# Internal Audit Report

# Security Arrangements for Publicly Accessed Council Premises

September 2024 – updated May 2025

CD2406

| | |
|---|---|
| **Overall Assessment** | **Limited Assurance** |

# Contents

Executive Summary .....3
Background and scope.....4
Findings and Management Action Plan.....5
Appendix 1 – Control Assessment and Assurance Definitions.....17
Appendix 2 – Areas of Audit Focus and Control Objectives.....18

This Internal Audit review was conducted for the City of Edinburgh Council under the auspices of the 2024/25 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2024. The review is designed to help the City of Edinburgh Council 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 Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations 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 City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings have been raised with senior management and elected members as appropriate.

# Executive Summary

| Overall Assessment | Limited Assurance |
|---|---|

## Overall opinion and summary of findings

Review of security arrangements for publicly accessed Council premises has highlighted that while there are arrangements in place to manage physical premises security, there are significant design and operating effectiveness gaps in the policies, procedures and controls.

The following improvements are required to effectively manage the security risks faced at individual properties and across the estate:

- policy and procedures should be agreed and documented, and training provided to Duty Holders to ensure they are equipped with the necessary skills and knowledge to perform their duties
- a process to centrally record and monitor security incidents is required to ensure the risk profile across the estate is understood
- actions from reviews performed by the Security Manager should be tracked to ensure issues are addressed
- budgetary responsibility and authorisation for security related works should be agreed
- risks associated with premises security should be identified, recorded, assessed, and managed in line with the Council's Risk Management Framework.

## Areas of good practice

- Duty Holders visited during the audit were knowledgeable on the security issues they faced based on historical incidents, outstanding requests/ repairs, and funding barriers
- the list of premises Duty Holders was up-to-date, with all named responsible officers sampled still in post, and all properties visited had a Duty Holder assigned.

## Phased Implementation

Recognising the need to establish a coordinated and consistent approach to managing security of premises across the Council, a phased implementation approach was adopted to ensure that detailed management actions which address the findings and recommendations were developed. These management actions and implementation dates have now been provided, and included in this report.

## Audit Assessment

| Audit Area | Control Design | Control Operation | Findings | Priority Rating |
|---|---|---|---|---|
| 1. Policies and procedures for publicly accessed Council premises |  | N/A | Finding 1 – Security policy, procedures, and training | High Priority |
| 2. Central security arrangements for publicly accessed Council premises |  |  | Finding 3 – Security reviews and recommendations | Medium Priority |
| | | | Finding 4 – Security budgets for publicly accessed Council premises | High Priority |
| 3. Local security arrangements for publicly accessed Council premises |  |  | Finding 2 – Recording & management of incidents and works | High Priority |
| 4. Risk management - publicly accessed Council premises |  | N/A | Finding 5 – Security risk management | High Priority |



See Appendix 1 for Control Assessment and Assurance Definitions

# Background and scope

The City of Edinburgh Council (the Council) has a duty of care to ensure the security and protection of their communities, employees, public buildings, and assets. Ensuring Council publicly accessed Council premises are secure is essential to safeguarding the Council from data breaches, emergency incidents, criminal activity, and anti-social behaviours. Security is also essential for the health and safety of both employees and visitors to Council premises.

The Council is responsible for a diverse range of publicly accessed Council premises with varying ages, conditions, and uses. This requires the security of individual properties to be considered on a case-by-case basis. There are currently no overarching policies and procedures covering security arrangements at Council premises. Additionally, external facilities management contractors are responsible for some security aspects of PPP contracted schools.

The Terrorism (Protection of Premises) draft bill (known as Martyn's Law) which aims to ensure public premises and events are better prepared for, and protected from, terrorist attacks is currently in draft and consultation by the UK Government. This legislation will likely require Council to mitigate the impact of a terrorist attack and reduce harm, by taking steps according to building or event capacity. Following the conclusion of the consultation process, the Government will introduce the Bill to Parliament as soon as parliamentary time allows and it is expected to require a detailed understanding of the current state of security across the Council's estate, as well as new controls to be designed and implemented to ensure the Council meets its statutory obligations once known.

