Archives & Records Association
UK & Ireland

Security Guidance

June 2024

Come and join us...

Contents

Archives & Records Association
UK & Ireland

Foreword

This security guidance document has been prepared for the Archives & Records Association – ARA (UK & Ireland) and its members. It will not answer all of the security questions that you may have but it will provide a solid basis upon which security risk management decisions can be taken. It should be read in conjunction with the guidance in relation to Archives Accreditation.

Due to the nature and type of organisations that are members of the ARA, the guidance has been written to apply to a wide range of venue types and in a manner that is sensible, proportionate, and easy to understand. Not all venues can afford specific physical or technical security systems, nor do they have additional human resources to devote to security so a balanced approach that is risk and resource-based must be offered.

This guidance aims to provide advice and guidance needed for members to make informed decisions about security risk management, how to use available resources and actions to consider to proactively protect their staff, users and assets. All organisations will have their own particular ways of working and there are different methodologies that can be applied to areas such as risk management. This document offers a particular approach but members should select and interpret the different sections with regard to their own circumstances.

The guidance aims to follow a logical sequence that will enable the reader to consider a wide range of issues that could adversely impact the security and integrity of archives and collections at their venues. To support ARA members Appendix 1 is a 'Signpost Document' designed to provide the reader with more detailed information and guidance if that is sought.

While written for the ARA many of the security measures described in this guidance are equally transferable to other cultural venues and sites whether holding archives or not. Wider stakeholders have been consulted as a part of this guidance development to ensure that it is not only accurate and timely, but that it is also aligned, as far as possible, with future legislation and international good practices.

The guidance was developed by Trident Manor Ltd. with input from the ARA Security & Access Group and others with relevant expertise. This guidance will be subject to periodic reviews and updated by the ARA Security & Access Group as required. Thanks are due to the SAG group and to Andy Davis of Trident Manor for producing the documentation. We are also grateful to The National Archives for funding this important project.

2 What is Security?

Before starting to write guidance and advice about 'Security' it is appropriate to understand what 'security' in the context of this document is. Security is defined as ***"The condition of being protected from loss, harm, or damage."*** [1]

What is important to recognise is that 'security' doesn't just happen! To create the 'condition' positive actions have to be taken that support the achievement of 'protection' and these normally require the implementation of security measures which can be physical, technical, operational, or educational.

Good security is a continuous and proactive activity that should be practised by everybody within an organisation and be everybody's responsibility.

[1] ASIS International, Risk Assessing Standards, 2016

3 Governance & Documentation

The development of governance and documentation helps organisations to manage security threats, risks, and vulnerabilities, and to record the decisions that have been made. It is important to ensure that everybody within an organisation understands what is expected, who is responsible for protective security, and how it is expected to be implemented.

The size and style of security governance will be dictated by the complexity of the operations, the nature and structure of the organisation, the threats that are faced, and the risks those threats pose.

Any security documentation that is created should be in a style that can be easily understood, not too technical, and is pragmatic. The overcomplication of any documentation will result in it either not being read, or worse, not being understood by those who are expected to deliver and use it to protect people and assets. "Assets" can be understood as collections, records, buildings or equipment – anything that the archive identifies as needing protection. It is often helpful to state upfront that the protection of living people always takes precedence over the protection of assets. Generally, security governance and documentation will fall into the following categories:

- Security Risk Management Policies
- Protective Procedures
- Emergency Planning

A critical point with any security documents which in themselves can provide information which would be of value to adversaries is that they must be protected and only circulated on a restricted basis. For example, not everybody needs to know and understand how the documentation of archives works, nor do they need access. Information should be shared on a ***'Need to Know-Need to Access Basis'.***

Where appropriate, governance and documentary materials should be categorised in accordance with their sensitivity and restrictions applied accordingly (e.g. storing them in an area of the network with limited access). This will reduce the risk of accidental and intentional disclosure of sensitive materials.

3.1 Security Risk Management Policies

An organisation's security risk management policy will outline the rules, expectations, and approaches that are to be taken to protect the organisation's assets from loss, harm, or damage. It is directional and can come in many formats such as a stand-alone document or as part of a wider organisational policy. An organisation may deem that particular documentation is unnecessary, but this is a risk management decision itself.

Best practice recommends that a security risk management policy is established to avoid confusion and to ensure the protection of assets takes place in an expected manner. From a legal perspective, it also means that a defendable approach is developed upon which actions can be assessed, as opposed to an inference being made because of the lack of a policy or protective direction.

Any security risk management policy should be based upon realistic risks that exist or can be expected to impact the organisation and its assets, now or in the future. Where possible the policy should be specific to the archive, library, or collection, even when the venue/ operation may be a part of a wider organisation. To confirm the policy's importance, it should be approved by the most appropriate person, preferably the risk owner or other senior responsible person.

This guidance document is not prescriptive, as long as any policy created contains relevant information to protect the organisation's assets then it is appropriate. However, careful consideration needs to be taken to ensure that all security risks that exist are covered either within this or another policy. If separate there should be some cross-referencing to ensure that risks have been captured and considered.

