

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
101	IG Management	Does the Trust have adequate governance in place to support the current and evolving Information Governance agenda?	IGSoC Version 6.0 (July 2008). Para. 2.2. Completion of the Information Governance toolkit to the required standard and submission of the RA01 * where applicable) are prerequisites of the IGSoC submission. An IGSoC approved by NHS CFH is required before access to services is granted.		
102	IG Management	How would you assess your Trust's ability to access expertise across the Confidentiality & Data Protection Assurance agenda?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2.; 3.3. and 3.4)	Commitment 10: We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.	
103	IG Management	How would you assess your Trust's ability to access expertise across the Information Security agenda?	IGSoC Version 6.0 (July 2008) . Para. 5.1. The ASR should appoint a person to have responsibility for the security management of the ASR's network connection(s) and their locally connected systems.	Commitment 10: We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.	BS ISO/IEC 27002:2005, control 6.1.1, states: Management should actively support security within the organisation, through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities. In particular, sub section (f) requires management to approve assignment of specific roles and responsibilities for Information security across the organisation.
104	IG Management	How would you assess your Trust's ability to access expertise across the Information Quality and Records Management Agenda?			

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
105	IG Management	Does the Trust have in place comprehensive IG Policy and associated Strategy and Improvement Plans all signed off by the Board?			BS ISO/IEC 27002:2005 – Controls 4 & 5 – Information Security Policy.
106	IG Management	Does the Trust have up to date and tested business continuity plans for all critical infrastructure components and core information systems?			BS ISO/IEC 27002:2005 - Section 14 States: A Business Continuity Management process should be implemented to minimise the impact on the organisation and recover from loss of information assets to an acceptable level through a combination of preventative and recovery controls
107	IG Management	Does the Trust have a comprehensive Board endorsed Information Lifecycle Management Policy/Strategy and implementation plan?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2;. 3.3. and 3.4)		
108	IG Management	Has the Trust implemented its Information Governance management arrangements to ensure the NHS CFH Statement of Compliance (SoC) is satisfied?	IGSoC Version 6.0 (July 2008) Para.7.2. (the) ASR must meet NHS CFH information governance requirements as identified in the NHS Information Governance Toolkit. Compliance with the IGSoC is reconfirmed annually through submission of the IGT to the appropriate level.		

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
109	IG Management	Does the Trust ensure that staff and those working on behalf of the Trust comply with the terms and conditions set out on the RA01 form?	IGSoC Version 6.0. (July 2008) Para. 4.1.10. The ASR is required to enforce, through local disciplinary or contractual measures, where necessary, the Information Governance standards and processes including, where appropriate, the registration process and adherence to conditions identified in the RA01 registration form signed by its Authorised Users.	Commitment 10: We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.	
110	IG Management	Does the Trust ensure that it has formal contractual arrangements that include compliance with information governance requirements, with all contractors and support organisations?	IGSoC Version 6.0. (July 2008) Para. 4.1.10. The ASR is required to enforce, through local disciplinary or contractual measures, where necessary, the Information Governance standards and processes including, where appropriate, the registration process and adherence to conditions identified in the RA01 registration form signed by its Authorised Users.	Commitment 9: We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policy and controls as the NHS does. We will enforce this duty at all times.	BS ISO/IEC 27002:2005 controls 6.1.5: Confidentiality Agreements and 6.2.3: Addressing Security in Third Party Agreements.
111	IG Management	Does the Trust ensure that all individuals carrying out work on behalf of the Trust have employment contracts which require compliance with information governance standards?	IGSoC Version 6.0. (July 2008) Para. 4.1.10. The ASR is required to enforce, through local disciplinary or contractual measures, where necessary, the Information Governance standards and processes including, where appropriate, the registration process and adherence to conditions identified in the RA01 registration form signed by its Authorised Users.	Commitment 9: We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policy and controls as the NHS does. We will enforce this duty at all times.	BS ISO/IEC 27002:2005 controls 8.1.3: Terms and Conditions of Employment Contracts.

