Internal Audit Report
For
Leeds and York Partnership NHS Foundation Trust

Data Security and Protection Toolkit
LY16/2019

Contents

	Page
Section 1 – Executive Summary	2
Section 2 – Audit Background, Objectives, Scope and Report Circulation	12
Section 3 – Schedule of Findings and Recommendations	16
Section 4 – Key to Internal Audit Reports	19

Report Author: John Roberts
Report Version: Final
Report Date: 27 March 2019

Objective

The objective of this audit was to provide assurance that the Trust has appropriate systems and processes in place to demonstrate compliance with the national Data Security and Protection (DSP) Framework, in accordance with DSP Toolkit requirements. The audit included a review of evidence for a sample of 14 requirements ('assertions') to support the claims made in the self-assessment.

Overall Opinion

Significant	Audit testing reviewed 31 of the 100 mandatory evidence questions from the DSP Toolkit, covering 14 of the 40 assertions applicable to mental health trusts. Requirements were included from across all ten of the National Data Guardian's core data security standards. Our review found that there was appropriate evidence to support 10 of the 14 assertions reviewed and these reflect fairly the position within the organisation; four assertions are broadly supported, but we provide minor recommendations in Section 3 to assist you in strengthening your arrangements further. Our review found that an appropriate process was implemented for the timely completion and publication of the DSP Toolkit self-assessment. This was led by the Trust's Head of Information Governance (Data Protection Officer/Information and Knowledge Manager) with support from relevant leads from the Informatics and Reporting teams. The Board is expected to approve the DSP Toolkit submission on 28 March 2019 in advance of submission on 31 March 2019.

