Edinburgh Integration Joint Board

Internal Audit Report

Cyber Resilience

19 February 2026

EIJB2501

Overall Assessment	Advisory

Contents

This internal audit review is conducted for the Edinburgh Integration Joint Board under the auspices of the 2025/26 internal audit plan approved by the Audit and Assurance Committee in March 2025. The review is designed to help the Edinburgh Integration Joint Board assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Global Internal Audit Standards (UK Public Sector) and as a result is not designed or intended to comply with any other auditing standards.

Where recommendations are included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the Edinburgh Integration Joint Board of the issues and weaknesses arising from this audit does not absolve management of this responsibility.

Executive Summary

Overall opinion and summary of findings

Recent high-profile cyber incidents affecting Scottish public bodies including NHS Dumfries and Galloway and Comhairle nan Eilean Siar have demonstrated the severe operational disruption, data compromise, and prolonged recovery periods that can result from cyberattacks. These events highlight the critical importance for Integration Joint Boards (IJBs) to seek robust and ongoing assurance on cyber resilience from their partners.

The Edinburgh Integration Joint Board (EIJB) does not own or operate its own IT systems, but is instead dependent on the Council and NHS Lothian IT infrastructure, and the robustness of partner cyber security and resilience arrangements.

As a Category 1 responder under the Civil Contingencies Act 2004, the EIJB must ensure that it has taken reasonable steps to assure itself that the partner systems it relies on are resilient and that the continuity of EIJB functions is protected.

This review identified areas in the EIJB's cyber resilience assurance arrangements, which could impact ability to maintain delivery of key functions and protect sensitive data during a cyber incident. The recommendations aim to strengthen assurance:

- developing a Cyber Strategy to define the EIJB's strategic objectives for cyber resilience aligned to its responsibilities under the Civil Contingencies Act
- enhancing assurance and scrutiny by introducing regular reporting to the EIJB on partner cyber resilience arrangements including testing outcomes, incident updates, and overall preparedness
- clarifying roles and responsibilities through an expanded Memorandum of Understanding (MoU) to cover tri-party cybersecurity responsibilities across the EIJB and its partners
- embedding cyber risk management by including a cybersecurity risk in the EIJB risk register to increase visibility and support proactive mitigation planning.

Areas of good practice identified

- arrangements for information sharing and processing for the EIJB, the Council, and NHS Lothian, are set out in an MoU, which has documented the security measures for protecting personal data
- cyber risks are included in the risk registers for the Council, the Edinburgh Health and Social Care Partnership (EHSCP) and NHS Lothian, with mitigating actions routinely reviewed
- the EHSCP risk register is routinely reviewed by the EIJB Audit and Assurance Committee.

Audit Assessment

Audit Area	Control Design	Control Operation	Observations	Priority Rating
1. Governance and Accountability			1 – EIJB Cyber Strategy	1
2. Oversight and Assurance			2 – Assurance on Partner Cyber Resilience Arrangements	1
3. Information Governance			3 – Cyber Resilience Roles and Responsibilities	2
4. Risk Management			4 – Identifying and Mitigating Cyber Risks	2

See Appendix 1 for Control Assessment and Priority Rating Definitions

Background and scope

The legislation which underpins integration is the Public Bodies (Joint Working) (Scotland) Act 2014. The Act places a duty on Health Boards and Local Authorities to enter into arrangements to delegate functions and appropriate resources, ensuring the effective delivery of health and social care services. In line with the requirements set out in the Integration Scheme, the Edinburgh Integration Joint Board (EIJB) relies on its partners, the City of Edinburgh Council (the Council) and NHS Lothian (NHSL), to provide an array of professional, technical, and administrative support services including ICT infrastructure and related support

The National Institute of Standards and Technology (NIST) defines cybersecurity as "The ability to protect or defend the use of cyberspace from cyberattacks." Cybersecurity is a subset of overarching information security, which NIST defines as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." Effective cyber resilience strengthens the overall control environment and protects information assets from unauthorised access, disruption, alteration, or destruction.

