

NHS Lothian Internal Audit Report 2022/23 Information Sharing

Assurance Rating: **Significant Assurance**

Date: 03/04/2023

Final Report

Contents

The contacts in connection with this report are:

Emily Mayne
Director
T: 0141 223 0785
E: emily.j.mayne@uk.gt.com

Jamie Fraser
Internal Audit Assistant Manager
T: 0141 223 0886
E: jamie.a.fraser@uk.gt.com

1 Executive Summary

2 Management Action Plan

3 Appendices

Timetable

- Date closing meeting held: 23/02/2023
- Date draft report issued: 12/03/2023
- Date management comments received: 22/03/2023
- Date Final report issued:
- Date presented to Audit and Risk Committee: 17/04/2023

This report has been prepared solely for internal use as part of NHS Lothian's internal audit service. No part of this report should be made available, quoted or copied to any external party without Internal Audit's prior consent.

Executive Summary

Introduction

Information sharing, to meet the needs of people, practitioners and organisations, is essential to support Scotland's commitment to integrated, person-centred care, across adult and children's services. The Scottish Information Sharing Toolkit is an evolution of the former SASPI (Scottish Accord on the Sharing of Personal Information 2011) and the former Gold Standard in the direction of minimising personal and non-personal information risks across organisations. The toolkit applies to all public sector organisations, voluntary sector organisations and those private organisations contracted to deliver relevant services to the public sector and who provide services involving the health, education, safety, crime prevention and social wellbeing of people in Scotland.

The Caldicott Review 'To share or not to share' specified that, "The duty to share information can be as important as the duty to protect patient confidentiality". Health and social care professionals must have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles. They should be supported by the policies of their employers, regulators and professional bodies.

Any agreement for systematic sharing of information between different data controllers must be recorded in the format of an Information Sharing Agreement, regardless of the existence of an overarching memorandum of understanding. An Information Sharing Agreement sets out the common decision on the more contextual aspects of sharing.

Information can relate to patients, staff (including temporary staff), members of the public, or any other identifiable individual, however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

Scope

The objective of the audit was to evaluate the adequacy of internal controls in place around information sharing with third parties.

Through our planning work we identified the following potential risks which formed the basis of the audit work undertaken:

- There are no arrangements in place to support and promote information sharing for coordinated and integrated care, and staff are not provided with clear guidance on sharing information for care in an effective, secure and safe manner.
- There is a lack of guidance in place to inform staff of when to apply the Caldicott principles or GDPR principles in relation to information sharing resulting in staff being unable to resolve issues and / or conflicts that arise.

- There are no information sharing agreements / protocols in place between NHS Lothian and third party organisations for safe and secure sharing of information.
- Data Protection Impact Assessments are not conducted prior to entering into an information sharing agreement / protocol resulting in NHS Lothian not being aware of any risks or potential negative effects.

Approach

Our audit approach was as follows:

- Obtain understanding of the key areas outlined in scope above, through discussions with key personnel, review of management information and walkthrough test, where appropriate.
- Identify the key risks relevant within Information Sharing processes
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the controls in place.

It is Management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit should not be seen as a substitute for Management's responsibilities for the design and operation of these systems.

Acknowledgments

We would like to thank all staff consulted during this review for their assistance and cooperation

Limitations in Scope

Please note that our conclusion is limited by scope. It is limited to the risks outlined above. Other risks that exist in this process are out with the scope of this review and therefore our conclusion has not considered these risks. Where sample testing has been undertaken, our findings and conclusions are limited to the items selected for testing.

This report does not constitute an assurance engagement as set out under ISAE 3000.

Executive Summary

Summary of Findings

We have concluded that the controls in place in respect Information Sharing provide a **Significant** level of assurance. The table below provides a summary of the findings. The ratings assigned are based on the agreed internal audit rating scale (**Appendix 3**).

Detailed findings, recommendations and agreed management actions are found in Section 2 of this report.