Assurance on Key Control Objectives

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
The Trust has robust policies, systems and procedures for the timely completion and submission of the DSP Toolkit self-assessment.	✓ The Data Security and Protection (DSP) Toolkit submission has been completed by the Trust's Information Governance team, overseen by the IG Lead (Data Protection Officer/Information and Knowledge Manager). ✓ The collection of evidence related to the assertions made has been supported by relevant leads in the Informatics and Reporting teams. ✓ Evidence and supporting documents collected are mostly stored on a central evidence base on the shared drive. Other evidence is accessible via the Trust's Staffnet. ✓ The Board is expected to approve the DSP Toolkit submission on 28 March 2019 in advance of submission on 31 March 2019.	**Significant**	**0**	**0**	**0**
1.1 There is senior ownership of data security and protection within the organisation.	✓ The roles of SIRO and Caldicott Guardian are assigned to the Trust's Chief Financial Officer and Medical Director respectively. The roles of Deputy SIRO and Deputy Caldicott Guardian are assigned to the Chief Information Officer and Data Protection Officer. ✓ Other specialist staff with responsibility for data protection and/or security include the Head of ICT Network Services, ICT Network Support Manager, Head of IT Service Delivery, Systems Engineering Manager, and Information Governance Support Officer. ✓ Roles and responsibilities of the SIRO, Caldicott Guardian, Data Protection Officer and Information Governance Support Officer are set out in the Information Governance Policy.	**Significant**	**0**	**0**	**0**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public.	✓ An Information Governance Policy is in place which provides the legal and ethical framework under which Personal Confidential Data and otherwise confidential information is processed. It includes the Trust's approach to data quality, information security, confidentiality, information sharing and information retention and disposal. It has been agreed in the separate audit report for the General Data Protection Regulations that this will be developed to be a Data Protection and Information Govrnancee Policy. ✓ The Information Governance Policy is supported by further policies and procedures covering health records, confidentiality code of conduct, Freedom of Information, data quality, corporate records management, medical records subject access requests and safe haven guidance. ✓ The Trust also has a suite of IT policies and procedures which cover encryption, internet use, email use, network security, portable computing devices and information security. ✓ Testing confirmed that all policies and procedures have generally been reviewed and updated in accordance with the Trust's one year or three year review cycle. However, the review dates for the Data Quality Policy and PARIS Data Collection and Input Procedure have been extended as these refer to the PARIS system which is to be replaced. ✓ Policies and procedures are reviewed and approved by the Information Governance Group and are ratified by the Policy and Procedures Group.	**Significant**	**0**	**0**	**0**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
1.7 Effective data quality controls are in place.	✓ The Data Quality Policy sets out a framework for capturing and maintaining high levels of data quality within the Trust. ✓ The Data Quality Policy specifies the roles and responsibilities for data quality, the requirement to comply with national data standards and dataset requirements, and processes in place to validate the accuracy, completeness and timeliness of data, and processes in place to monitor policy compliance. ✓ The Clinical Coding audit requirement is fulfilled by commissioning an annual audit of 50 finished consultant episodes. The most recent annual audit was completed in November 2018 and reported that the highest level of coding accuracy had been achieved. ✓ Data Quality updates are submitted to the Information Governance Group each month. These provide data quality performance data and a summary of data quality reviews undertaken. ✓ An internal Data Compliance Audit of the input of data into Trust systems was completed and reported to the Information Governance Group in December 2018.	**Significant**	**0**	**0**	**0**
2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	✓ New starters to the organisation receive a short presentation on information governance, the Data Protection Act and information security matters as part of their attendance at corporate induction. ✓ New starters receive induction awareness training in advance of their corporate induction if access to the PARIS system is required prior to their corporate induction.	**Significant**	**0**	**0**	**0**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
	✓ A process is in place to capture any new starters that have not received induction awareness training and to follow these up. This includes new starters that do not work directly for the Trust such as agency staff and medical placement students. ✓ Security and confidentiality of information clauses are included as standard in all contracts of employment.				
3.3 Staff pass the data security and protection mandatory test.	✓ The Trust has a robust approach to chasing IG training compliance, with reminders and reports being issued to staff and managers via the Trust's e-learning platform, and active follow up of those staff with expiring training compliance. ! 93.5% of Trust staff had completed their annual data security awareness training as of 12 March 2019 against a requirement for at least 95% of all staff to have passed in the period 1 April 2018 to 31 March 2019. Overall, the compliance rate has fluctuated throughout the year achieving 95% in August 2018.	**Significant**	**0**	**0**	**0**
3.4 Staff with specialist roles receive data security and protection training suitable to their role.	✓ Staff identified as requiring role specialist training include the SIRO, Caldicott Guardian, Data Protection Officer (Information and Knowledge Manager), the Information Governance Support Officer, IT Managers, Clinical Coding and Medical Records staff. ✓ Specialist training is role specific and any training needs are identified through the personal development review process. ✓ The Trust is not aware of any current training gaps. Examples of training provided include HSCIS and FoIA training completed by the Data Protection Officer and Information Governance Support Officer, and Caldicott Guardian training completed by the Data Protection Officer. The Head of ICT Network Services is currently undertaking CISSP (Certified Information Systems Security Professional) and SSCP (Systems Security Certified	**Significant**	**0**	**0**	**0**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