Cyber resilience is a critical risk for public bodies, particularly those delivering essential health and social care services. The EIJB is a Category 1 responder under the Civil Contingencies Act 2004, and a cyber-attack is one of the most serious risks to the delivery of services delegated to the EIJB, with a reliance on assurance from its partners. This includes gaining assurance from its partners on the implementation of effective business continuity arrangements.

Recent incidents affecting local authorities and NHS Boards

High profile incidents at NHS Dumfries and Galloway, and Comhairle nan Eilean Siar, have demonstrated the scale of operational disruption and data loss that can result from sophisticated cyber-attacks. Both cases involved significant systems outage, loss of access to core data, and the compromise of sensitive personal information, with long recovery periods and substantial impacts on service delivery.

The recovery from the Comhairle nan Eilean Siar cyber-attack has taken substantial resources to implement and placed considerable pressure on staff over a sustained period. There are still systems which are not fully rebuilt almost two years on from the attack.

For an IJB, these incidents highlight the importance of receiving robust and ongoing assurance from its partners, the Council and NHS Lothian, on the robustness of their cyber security and business continuity arrangements and ability to protect health and social care data.

Scope

As this is an emerging area of risk for the EIJB, this advisory review sought to review the EIJB's arrangements for obtaining assurance over the delivery of key functions and services and the protection of data, despite adverse cyber security incidents, and includes assurances provided by the EIJB's partners.

Alignment to EIJB Risks

- the EIJB is unable to operate effectively as a public body
- the EIJB has insufficient assurance from assurance providers to support effective delivery of scrutiny responsibilities
- the EIJB does not comply with the necessary legislative and regulatory requirements.

Limitations of Scope

The audit did not consider the operational cyber resilience controls managed by the Council and NHS Lothian, as the audit scope focused on the assurance the EIJB requests and is provided by these partners.

Reporting Date

Audit work concluded on 4 February 2026, and audit findings and opinions are based on the conclusion of work as at that date.

Observations and Management Actions

Observation 1 – EIJB Cyber Strategy

Priority Rating	1

In January 2021, the Scottish Government published its response to the consultation to include Integration Joint Boards and Category 1 Responders under the Civil Contingencies Act 2004 (the Act). This concluded that there were neither clear equality, operational nor strategic planning barriers to progressing the proposal and legislating for IJB inclusion within the Act. Consequently, the EIJB is required under the Act to put in place business continuity arrangements which, within the sphere of cyber resilience, would necessitate a cybersecurity strategy designed to ensure system resilience and the protection of sensitive and personal data.

The EIJB does not have a cybersecurity strategy in place. As such, the EIJB has not formally considered its strategic objectives around cyber resilience, and how it can ensure that there are adequate processes in place that can prevent, detect, and recover from cyber-attacks.

Risks

Regulatory

- records and personal information are vulnerable to theft, misuse, or accidental disclosure
- there is an increased risk of breaches of legal obligations, leading to penalties and loss of public trust.

Strategic

- cyber incidents can halt critical health and social care services, directly impacting patient safety and the ability to deliver integrated care
- the EIJB may be slower to detect, respond, and recover from cyber-attacks.

Recommendations and Management Actions: EIJB Cyber Strategy

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
1.1	An EIJB cyber strategy should be developed to reflect the EIJB's responsibilities under the Civil Contingencies Act including consideration of the following: • setting out a clear strategic intent that cyber resilience and a commitment to maintaining delivery of health and social care services and protecting sensitive and personal data is a priority • information on ICT infrastructure arrangements including reliance on partners assurance that emergency and major incident plans that include	HSCP officers will work collaboratively with partner digital teams to develop an EIJB cyber strategy.	Chief Officer, EIJB	Head of Strategic Change	31/01/2027

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
	cyber scenarios impacting EIJB delegated services are in place • partner roles in contributing to risk assessments that include cyber threats to health and social care services • reference to partner arrangements for business continuity planning, business impact analysis and testing arrangements for plans • arrangements for EIJB assurance and scrutiny of partner cyber resilience arrangements (as per Observation 2) • formal agreement on roles and responsibilities including the Memorandum of Understanding (MoU) (as per Observation 3) • cyber training and development needs for EIJB members (see recommendation 2.3) • EIJB risk management arrangements for cyber security including risk assessment and escalation protocols (as per Observation 4) • lessons learned arrangements following an incident affecting partner systems which impact delivery of EIJB functions.				