Examples of other standard policies which should intersect with Security policy include:

- Health and Safety Policy
- Information Security Policy
- Collections Management Policy
- Preservation Policy

A Security Risk Management Policy should provide the direction for the organisation to follow and should/can include the following non-exhaustive areas:

- Organisational mandate and commitment
- Approach to security risks
- Security responsibilities & risk owners
- Creating security in depth
- Operational security activities
- Approaches to security education and training
- Process for review of policies, procedures and incidents

3.1.1 Mandate and Commitment

This sends a message to the organisation that the Leadership Team has bought into the Security Risk

Example 1:
Security Policy Statement – Mandate & Commitment

The Senior Leadership Team (SLT) is committed to supporting, resourcing, and providing the strategic direction needed to protect all organisational assets. All staff are responsible for proactively reducing the security risks that exist or are anticipated. The policy will:

- Provide a framework that enables security risk management activities to take place in a consistent, sustained, and controlled manner.
- Clearly define what organisational security responsibilities exist, and at which level.
- Help reduce the risks to personal safety and security of staff, contractors, and visitors to the organisation.
- Reduce the risk of assets being lost, stolen, damaged or degraded.
- Improve the protection of information and data.
- Help develop a proactive security culture.
- Optimise the efficiency of security operations.
- Increase the robustness of the organisation's security approach and minimise the security threats that exist.

The SLT acknowledges the importance of integrating security measures and strategies, (human, technical and physical) to ensure cost-effectiveness and appropriately layered systems. Our approach to security risk management focuses on preventing incidents as well as enhancing the capacity to respond effectively to them when they occur.

A.N. Other
Chair of Organisation **31st July 2023**

Management Policy and is committed to supporting it. It highlights key areas that have been considered important for the protection of the organisation and its assets. It is possible to have the mandate and commitment shown as a separate document (Example 1) similar to a Health & Safety Policy Statement.

In doing so the key areas and commitments of the Leadership Team can be highlighted, and the 'Security Policy Statement' be displayed in a manner that will increase the likelihood of it being read and understood by staff.

3.1.2 Approach to Security Risk Management

This part of the policy is a high-level directive and not a risk assessment of the organisation or its assets.

This may be part of a wider organisational risk management policy but should include the specific security risks which archives, libraries, and collections have to consider outside a more general cross-organisational approach.

All organisations should seek to manage and reduce security risks, ***'As Low as Reasonably Practicable'*** with the important part being the word ***'Practicable'***. Practicable means that security measures, treatments, or acceptance should be such that they do not adversely impact the operational capabilities, financial constraints, or the reputation of the organisation.

No organisation can remove all the risks that exist, many members of the ARA may not have the financial or personnel resources to do so, but all organisations can seek to manage them.

The policy should outline the risk management approach that will be taken to:

- Identify the threats.
- Understand the risks the threats pose.
- Identify security vulnerabilities.
- Appropriately treat and manage risks.

Where a Risk Management Policy is cross-organisational the approach may already exist, if so, the security risk management policy should link to or derive from this. (See Tip 1) By adopting this approach the specific risks facing archives, libraries, or collections are being captured and considered.

Tip 1:

Where an organisational risk management policy already exists add the security risk management policy as an Appendix. If an organisational security risk management (SRM) policy already exists consider adding the archive, library, or collection SRM policy as an Appendix to that larger one.

Where documents and templates are available to support the risk management approach used, they should be attached as an Appendix to any policy.

3.1.3 Security Responsibilities & Risk Owners

The policy should identify who is the organisational/departmental lead on security. In larger organisations, the Leadership Team may delegate this to an appropriate named individual. They should be identified as should anybody with a specific remit around security. The 'Risk Owners' will normally be the Leadership Team and the fact that they delegate security responsibilities does not normally absolve them of risk ownership. In smaller organisations, the security responsible person could have multiple roles and responsibilities while also being the 'Risk Owner'.

Security responsibilities and risk ownership will often be dictated by the shape, size, and characteristics of the organisation and the assets being held. The larger the organisation the more likely that security professionals will be employed and that a greater need for cross-departmental working will be required.

Tip 2:

When there are multiple departments within an organisation it is sometimes better to have a 'Security Committee' where representatives from different departments can come together to discuss and agree security policy implementations. This way silos are broken down and everybody can add their point of view to any discussion. This demonstrates inclusivity and reduces the likelihood of unintentional oversights or omissions occurring.

All organisations should consider oversight of the risk owners' activities either by committee or external independent audit processes.

Any policy should be a tool for the development and progression of a positive security culture within any organisation, it should highlight that it is everybody's responsibility to protect organisational assets. Clearly defined job descriptions are a great tool to achieve this and help start the development of the security culture.

3.1.4 Creating Security in Depth

Creating Security in Depth is covered in greater detail in Part 5 of this guidance, but it is beneficial for the policy document to provide the direction that the organisation takes with regard to security programme design. It should articulate that single levels of security should be avoided as far as possible and each layer that is added should support other measures to increase the overall protective robustness.

The policy should clearly define any standards that are being adopted, such as LPS1175 for physical security standards[2] and BS 8243 for intruder detection systems. It should also include any guidance that is required to meet regulatory requirements such as Annex E for 'Transportation Guidance' when lending under the Government Indemnity Scheme[3].

Security in depth is created by applying multiple layers of protective measures so that a robust protective programme is created. Relying on a single layer of security means that a criminal or adversary only has to bypass one layer of protection before they reach an organisation's assets. Therefore, this should be clearly defined in the policy. (See Example 2 overleaf)

[2] https://www.redbooklive.com/download/pdf/LPS1175.pdf

[3] https://www.artscouncil.org.uk/supporting-arts-museums-and-libraries/supporting-collections-and-cultural-property/government-indemnity-scheme

Example 2:
Creating Security in Depth

The Senior Leadership Team (SLT) recognises that the most robust protective security is created by adopting a multi-layered approach to the protection of the organisation's assets. Single layers of security should be avoided wherever possible and practicable.

