NHS
National Institute for
Health Research

Clinical Research Network

Applying the IG Toolkit in NIHR CRNCC

A Practical Approach

Supporting research to make patients, and the NHS, better

CRNCC Aims

CRNCC wish to assure that they are following good practice in managing their information systems and undertaking data processing :

- Comply with IG criteria set out in the NHS IG Toolkit
- Conform to Information Security good practice as set out in ISO27001
- Conform to law and policy
- Ensure that policies and procedures are consistent with those of the host organisation (University of Leeds)

About the CRNCC

- CRNCC is not a legal entity but operates under the aegis of DH, who have contracts with UoL for provision and management of premises, services and staffing.
- DH are Data Controller for the information processed by CRNCC
- UoL are Data Controller for staff data
- Infrastructure is part provided and supported by UoL, part by CRNCC

.......It’s complicated! Determining ownership and responsibilities isn’t straightforward.

Issues in Applying the IG Toolkit

- CRNCC holds data about research activity being undertaken across the research network but doesn’t hold or process clinical data
- CRNCC isn’t really a Secondary Use Organisation, but there isn’t a better option in the IG Toolkit
- Some of the assessment criteria don’t really fit – particularly those that focus on the handing of clinical data

..........Danger of turning into a cumbersome academic exercise without real relevance to the organisation.

An Alternative Approach

- Rather than taking a ‘top down’ approach to ‘tick boxes’ in the Toolkit, use a bottom up approach to do what’s relevant to the business

- If you cover what’s important, you will comply with the aims of the Toolkit

Major Categories

- **Governance**

  Does the organisation have appropriate ownership, understanding and control of its information assets?

- **IT assurance**

  Is the processing environment secure and stable ?

- **Business process assurance**

  Are risks identified and managed ?

- **Legal compliance**

  Are we complying with relevant law and policy ?