Observation 2 – Assurance on Partner Cyber Resilience Arrangements

Priority Rating	1

The EIJB does not own any IT systems directly, but instead relies on its partners' ICT infrastructure, governance frameworks, and incident response capabilities. Therefore, weaknesses or vulnerabilities within either organisation could directly affect the continuity and safety of integrated services.

Given the increasing frequency and complexity of cyber-attacks across the public sector, the EIJB should have clear visibility of each partner's preparedness, resilience plans, testing regimes, and assurance that lessons are learned from national and local cyber incidents. For example, in the case of the incident at Comhairle nan Eilean Siar, the post-incident review noted that prior to the attack there had been known weaknesses in the Council's IT infrastructure, cyber governance, incident response, and disaster recovery arrangements – vulnerabilities that had not been remediated.

In November 2025, the Accounts Commission published a Section 102 report on the significant cyber-attack on Comhairle nan Eilean Siar in November 2023 which highlighted the following:

- local systems were used instead of using cloud-based resources
- there was a lack of robust back-ups
- cyber recovery exercises were not performed regularly
- inconsistent application of business continuity planning
- IT resource issues
- no clear oversight of IT risks
- no formal communications strategy.

A summary of the lessons for IJBs in relation to the S102 report findings is provided in Appendix 3.

IJBs should exercise due diligence to ensure they gain sufficient assurance that partners maintain effective controls over business continuity, recovery and data protection, and lessons are learned from high-profile incidents and key issues highlighted.

While the EHSCP's risk register, which contains cyber risks, is regularly reviewed by the EIJB's Audit and Assurance Committee, there are no established arrangements to ensure the EIJB is provided with regular assurance on its partners' cyber resilience arrangements. Previous audit work for partners confirms that they do have established arrangements, however no reporting on the completeness and robustness of these is requested or provided to the EIJB.

In addition, it is important that Board members have sufficient understanding of cyber resilience to ensure accountability of partners, enable effective scrutiny through informed and challenging questions, and to recognise when reports on such matters are high-level or provide insufficient detail.

Induction learning for EIJB members includes cybersecurity materials. However, these materials are not of the depth required for the effective oversight and governance of cybersecurity activities.

Risks

Regulatory

- the IJB is not provided assurance that partner IT systems and cyber resilience arrangements meet required standards, and that the impact to delivery of health and social care services will be minimised during an incident
- weak governance and false confidence in a high-risk area due to generic training which does not reflect the complexity of partner ICT infrastructure arrangement and risks, and an over-reliance on officer judgement.

Recommendations and Management Actions: Assurance on Partner Cyber Resilience Arrangements

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
2.1	The EIJB should request regular assurance (e.g. annually) from its partners on the robustness of their cyber resilience arrangements including preparedness, resilience plans, testing regimes, and lessons learned from national and local incidents, to gain understanding and assurance of how each partner would respond to a cyber incident that could disrupt delivery of health and social care services or compromise sensitive or personal data. The assurance should consider shared or interdependent systems such as finance, care management, payroll and telephony systems hosted or supported by partners, and provide sufficient assurance that the EIJB is discharging its responsibilities under the Civil Contingencies Act.	HSCP officers will request that partners provide assurance to the EIJB on an annual basis in relation to cyber resilience arrangements.	Chief Officer, EIJB	Head of Strategic Change	31/01/2027
2.2	In line with recommendation 2.1, following reporting on each partner's cyber resilience arrangements, any issues that require corrective actions by partners should be recorded in an action tracker, with the responsible officers and timescales for completion clearly stated.	HSCP officers will request that partners provide assurance to the EIJB on an annual basis in relation to cyber resilience arrangements. A tracker will be implemented which will set out responsible officers and timescales.	Chief Officer, EIJB	Governance and Business Manager	31/03/2027
2.3	Training needs assessments for EIJB members should consider member knowledge and confidence related to cyber resilience, including Category 1 responder responsibilities, the EIJB Cyber Strategy, and assurance arrangements.	Board member understanding of cyber resilience will be picked up as part of the Board training needs analysis.	Chief Officer, EIJB	Governance and Business Manager	31/01/2027