We identify security measures as consisting of the following types:

- Physical security measures
- Technical security measures
- Operational security practices
- Continuous security training and education

The purpose of 'security in depth' is to support the principles of:

- **Deter** Makes the venue/organisation unattractive to adversarial threats.
- **Detect** Spots potentially illegal activities and initiate a form of response.
- **Delay** Slows down any adversarial attack using the above security measures.
- **Respond** Enables a timely response before any attack is completed.

Each measure should support and enhance the other and through careful consideration and design security risks and vulnerabilities to the organisation will be mitigated.

Where in-house expertise is unavailable, professional advice and guidance can be sought from the police, professional bodies, or suitably qualified individuals.

By adopting this approach, security risk management subjectivity should be greatly reduced.

3.1.5 Operational Security Activities

This part of the policy should address behavioural aspects of the organisation's approach to security risk management. It can include the security profile that the Leadership Team expect to be taken, including a reaffirmation of the fact that the protection of the organisational assets is everybody's responsibility. All security operations should be risk-based.

Tip 3:

Do not include practices and procedures in the main body of a security policy, reference them and add them as an Appendix to the policy. In doing so the flow of the Policy (a strategic document) is not interrupted by detailed operational practices (which are likely to need to be updated more frequently than the policy itself).

The policy document should highlight the need for continued awareness and vigilance by all staff and that practices and procedures[4] exist to help protect the organisation's staff, users and assets. The nature and characteristics of the organisation will dictate how detailed they need to be.

Where necessary, and subject to the requirements, reference can be drawn to key operational activities undertaken at or by the organisation. (Example 3)

[4] See Section 3.2 for a detailed breakdown.

Example 3:
Operational Security – Procedures

To help deliver this policy, Operational Procedures and Practices exist to ensure that a structured approach is taken to protect the organisational assets. These procedures are specific to (Venue) which is a part of (##) Organisation.

There are situations where the procedures cross different departmental working practices. Where this occurs the lead department will be identified, and they are to ensure that broader cross-departmental engagement takes place to minimise risks.

A complete list of Operational Security Practices/Procedures can be found in Appendix 'XX' of this policy, the following are viewed as key activities:

- Opening and Closing Procedures
- Access Control Procedures
- Personal Safety & Security Procedures
- Search/Reading room Protocols (Collaborative protective security activity)
- Access to Collections (Collaborative protective security activity)
- Security Transportation of Documents
- Exhibition Security Procedures
- Lockdown/Evacuation Procedures
- Reader Admission Procedure
- Exhibition Loans Procedure
- Record keeping and documentation
- Disaster Response and Recovery

3.1.6 Approaches to Security Education and Training

Security does not just happen. To ensure its effectiveness, people should be educated about the organisational approach to security and the protection of assets. The policy should stress the importance of security education and training equally as much as physical and operational security measures; you can have all the security in the world but this will fail if staff are not educated on the following:

- What exists.
- Why it exists.
- What individuals are to do.

AND

- How to do it.

There is a risk that time, money, and effort may be wasted, security measures may not be implemented or gaps may be created, simply because effective training did not take place.
The policy should outline the support for continual security learning and development from induction through to attending specialist programmes, as necessary. This again will be dictated by organisational size, nature, and budget.

3.1.7 Reviews

Policies are subject to changes and variations in operational practices, the threat profile, and security incidents that may have occurred. It is important that reviews are scheduled and identified within a policy so that those accountable for the maintenance of documentary governance understand when deliverables have to be undertaken and confirm that it remains valid, and up to date. The documents requiring reviewing will vary. (Example 4)

These reviews should form part of the security risk management Annual Report prepared for an organisation to ensure compliance with any policy that exists and demonstrate best practise. External audit reviews are also beneficial in providing additional scrutiny and perspective.

3.2 Protective Procedures

While the 'Policy' provides the strategic direction, practices and procedures provide the operational instructions to support the protection of organisational assets. From an organisational perspective an (operational) 'procedure' is defined as, "A set of step-by-step instructions compiled by an organization to help workers carry out routine operations."

The term Protective Procedures is used instead of 'Security Procedures' because many procedures are not definable as 'security', but most can be seen to add a protective value to the safeguarding of organisational assets and individuals.

Many organisational activities and procedures may rest with different departments or individuals who may have nothing to do with a defined security role or function. (Within the broader cultural community this is more often the case.)

Where security personnel are used at venues, they will normally be given a set of SOPs (Standard Operating Procedures) or Assignment Instructions (AI). These define how they will carry out their security duties while at work. These instructions should be checked and verified to ensure that they meet the organisational needs and do not accept unnecessary liability.

As with all documentary governance, there is no need to overcomplicate things and any procedure should be of a size that will include the necessary information but not be so long as to discourage individuals from reading it.

Example 4:

Review	**Frequency**
Annual report	Annually (subject to size and nature of the organisation)
Policy	Annually
Practices & procedures	Biannually (or after a major incident)
Threat, risk and vulnerability assessments / risk registers	Annually – subject to risk (or following a major incident)
Security training	On recruitment, quarterly, continuously
Security job description	Annually

In an ideal world a 'procedure on a page' would be great, however, many operational activities are rather more complicated.

The format and structure of any procedure is often dictated by wider organisational approaches. However, a standardised format helps the reader understand the sequence of processes and is therefore sometimes easier to follow.

Tip 4:

As far as possible maintain a standardised format to all procedures within an organisation or department.

There are some procedures that all organisations, irrespective of size, contents, and personnel should possess and others can be added based on the operational context, value, and wider organisational requirements. Example 3 above highlights some of the more common procedures that would be expected in ARA members' venues.