Significant Assurance					
	HIGH	MEDIUM	LOW	ADVISORY	
	-	-	4	-	
Ref	Risk Area	H	M	L	A
1	There are no arrangements in place to support and promote information sharing for coordinated and integrated care, and staff are not provided with clear guidance on sharing information for care in an effective, secure and safe manner.	-	-	-	-
2	There is a lack of guidance in place to inform staff of when to apply the Caldicott principles or GDPR principles in relation to information sharing resulting in staff being unable to resolve any issues and/or conflicts that arise.	-	-	2	-
3	There are no information sharing agreements/protocols in place between NHS Lothian and third party organisations for safe and secure sharing of information.	-	-	2	-
4	Data Protection Impact Assessments are not conducted prior to entering into an information sharing agreement / protocol resulting in NHS Lothian not being aware of any risks or potential negative effects.	-	-	-	-
Total		-	-	4	-

Additionally, of our sample of 10 Data Sharing Agreements, we identified that seven were not in place before information was agreed to be shared with third party organisations. We were informed that the Board were requested to undertake projects by Scottish Government at short notice and therefore requires an agreement to be prepared retrospectively.

The review period for Data Protection Impact Assessments and Data Sharing Agreements is not always consistent or aligned. However, management noted that this is because the documents are not prepared at the same time and the level of risk associated with the data sharing agreement will also determine the frequency of review. At present, the review process is not documented within guidance documentation; however, with the Information Asset Register online app due to be released with a new review process, the guidance documentation could be updated to reflect this.

Areas of Good Practice

There is a Data Protection Policy and supporting guidance documentation in place that sets out the processes and legislation that should be followed by staff as well as their responsibilities of staff in relation to data protection and data sharing. Policy and guidance documentation is easily accessible on the staff intranet.

Staff receive appropriate training in the form of the mandatory Information Governance training modules as well as specific data protection and data sharing training delivered by the Information Governance and Data Protection Team. There are a number of training and guidance resources available for staff which Information Governance advertise and make available via their own Information Governance Intranet Page.

NHS Lothian makes use of Fairwarning, which is a monitoring system that tells the organisation who, where and when staff (including third party organisation) are inappropriately accessing or downloading information on to electronic devices and what kind of information. A number of reports are run routinely each month that capture any inappropriate access. These reports are reviewed by the Information Governance Project Manager responsible for the process within the Information Governance Team. The purpose of this review is to exclude from the reports any 'false positives'. After removing these "false positives" the remaining potentially inappropriate record access requires to be reviewed by the member of staffs' Service Directorate with the support of employee relations (ER) where required. Potentially inappropriate breaches identified at any of third party organisations that have entered into Data Sharing Agreements with NHS Lothian are forwarded to the agreed individuals within the employing body and NHS Lothian requires a report back after the investigation has concluded. NHS Lothian has the right to withdraw access to systems at any time.

Main Findings

Guidance documentation for Project Managers and Data Sharing were last updated in October 2022; however, there is no next review date recorded.

We identified that for a sample of Data Sharing Agreements, there was a corresponding Data Protection Impact Assessments in place. However, approval of these was not always appropriately recorded in the documents centrally held by the Information Governance team.

Executive Summary

Developments for 2023/24

The Information Governance team has developed an Information Asset Register app which will be used by staff to register information assets by completing an online form in the app. Information Asset Owners will be asked to attach any agreements in place such as a Data Protection Impact Assessment and Data Sharing Agreement. This will ensure that all documents are stored centrally in one place. A Power Automate Flow will be set up to email the asset responsible admin and asset owner as the asset nears its review date.

Follow Up

Approximately two weeks following issue of the final Internal Audit report, a member of the Audit Team will issue an 'evidence requirements' document for those reports where management actions have been agreed.

This document forms part of the follow up process and records what information should be provided to close off the management action.

The follow-up process is aligned with the meetings of the Board's Audit & Risk Committee. Audit Sponsors will be contacted on a quarterly basis with a request to provide the necessary evidence for those management actions that are likely to fall due before the next meeting of the Audit and Risk Committee.

Risk Area 3: There are no information sharing agreements/protocols in place between NHS Lothian and third party organisations for safe and secure sharing of information.

LOW

Finding 1 – Approval of Data Sharing Agreements and Data Protection Impact Assessments is not appropriately recorded

Control

NHS Lothian adhere to the national data sharing guidance as outlined in the Information Sharing Toolkit Scotland which includes a Data Sharing Agreement Template.