Observation 3 – Cyber Resilience Roles and Responsibilities

Priority Rating	2

Section 11 of the Edinburgh IJB Integration Scheme states that arrangements for the sharing and joint processing of information among the Council, NHS Lothian, and the EIJB are set out in a Memorandum of Understanding (MoU), which is designed to promote and support appropriate information governance for the integration of health and social care services.

The MoU states that NHS Lothian and the Council retain Data Controller responsibility in relation to the processing of personal data for delegated functions. The MoU is focused on the management of personal data and does not cover protection of systems and the cyber resilience responsibilities of the EIJB and its partners.

A tri-party MoU for cyber security and data would provide clarity on responsibilities, expectations, and coordinated actions for protecting systems, data, and service continuity.

In addition, although the Integration Scheme states that the MoU should be periodically reviewed, the current version is dated 2018 and does not state when it will next be reviewed.

Risks

Strategic

- without clearly stated and agreed roles and responsibilities, the EIJB cannot be assured that its cyber risks are being fully considered.

Recommendations and Management Actions: Cyber Resilience Roles and Responsibilities

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
3.1	The EIJB should review the MoU to ensure it provides a tri-party understanding of cyber resilience responsibilities, expectations, and coordinated actions for protecting systems, data, and service continuity. Best practice on what the MoU could aim to cover includes: • purpose and scope, and a shared aim to protect the confidentiality, integrity, and availability of all systems and data • the services, datasets, ICT infrastructure, and functions covered by the agreement • clear roles and responsibilities on cyber security and resilience duties including infrastructure,	HSCP officers will work collaboratively with partners to set out cyber resilience responsibilities as part of the MoU or as a separate operational document.	Chief Officer, EIJB	Head of Strategic Change	31/03/2027

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
	patching schedules, and vulnerability management. Once updated, the MoU should be reviewed at least every 3 years or following a local or national incident or change in required standards.				

Observation 4 – Identifying and Mitigating Cyber Risks

Priority Rating	2

Risk management enables risks to objectives to be identified, recorded, and managed. This provides greater assurance that objectives are achieved on an ongoing basis.

The EIJB's risk register does not contain any specific risk on cybersecurity. However, both the EHSCP and NHS Lothian maintain risk registers which include risks relating to cybersecurity, for example:

- HSCP - under Section 6 Resilience and Business Continuity, risk 6.1 has recorded 'there is a risk that the partnership is not able to respond effectively to a resilience incident'. Activity taken to address this risk includes implementing actions arising from cybersecurity audits alongside resilience processes in place, and routinely tested
- NHS Lothian – risk 5322 of the Corporate Risk Register has recorded the risk of cyber-attacks on clinical and business critical systems, alongside the mitigating controls in place. In addition, in November 2025 the NHS Lothian Audit and Risk Committee considered a cybersecurity risk assurance report.

Also, the Council's Internal Audit team reported on Directorates Cyber Incident Response in October 2024, and Organisational Resilience in October 2025.

The EHSCP's risk register is regularly reviewed by the EIJB Audit and Assurance Committee.

Risks

Strategic

- cybersecurity risks are not identified, captured and recorded, and mitigations are not put in place to avoid or reduce the impact of risks.

Recommendations and Management Actions: Identifying and Mitigating Cyber Risks

Ref.	Recommendation	Agreed Management Action	Action Owner	Lead Officers	Timeframe
4.1	The EIJB should consider including a specific cybersecurity risk in its risk register. Review of the risks should include the issues set out in this report in relation to: • the overall EIJB cyber strategy • assurance and scrutiny of partner cyber resilience arrangements • cyber resilience roles and responsibilities.	Officers will ensure the risks relating to cyber are fully articulated within the EIJB risk register.	Chief Officer, EIJB	Governance and Business Manager	31/07/2026

Appendix 1 – Control Assessment and Priority Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed		Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory		Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity		Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity		Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	**N/A**	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Rating	Suggested timescale for remediation
Priority 1	The action to address the identified gap should be treated as a priority and implemented within 3-6 months.
Priority 2	The action to address the identified gap is important to implement but not as urgent in respect of timelines and should be implemented within 6-12 months.
Priority 3	The action to address the identified gap is relatively less important and should be implemented by a defined date when time and resources allow.