3.3 Emergency Planning

Emergency planning is a critical element of all cultural venues' protective governance. Fire will always be one of the main threats that archives and libraries will face because of the capacity for damage to contents. However, other emergency planning scenarios need to be considered.

Each organisation should maintain emergency plans in an acceptable format that can be easily reviewed, actioned, and updated as necessary. Consideration should be given to having paper copies in a defined secure location as well as online files, so that relevant information can be readily accessed in the event of an emergency, e.g. a power outage. As with all governance, it is the content that is critical and not the size of the plan.

Sometimes it is helpful to distinguish between what is an emergency and what would be classed as a crisis.

An emergency is defined as, "something dangerous or serious, such as an accident, that happens suddenly or unexpectedly and needs fast action to avoid harmful results." [5]

A crisis is defined as, "a situation that significantly falls outside normal business operations, and which has the ability to severely impact continued operations and its financial well-being."

Additional ***crisis*** characteristics include:

- Unexpected, immediate exposure to **significant** threats, violence, or damage situations – whether perceived or actual.
- **Significant** media interest that needs to be proactively addressed and managed to maintain reputational trust and support. (Regional, national, and international)

In this guidance **'significant'** means where the event is of a sufficient size and nature to be worthy of immediate attention and where long-term effects, survivability or adverse impacts on the organisation have the **potential** to occur. Then it would normally be defined as a crisis.

A 'crisis' is normally something that has the potential to impact at the corporate level and normally requires a strategic response and can be seen as an escalation from an incident to an emergency, and then onto a crisis.

[5] https://dictionary.cambridge.org/dictionary/english/emergency

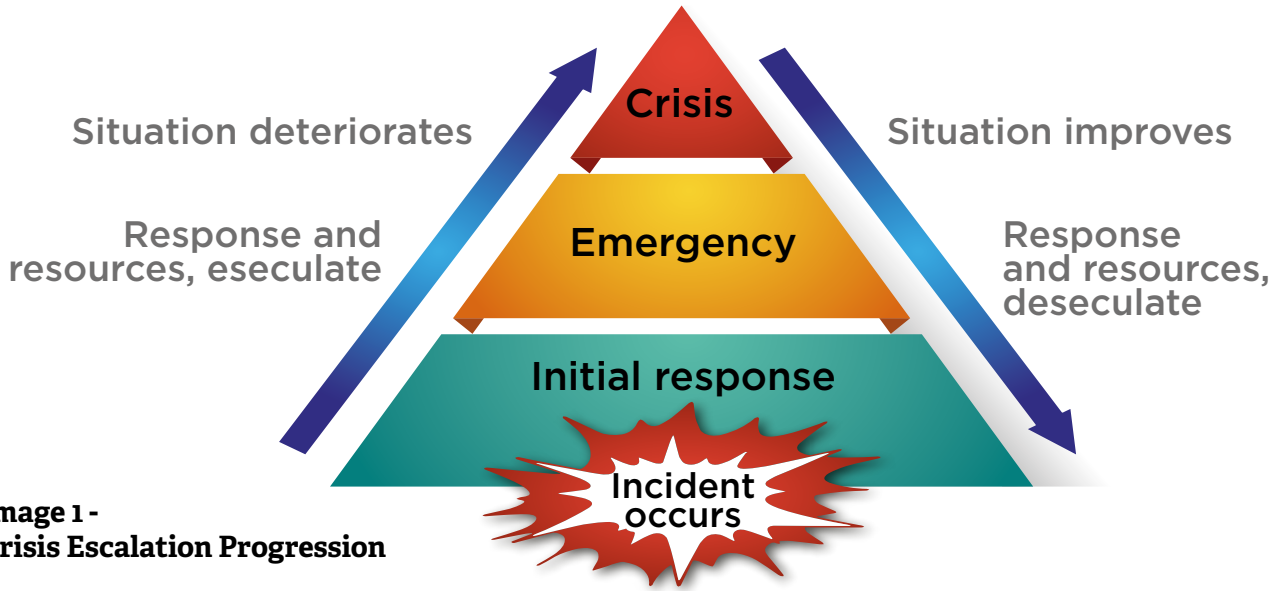

Image 1 -
Crisis Escalation Progression

While Image 1 shows a process not all incidents follow the same pattern, and the nature of the incident could categorise it as an emergency or crisis straight away.

It is always helpful for organisations to know and understand what type of events require certain responses so that appropriate resources are allocated, and subjectivity reduced.

Tip 5:

As an organisation, agree and identify the type of events that would be dealt with through:

- Incident management
- Emergency response
- Crisis management

The important thing is not the title, size, or type of document produced, it is the content and everybody's understanding of what is to be done and by whom.

Where relevant the following (non-exhaustive) may feature within an organisation's Emergency Planning considerations:

Example 5:

Emergency Planning Considerations
Fire Plan

Water ingress response

Salvage Plan

Loss of utilities

Injuries or death at the venue

Major loss/theft of documents

Data breach

Health and Safety violation
Act of terrorism

Protester/activism

Significant financial event

Significant environmental incident

Industrial action

Emergency planning should be organisation and site-specific. It should be based on the realistic risks that exist from natural and adversarial threat sources and it should be fully understood by everybody who is expected to play a part in the plan's implementation. The plans should be tested and reviewed at least annually unless a significant event has taken place that has led to the implementation of the plan (which should then be reviewed to assess how well it actually worked).

4 Risk Management: Threat and Vulnerability

Any security strategies, advice, or guidance should be risk-based to ensure that efforts are targeted towards the threats that can cause the most harm, especially where weaknesses exist and can be exploited. While there are software packages available to help with this process anybody can do it by adopting simple processes.