	Practitioner) training. ✓ Clinical Coding staff complete refresher training on a 3-yearly basis (due and booked for 2019). ✓ Medical Records staff have previously undertaken SAR training using relevant HSCIC training modules.				
4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.	✓ An automated process is in place to notify the Systems Management team of staff that leave the Trust. The Systems Management team review user accounts to make sure they have been deactivated to prevent access to the network and to ensure that access is blocked to the following patient information systems: PARIS / Bighand / EMPA and LCR. ✓ Break Glass reports identify PARIS users that access the system to view the records of patients not in their area of care. These are monitored for inappropriate access and to ensure that access permissions are set appropriately. ✓ An audit of user access was completed on 1 February 2019. This covered network access and access to patient information systems.	**Significant**	**0**	**0**	**0**
5.1 Process reviews are held at least once per year.	✓ Information security breaches and near misses reported via DATIX are recorded on receipt. All breaches and near misses are investigated and this includes a review of associated processes as determined by root cause analysis where appropriate. ✓ Information security breaches and near misses are reported monthly to the Information Governance Group. The group provides a forum to identify trends and lessons learned.	**Significant**	**0**	**0**	**1**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
	! The Trust does not have arrangements in place for periodic proactive reviews to identify and improve processes for accessing and using systems and data which can be commonly attributed to data security incidents and workarounds.				
6.4 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.	✓ There have been no incidents in the reporting period (1 April 2018 to 31 March 2019) caused by a known vulnerability being exploited. ✓ Advisory bulletins received from NHS Digital CareCERT are logged on receipt and allocated to the network and desktop support teams for investigation. Notified threats are assessed for exposure to the threat and then for potential severity/impact if there is any exposure. ✓ A summary of CareCERT bulletins received, analysed by threat level is reported monthly to the Information Governance Group.	**Significant**	**0**	**0**	**0**
7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action.	✓ The Trust maintains a Trustwide Major Incident Response Plan and individual Business Continuity Plans covering specific areas of the organisation. ✓ The Business Continuity Management Framework Policy sets out the general principles underpinning the business continuity arrangements for the Trust. ! An IG Business Continuity Plan is in place which covers potential events such as major IT system failure, loss of IT network functionality, being unable to access usual base and absence of key personnel. However, data security incidents are not specifically featured. ! The IG Business Continuity Plan has not been formally approved and endorsed by the SIRO.	**Significant**	**0**	**0**	**2**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
	✓ The plan is stored internally on a local shared drive and externally via a dedicated NHS Mail BCDR account which is accessible by the Trusts BCDR leads, service desk etc. ✓ Processes are in place which allow the Trust to alert and contact its staff in an emergency.				
7.2 There is an effective annual test of the continuity plan for data security incidents.	✓ A Disaster Recovery day was held on 4 October 2018 to test business continuity plans, including the IG plan. ! The Disaster Recovery day was attended by the Chief Information Officer (Deputy SIRO), the Data Protection Officer (Deputy Caldicott Guardian) and other members of the Informatics and Reporting teams. However, there was no active Board representation. ✓ Business continuity plans, which incorporate an emergency contact list, were reviewed and updated following the Disaster Recovery day. ! A hardcopy of the emergency contact list is not held. ✓ Processes in place to respond to a cyber-attack were considered as part of the Disaster Recovery day. Following agreement by the Information Governance Group, a separate record is now included on the CareCERT threat log of high severity alerts received from NHS Digital.	**Significant**	**0**	**0**	**2**
8.1 All software has been surveyed to understand if it is supported and up to date.	✓ SNOW asset management software is used by the Trust to identify all software in use at the Trust. The SNOW database is updated whenever a device connects to the network. ✓ The SNOW database is generally reviewed weekly e.g. to identify any software installed without admin rights.	**Significant**	**0**	**0**	**1**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
	! Microsoft Windows and Office updates are identified from the Microsoft update web-portals. However, for other applications there is no formal process to identify available updates and patches. ! Updates and patches are generally rolled out centrally when users connect devices to the network. However, updates to Adobe require update by individual users locally. ✓ The Trust is currently rolling out Windows ATP which will provide an additional line of defence against malware and virus activity. ✓ A small number of devices are used at remote sites with no local area network. These are set up, by exception, to pick up updates from user networks.				
9.3 All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them.	✓ The scope of IT penetration testing is routinely discussed and agreed with the Deputy SIRO. ✓ Cyber Essentials Plus IT penetration testing was undertaken in April/May 2018 by a CREST registered supplier. The Trust achieved Cyber Essentials certification. ✓ In February 2019 the Trust completed further Cyber Essentials Plus testing and undertook a separate IT Health Check. ✓ Cyber security updates are submitted to meetings of the Information Management Steering Group which is attended by the SIRO and Deputy SIRO. This includes details of action taken/being taken in relation to recommendations raised as a result of penetration testing undertaken.	**Significant**	**0**	**0**	**0**