Project managers are required to complete Data Protection Impact Assessment and send this to IT Security using the e-Health Call Logging System once complete. IT Security completes a risk assessment and make recommendations, including whether a Data Sharing Agreement should be completed. If necessary, once a data sharing agreement has been completed, this is sent to the Data Protection Team using the e-Health Call Logging System.

The Data Protection team review the data sharing agreement and once agreed, they then request that the project team send the data sharing agreement to the other organisation(s) for their sign off, typically the Chief Executive Officer. Once signed off by all organisations, the data sharing agreements are submitted to the NHS Lothian Caldicott Guardian for review and sign off.

Observation

We performed sample testing to confirm that for 10 Data Sharing Agreements, there was an accompanying Data Protection Impact Assessment, the correct approvals were in place and that each document was up to date. Details of our sample testing can be found at **Appendix 2**. We identified the following was missing from the documentation we obtained:

- Six Data Sharing Agreements did not have the date of sign off documented
- Two Data Sharing Agreements did not have sign off documented
- Three Data Protection Impact Assessments did not have the Information Asset Owner sign off documented
- One Data Protection Impact Assessment did not have the date of the Information Asset Owner sign off documented

We did ascertain from management that the date of approval obtained from the required individuals for the Data Sharing Agreements and Data Protection Impact Assessments in our sample are recorded within the Register of Data Sharing Agreements held by the Information Governance team.

Additionally, we identified that seven of the Data Sharing Agreements in our sample were signed off after the commencement of information sharing. We were informed by management that the Board were requested to undertake projects by the Scottish Government at short notice which result in Data Protection Impact Assessments and Data Sharing Agreements being completed retrospectively.

Additionally, three Data Sharing Agreements were signed off by a previous Caldicott Guardian; however, we note that these agreements are not yet due for review and management agreed that the current Caldicott Guardian would be involved in reviewing these agreements.

At present, there is a lack of oversight within the Board governance structure of the organisation in relation to data sharing agreements and data protection impact assessments being developed retrospectively following the commencement of information sharing.

Risk

Information could be shared with third parties in an unsecure and inappropriate manner in the absence of appropriately approved data sharing agreements. A lack of oversight around appropriately authorised data sharing agreements may create a culture where inappropriate information sharing is accepted.

Recommendations

- 1) Authorisation of the Data Protection Impact Assessments and Data Sharing Agreements should be strengthened:
 - Management should ensure that sign off and date of sign off is recorded in the Data Protection Impact Assessments and Data Sharing Agreements.
 - For Data Sharing Agreements signed off by a previous Caldicott Guardian, these should be reviewed and signed by the current Caldicott Guardian at the next review of the document.
- 2) Management should ensure that, where possible, Data Protection Impact Assessments and Data Sharing Agreements are in place before information is shared with third party organisations. Management should introduce quarterly exception reporting to the Digital Portfolio Group which outlines any data sharing agreements and data protection impact assessments that were introduced retrospectively and the reason for this.

Management Response

Sign off correspondence is retained by the Caldicott Guardian office and has additional data including dates of data sharing. Sign off after commencement of sharing can be for a number of reasons. It may be a refreshed document, or the department sharing has not requested any assistance until after the event (e.g. a national programme). The auditor requests that this detail must be in one final document (as opposed to a suite of signed documents) and this is accepted.

Management Action

1. All departmental Data Protection Impact Assessments and Data Sharing Agreements must have sign off and date of sign off is recorded in the document.
2. As action 1 to retrospectively review and refresh as required existing Data Protection Impact Assessments and Data Sharing Agreements.
3. Any departmental Data Protection Impact Assessments and Data Sharing Agreements not signed by Department Information Asset Owner/3rd sector prior to sharing commencement will be reported as part of the Digital Portfolio Group standing agenda item for Information Governance compliance report (2 monthly).

Responsibility: Information Governance and Security Manager / Information Asset Owners

Target Date:
1. 30th April 2023
2. 31st December 2023
3. 30th April 2023

Risk Area 2: There is a lack of guidance in place to inform staff of when to apply the Caldicott principles or GDPR principles in relation to information sharing resulting in staff being unable to resolve any issues and/or conflicts that arise.