## Scope

The objective of this review was to assess the adequacy of design and operating effectiveness of the key controls established to ensure the Council effectively manages physical and building security for publicly accessed Council premises.

## Alignment to Risks and Business Plan Outcomes

The review also assesses the assurance level in relation to the following Corporate Leadership Team risks:

- Health and Safety (including public safety)
- Regulatory and Legislative Compliance
- Financial and Budget Management
- Property
- Resilience
- People
- Reputational Risk.

Business Plan Outcomes:

- Edinburgh is a cleaner, better maintained city that we can all be proud of.

## Limitations of Scope

The following areas were excluded from scope:

- a detailed review of CCTV arrangements
- resilience arrangements
- fire and flood threats.

## Reporting Date

Testing was undertaken between 24 June 2024 and 15 August 2024. Audit work concluded on 15 August 2024, and audit findings and opinion are based on the conclusion of work as at that date.

An initial report detailing the findings, recommendations and the proposed phased implementation approach was presented to the Governance, Risk and Best Value Committee (GRBV) in October 2024. A copy of the full audit report with agreed management actions was re-presented to GRBV in June 2025.

# Findings and Management Action Plan

## Finding 1 – Security policy, procedures, and training

| Finding Rating | High Priority |
|---|---|

The Council's Corporate Property Strategy, approved in August 2023, aims to create a property estate which: is future proofed, leads to operational and resource efficiencies, maximises the use of assets to deliver Council policies, complies with health and safety and other regulatory requirements, and takes a balanced view of costs and benefits in each business case for change, amongst other aims. This presents an opportunity to embed publicly accessed Council premises security into policies, procedures, and decision making.

The following gaps which may impact the effectiveness of security related policies, procedures, and training have been identified:

**Overarching Security Policy**

There is no overarching Council security policy setting out the wider roles, responsibilities, budgetary authorities, governance, inter-dependencies, escalation processes, and relevant legislation for colleagues across the Council who are responsible for the physical security of publicly accessed Council premises. As a result, the approach to security is siloed, with limited collaborative working between the various teams who are stakeholders in building security.

**FM Security Team Policy and Operating Procedures**

A draft Security Policy was created by the FM Security Team in line with the requirements of the SLA in October 2021, aimed at defining the roles and responsibilities of the FM Security Team. However, this document was not finalised and approved, and supporting standard operating procedures were not documented.

**Duty Holder Procedures**

Health and Safety Duty Holders are responsible for undertaking statutory health and safety duties in addition to their normal managerial roles, as well as identifying, assessing, and controlling health, safety and welfare risks under their management. They are also responsible for the security of each premises and designing controls to manage security as it relates to their building.

There are no standard operating procedures or guidance documents available to assist Duty Holders in undertaking their security duties. There is a Health and Safety Duty Holder Guidance document, but this does not refer to security. Missing processes include routine review of the state of physical security at each premises, performing security risk assessments, reporting security incidents, and escalating security concerns.

**Duty Holder Training**

There is no training provision to inform Duty Holders undertaking their security responsibilities. Basic security training (including free resources where available) should be included in Duty Holder essential learning requirements.

**Property and Facilities Management Service Level Agreement (SLA)**

The Property and Facilities Management SLA sets out the objectives, services provided, key deliverables and approach to the provision of physical security services by the FM Security Team. However, the current version of the SLA is dated 2018 and therefore may require review to ensure it remains appropriate.

### Risks

- **Regulatory and Legislative Compliance –** legal action or fines for failing to protect premises adequately, including breaches in data protection or health and safety legislation
- **Reputational Risk -** adverse publicity resulting from security breaches and incidents
- **Health and Safety (including public safety) -** lack of policy and guidance relating to the security of premises and ensuring adequate consideration of health and safety including public safety
- **People –** insufficient policy and guidance to ensure effective security provision which may result in a negative people impact
- **Property –** lack of clarity of policy and guidance leading to potential impacts to Council colleagues and citizens accessing Council premises.