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
112	IG Management	Does the Trust's induction procedures effectively raise the awareness of Information Governance?		Commitment 9: We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policy and controls as the NHS does. We will enforce this duty at all times.	
113	IG Management	Does the Trust assess staff training needs and ensure job/role specific information governance training is provided to all staff?	No specific reference in SoC- Included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2;. 3.3. and 3.4)	Commitment 9: We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policy and controls as the NHS does. We will enforce this duty at all times.	
120 NEW	IG Management	Does the Trust have assurance that its registration authority managers, agents and sponsors have sufficient knowledge and skills(including latest software, operational process, guidance and its integration into Trust policies and procedures) to discharge their RA responsibilities?			

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
121 NEW	IG Management	Does the Trust have a Board level Senior Information Risk Officer (SIRO) who takes ownership of the Trust's information risk policy, acts as advocate for information risk on the board and provides written advice to the accounting officer on the content of their Statement of Internal Control in regard to information risk?			
201	Confidentiality and Data Protection	Does the Trust have a confidentiality code of conduct that provides staff with clear guidance on the disclosure of patient personal information?	No specific reference - included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2.; 3.3. and 3.4)	Commitment 2: When we provide health care, we will share your record with the people providing care or checking its quality.(unless you have asked that we limit how we share your record).	
202	Confidentiality and Data Protection	Does the Trust ensure that patients are generally asked before their personal information is used in ways that do not directly contribute to, or support the delivery of, their care and that patients' decisions to restrict the disclosure of their personal information are appropriately respected?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2.; 3.3. and 3.4)	Commitment 3: We will not share information that identifies you (particularly with other governance agencies) for any reason other than providing your care, unless:• you ask us to do so;• we ask and you give us specific permission;• we have to do this by law;• we have special permission for health or research purposes; or we have special permission because the public is thought to be of greater importance than your confidentiality. If we share information without your permission, we will make sure that we keep to the Data protection Act ,the NHS confidentiality code of practice and other national guidelines on best practice.	

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
203	Confidentiality and Data Protection	Does the Trust ensure that patients are informed about the proposed uses of their personal information and the importance of providing accurate information to NHS staff?		Commitment 3: We will not share information that identifies you (particularly with other governance agencies) for any reason other than providing your care, unless:• you ask us to do so;• we ask and you give us specific permission;• we have to do this by law;• we have special permission for health or research purposes; or we have special permission because the public is thought to be of greater importance than your confidentiality. If we share information without your permission, we will make sure that we keep to the Data protection Act ,the NHS confidentiality code of practice and other national guidelines on best practice.	
204	Confidentiality and Data Protection	Does the Trust have effective procedures for ensuring that detailed questions, raised by patients about how their information may be used, can be answered?		Commitment 7: We will deal fairly and efficiently with your questions, concerns and complaints about how we use information about you.	
205	Confidentiality and Data Protection	Does the Trust have appropriate procedures for recognising and responding to patient requests for access to their health records?		Commitment 1: When we receive a request from you in writing, we must normally give you access to everything we have recorded about you. We may not give you confidential information about other people, or information that a health professional considers likely to cause serious harm to the physical or mental health of your or someone else. This applies to paper and electronic records. However, if you ask us to, we will let other people see health records about you.	