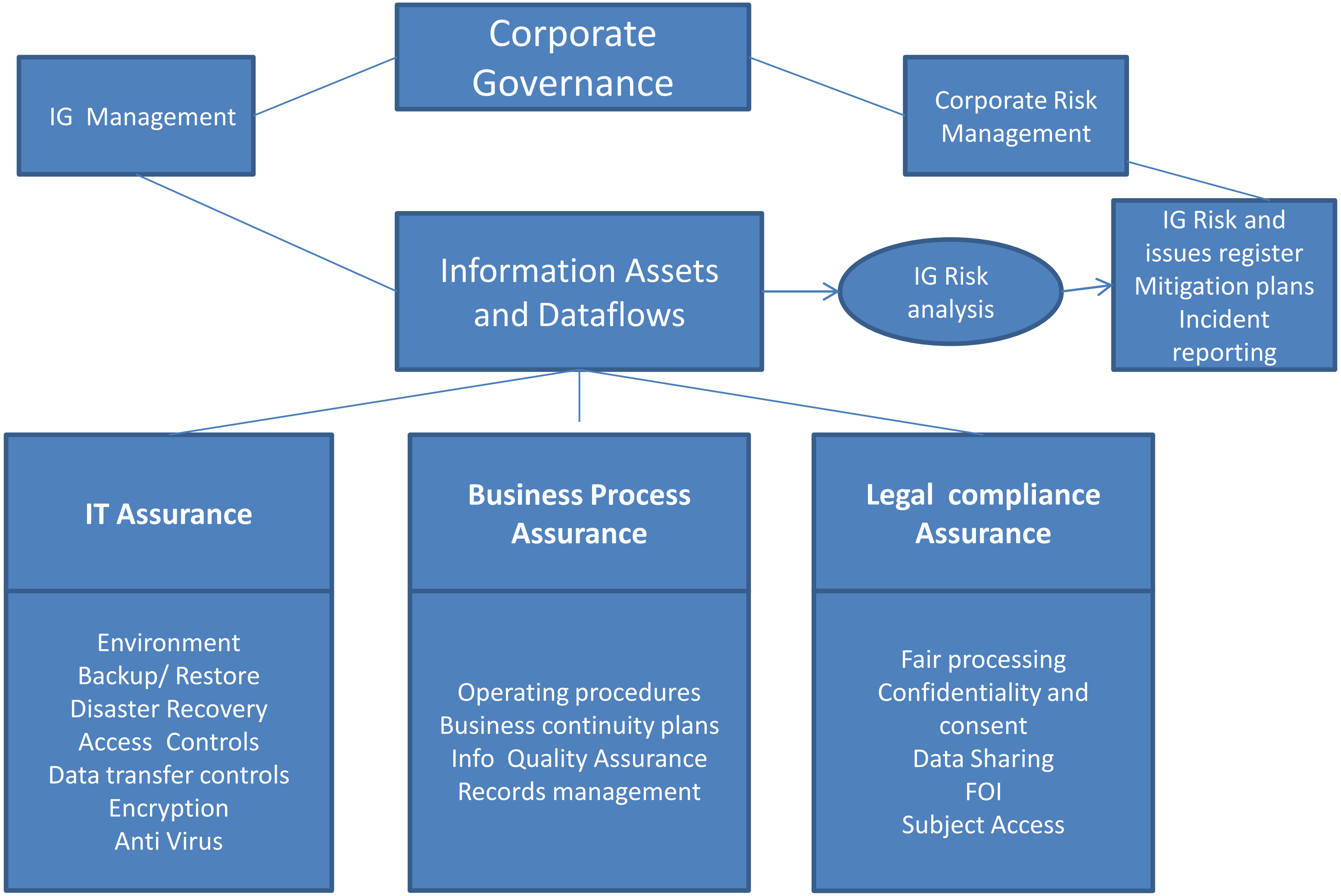
Information Asset Register

- **Key to understanding the organisation’s use of information:**
  - What information systems do you have? For each:
    - What is it used for?
    - What sort of information does it contain?
    - What would be the consequences of data loss or wrongful access ?
    - How ‘business critical’ is the system?

- **Acts as the basis for a business focused approach to information governance**
  - Takes it away from being an abstract process (‘box ticking’)
  - Focus on doing things that are right for your business

How do the Bits Fit Together?

NHS
National Institute for Health Research
Clinical Research Network



Corporate Governance

IG Management

Corporate Risk Management

Information Assets and Dataflows

IG Risk analysis

IG Risk and issues register
Mitigation plans
Incident reporting

IT Assurance

Environment
Backup/ Restore
Disaster Recovery
Access Controls
Data transfer controls
Encryption
Anti Virus

Business Process Assurance

Operating procedures
Business continuity plans
Info Quality Assurance
Records management