This section will outline key considerations including the following:

- What needs protecting? (People / Assets)
- What can harm them? (Threats)
- The likelihood and impact of loss, harm, or damage. (Risks)
- Where gaps exist that can be exploited by threats. (Vulnerabilities)

Image 2 – Process of Managing Risks

A Threat is defined as, "***A potential cause of an unwanted incident which may result in harm to individuals, assets, a system or organization, the environment, or the community***."[6] The important thing to note is that a threat is the 'cause' of the potential loss, harm, or damage, while a risk is the 'effect' caused by assessing the likelihood against the consequences/ impact of the threat occurring.

Many people confuse threat with risk and believe that they are interchangeable, they are not, Threat = **Cause**, Risk = **Effect.**

A vulnerability is defined as, ***"The conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards."*** In a security context, a vulnerability is ***something that can be exploited by a threat.***

To support the risk assessing process a document containing risk management descriptors has been included at Appendix 2 of this guidance.

4.1 [7]Asset Identification and Categorisation

Before undertaking any threat, risk, or vulnerability assessment it is important to know and understand what you want to protect. People naturally take priority. By categorising assets such as collections, buildings or equipment (e.g. as Critical, Important or Ancillary) you get a greater understanding of where protective resources need to be focused. The less critical an asset, the lower the effort needed to protect it, unless by breaching it a greater risk is created for a more critical asset. (See Appendix 2 for a supporting table that can be used.)

This method of asset categorisation can equally apply to existing asset registers or to new ones created using Excel or bespoke asset management software programmes. Effective registers have been seen that are as simple as having a page for each of the asset ratings.

In its most basic form, an asset register that contains the name of the asset, location, and criticality (alongside any special instructions) is all that is needed to help during the risk assessment process especially when considering the proportionality of measures.

By understanding what assets exist, where they are, and their criticality to the organisation, any threat evaluation, and the risk they pose will be contextualised alongside any vulnerabilities that are found.

[6] ASIS/RIMS – Risk Assessment Standard - 2015
[7] Best practice would dictate that an organisation has an asset register but that is not always the case. From a protective perspective it is normally appropriate to list assets that can or do have a direct impact on operational activities. It will be down to the venue to agree what assets are recorded and where, equally it may be that this relates to archives or collections only.

4.2 Threat Identification and Evaluation

When organisations look at threat sources from a 'security' context they primarily look at the criminal threat. However, as shown in the definition there is no reference to crime; it only talks about protecting from loss, harm, or damage. When considering the threats that can impact an organisation it is better to look much wider[8].

To make an assessment truly effective it is better to be specific rather than just looking at the 'general' threat source. While assessing 'general' threat sources such as 'crime' there are too many variables which if not examined closer could result in inappropriate protective measures being applied or vulnerabilities created. By considering specific threats a greater accuracy in the overall assessment process will be achieved.

When assessing threats, it is important to consider realistic threats that have, can, and could impact on the venue, collections and archives. Not all threats will be relevant.

By considering the assets being held a list of different threat sources can be prepared to enable the risks they pose to be assessed.

[8] There can be cross-over with health and safety and other legislation providing they have been identified and assessed during a process that is acceptable.

Example 6:

General Threat	Specific Threat
Crime (This can be further broken down, but for the example, it is shown as the overall general threat instead of breaking it down into theft, violence, etc.)	• Burglary • Organised crime • Insider threat • Fraud
Social	• Drugs • Anti-social behaviour • Industrial actions
Environmental	• Flooding • Wildfire • Landslides
Medical	• COVID • Avian flu • Norovirus
Infrastructure	• Loss of IT • Failure of environmental controls (e.g. air conditioning) • Water contamination • Power outages
Terrorism	• Marauding attack (firearms or bladed/ blunt force weapons) • Vehicle as weapon • Improvised Explosive Devices (IEDs) • Fire as a weapon • Chemical, biological and radiological (CBR) • Cyber
Other	• Human error • Information disclosure

4.3 Risk Assessing

Risk management is an identified business discipline, and organisations should have a Risk Management Policy and a Risk Register (sometimes associated with the Asset Register), though unfortunately not all do.

This guidance will outline a basic risk assessing process that can be followed by all. Some venues may have the luxury of risk management software, however, that does not and should not negate organisations undertaking a risk assessment process or at least stress testing any software programme's findings.

Where possible it is always recommended that a collaborative approach is taken to risk assessing as it reduces the likelihood of unintentional biases creeping in and not being challenged.

Any risk assessment must consider the organisation's risk appetite and tolerance levels and one of the easiest ways of achieving this and avoiding subjectivity is to use a process that is cross-organisational and based on clearly defined descriptors that have been agreed and approved by the leadership team. (See Appendix 2 for examples that can be used.)

Most processes are based on numerical descriptors often associated with a colour that supports the numerical allocation. This process should be adopted for the likelihood of the threat and the consequences of it occurring. An overall risk score is generated by multiplying the likelihood score by the consequences score. Subject to the organisation a different number of ratings can be applied (3= Low, Moderate, High, through to 7 which becomes too complex for many.)

Tip 6:

Tip 6: Using 5 x 5 ratings allows greater accuracy (than just using 3) in the evaluation and remains relatively easy to follow (as opposed to 7).

Appendix 2 demonstrates the use of colours to help identify and highlight where priorities are when it comes to the risk treatments. A venue may contain items that are not attractive to criminals so the threat from criminals may be viewed as low or very low. However, if the venue contained special collections and materials that had a high value and were attractive to criminals the risk scores would differ and be much higher. (See Example 7)

Example 7:

A local authority archive contains three stacks of paper-based social history materials (assets) that have little financial value and would not be attractive to criminals.