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
206	Confidentiality and Data Protection	Has the Trust established appropriate confidentiality audit procedures to monitor access to confidential patient information?	IGSoC Version 6.0 (July 2008) Para. 8.2 The ASR shall have a process for internal information security audit and management of alerts. This process should be tested for compliance at least twice in any twelve month period.	Commitment 12: We will take action when someone has deliberately accessed records about you without permission or good reason. This can include disciplinary action, ending a contract, firing an employee or bringing criminal charges.	
207	Confidentiality and Data Protection	Has the Trust agreed protocols governing the sharing of patient-identifiable information with other organisations where this is required?		Commitment 2: When we provide health care, we will share your record with the people providing care or checking its quality.(unless you have asked that we limit how we share your record)	
208	Confidentiality and Data Protection	Has the Trust mapped all flows of person identifiable information, assessed risks in line with Department of Health guidelines and put in place safe haven procedures for all routine flows of person identifiable information to the organisation?	IGSoC Version 6.0 (July 2008) Para. 8.4. The ASR acknowledge that, if required to process personal data (as the term 'personal data' is defined in section 1(1) of the Data Protection Act 1998), in the course of providing the NHS CFH services, it shall do so only on the instruction of an appropriate Data Controller and shall maintain in place, having regard to the state of technological development and the cost of implementation, all appropriate measures, procedures and policies to protect the security and integrity of any such personal data.	Commitment 10: We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.	

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
209	Confidentiality and Data Protection	Does the Trust ensure that all person identifiable data processed outside the UK complies with the Data Protection Act 1998 and Department of Health guidelines	IGSoC Version 6.0. (July 2008) Para. 12.1. ASRs shall ensure that they meet the requirements of DH and NHS CFH policy on personal data leaving England, or being viewed from overseas, by completing and complying with the Information Governance Offshore Support Requirements.		
210	Confidentiality and Data Protection	Does the Trust ensure that all new processes, software and hardware, comply with confidentiality and data protection requirements?			
301	Information Security Management	Does the Trust have a formal information security risk assessment and management programme that is implemented and regularly reviewed?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2;. 3.3. and 3.4)		BS ISO/IEC 27002:2005 controls 4.1/4.2: Risk Assessment and Treatment.
302	Information Security Management	Does the Trust have documented and accessible information security event reporting, investigation and resolution procedures in place that are explained to all staff?	IGSoC Version 6.0. (July 2008). Para. 8.5. Any threat or security event affecting or potentially affecting the security of NHS CFH provided infrastructure or services must be immediately reported via the NHS CFH incident reporting arrangements and/or other contacts provided by NHS CFH, for example the local RA manager for Smartcard incidents.	Commitment 12: We will take action when someone has deliberately accessed records about you without permission or good reason. This can include disciplinary action, ending a contract, firing an employee or bringing criminal charges.	BS ISO/IEC 27002:2005 control 13: Information Security Incident Management.
303	Information Security Management	Has the Trust established business processes that ensure all staff smartcards and access profiles issued are appropriate and satisfy their obligations as RAs?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2;. 3.3. and 3.4)		BS ISO/IEC 27002:2005, control 15.1.4: Data Protection and Privacy of Personal Information

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
305	Information Security Management	Does the Trust ensure that operating and application information systems under its control support appropriate access control functionality?	IGSoC Version 6.0. (July 2008) Para. 5.4. Access to NHS CFH infrastructure and connected systems are subject to appropriate access and authentication controls that meet the NHS CFH Information Governance standards(as amended from time to time). Those services not applicable to Smartcard access and authentication controls should have suitable policies, procedures, processes, controls and monitoring to ensure NHS CFH standards are met.	Commitment 10: We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.	BS ISO/IEC 27002:2005 controls 11.1/11.5. & 11.6: Business requirements, operating systems and application and information access controls.
306	Information Security Management	Are there defined, documented and agreed access rights for all users of Trust information systems and services?	IGSoC Version 6.0. (July 2008) Paras. 4.1.15 & 4.1.15.1. The services provided by NHS CFH to the ASR must be used for accessing NHS CFH accredited systems and services and not for inappropriate browsing of other internal and internet systems.	Commitment 11: We will keep a record of everyone who accesses the information the NHS Care Records Service holds about you. You will be able to ask for a list of everyone who has accessed records about you and when they did so. There may be times when someone will need to look at information about you without having been given permission to do so beforehand. This may be justifiable, for example, if you need emergency care. We will tell you if the action cannot be justified.	BS ISO/IEC 27002:2005, controls 11.1-11.5: Business and user management and responsibilities for access.
307	Information Security Management	Has the Trust established a register of all its major information assets and assigned responsibility or 'ownership' for each?	No specific reference -included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2.; 3.3. and 3.4)		BS ISO/IEC 27002:2005, control 7: Asset Management