## Recommendations and Management Action Plan: Security policy, procedures, and training

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| 1.1 | Key stakeholders for building security of publicly accessed Council premises should be identified, and a Council-wide security policy should be developed, consulted on and approved, outlining:<br>• the role of building security as it relates to our estate and the stakeholders of Council-owned property<br>• the responsibilities and requirements of Duty Holders and other stakeholders in ensuring that of our buildings including third party supplier provision and resources<br>• processes and procedures designed to manage and monitor the security of the operational estate<br>• links to other relevant policies, procedures, and legislation where appropriate, such as fire and building regulations with relevant internal contacts<br>• reliance on other key processes such as contract management for school PPP contracts.<br>The policy should be subject to approval and regular review and held centrally on the Orb for colleague access. Stakeholders should be engaged to ensure they are aware of their role and responsibilities. | A Council wide Security Policy will be developed through the recently created Security Audit Short Life Working Group (SLWG). The Policy will include the responsibilities of Duty Holders (DH), stakeholders including third party supplier provision and resource. Additionally, relevant procedures, legislation and policies will be referenced within the Policy.<br>The Policy will be subject to regular review and held centrally on the Orb for colleagues to access. | Executive Director of Corporate Services | Head of Health, Safety and Risk | 30/04/2026 |
| 1.2 | Security procedures for Duty Holders of publicly accessed Council premises should be documented, approved, and communicated to relevant officers. This should include requirements for designing local controls and where to seek advice, including:<br>• access controls and key/code management<br>• CCTV processes and procedures | Security guidance for Duty Holder will be developed through the recently created Security Audit Short Life Working Group (SLWG) to complement the Security Policy which will form part of the Duty Holder Guidance. | | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management | 31/08/2026 |

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| | • staff and visitor management<br>• boundary and perimeter management<br>• systems testing e.g. alarms and doors<br>• fire and theft prevention controls<br>• fire and emergency plans and protocols that should be in place and be practiced periodically, e.g. evacuation<br>• deterrent controls such as signage and lighting<br>• incident reporting<br>• the procurement of security assets<br>• security risk assessments and management.<br>Procedures should be subject to approval and regular review and held centrally on the Orb for colleague access. Stakeholders should be engaged to ensure they are aware of their role and responsibilities.<br>The Council should also consider combining security roles, responsibilities, and procedures for Duty Holders into the Duty Holder Guidance Document. | The guidance will be published on the Orb within the Health and Safety Pages with a specific page dedicated to building security. | | | |
| 1.3 | Standard operating procedures for second line functions whose decisions have an impact on security of publicly accessed Council premises should be reviewed/documented to confirm they are aligned with the security policy and supporting procedures. This should include (but not be limited to):<br>• security procedures for property lets (e.g. hiring of school and other community spaces to public groups for meetings and activities)<br>• assurance from other partners and groups over the security procedures in place at Council owned properties and events where the Council | The Security Oversight Group will work with second line functions to ensure appropriate Standard Operating Procedures are put in place to reflect the objectives of the Council's Security Policy. On an annual basis, the Security Oversight Group will seek assurance from second line functions that safe operating procedures are in place in line with the security Policy.<br>Regular "Risk Matters" communications will be developed in response to incidents and shared with all Duty Holders to support continual improvement. | Executive Director of Corporate Services | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management | 30/06/2026 |

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| | is a stakeholder (e.g. Community Centres, Facilities Management contractors in schools).<br>Duty Holders should be made aware of relevant processes and procedures to allow them to develop local controls based on their needs, as well as those of the users of the building, other stakeholders, and any limitations of the building itself. | | | | |
| 1.4 | Training should be provided to ensure that Duty Holders and relevant support teams have the appropriate skills, knowledge and understanding of processes to help keep our buildings secure. | A training package will be developed jointly by Corporate Health and Safety and the Council FM Security team on Security requirements to allow Duty Holders to fulfil relevant roles and responsibilities | Executive Director of Corporate Services | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management | 30/06/2026 |
| 1.5 | A Council-wide quality assurance process should be designed to review and confirm all relevant teams comply with relevant security Policy and procedures for publicly accessed Council premises, and that required documentation is held to evidence compliance, demonstrate effective governance and decision making, and is available for inspection and audit purposes, where required. | The creation of an appropriate Security oversight group for Publicly Accessed buildings will be established to support a quality assurance process including evidential compliance of security Policy and procedures (due June 2026) being followed | | | 31/10/2026 |
| 1.6 | The Facilities Management SLA should be reviewed to ensure it remains appropriate for both Facilities Management and the wider Council approach to security of publicly accessed Council premises | Where the FM SLA is applied, it will be reviewed following approval of Security Policy to ensure the SLA aligns with appropriate commitments | Interim Executive Director of Place | Acting Head of Service – Soft Facilities Management | 30/06/2026 |