The likelihood of both theft and arson (intentional damage by fire) is scored as 2 (Low), however the consequences of arson are scored higher than theft at 5 (Critical). Therefore, the risk of theft-related threats is Low (2x3=6) however the risk posed by arson is higher (2x5=10) which using the scoring matrix increases the risk to Moderate.

There are of course other kinds of value than monetary value and this is where it is essential that archives understand their holdings and their cultural, social and evidential value which could expose them to different kinds of risk.

A point to note regarding the risk posed by the terrorist threat, especially in the context of ARA members, while the assessed likelihood may be low or very low, the consequences will always be critical due to the increased likelihood of loss of life. Therefore, risk mitigation measures must always be considered.

Tip 7:

It is also important to consider 'risk transference' from any neighbouring or adjoining businesses and organisations. Are they at a greater risk of any particular threat, organised crime, terrorism, or protesters? If so your score should consider and reflect that.

The above is a basic approach to risk assessing that all organisations and ARA members can take. However, the risk assessing process can go a stage further and identify 'risk mitigations' followed by a re-evaluation of the scores. Effective risk treatments should reduce the final risk rating, but that is not always the case and sometimes the final risk score cannot be changed, they are already "as low as reasonably practicable".

The risk assessment can be desk-based but is better being done as both a documentary review and a site visit. During the site visit, it is often possible to incorporate the risk re-evaluation with the undertaking of a vulnerability assessment. This not only helps contextualise the threats and the risks that exist but also assess existing protective measures while looking for vulnerabilities.

4.4 Vulnerability Assessments

A vulnerability assessment is the identification, categorisation, and prioritisation of weaknesses that can impact the integrity of an organisation's assets and seek ways to reduce or manage them.

One of the easiest ways to identify vulnerabilities is to reverse mindset, i.e. think like the threat source. When looking at adversarial threats it can help to put yourself in the position of the adversary so you can ask yourself the question, ***"If I was going to attack this place*** (criminal, terrorist, or protester) ***how would I do it?"***

When adopting this approach, it is always better to start where the adversary would start, outside the building and grounds, before working your way into the most secure part of the building/venue, which hopefully an intruder will not be able to access.

This is where understanding the threats and the level of risk that they pose is important as it can be contextualised so that realistic considerations are made, and the assessment does not head off into some fantasy world as depicted by Hollywood blockbusters.

It is also sometimes beneficial to identify the type of vulnerability whether **physical, operational, technical, or educational**, which corresponds with the types of (non-IT) protective security measures that exist. This can help when considering solutions to address the vulnerabilities.

It is sometimes easier to create a simple vulnerability assessment spreadsheet where vulnerabilities that are identified can be recorded and then evaluated for the level of harm they pose to the assets (subject to the asset criticality). That way a record that can be cross-referenced against other documents can be made and vulnerabilities are not forgotten.

Once vulnerabilities have been identified and recorded you can then switch mental roles and start to 'TIaD' (Think like a Defender), asking ***"How can I address these vulnerabilities to reduce or prevent the risk we face."*** In 90% of cases, non-experts can identify sensible solutions. Sometimes professional help and assistance may be required to identify the vulnerabilities and then understand the best way of reducing and managing them, so risks are lowered.

Remember not all vulnerabilities have to be addressed or can be addressed. Sometimes if the risk posed by the threat and the vulnerability does not impact any important or critical assets then the risk/vulnerability can be accepted.

If accepted it should be recorded in either the vulnerability or risk assessment documentation to show that it was not an oversight, it was an informed decision.

5 Creating Security in Depth

The best way to secure any venue and its contents is to create multiple layers of security consisting of physical, technical, operational, and educational security measures that collectively offer robust and resilient layers of protection. It is always better to overarch and interlock security measures so that they always support the efforts of another, and you are not faced with a situation where there are no or limited lines of security.

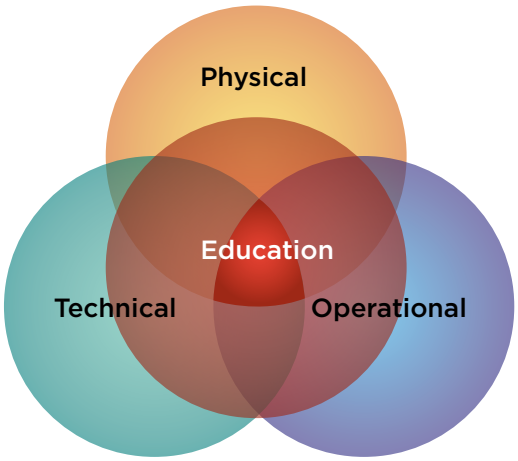

Image 3 – Protective layered security

Where there are only single layers of protection there will always be vulnerabilities that once exploited can result in the loss of assets. Therefore, when you have critical assets, they should always be behind multiple protective layers and preferably away from external walls or access points. The goal is to achieve the red area in Image 3.

As outlined earlier the purpose of security in depth is to create a situation where an adversary is deterred, detected, or delayed, and a response is generated before loss or harm occur.

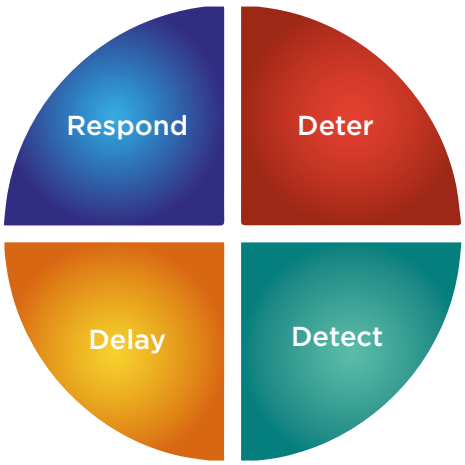

Image 4 – DDDR principles

Example 8:

Deter:
If by appearance alone somebody sees robust physical barriers, technical systems such as CCTV and Intruder Detection Systems (IDS), and effective search and patrolling activities, the likelihood of the adversary being deterred is increased and risks are reduced.