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
308	Information Security Management	Does the Trust ensure that digital information shared with other Organisation's is secured in transit?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2;. 3.3. and 3.4)		BS ISO/IEC 27002:2005, control 18.8: Exchange of Information
309	Information Security Management	Does the Trust have adequate procedures in place to ensure the availability of information processing facilities, communications services and data?			BS ISO/IEC 27002:2005 Section 14 states: A Business Continuity Management process should be implemented to minimise the impact on the organisation and recover from loss of information assets to an acceptable level through a combination of preventative and recovery controls. BS ISO/IEC 27002:2005, controls 10.5 & 12.2: Back Ups and Correct Processing in Application
310	Information Security Management	Does the Trust have procedures in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error?			BS ISO/IEC 27002:2005, control 9.2: Physical and Environmental Security (Equipment)
311	Information Security Management	Does the Trust ensure that its information systems are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code?			BS ISO/IEC 27002:2005, control 10.4: Protection Against Malicious and Mobile Code

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
312	Information Security Management	Does the Trust have in place appropriate procedures for ensuring that the development and introduction of any new local information systems, software, IT projects and, more generally, IT support activities are conducted in a secure and structured manner?			BS ISO/IEC 27002:2005, controls 10.1.1 - 4, 10.3 & 12.1: Communication and Operation Management (Procedures)
313	Information Security Management	Does the Trust have appropriate procedures in place to ensure that communication networks under the Trust's control operate in a secure manner?	IGSoC Version 6.0 (July 2008). Para. 5.2. The ASR shall manage their networks and connected systems in accordance with their local policies written to incorporate the requirements of IGSoC clauses 3.2, 3.3 and 3.4 (i.e. Standards & Policy)		BS ISO/IEC 27002:2005, control 10.6: Network Security Management
314	Information Security Management	Does the Trust have appropriate procedures for ensuring that mobile computing and teleworking are conducted in a secure manner?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2.; 3.3. and 3.4)		BS ISO/IEC 27002:2005, controls 11.7: Mobile Computing and Tele-working
315	Information Security Management	Does the AMT satisfy its security management requirements to protect the Airwaves Communications Service?	IGSoC Version 6.0 (July 2008). Para. 4.1.14. Use of the Airwave service shall be in accordance with the Airwave Codes of Connection and Practice (as amended from time to time) and made available to Airwave users		BS ISO/IEC 27002:2005, control 9.2: Physical and Environmental Security (Equipment) BS ISO/IEC 27002:2005, control 10.6: Network Security Management
322 NEW	Information Security Management	Does the Trust ensure that Registration Authority equipment (hardware and software) and consumables meet current specification and is it adequately maintained and stored?	No specific reference, included under general requirements in the IGSoC around Legislation, Best Practice and Policy. (Paras 3.1.; 3.2.; 3.3. and 3.4)		

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
401	Clinical Information Assurance	Does the Trust have a strategy to ensure the correct NHS Number is recorded for each active patient and ensure that it is used routinely in clinical communications?			
402	Clinical Information Assurance	Does the Trust have documented and implemented procedures for the identification and resolution of duplicate or confused patient records (i.e. where two or more patients share a record)?		Commitment 8: We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We would normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you are suffering distress or harm as a result of information being held in your record, you can apply to have the information amended or deleted.	
403	Clinical Information Assurance	Does the Trust have Trust-wide, multi-professional audit of clinical record standard, including accuracy, for all professional groups in all specialities?		Commitment 8: We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We would normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you are suffering distress or harm as a result of information being held in your record, you can apply to have the information amended or deleted.	