# Finding 2 – Recording and management of incidents and works

| Finding Rating | High Priority |
|---|---|

Due to the availability of resources and the volume of security incidents across the estate, the FM Security Team is limited in their ability to provide pro-active, and preventative security advice to the highest risk properties. The Council's Security Manager therefore responds on a reactive basis to large volumes of security incidents and requests after being informed an incident has occurred. The effectiveness of this approach relies on sound processes of incident reporting and risk management.

**Recording and Managing Incidents**

There is no central recording place for security incidents or requests. Various channels are used by duty holders to report incidents; therefore, the FM Security Team rely on other services alerting them of issues. Reporting of incidents currently happens via:

- **The SHE portal** is the Council's current system for reporting health and safety incidents. Depending on the type of incident, it could be recorded on the SHE portal. The portal does not have any categories or sub-categories relating to security incidents and so reporting on a per property basis was not available. The SHE portal is due for replacement in October 2024
- **Significant Occurrence Notification** forms are used within Children, Education and Justice Services as well as the Health and Social Care Partnership, to inform senior management of significant incidents in front-line services. These are not used across other Directorates

**Security Incident Reporting**

There is no reporting of security incidents or performance data to an oversight group or committee of the Council. As a result, the wider strategy and decision-making process around security obligations, investment and resource allocation may not be fully informed.

**Unresolved works potentially impacting security**

The Corporate Property Helpdesk is used for general facilities management support requests such as repairs or requests for assistance/advice.

Control weaknesses were identified in a February 2024 Internal Audit report which affect the helpdesk's ability to track and see requests through to an appropriate resolution in a timely manner.

Site visits identified examples of previously raised security requests which had not been addressed, including:

- faulty access controls on the main entrance of a high-risk premises, reported in June 2024. Works were still outstanding at the time of the audit visit in August 2024
- one boundary wall with a neighbouring residential property which is derelict and has temporary fencing erected. Correspondence showed this was first reported before 2021
- trees marked for felling for a number of years, but the works not completed, allowing easy access to grounds and damaging outbuildings
- multiple properties with CCTV cameras which were out of order or inadequate for the building's needs.

## Risks

- **Financial and Budget Management –** inadequate financial planning and unexpected costs
- **Health and Safety (including public safety) –** risk of theft (including data theft), vandalism, and the compromised safety of employees and visitors.
- **Resilience –** inability to respond appropriately to incidents
- **Service Delivery –** security incidents may disrupt the day-to-day operations of the Council
- **Regulatory and Legislative Compliance –** legal action or fines for failing to protect premises adequately, including breaches in data protection or health and safety legislation
- **Reputational Risk -** adverse publicity resulting from security breaches and incidents.

## Recommendations and Management Action Plan: Recording and management of incidents and works

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| 2.1 | A process to centrally capture, record, monitor, and report security incidents and requests should be agreed, including consideration of building into the myHS system. If this is not feasible, then a consistent Council wide process and supporting controls should be implemented. | The new “myHS” system will be used to establish a security incident reporting process and workflow to support action response. | Executive Director of Corporate Services | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management | 30/06/2026 |
| 2.2 | A process to escalate any unresolved security issues should be agreed and implemented. This could link to the new controls arising from the Corporate Property Helpdesk audit report completed in February 2024. | The Security Short Life Working Group (SLWG) will develop the process for escalation. This will link into the establishment of responsibilities and duties within Security Oversight Group for addressing unresolved actions as appropriate. | Interim Executive Director of Place | Acting Head of Service – Soft Facilities Management<br>Head of Health, Safety and Risk | 30/11/2026 |

## Finding 3 – Security reviews and recommendations

| Finding Rating | Medium Priority |
|---|---|

When responding to security incidents or engaging in other projects and programmes, the Council's Security Manager may determine that a security review of the premises is required. A report of outcomes and controls is prepared with recommendations to address any gaps, as well as documenting any risks posed by the building itself which cannot be addressed with additional controls. These are provided to the relevant Duty Holder or Business Manager (e.g. Headteacher, Care Home Manager) to take actions forward.

