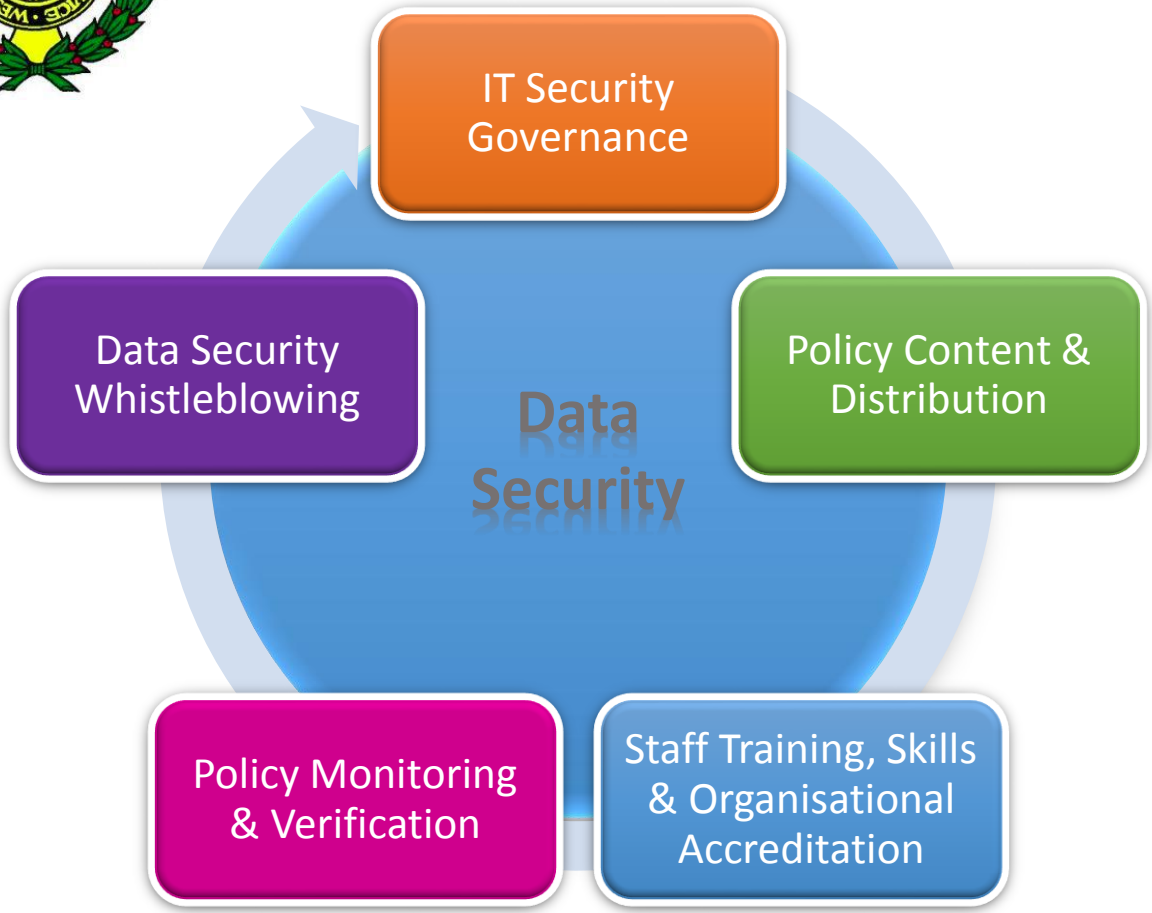
www.nhscybersecurity.co.uk

Information Security & Assurance Service

Providing assurance as to the ongoing Confidentiality, Integrity and Availability of your data and systems.



A. IT Audit	B. Technical Testing
•1.Data Security Governance •2.IT / Data Security Policy •3. Staff and Organisation Accreditation •4.IT Asset Management •5.Data Flow Mapping •6.IT Asset Risk Assessment •7.Change Control (existing and new systems) •8.Activity Monitoring •9.Asset Physical Security •10.Service Availability •11.Data Sharing & 3rd Party Arrangements •12.Whistleblowing and Incident Response	•1.Asset Logical Security •2.Penetration Testing •3.Continuous Vulnerability Scanning •4.Posture Monitoring •5.Social Engineering Testing •6.Device Disposal Verification •7.Encryption Verification •8.Disaster Recovery

Our objective – To provide assurance as to the ongoing confidentiality, integrity and availability of your systems and data.

1. Data security / IT governance arrangements.
2. User education and training on IT and data security.
3. Secure configuration of hardware, software and supporting policies and procedures.
4. Controlled user account management and use of administrative privileges.
5. Continuous vulnerability assessment and response.
6. Activity monitoring and compliance with policies.

www.nhscybersecurity.co.uk

Information Security & Assurance Service

IT Security Governance	• Independent verification of the data and cyber security governance framework, approach and culture within an organisation. • Sharing of best practice and practical examples from other similar organisations.
Policy Content & Distribution	• Review of relevant policy content to ensure all relevant inclusions are present and reflect best practice. • Analysis of policy distribution procedures and testing of staff awareness.
Staff Training & Specialist Skills	• Review of staff mandatory training and tailoring to staff groups. • Assessment of organisational access to relevant expertise. • Review of accreditations and certifications held by the organisation. • Testing of staff awareness via social engineering testing.
Policy Monitoring & Verification	• Assessment & testing of activity monitoring capabilities. • Review of policy monitoring and enforcement controls. • Testing of staff awareness of policies and content. • Undertaking of a broad range of technical testing and data and cyber security related audits.
Data Security Whistleblowing	• Independent opinion regarding the organisations whistle blowing procedure and culture in relation to data and cyber security. • Sharing of best practice and practical examples from within similar environments.

Continuous Cyber Security Vulnerability Assessment and Posture Monitoring

A. IT Audit

- 1.Data Security Governance
- 2.IT / Data Security Policy
- 3. Staff and Organisation Accreditation
- 4.IT Asset Management
- 5.Data Flow Mapping
- 6.IT Asset Risk Assessment
- 7.Change Control (existing and new systems)
- 8.Activity Monitoring
- 9.Asset Physical Security
- 10. Service Availability
- 11.Data Sharing & 3rd Party Arrangements
- 12.Whistleblowing and Incident Response

B. Technical Testing

- 1.Asset Logical Security
- 2.Penetration Testing
- 3.Continuous Vulnerability Scanning
- 4.Posture Monitoring
- 5.Social Engineering Testing
- 6.Device Disposal Verification
- 7.Encryption Verification
- 8 Disaster Recovery

We utilise leading security products and can automatically undertake vulnerability scans of your organisations Internet and N3 facing systems.

We have also developed a 'Posture Monitor' service which informs organisations of changes to their externally facing services. This has lead to Trusts reviewing their change control procedures after our service identified events such as unauthorised firewall changes.