton effectively and ethically;
  - **Sharing** information lawfully and appropriately.

- **Common factor:** NHS Data and Services

University adoption of the NHS IG Toolkit

Currently mandated for some activities

BUT universities:

- Do not share the same business model as the NHS
- Deal with other agencies, not just NHS
- IG Toolkit is not an international standard

ISO27001 is an international standard

Information Security Management Systems

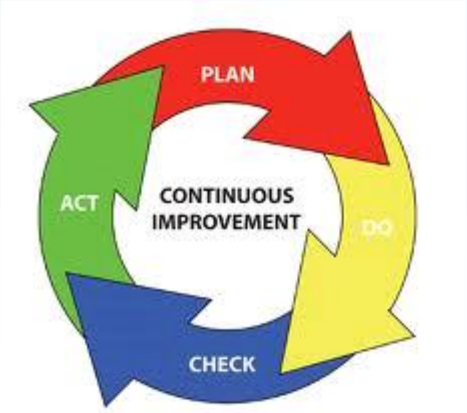
International standard for information security

- 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)

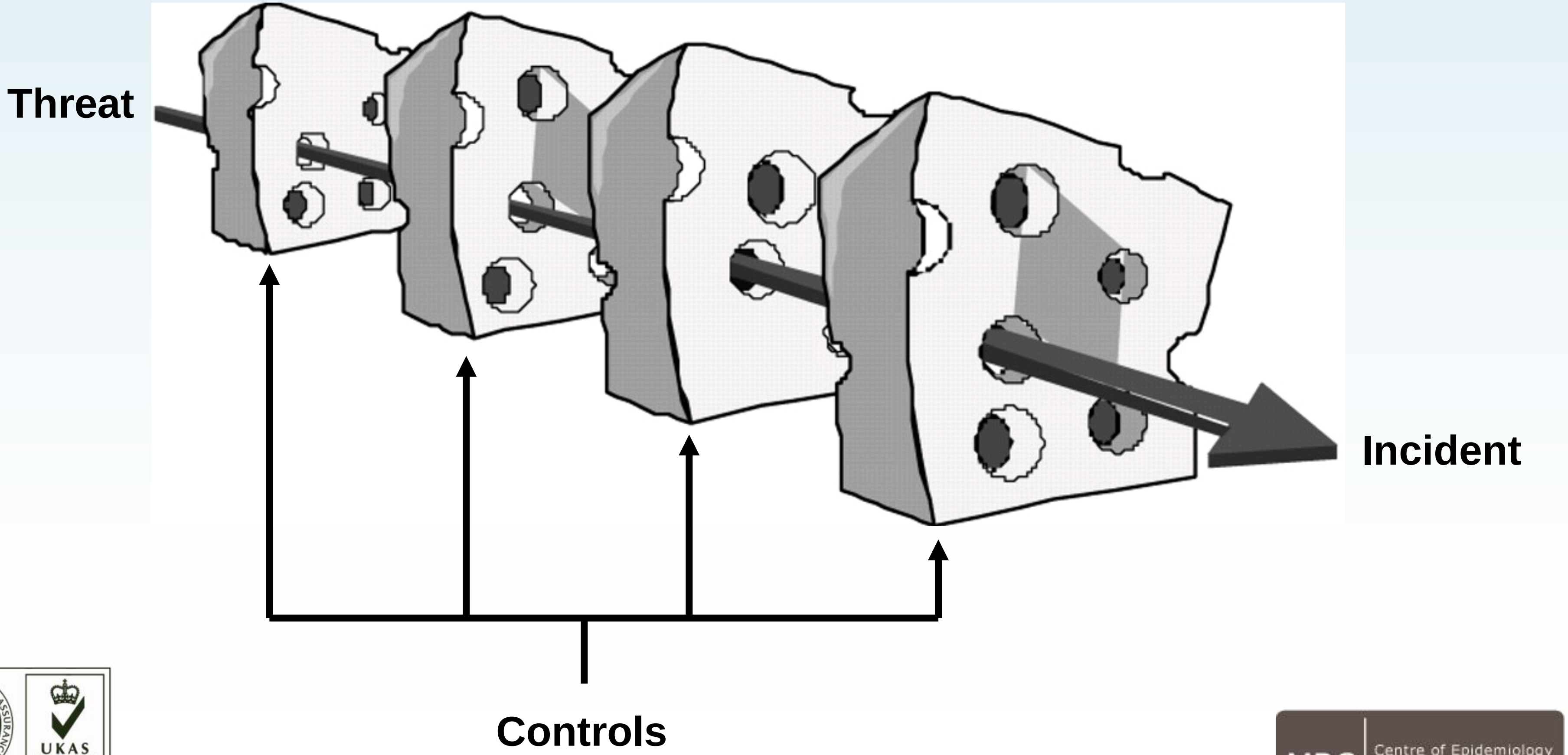
An ISMS is dynamic



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)