The reports are informal and lack sufficient detail to understand when and why the review was undertaken and who needs to be involved to resolve any highlighted issues. Management have advised that recommendations are often not progressed due to barriers, including unclear budget responsibility and a lack of available funds for adaptations to the existing estate (see Finding 4).

There is also no process to record, track, and monitor the recommendations made by the Security Manager through to resolution. Residual risks faced by the Council because of the security findings are also not recorded on a relevant risk register for monitoring and tracking (see Finding 5).

### Risks

- **Health and Safety (including public safety)** – risk of theft (including data theft), vandalism, and the compromised safety of colleagues and visitors
- **Resilience** – inability to respond appropriately to incidents
- **Service Delivery** – security incidents may disrupt the day-to-day operations of the Council
- **Regulatory and Legislative Compliance** – legal action or fines for failing to protect premises adequately, including breaches in data protection or health and safety legislation
- **Reputational Risk** - adverse publicity resulting from security breaches and incidents.

## Recommendations and Management Action Plan: Security reviews and recommendations

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| 3.1 | A report template should be developed to formalise the security reports for publicly accessed Council premises and ensure consistent and relevant details are reported such as when and why the review was undertaken, and who is the intended recipient and owner of actions raised. Management should also consider circulating reports to all relevant stakeholders. | A report template to respond to requests seeking advice and in response to security incidents will be developed. This will be aligned to the "myHS" system to enable tracking of allocated actions. | Interim Executive Director of Corporate Services | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management<br>Security Manager | 31/08/2026 |
| 3.2 | A process for monitoring progress towards implementing security recommendations raised in security reviews should be implemented. Any residual risks should be | The Security Short Life Working Group (SLWG) will develop the process. This will link into the | | Head of Health, Safety and Risk | 31/08/2026 |

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| | recorded within service and directorate risk registers and managed in line with the Council's Risk Management Framework (see Finding 5). | establishment of responsibilities and duties within Security Oversight Group for addressing and monitoring actions as appropriate.<br>The Security Oversight group will work closely with CRT.<br>The existing risk escalation process through established risk registers will be utilised to ensure unmitigated building security risk(s) are escalated appropriately. | | Acting Head of Service – Soft Facilities Management<br>Operations Manager | |
| 3.3 | An escalation route for recurring or unmitigated building security risks should be designed and implemented to ensure that relevant senior managers are aware of ongoing security issues. | The Security Short Life Working Group (SLWG) will develop the escalation route process for recurring or unmitigated building security risks. These will be taken forward as part of the roles and responsibilities at the Security Oversight Group. | Interim Executive Director of Place | Acting Head of Service – Soft Facilities Management<br>Head of Health, Safety and Risk<br>Operations Manager, Place | 31/08/2026 |

# Finding 4 – Security budgets for publicly accessed Council premises

| Finding Rating | High Priority |
|---|---|

**Repairs and Maintenance**

Budget responsibility for the maintenance and repair of existing security infrastructure at publicly accessed Council premises lies with Facilities Management's Repairs and Maintenance team, with exception of specific departments such as Housing and Concierge who hold their own repairs and maintenance budget, as well as PPP-contracted schools where the FM contractor is responsible for maintenance and repairs of existing infrastructure.

**New security assets and replacement of end-of-life assets**

There is no allocated budget for the replacement of end-of-life security assets, or the additional capital expenditure required to enhance security measures in publicly accessed Council premises.

Additionally, when security works are required, it is currently the Duty Holder who is responsible for securing funding to pay for upgrades. As Operational Services do not have a security budget, these works are often unfunded and therefore do not progress.

There is no process to centrally authorise and prioritise security works, or to provide support to implement alternative controls to manage risks where costs are not achievable.