LOW

Finding 2 – Guidance documentation does not have next review dates recorded

Control

There is a Data Protection Policy and supporting Data Protection Impact Assessment and Data Sharing guidance as well as Project Manager guidance in place which has been shared with staff. These documents inform staff on how to share information for care in an effective, secure and safe manner. The guidance also provides staff with information on how to implement the Caldicott and GDPR principles.

Observation

We reviewed the above documents and have not identified anything that we need to bring to management’s attention. As part of our review of the Data Sharing Guidance and Project Managers Guidance we confirmed that they were last updated in October 2022. Policy and guidance documentation is subject to review every three years; however, neither document has a next review date recorded.

Risk

Without adequate version control including next review date, guidance documentation may not be updated resulting in staff utilising out of date guidance and following processes that are non-compliant with legislation.

Recommendation

Management should ensure that a next review date for guidance documentation is documented.

Management Response

Accepted

Management Action

Review dates on Data Sharing Guidance and Project Managers Guidance document will be reviewed and updated.

Responsibility: Information Governance and Security Manager

Target Date: 30th April 2023

Risk area 2: There is a lack of guidance in place to inform staff of when to apply the Caldicott principles or GDPR principles in relation to information sharing resulting in staff being unable to resolve any issues and/or conflicts that arise.

LOW

Finding 3 – Review period for Data Protection Impact Assessments and Data Sharing Agreements is not consistent or aligned

Control

Data Sharing Agreements and Data Protection Impact Assessments are reviewed at regular intervals by the Project Manager, Information Governance and Data Protection teams, Caldicott Guardian and third party organisations.

Observation

We ascertained through our sample testing that the Data Sharing Agreements and Data Protection Impact Assessments were up to date and had next review dates documented. However, the review period for Data Sharing Agreements and Data Protection Impact Assessments is not always consistent and the review dates are not aligned for review at the same time. However, management noted that the review periods are driven by the level of risk associated with the agreements and the length of time the agreement is to last, and so will not always be aligned. Additionally, Data Protection Impact Assessments are completed first and then a decision is made as to whether a Data Sharing Agreement is needed so the review dates would be not be in alignment.

The guidance documents also do not make reference to how often a review of the agreements should take place. The new Information Asset Register online app will require all documents for every project to be reviewed every 12 months by the Information Governance and Data Protection teams. Information Asset Owners will contact the asset owner to ask them to review the assets and documents. As such, the guidance documentation should include this new review process.

Recommendation

Management should ensure that following the implementation of the new Information Asset Register app, the guidance documentation for Data Protection Impact Assessments and Data Sharing is updated to reflect the review process for assessments and agreements in place.

Management Response

Review period/dates for Data Sharing Agreements and Data Protection Impact Assessments vary according to risk rating and project length so will not be standard. The new IAR app will automate reminders for review, but review currently takes place.

Management Action

As existing plan, the Information Asset Register App development to conclude, and will be implemented to assist automation of the existing process of document review.

Responsibility: Information Governance and Security Manager

Target Date: 31st August 2023

Appendix 1 – Staff Involved and Documents Reviewed

Staff Involved

- Information Governance and Security Manager
- Data Protection Manager
- Information Governance Project Manager
- Information Governance Project Officer

Documents Reviewed

- Data Protection Policy May 2022
- Data Protection Impact Assessment Guidance September 2022
- Data Sharing Guidance October 2022
- Project Managers Guidance October 2022
- Data Protection Impact Assessment Template
- Data Sharing Agreement Template
- Register of Data Sharing Agreements
- Information Governance Newsletters – Spring 2022, Summer 2022, Winter 2022
- Information Governance Training Strategy October 2022
- Information Governance Mandatory Training Completion Rates February 2023
- Information Asset Register guidance