Threat

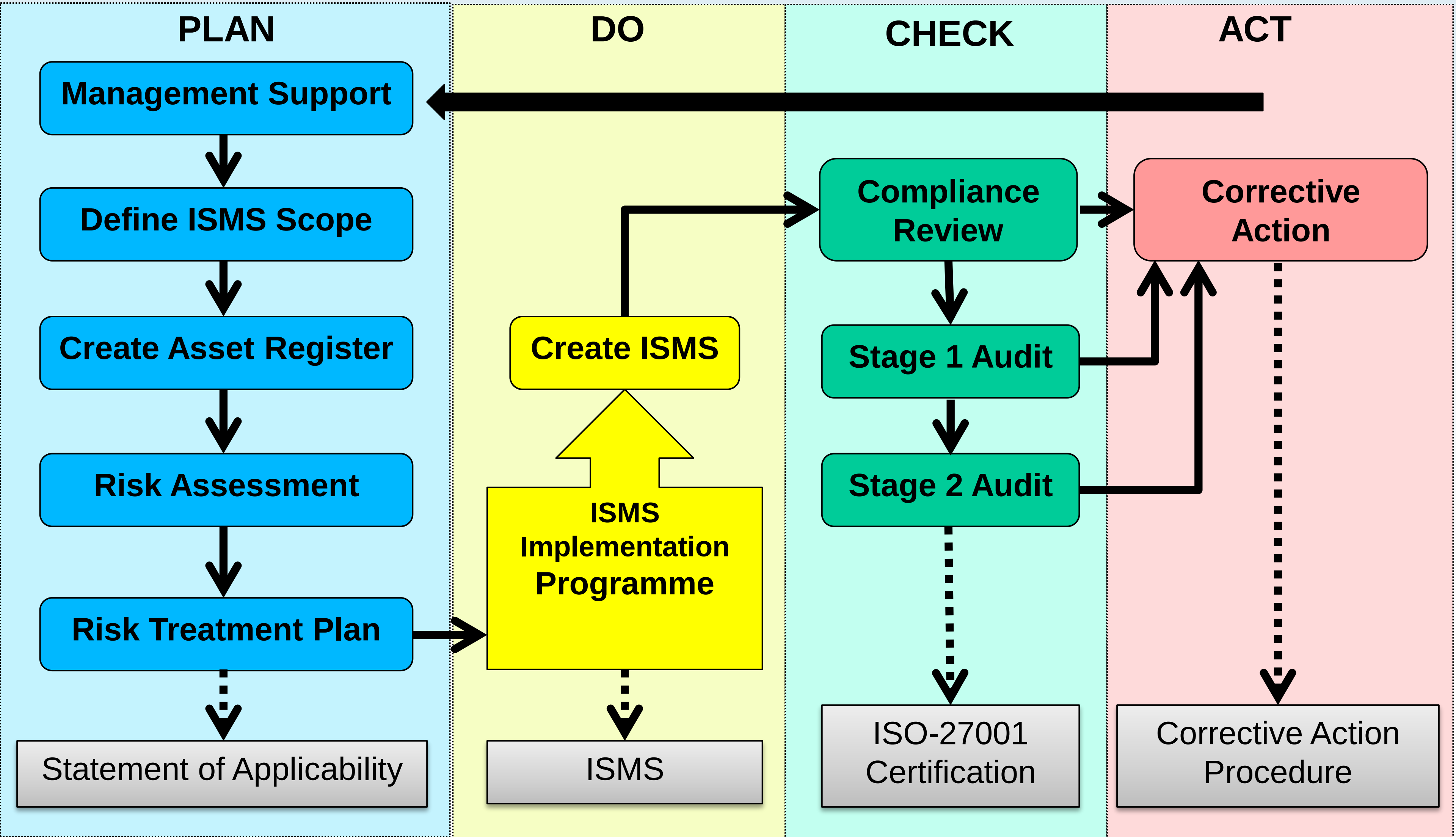
Incident

Controls

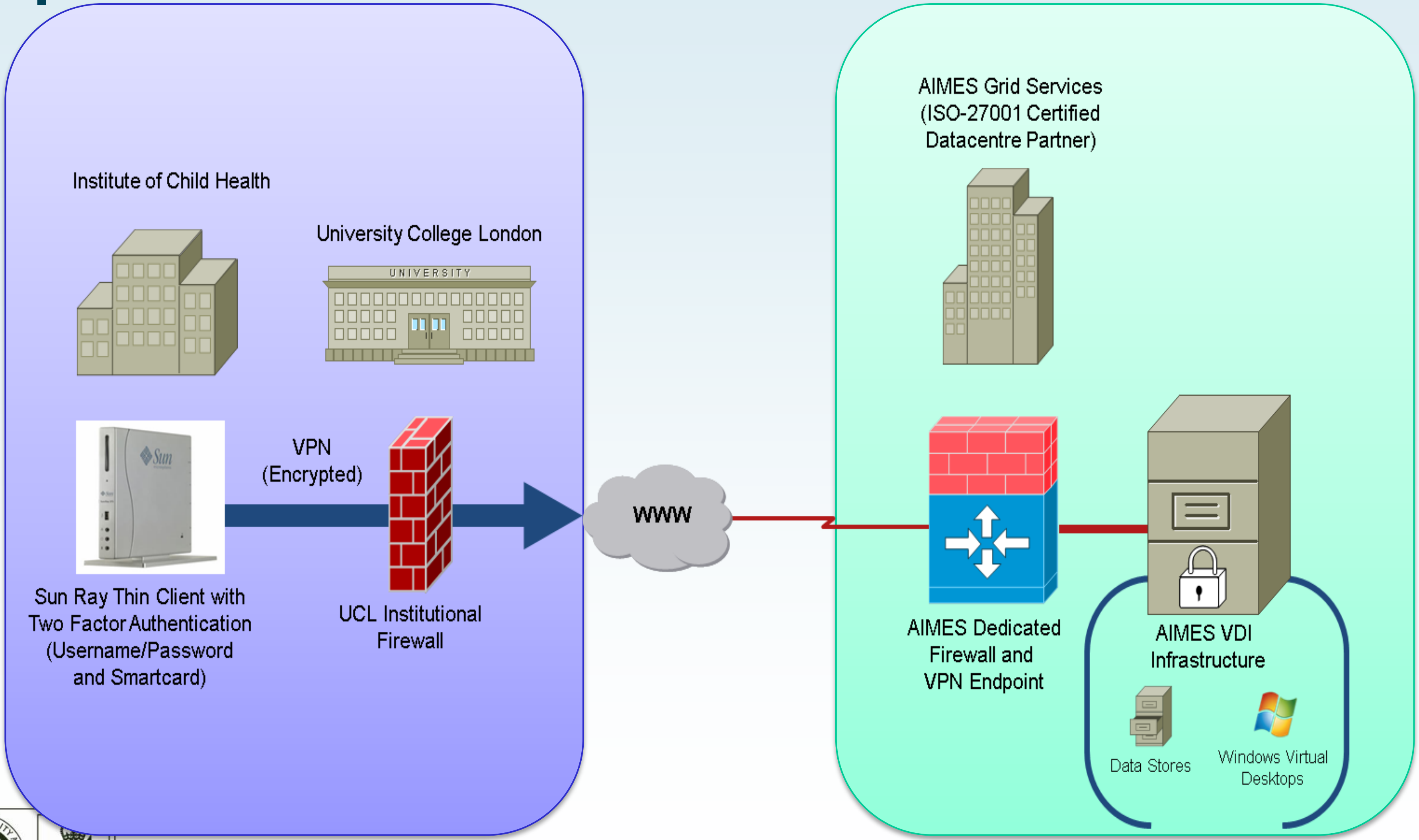
Generic requirements

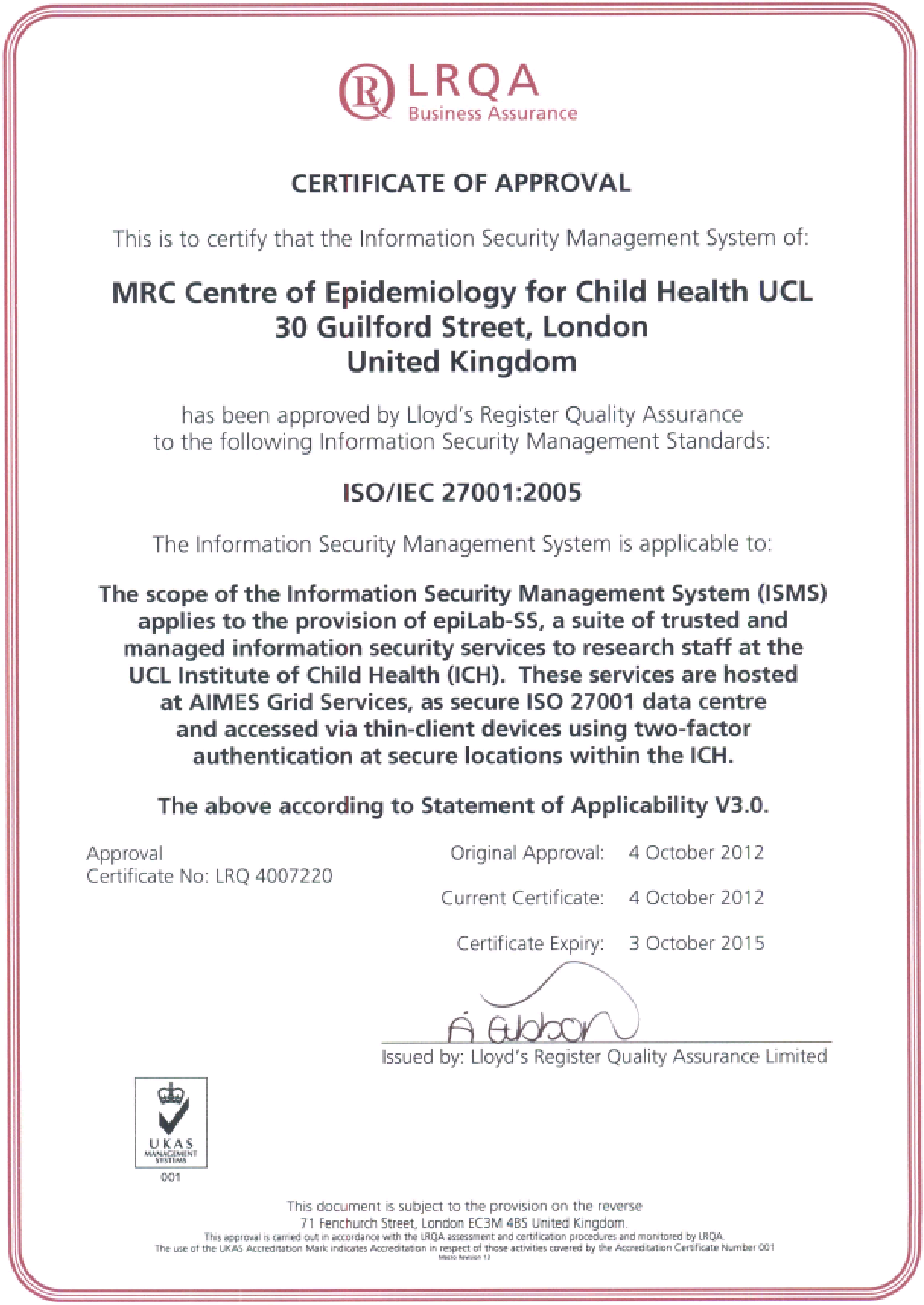
- Secure data enclave
- Secure endpoints
- General-purpose desktop environment
- Scalable architecture
- Standard technology
- Minimal bespoke software

Information Security Management System (ISMS) Development



epiLab-SS architecture





LRQA
Business Assurance

CERTIFICATE OF APPROVAL

This is to certify that the Information Security Management System of:

MRC Centre of Epidemiology for Child Health UCL
30 Guilford Street, London
United Kingdom

has been approved by Lloyd's Register Quality Assurance
to the following Information Security Management Standards:

ISO/IEC 27001:2005

The Information Security Management System is applicable to:

The scope of the Information Security Management System (ISMS) applies to the provision of 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, as secure ISO 27001 data centre and accessed via thin-client devices using two-factor authentication at secure locations within the ICH.

The above according to Statement of Applicability V3.0.

Approval
Certificate No: LRQ 4007220

Original Approval:	4 October 2012
Current Certificate:	4 October 2012
Certificate Expiry:	3 October 2015

Issued by: Lloyd's Register Quality Assurance Limited

UKAS
MANAGEMENT SYSTEMS
001

This document is subject to the provision on the reverse
71 Fenchurch Street, London EC3M 4BS United Kingdom.
This approval is carried out in accordance with the LRQA assessment and certification procedures and monitored by LRQA.
The use of the UKAS Accreditation Mark indicates Accreditation in respect of those activities covered by the Accreditation Certificate Number 001
Macro Revision 13

LLOYD'S REGISTER QUALITY ASSURANCE
ISO/IEC27001

UKAS
MANAGEMENT SYSTEMS
001

Top tips for success

1. **Security, security and security** Effective information security is absolutely fundamental in the management of all data, particularly for healthcare and medical research.
2. **Align with the NHS** The underlying business model for research organisations is fundamentally different to that of the NHS so it's important to develop an *independent* IG framework aligned with the NHS.
3. **Consider the Enterprise** Think in terms of an Enterprise Information Security Architecture (EISA), applying a comprehensive and rigorous methods for describing structure and behaviour in support of your organisational model.
4. **Don't wait, iterate** It takes time to get it right. Start now and begin to see the benefits.

Who needs governance anyway …?

Winchester House

- 38 years to build
- $5.5 million by1922
- 160 rooms including:
  - 40 bedrooms
  - 2 ballrooms
  - 47 fireplaces
  - 10,000 window panes
  - 17 chimneys
  - two basements
  - three elevators

MRC Centre of Epidemiology for Child Health