## Risks

- **Financial and Budget Management** – inadequate financial planning and unexpected costs
- **Health and Safety (including public safety)** – risk of theft (including data theft), vandalism, and the compromised safety of colleagues and visitors
- **Service Delivery** – security incidents may disrupt the day-to-day operations of the Council
- **Regulatory and Legislative Compliance** – legal action or fines for failing to protect premises adequately, including breaches in data protection or health and safety legislation
- **Reputational Risk** - adverse publicity resulting from security breaches and incidents.

# Recommendations and Management Action Plan: Security budgets for publicly accessed Council premises

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| 4.1 | Budget responsibility for the maintenance, repair, and replacement of existing security infrastructure, as well as responsibility for funding the procurement of security adaptations for publicly accessed Council premises should be confirmed and agreed by all stakeholders. | The Facilities Management Maintenance and Repair budget is set up to repair and maintain.<br>For Adaptations and End-of-Life assets, a process will be developed by the Security Short Life Working Group (SLWG) and it will become the responsibility of the Security Oversight Group to manage the agreement of proposals. The Security Oversight Group's membership will have representatives from Education, Strategic Asset Planning and Facilities Management. Any capital projects that are to be delivered, will be progressed through existing mechanisms which | Interim Executive Director of Place | Head of Facilities<br>Head of Strategic Asset Planning | 30/04/2026 |

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| | | have been established due to the introduction of building improvement plans for all operational properties, supported by the 2025/26 Council budget. | | | |
| 4.2 | A process should be implemented to capture all outstanding security works for publicly accessed Council premises and report these to an appropriate oversight group for prioritisation and authorisation. Prioritisation should be risk-based and in line with an agreed criterion. | The Security Short Life Working Group (SLWG) will develop a risk-based prioritisation process. These will be taken forward as part of the roles and responsibilities at the Security Oversight Group. | Interim Executive Director of Place | Acting Head of Service – Soft Facilities Management<br>Head of Health, Safety and Risk<br>Operations Manager | 30/11/2026 |

## Finding 5 – Risk management - publicly accessed Council premises

| Finding Rating | High Priority |
|---|---|

Physical premises security controls are key to mitigating health and safety, resilience, data security, and business continuity risks. The observations outlined in Findings 1 – 4 present challenges for colleagues across the Council to assess and manage the current level of risk faced across the estate in relation to security of publicly accessed Council premises as well as the effectiveness of security controls as they relate to their individual roles and associated risks. In addition, there is no risk register which captures physical premises security risks for individual premises and the wider estate.

Conflicting legislation can also give rise to conflicting security risks, such as fire legislation requiring exits with pushbuttons at child-friendly heights, which increases the risk of children letting themselves out the building. This places a reliance on manual supervision rather than secondary, physical security controls should a child circumvent supervision. While compliance with other legislation is viewed as equally important, education colleagues faced with this dilemma find it difficult to balance this with the security risks associated with a child potentially letting themselves out the building.

Statutory obligations in relation to premises security are expected to change with the introduction of 'Martyn's Law' which is currently being consulted by the UK Government. The proposed bill will impose requirements on certain premises and events to increase their preparedness for, and protection from terrorist attacks. The Council may be required to take proportionate steps, depending on the size and nature of the activities that take place at each premises. Discussions on the implications of the new bill to the Council are in the early stages including provision of a briefing note to the Chief Executive on the scope of the Bill and proposed recommendations. It is understood that once the legislation is enacted it will be carefully scrutinised, following which a full Council Protect Strategy, with clear actions, will be produced by the Council's Protect Single Point of Contact for consultation and approval.

### Risks

- **Financial and Budget Management** – inadequate financial planning and unexpected costs
- **Health and Safety (including public safety) –** risk of theft (including data theft), vandalism, and the compromised safety of employees and visitors
- **Governance and Decision Making** – uninformed decision making around the use of buildings
- **Regulatory and Legislative Compliance –** legal action or fines for failing to protect premises adequately, including breaches in data protection or health and safety legislation.