Legal compliance Assurance

Fair processing
Confidentiality and consent
Data Sharing
FOI
Subject Access

IG Toolkit vs ISO 27001

- **NHS IG Toolkit**

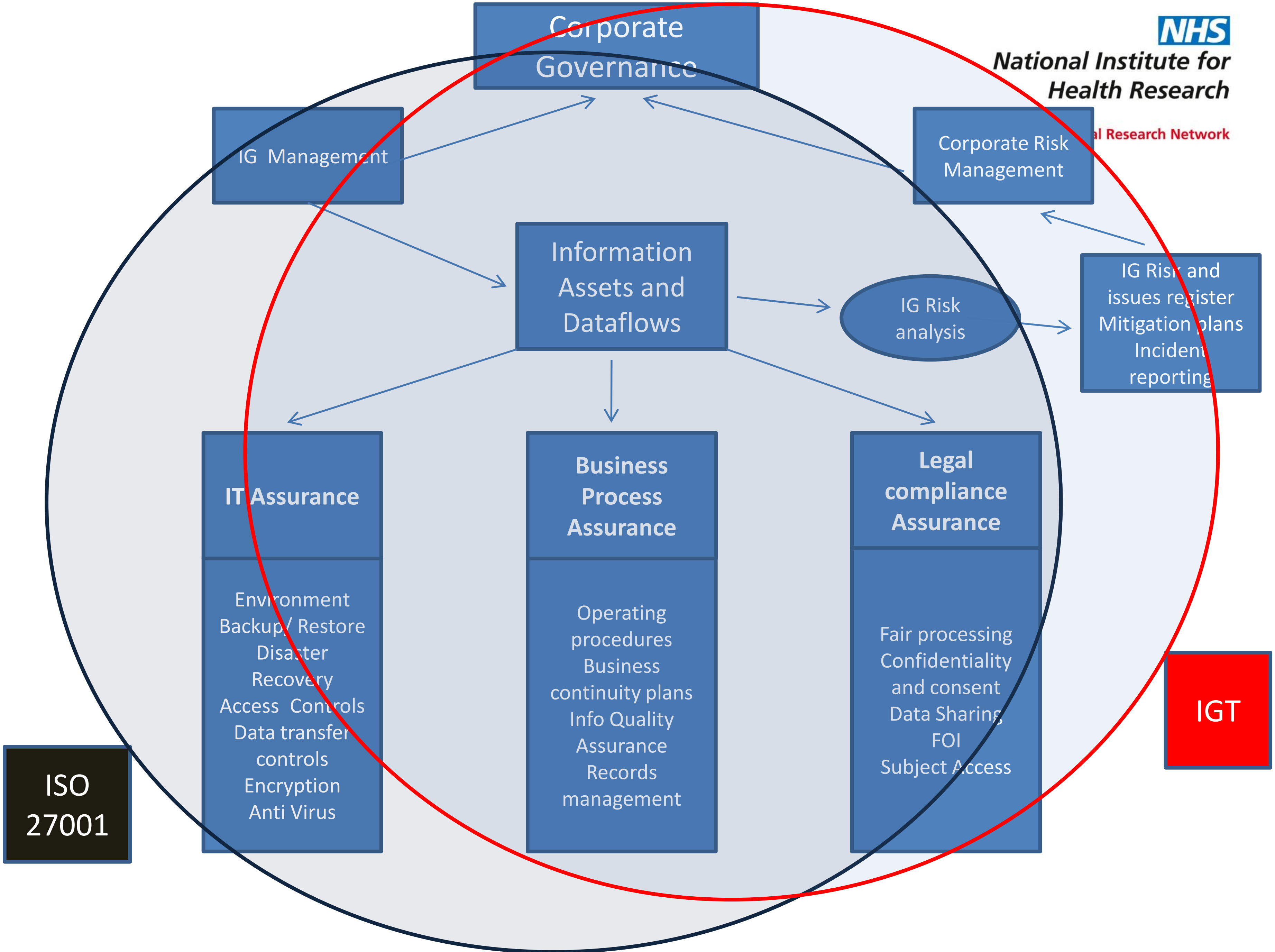
  Focuses on secure management of information, particularly the handling of clinical data

- **IS0 270001**

  Focuses on controlling the technical infrastructure, securing the information environment, and ensuring business continuity

......Lots of overlap

NHS
National Institute for
Health Research
al Research Network



Corporate Governance

IG Management

Corporate Risk Management

Information Assets and Dataflows

IG Risk analysis

IG Risk and issues register
Mitigation plans
Incident reporting

IT Assurance

Environment
Backup/ Restore
Disaster Recovery
Access Controls
Data transfer controls
Encryption
Anti Virus

Business Process Assurance

Operating procedures
Business continuity plans
Info Quality Assurance
Records management

Legal compliance Assurance

Fair processing
Confidentiality and consent
Data Sharing
FOI
Subject Access

ISO 27001

IGT

Comparison of Scope
NHS IGT Vs ISO 27001

In Both	In IGT but not 27001	In 27001 but not IGT
Security policy	10 -200 Staffing – IG skills	Secure areas – physical and environments controls
Organisational responsibilities	10-202 Use of personal information other than for direct health care	Information system development controls
Compliance with legal requirements	10-208 Subject Access Request handling	Operating system controls
Confidentiality agreements, Contractual requirements – staff, service contracts, third parties	10-300 Staffing - Information security skills	Intellectual property Rights
Training and awareness	10-317 Requirements for SIRO	Compliance with technical standards
Access controls	10-323 Specific protection requirements for personal and sensitive data	Information systems audit
Data sharing and information exchange protocols	10-324 Anonymisation and pseudonymisation	
Asset control	10-400 Staffing - Records management skills	
Risk assessment and Business continuity planning	10-601 Corporate records management	
Incident reporting and management	10-603 Procedures for FOI	
Information classification	10-604 Corporate records audit	
Retention, deletion and disposal		
Network security		
Antivirus and malicious code		