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			Major	Moderate	Minor
10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance.	✓ IT suppliers responsible for data processing were identified by the Trust during GDPR readiness work. ✓ A documented due diligence exercise has been undertaken by the Data Protection Officer to confirm that the above IT suppliers are not included on the Information Commissioner's Office (ICO) Enforcement action list. ✓ Contracts with the above IT suppliers have been prepared using standard NHS Terms and Conditions for the Purchase and Supply of Goods and Services. These contracts include the NHS standard contract data security clause.	**Significant**	**0**	**0**	**0**
Overall		**Significant**	**0**	**0**	**6**

Background Information

The Data Security and Protection (DSP) Toolkit is the successor framework to the Information Governance Toolkit. It was developed by NHS Digital in response to The National Data Guardian's (NDG) Review of Data Security, Consent and Opt-Outs published in July 2016 and the Government's response published the following year.

The DSP Toolkit represents a key element of the Trust's Board Assurance Framework, providing an internal, self-assessed, position statement on compliance with the NDG Standards.

Under the General Conditions of the NHS Standard Contract (Clause 21.6): "The Provider must ensure that it's NHS Information Governance Toolkit (or any successor framework) submission is audited in accordance with Information Governance Audit Guidance where applicable. Organisations are required to have their toolkit submissions reviewed prior to submission, which is due by 31 March 2019.

As well as recommending that health and care organisations strengthen their data security arrangements, the NDG also identified the need to demonstrate effectiveness through enhanced internal data security audit and external validation. Accordingly, our audit approach considered the adequacy of the Trust's information governance arrangements, taking into account any indications of exposure to information risk, as well as the validity of the Toolkit submission.

Key Risks

Potential key risks associated with this area include:

- Non-compliance with the national DSP Framework, constituting a breach of the NHS England standard contract terms.
- Lack of accountability for data security and protection, resulting in failure to identify, communicate and implement standards.
- Failure to define and publicise expected behaviours.
- Poor quality data adversely impacting on delivery of healthcare and essential support services.
- Staff are not equipped to understand and deliver their obligations.
- Access to personal data is not controlled in accordance with legal and NHS guidelines.
- Repeat data breaches resulting from failure to address problem processes.
- Persistent vulnerability to Cyber-attacks against services.
- Failure to sustain critical business operations in the event of IT being unavailable.

- Failure to identify weaknesses in continuity plans.
- Risk owners are unaware of vulnerabilities and unable to make informed decisions about priorities for investment.
- Lack of approved strategy for protecting IT systems from cyber threats.
- IT suppliers are not held to account for protecting the personal confidential data they process.

Objectives & Scope

The objective of this audit was to provide assurance that the Trust has appropriate systems and processes in place to demonstrate compliance with the national Data Security and Protection (DSP) Framework, in accordance with DSP Toolkit requirements. The audit included a review of evidence for a sample of 14 requirements ('assertions') to support the claims made in the self-assessment.

In order to meet this objective, the audit focused on the following key control objectives (items 2-15 equate to the sample of Toolkit assertions selected for the year 2018-19):

1. The Trust has robust policies, systems and procedures for the timely completion and submission of the DSP Toolkit self-assessment
2. There is senior ownership of data security and protection within the organisation (Toolkit Assertion number 1.1)
3. There are clear data security and protection policies in place and these are understood by staff and available to the public (1.2)
4. Effective data quality controls are in place (1.7)
5. Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards (2.3)
6. Staff pass the data security and protection mandatory test (3.3)
7. Staff with specialist roles receive data security and protection training suitable to their role (3.4)
8. Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration (4.2)
9. Process reviews are held at least once per year (5.1)
10. Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses (6.4)
11. There is a continuity plan in place for data security incidents, and staff understand how to put this into action (7.1)
12. There is an effective annual test of the continuity plan for data security incidents (7.2)
13. All software has been surveyed to understand if it is supported and up to date (8.1)
14. All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them (9.3).
15. Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance (10.2).

Methodology

The objectives of this review were achieved by:

- Discussions with key staff to gain an understanding of the Trust's Toolkit self-assessment process.
- Review of the data security and protection management framework, policies and procedures in place.
- Testing a sample of 14 assertions and associated mandatory evidence items.
- Fieldwork will be undertaken to ensure controls are operating as expected, including:
  - Discussions and enquiries with relevant staff
  - Review of supporting documentation including sample job descriptions, incident reports, minutes of meetings and mandatory documentation of processing activities.

Limitations

The assurance given is based on the review work undertaken and is not necessarily a complete statement of all weaknesses that exist or potential improvements. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, no complete guarantee or warranty can be given with regard to the advice and information contained. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Report Circulation

Draft	Final	Recipient Name	Recipient Title
✓	✓	Dawn Hanwell	Deputy Chief Executive and Chi8ef Financial Officer (SIRO)
✓	✓	Bill Fawcett	Chief Information Officer
✓	✓	Carl Starbuck	Information and Knowledge Manager
	✓	Claire Kenwood	Medical Director (Caldicott Guardian)
	✓	Russell Hornshaw	Head of IT Service Delivery
	✓	Cath Hill	Associate Director for Corporate Governance

Acknowledgement

The auditor is grateful for the assistance received from management and staff during the course of this review. The following members of the Audit Yorkshire team were involved in the production of this report:

Head of Internal Audit:	Helen Kemp-Taylor
Audit Manager:	Sharron Blackburn
Senior Auditor:	John Roberts
Date:	27 March 2019

Finding	Risk	Recommendation	Priority	Management Response	Responsible Officer	Target Date
Process Reviews Information security breaches and near misses reported via DATIX are recorded on receipt. All breaches and near misses are investigated and this includes a review of associated processes as determined by root cause analysis where appropriate. However, the Trust does not have arrangements for in place for periodic proactive reviews to identify and improve processes for accessing and using systems and data which can be commonly be attributed to data security incidents and workarounds.	Repeat data breaches resulting from failure to address problem processes. The requirements of Data Security Standard 5.1 are not fully met.	1. The Trust identifies (e.g. from common themes) the processes for accessing and using systems and data which can be commonly attributed to data security incidents and workarounds. An effective procedure is established for a suitable multi-disciplinary forum to review a sample of these processes on a rolling basis each year to identify and improve processes so as to ensure they are robust and designed with end users in mind.	**Minor**	CS currently presents a quarterly report to the Trustwide Clinical Governance Group of breach incidents, including the identification of "hot spot" sites or breach "themes". To build on this by offering face-to-face time with teams where issues recur, to ensure that process mapping and root cause analysis is brought to bear to solve recurrent incidents themes, when common causes are identified.	Carl Starbuck, Information and Knowledge Manager	Next TWCGG attendance – 04/04/2019

Finding	Risk	Recommendation	Priority	Management Response	Responsible Officer	Target Date
Business Continuity Plan An IG Business Continuity Plan is in place which covers potential events such as major IT system failure, loss of IT network functionality, being unable to access usual base and absence of key personnel. However, data security incidents are not specifically featured. The IG Business Continuity Plan has not been formally approved and endorsed by the SIRO.	Failure to sustain critical business operations in the event of T being unavailable. The requirements of Data Security Standard 7.1 are not fully met.	2. The IG Business Continuity Plan is expanded to include data security content. 3. The IG Business Continuity Plan is formally approved and endorsed by the SIRO.	**Minor** **Minor**	CS to add this content to IG BC/DR plan. To hold blank template data logging spreadsheets which can be used on PC desktops in the event of system outages as a BC measure CS to have the SIRO endorse the revised plan.	Carl Starbuck, Information and Knowledge Manager Carl Starbuck, Information and Knowledge Manager	31/05/2019 31/05/2019
Business Continuity Plan Testing A Disaster Recovery day was held on 4 October 2018 to test business continuity plans, including the IG plan. The Disaster Recovery day was attended by the Chief Information Officer (Deputy SIRO), the Data Protection Officer (Deputy Caldicott Guardian) and other members of the Informatics and Reporting teams. However, there was no active Board representation.	Failure to identify weaknesses in continuity plans. The requirements of Data Security Standard 7.2 are not fully	4. Testing of Disaster Recovery arrangements, including Business Recovery Plans, include active Board representation. 5. A hardcopy of the emergency contact list is retained as required by Data Security Standard 7.2.	**Minor** **Minor**	BF to invite SIRO to participate in future BC/DR exercises. BF to ensure all members of the ICT Senior Management Team hold hard copies of the emergency	Bill Fawcett, Chief Information Officer Bill Fawcett, Chief Information Officer	31/05/2019 31/05/2019

Finding	Risk	Recommendation	Priority	Management Response	Responsible Officer	Target Date
Business continuity plans, which incorporate an emergency contact list, were reviewed and updated following the Disaster Recovery day. However, a hardcopy of the emergency contact list is not held as required by Data Security Standard 7.2.	met.			contact list, or alternatively hold the list via an off-network accessible medium (e.g. laptop desktop folder, smartphone document storage)		
Software Update/Patches Microsoft Windows and Office updates are identified from the Microsoft update web-portals. However, for other applications there is no formal process to identify available updates and patches. Updates and patches are generally rolled out centrally when users connect devices to the network. However, updates to Adobe require update by individual users locally.	Risk owners are unaware of vulnerabilities and are unable to make informed decisions about priorities for investment. The requirements of Data Security Standard 8.1 are not fully met.	6. A formal process is established which identifies available updates and patches in relation to software (other than Microsoft Windows and Office).	**Minor**	RH to develop an appropriate approach via the ICT engineering team and report this back to the IG Group.	Russell Hornshaw, Head of IT Service Delivery	31/05/2019