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
404	Clinical Information Assurance	Does the Trust have paper health records of a standard design within the Trust, combined with a locally agreed standard format for filing within the health record?		Commitment 8: We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We would normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you are suffering distress or harm as a result of information being held in your record, you can apply to have the information amended or deleted.	
405	Clinical Information Assurance	Does the Trust have robust procedures and processes for monitoring all data collection activities across the Trust?			
406	Clinical Information Assurance	Does the Trust have processes and procedures in place to enable it to regularly monitor, measure and trace paper health records?			
407	Clinical Information Assurance	Does the Trust ensure that Accident and Emergency records are contained within the main record for patients who are subsequently admitted and is there a system to ensure that the GP is sent a copy of the A&E record?			

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
408	Clinical Information Assurance	Does the Trust have procedures in place to ensure that when new services are provided, or where changes within the system are made, that these do not adversely impact on information quality?			<p>BS ISO/IEC 27002:2005 is the international standard for information security management and replaces BS ISO/IEC 17799: 2000.</p> <p>BS ISO/IEC 27001:2005 BS7799-2:2005 replaces the 2002 version of BS7799 part 2 and is used to formulate an Information Security Management System (ISMS) for those organisations wishing to fully comply with the standard.</p>
501	Secondary Use Assurance	Does the Trust ensure that NHS standard definitions, values and validation programmes are incorporated within key systems and that local documentation is updated as standards develop?			
502	Secondary Use Assurance	Does the Trust use external data quality reports for monitoring and improving quality?			
503	Secondary Use Assurance	Does the Trust have procedures to ensure that staff routinely check information about patients with the source so that corrections are made as necessary to appropriate records and does the Trust routinely undertake activity reconciliations between the patient record and data on PAS?		<p>Commitment 8: We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We would normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you are suffering distress or harm as a result of information being held in your record, you can apply to have the information amended or deleted.</p>	

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
504	Secondary Use Assurance	Does the Trust have documented procedures for using both local and national benchmarking to identify possible data quality issues and to analyse trends in information over time to ensure that large changes are investigated and explained?			
505	Secondary Use Assurance	Does the Trust have in place a robust programme of internal and external data quality/clinical coding audit in line with the requirements of the Audit Commission and NHS Connecting for Health?		Commitment 8: We will take appropriate steps to make sure information about you is accurate. You will be given opportunities to check records about you and point out any mistakes. We would normally correct factual mistakes. If you are not happy with an opinion or comment that has been recorded, we will add your comments to the record. If you are suffering distress or harm as a result of information being held in your record, you can apply to have the information amended or deleted.	
506	Secondary Use Assurance	Does the Trust have a documented procedure and a regular audit cycle for accuracy checks on patient data?			
507	Secondary Use Assurance	Has the Trust completed and passed the Completeness and Validity check for data as detailed in the guidance documents?			
508	Secondary Use Assurance	Is the Trust involving clinical staff in validating information derived from the recording of clinical activity?			

Information Governance Toolkit - V6 - Standards Comparison - August 2008

Req	Initiative	IGT Requirement	IGSoC Requirement	CRG Commitment	BSI/IEC 27002:2005 Control
509	Secondary Use Assurance	Does the Trust have (or access) a formal, targeted training programme for all staff involved in the collection and management of patient-related data covering the operation of key systems?			
510	Secondary Use Assurance	Does the Trust use training programmes for clinical coding staff entering coded clinical data that are comprehensive and conform to National Standards?			
511	Secondary Use Assurance	Does the Trust have sufficient governance processes in place to ensure adherence to the principles enshrined in the Code of Conduct for Payment by Results?			
601	Corporate Information Assurance	Does the Trust have documented and implemented procedures for the creation and filing of electronic corporate records to enable efficient retrieval and effective records management?			
602	Corporate Information Assurance	Does the Trust have documented and implemented procedures for the creation, filing and tracking/tracing of paper corporate records to enable efficient retrieval and effective records management?			
603	Corporate Information Assurance	Does the Trust have publicly available, documented and implemented procedures to ensure compliance with the Freedom of Information Act 2000?			
604	Corporate Information Assurance	Has the Trust carried out an audit of its corporate records and information as part of the records lifecycle management strategy?			