Appendix 2 – Areas of Audit Focus and Control Objectives

Audit Areas	Control Objectives
Governance and Accountability	• cybersecurity strategy and objectives have been established and agreed by the EIJB, and they are periodically updated and approved by the EIJB • the strategy and objectives cover all necessary aspects of cybersecurity, and include reference to relevant guidance and legislation • roles and responsibilities of the partner organisations have been clearly defined.
Oversight, Assurance, and Audit	• cyber security information required by the EIJB has been clearly stated, including what will be provided, when, and how frequently • cybersecurity information is provided to the EIJB in line with its requirements, and allows the EIJB to have effective oversight of the work performed, perceived threats, and actions being taken to mitigate them • issues identified are clearly stated in an action tracker, together with responsible officers and implementation dates, with the tracker being regularly provided to the EIJB • assurance mechanisms are in place to regularly assess the cyber security arrangement of partner organisations, with reporting on this being provided to the EIJB • a cyber assurance map been developed to identify assurance sources and gaps • EIJB members receive cyber resilience training where relevant in order to provide effective oversight.
Information Governance and Data Protection	• data ownership and protection responsibilities of partner organisations have been clearly defined • there is reporting to the EIJB on any data breaches or near misses.
Risk Management	• risks related to cybersecurity are identified, recorded and managed within the EIJB risk register, and regularly reviewed to ensure appropriate mitigating actions are in place and remain effective, with referrals to the partner organisations made where relevant.

Appendix 3 – Relevant Section 102 Report Findings

1. Cyber Resilience of Partner Systems

Finding: Many systems were hosted locally so were more vulnerable than cloud-based systems. Backups stored at the disaster recovery site were not sufficiently robust.

Where the IJB should seek assurance:

- confirm that both the Council and NHS Board use resilient, cloud-based or hybrid infrastructure
- seek evidence of robust, tested backup and recovery arrangements, including air-gapped backups.

2. Preparedness and Testing

Finding: Cyber and disaster recovery exercises were conducted on an ad hoc basis. A Cyber Incident Response Plan and Disaster Recovery Plan had not been finalised.

Where the IJB should seek assurance:

- request confirmation from partners that cyber incident and disaster recovery plans are in place, approved, and tested
- ensure joint exercises are conducted, especially where systems or services are shared.

3. Business Continuity Planning (BCP)

Finding: The application of the BCP was inconsistent across departments. Departmental BCPs were not used, as the scale of the attack exceeded anticipated scenarios.

Where the IJB should seek assurance:

- seek assurance that departmental BCPs are aligned with corporate plans and include cyber scenarios
- confirm that manual workarounds for critical services (e.g. payroll, care delivery) are documented and tested.

4. Staff Capacity and Training

Finding: 30% of IT positions were vacant. Information security training had lapsed, and uptake was not monitored.

Where the IJB should seek assurance:

- seek assurance that both partners have sufficient IT staffing to support cyber resilience
- confirm that mandatory cyber training is up-to-date, with monitored completion rates.

5. Governance and Risk Oversight

Finding: The risk register lacked key information such as timescales and responsible officers. There was no clear committee responsibility for oversight of IT risks.

Where the IJB should seek assurance:

- ensure that cyber risks are included in the IJB's strategic risk register
- confirm that partner organisations have clear governance structures for cyber risk, with regular reporting to the IJB.

6. Communication and Incident Coordination

Finding: There was no formal communications strategy for disaster-related events. Internal communications were more sporadic.

Where the IJB should seek assurance

- request a joint communications protocol for cyber incidents, including how the IJB will be informed and involved
- ensure clear lines of communication with service users and staff during disruptions.