Audit Opinion

The following opinions provide management assurance in line with the following definitions:

Opinion Level	Opinion Definition	Guidance on Consistency
HIGH (STRONG)	High assurance can be given that there is a strong system of internal control which is designed and operating effectively to ensure that the system's objectives are met.	The system is well designed. The controls in the system are clear and the audit has been able to confirm that the system (if followed) would work effectively in practice. There are no significant flaws in the design of the system. Controls are operating effectively and consistently across the whole system. There are likely to be core controls fundamental to the effective operation of the system. A High opinion can only be given when the controls are working well across all core areas of the system. For example with 'Debtors' the controls over identifying income, raising debt, recording debt, managing debt, receiving debt, etc. are all working effectively – there are no serious concerns. Note this does not mean 100% compliance. There could be some minor issues relating to either systems design or operation which need to be addressed (and hence the report may include some recommendations) – however these issues do not have an impact on the overall effectiveness of the control system and the delivery of the system's objectives.
SIGNIFICANT (GOOD)	Significant assurance can be given that there is a good system of internal control which is designed and operating effectively to ensure that the system's objectives are met and that this is operating in the majority of core areas	The system is generally well designed - but there may be weaknesses in the design of the system that need to be addressed. In addition most core system controls are operating effectively – but some may not be. Whilst any weaknesses may be significant they are not thought likely to have a serious impact on the likelihood that the system's overall objectives will be delivered.
LIMITED (IMPROVEMENT REQUIRED)	Limited assurance can be given as whilst some elements of the system of internal control are operating, improvements are required in the system's design and/or operation in core areas to	The system is operating in part but there are notable control weaknesses. There are weaknesses in either design or operation of the system that may mean that core system objectives are not achieved. In terms of what differentiates a borderline Significant Opinion to a borderline Limited opinion – the main factors are the scale and potential impact of weaknesses found. Multiple weaknesses

	effectively meet the system's objectives	across a range of core areas would suggest a Limited Opinion level is applicable. However it also true that ONE weakness can suggest a Limited Opinion if it is fundamental enough to mean that a number of core system objectives will not be achieved.
LOW (WEAK)	Low assurance can be given as there is a weak system of internal control and significant improvement is required in its design and/or operation to effectively meet the system's objectives.	The audit has found that there are serious weaknesses in either design or operation that may mean that the overall system objectives will not be achieved and there are fundamental control weaknesses that need to be addressed. It should be borne in mind that Low Assurance is not 'No Assurance.' The key point here is that there is a good chance that the system may not be capable of delivering what it has been set up to deliver – either through poor systems design or multiple control weaknesses. The report will clearly state if 'No Assurance' is actually more applicable than low assurance.

Where limited or no assurance is given the management of the Trust must consider the impact of this upon their overall assurance framework and their Annual Governance Statement.

Priorities assigned to individual recommendations

Individual recommendations are graded in accordance with the severity of the risk involved to the Trust. Audit Yorkshire has a standard definition for each level of recommendation priority. This is represented in the table below:

Grading	Definition	Guidance on Consistency
Major (High)	Recommendations which seek to address those findings which could present a significant risk to the organisation with respect to organisation objectives, legal obligations, significant financial loss, reputation/publicity, regulatory/statutory requirements or service/business interruption.	These are recommendations which aim to address issues which if not addressed could cause significant damage or loss to the organisation. The expectation is that these recommendations would need to be taken as a matter of urgency. These recommendations should have a high corporate profile – with a clear implementation tracking process in place, overseen by the Board or a Board level committee.
Moderate (Medium)	Recommendations which seek to address those findings which could present a risk to the effectiveness, efficiency or proper functioning of the system but do not present a significant risk in terms of corporate risk.	These are recommendations which if not addressed could cause problems with the safe or effective operation of the system being reviewed. The recommendations should have appropriate profile within the division or business area in which the system being considered sits and some profile at Board /Audit Committee level also. These recommendations should be carefully tracked to ensure that action reduces the risks found
Minor (Low)	Recommendations which relate to issues which should be addressed for completeness or for improvement purposes rather than to mitigate significant risks to the organisation. (This includes routine/housekeeping issues)	All other recommendations fall into this category. This includes recommendations which further improve an already robust system and housekeeping type issues.