Appendix 2 – Sample Testing Results

Sample No.	Third Party	Purpose of Agreement	Date of NHS L Approval Per Tracker	DSA In Place?	Approval Documented	DPIA In Place?	Approvals Documented	Next Review Date	Up to date?	Comments
1	NHS NSS	ISD access to and use of NHS Lothian workforce data	01/07/2018	Yes - June 2018	Yes	Yes - June 2022	No - Information Asset Owner sign off date is not documented.	DSA - 01/06/2025 DPIA - 01/06/2025	Yes	The Data Sharing Agreement in place was signed off by the previous Caldicott Guardian. DSA states that information sharing commenced from June 2017, however, DSA was not signed off until July 2018.
2	Independent Schools	Provision of school nurses	01/08/2019	Yes - March 2019	No - the date in which the Medical Director (Caldicott Guardian) signed the DSA is not documented	Yes - August 2019	No - Information Asset Owner sign off not documented	DSA - 01/04/2023 DPIA - 01/08/2023	Yes	The Data Sharing Agreement in place was signed off by the previous Caldicott Guardian. It is documented that the information sharing is for the period 1/4/2019 - 31/3/2021; however, the review date for the DSA is April 2023. This suggests that the current DSA has expired.
3	South East Payroll Services Programme	Creation of multi board payroll service	02/02/2023	Yes - version 2 February 2023	No - On the DSA the only approval documented is by the NHS Lothian Medical Director; however, no date is provided. No approval documented for the other health boards involved.	Yes - January 2023	Yes	DSA - 23/01/2025 DPIA - 23/01/2025	Yes	Accountable Officers for Public Health Scotland and Healthcare Improvement Scotland are not documented Senior Information Risk Owners for Public Health Scotland and NHS Fife are not documented.
4	Common Services Agency (NSS ISD), East Lothian Council and NHS Lothian	Support the care of Service Users accessing and receiving drug and alcohol treatment for Tier Three and Tier Four interventions through improved service planning and design, informed by improved information. The electronic system will be known as the Drug and Alcohol Information System "DAISy")	22/10/2019	Yes - 22/10/2019	No - approval by NSS ISD is not documented.	Yes - January 2021	Yes	DSA - no date documented DPIA - 01/10/2023	Yes	The Data Sharing Agreement in place was signed off by the previous Caldicott Guardian.
5	NHS Lothian, NHS Borders, NHS Dumfries & Galloway and NHS Fife	SCAN Chemocare	01/08/2020	Yes - 01/06/2020	No - approvals provided but the date of sign off for NHS Borders is not documented	Yes - 10/03/2020	Yes	DSA - 10/08/2023 DPIA - 21/04/2023	Yes	DSA states that information sharing commenced from 30 June 2020 however, DSA was not signed off until August 2020.

Appendix 2 – Sample Testing Results

Sample No	Third Party	Purpose of Agreement	Date of NHS L Approval Per Tracker	DSA In Place?	Approval Documented	DPIA In Place?	Approvals Documented	Next Review Date	Up to date?	Comments
6	Edinburgh Health and Social Care Partnership	Data sharing agreement governing the receipt and disclosure of personal or identifiable information on behalf of patients/people accessing NHS Lothian services and improve Opiate Substitution Therapy (OST) Service.	01/05/2021	Yes - 14/04/2021	No - approvals provided but the date of sign off is not documented	Yes - 27/04/2021	Yes	DSA - 27/04/2023 DPIA - 27/04/2023	Yes	The DSA has two next review dates: 19 March 2023 and 27 April 2023. DSA states that information sharing commenced from March 2021, however, DSA was not signed off until April/May 2021.
7	Chest, Heart, Stroke Scotland (CHSS)	The aim of the CHSS Long Covid Support Service is to improve the quality of life for people who are living with the long-term impact of the COVID-19 virus by providing a pathway of support and advice from a team of nurses and allied health professionals via the Charity's advice line.	17/12/2021	Yes - January 2021	No - the date in which the Medical Director (Caldicott Guardian) signed the DSA is not documented	Yes - January 2021	No - Information Asset Owner sign off not documented	DSA - 17/12/2023 DPIA - 17/12/2023	Yes	It took 12 months for DSA to be signed off. DSA states that information sharing commenced from January 2021 until terminated by either party; however, DSA was not signed off until December 2021.
8	Hepatitis C Trust	To enable Hep C Trust staff to deliver BBV dry blood spot testing (HIV, HBV, HCV) and for results from NHS Lothian virology lab to be sent to HEP C trust staff via NHS email account, for fast, secure results. To enable two-way referrals to be made between NHS Lothian and Hep C trust by NHS email for purposes of partnership working to provide patient care and support for people at risk of Hep C and diagnosed with Hep C.	01/05/2022	Yes - April 2022	Yes	Yes - March 2022	No - Information Asset Owner sign off not documented in the DPIA.	DSA - 22/04/2024 DPIA - 28/03/2024	Yes	DSA has two review dates: 28/03/2024 and 22/04/2024 DSA states that information sharing commenced from April 2022, however, DSA was not signed off until May 2022.
9	Cyrenians	Sharing data in relation to the out of hours treatment of LEAPs patients at Firhill Residential Respite centre.	14/09/2022	Yes - July 2022	Yes	Yes - June 2022	Yes	DSA - 01/07/2024 DPIA - 22/06/2024	Yes	DSA states that information sharing commenced from July 2022, however, DSA was not signed off until September 2022.
10	The Health Agency	Westerhaven Cancer Support (service provided by The Health Agency) in relation to Improving the Cancer Journey	01/08/2022	Yes - June 2022	Yes	Yes	Yes	DSA - 01/06/2024 DPIA - 28/07/2024	Yes	DSA states that information sharing commenced from Will commence October 2021 and will end October 2025; however, DSA was not signed off until August 2022.