## Recommendations and Management Action Plan: Risk management - publicly accessed Council premises

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| 5.1 | Risks associated with individual publicly accessed Council premises should be identified, recorded, assessed, and managed in line with the Council's Risk Management Framework. Once known, the risk profile and landscape should be monitored to inform decision-making. | The creation of an appropriate Security Oversight Group for Publicly Accessed buildings will be established to support a quality assurance process. The Oversight Group will work closely with Risk Management Team. As part of the Oversight Group objectives, a risk assessment and monitoring process will be developed. | Interim Executive Director of Place | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management | 30/11/2026 |

| Ref. | Recommendation | Agreed Management Action | Action Owner | Lead Officers | Timeframe |
|---|---|---|---|---|---|
| 5.2 | A process should be implemented to ensure collaboration between teams to find solutions where conflicting risks are identified, and to limit reliance on manual or backup controls. | For all publicly accessed council buildings including multi-service/multi organisation occupation, suitable building user groups will highlight, action or escalate any conflicting risk situations.<br>The Security Short Life Working Group (SLWG) will develop the escalation process.<br>The Security Oversight Group for publicly accessed buildings will review any conflicting risk situations escalated items which cannot be resolved locally. The Oversight Group will work closely with the Risk Management Team. | Interim Executive Director of Place | Acting Head of Service – Soft Facilities Management<br>Head of Health, Safety and Risk | 30/11/2026 |
| 5.3 | Development of the Council's Protect Strategy should include consideration of risks to security of publicly accessed Council premises with engagement and communication across all key stakeholders. | The development of the Council Security Policy will take account of relevant Protect Strategy elements and will reflect these in the approach taken to manage the security risk through the policy and accompanying guidance. | Executive Director of Corporate Services | Head of Health, Safety and Risk<br>Acting Head of Service – Soft Facilities Management | 30/06/2026 |

# Appendix 1 – Control Assessment and Assurance 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 |

| Overall Assurance Ratings | |
|---|---|
| **Substantial Assurance** | A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. |
| **Reasonable Assurance** | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. |
| **Limited Assurance** | Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. |
| **No Assurance** | Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited. |

| Finding Priority Ratings | |
|---|---|
| **Advisory** | A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice. |
| **Low Priority** | An issue that results in a small impact to the achievement of objectives in the area audited. |
| **Medium Priority** | An issue that results in a moderate impact to the achievement of objectives in the area audited. |
| **High Priority** | An issue that results in a severe impact to the achievement of objectives in the area audited. |
| **Critical Priority** | An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency. |

# Appendix 2 – Areas of Audit Focus and Control Objectives

| Audit Areas | Control Objectives |
|---|---|
| Policies and procedures for Council premises | • policies and procedures for the security of Council premises are in place and up-to-date and reflect all control objectives stated below, including any relevant legislation. |
| Central Security Arrangements for Council premises | • the decision-making and governance approach for security of Council premises is robust, with security matters considered in a timely manner, costs are known, and responsibility for implementing actions clearly defined and monitored<br>• regular reviews of Council premises are undertaken to confirm that security arrangements are adequate and aligned with the needs of users of the buildings and relevant legislation<br>• when the security needs of building users change, the required changes, including costs, are determined and approved early in the decision-making process<br>• recommendations on security of Council premises are logged and reviewed by an appropriate senior officer and / or governance forum for oversight, with cost details, associated risks, and alternative measures outlined where appropriate<br>• a methodology has been designed to prioritise security of Council premises works, covering both repairs to existing infrastructure, and the installation of new security measures<br>• the budgets for premises security maintenance and upgrades are clearly stated and assigned to appropriate departments. |
| Local Security Arrangements for Council premises | • there is a named responsible officer for building security for all individual Council premises, responsible for overseeing and reviewing the adequacy and effectiveness of security arrangements<br>• officers responsible for security of premises have received adequate training and guidance to assist them in undertaking their duties<br>• responsible officers undertake the necessary inspections, assessments, and other duties on a regular basis to ensure the security of their buildings and maintain adequate records of outcomes and actions<br>• checks are performed to confirm that responsible officers have completed all relevant tasks and assessments in relation to building security in line with procedures<br>• a reporting line has been established for all responsible officers to escalate security of premises issues. |
| Risk management | • risks related to security arrangements for Council premises are identified, recorded, and managed within a service risk register, and regularly reviewed to ensure appropriate mitigating actions are in place and remain effective, with escalation to divisional and directorate level risk committees where required. |