Detect:
If there are CCTV systems that are being proactively monitored, motion sensors correctly positioned around the building, and an electronic access control system delineating public and private spaces there is a greater likelihood of detecting any adversarial activities (day/night) and a timelier response generated if they haven't already been deterred.

Delay:
Using a perimeter fence, the installation of robust doors, shutters and other physical barriers can delay an adversary reaching the intended target or critical assets, as can effective operational practices. These may prevent an attack from continuing and allow a timelier response, when supported by technical systems and effective operations.

Respond:
The response is normally generated by the activation (detection) of the technical system. The more effective the system the sooner the response (staff, security, or police). From initial notification until arrival at the scene the physical measures should provide an adequate delay during an attack that minimises the loss, harm, or damage caused to the organisational assets.

As can be seen from the above example the protective layers are mutually supportive and work to protect the organisation's assets. Due to the nature of archives, libraries, and other cultural venues, there is a need for the public and other third parties to have access and engagement with venues and their collections. That does not mean that the above principles and approach cannot be used, it is just that adjustments are to be made and different day/night strategies adopted.

The creation of effective security in depth should be a considered action. It should be based on realistic threats that exist or can be expected, it should consider the risk those threats pose, and it should faction in any vulnerabilities or areas of likely adversarial exploitation. Effective security in depth should make it harder for adversaries to be successful and reduce the risks being faced by venues.

As with all aspects of security it does not just happen and careful considerations must be made about balancing the robustness with the need to function as a venue, the type of measures used, cost, and overall benefits to the organisation. Planning, discussing, and agreeing on any security design is always appropriate and can reduce the risks of ineffective security designs and layers being introduced. Once designed, consider and test the effectiveness before proceeding with any new installations. Just because you have five layers of protection it does not mean assets are protected and vulnerabilities could have been created. (Image 5)

The size, nature, and value of the archive and collection might be such that professional security advice and guidance is needed, whether internally or externally. Preference should always be given to professionals who know and understand the cultural sector, and in particular archives, libraries, and dealing with special collections, not because they have superior technical knowledge but because they have a better understanding of the context in which security and operational matters need to harmonise.

It may not always be possible to implement certain types of security measures so there may be a need to double or triple up on other available options. This should not be used as a means of seeking a quick fix or cutting costs as this can increase risks and vulnerabilities, but it is an option providing the overall robustness and resilience is not compromised.

Introducing effective security in depth requires some knowledge of physical, technical, operational, and educational security measures. The following sections of this guidance will help increase their level of knowledge and make informed decisions about what is needed and best for their venues.

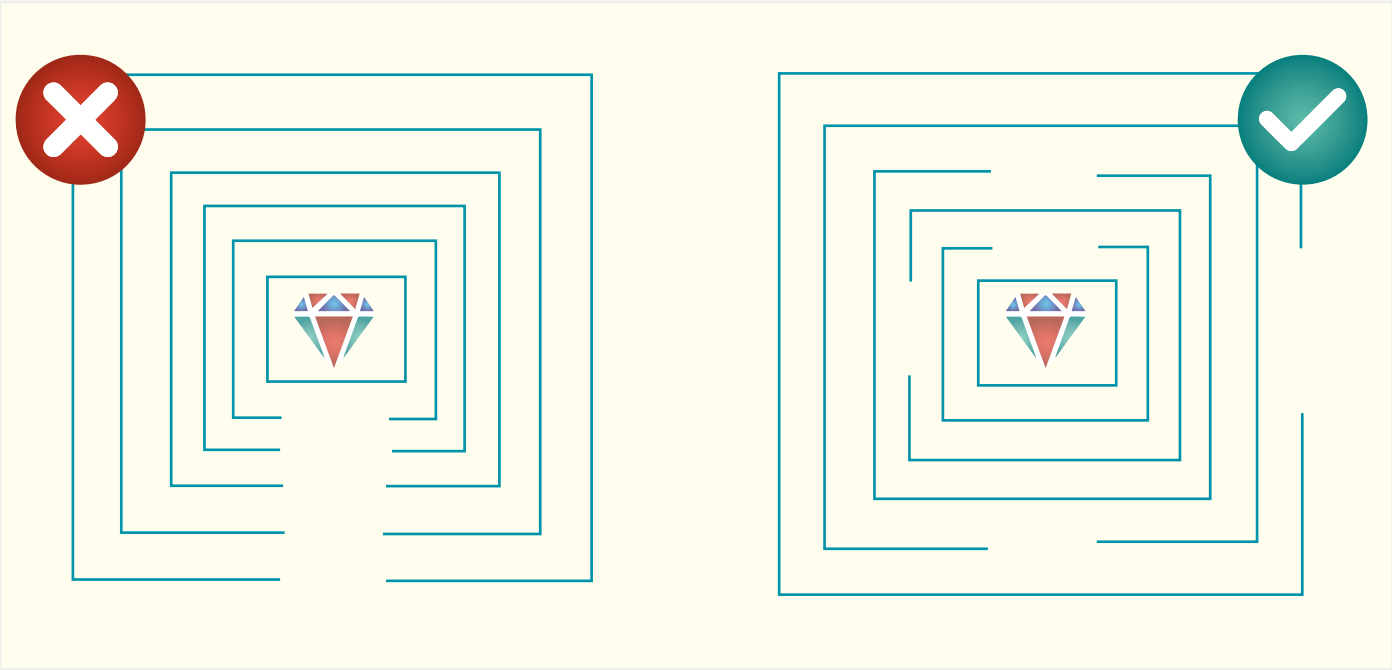

Image 5 – Effective layered security

6 Physical Security Considerations

Physical security is defined as "That part of security concerned with physical measures designed to safeguard people, to prevent unauthorised access to equipment, facilities, material, and documents; and to safeguard them against a security incident."