Appendix 3 – Our IA Report assurance levels

The table below shows the levels of assurance we provide and guidelines for how these are arrived at. We always exercise professional judgement in determining assignment assurance levels, reflective of the circumstances of each individual assignment.

Rating	Definition	When Internal Audit will award this level
Significant assurance	<p>The Board can take reasonable assurance that the system(s) of control achieves or will achieve the control objective.</p> <p>There may be an insignificant amount of residual risk or none at all.</p>	<p>There is little evidence of system failure and the system appears to be robust and sustainable. The controls adequately mitigate the risk, or weaknesses are only minor (for instance a low number of findings which are all rated as 'low' or no findings)</p>
Moderate Assurance	<p>The Board can take reasonable assurance that controls upon which the organisation relies to achieve the control objective are in the main suitably designed and effectively applied.</p> <p>There remains a moderate amount of residual risk.</p>	<p>In most respects the "purpose" is being achieved. There are some areas where further action is required, and the residual risk is greater than "insignificant".</p> <p>The controls are largely effective and in most respects achieve their purpose with a limited number of findings which require management action (for instance a mix of 'medium' findings and 'low' findings)</p>
Limited Assurance	<p>The Board can take some assurance from the systems of control in place to achieve the control objective, but there remains a significant amount of residual risk which requires action to be taken.</p>	<p>This may be used when:</p> <ul style="list-style-type: none"> There are known material weaknesses in key control areas. It is known that there will have to be changes that are relevant to the control objective (e.g. due to a change in the law) and the impact has not been assessed and planned for. <p>The controls are deficient in some aspects and require management action (for instance one 'high' finding and a number of other lower rated findings)</p>
No assurance	<p>The Board cannot take any assurance from the audit findings. There remains a significant amount of residual risk.</p>	<p>The controls are not adequately designed and / or operating effectively and immediate management action is required as there remains a significant amount of residual risk (for instance one Critical finding or a number of High findings)</p>

Appendix 3 – Continued

The table below describes how we grade our audit recommendations based on risks

Rating	Description	Possible features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in the design or application of activities or control that requires the immediate attention of management	<ul style="list-style-type: none"> ▪ Key activity or control not designed or operating effectively ▪ Potential for fraud identified ▪ Non-compliance with key procedures / standards ▪ Non-compliance with regulation
Medium	Findings that are important to the management of risk in the business area, representing a moderate weakness in the design or application of activities or control that requires the immediate attention of management	<ul style="list-style-type: none"> ▪ Important activity or control not designed or operating effectively ▪ Impact is contained within the department and compensating controls would detect errors ▪ Possibility for fraud exists ▪ Control failures identified but not in key controls ▪ Non-compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures, or which identify changes that could improve the efficiency and/or effectiveness of the activity or control but which are not vital to the management of risk in the business area.	<ul style="list-style-type: none"> ▪ Minor control design or operational weakness ▪ Minor non-compliance with procedures / standards
Advisory	Items requiring no action but which may be of interest to management or which represent best practice advice	<ul style="list-style-type: none"> ▪ Information for management ▪ Control operating but not necessarily in accordance with best practice