Good physical security is the cornerstone of effective protection of assets and as described above provides that delay while a response is mounted or may prove so effective that the attack is abandoned.

Effective physical security does not mean that there is a need to create a fortress that is uninviting to visitors, but it does mean that effective measures are considered based on the threats that exist and the risk they pose. It is always far easier and better if physical security measures are designed into a venue rather than retrofitting them (the same is true for technical systems), it is also normally more cost-effective.

As far as possible try to have security expertise working with the architects and project design team, especially if seeking coverage under the GIS (Government Indemnity Scheme). Police forces across the United Kingdom have DOCOs (Designing Out Crime Officers) and CTSAs (Counter Terrorism Security Advisers) from the Counter Terrorism Police (CTP) provide advice and guidance throughout the building design stages and can be an invaluable resource. However, they may not have the necessary experience of working within cultural settings and therefore advice and guidance from other sources may still be needed.

The same is true when considering introducing physical security measures into buildings that are 'Listed.' There are strict controls on what can be done at this type of property and professional guidance should be sought at the earliest opportunity so that time is not wasted considering a security measure that will never be accepted.

Where a property is listed never proceed without written permission being granted by the planning department as fines, the need to make good, and reputational damage can have a serious impact. Once permissions have been granted then effective physical security measures can be introduced.

When higher-grade physical security requirements are being considered these should be considered using appropriate standards that provide an adequate delay based on an attack using different types of tools. Some standards do not use appropriate testing methods and can result in unintentional vulnerabilities.

Tip 8:

Tip 8: Identify and engage with the local planning department at the earliest opportunity. Outline what you would like to achieve and explain the reasons why. The more you can justify that your proposals have been carefully considered the more likely approval can be granted. Consider it a collaboration and listen to what they say, compromises on both sides may be needed. They are not your enemy!

The testing undertaken by the Loss Prevention Certification Board and outlined in the Loss Prevention Standard LPS1195 is the most widely accepted within the cultural community and frequently used by Consultants from Arts Council England. However, other testing standards do exist, and physical security products tested by the National Protective Security Authority [9] (NPSA - formerly CPNI) and Secured by Design can be viewed as appropriate.

LPS1175 is the preferred standard due to the comprehensiveness of its testing processes relating to intruder resistance and physical security products, which is measured by the penetration delay achieved by the product, and not the total attack time which may be much longer. (Table 1)

DELAY	20 Minutes	A20	B20	C20	D20	E20	F20	G20	H20 **SR8**
	15 Minutes	A15	B15	C15	D15	E15	F15	G15	H15
	10 Minutes	A10	B10	C10	D10 **SR4**	E10 **SR5**	F10 **SR6**	G10 **SR**	H10
	5 Minutes	A5	B5	C5 **SR3**	D5	E5	F5	G5	H5
	3 Minutes	A3	B3 **SR2**	C3	D3	E3	F3	G3	H3
	1 Minute	A1 **SR1**	B1	C1	D1	E1	F1	G1	H1
TOOL KIT	**LPS 1175** Issue 8	A	B	C	D	E	F	G	H
	LPS 1175 Issue 7	A	B	C	D	D+	E	F	G

Table 1 – Extract from LPS1175: Issue 8.1 [10]

Different toolsets are used during the testing during the LPS1175 testing process which can be found on pages 28-34 of https://www.redbooklive.com/download/pdf/LPS1175.pdf.

When considering what physical security measures to implement it is often easier to work from the outside up to the most protected areas and thinking like a criminal (as with the vulnerability assessments).

When there is no in-house expertise then professional help should be sought from the police, professional security bodies, or trusted security professionals. Where relevant the following areas should be considered for physical security enhancements.

6.1Perimeter

A perimeter is defined as, **"the outer edge of an area of land or the border around it"** [11] and in a protective context identifies the outer line of control between public and private spaces. However, it is not always that easy as there may be a 'perimeter' at night but not during the day when the public have a right of access.

There may also be a boundary but no physical feature or one where natural topography has been used instead of a man-made structure. No two venues are the same and informed decisions need to be made based on the individual circumstances that exist. This could include not enforcing any perimeter controls and allowing everything up to the venue's curtilage to be surrenderable.

It has to be remembered that even fortresses have access points and as such breaches in the perimeter. These are often seen as a vulnerable point and any protection should be at the same level as the perimeter.

From a security risk management perspective, a clearly defined perimeter is a practical way of starting the

[9] https://www.npsa.gov.uk/physical-security
[10] BRE Global Ltd. https://www.redbooklive.com/download/pdf/LPS1175.pdf
[11] https://dictionary.cambridge.org/dictionary/english/perimeter

'security in depth' process. The threats/risks that exist will influence what is needed, budgets will influence what can be afforded, and aesthetics will need to be considered to ensure customer and internal acceptance.

Where a higher level of security is considered appropriate for any fence then the access points in that fence should offer an equal level of protection unless personnel are deployed at that location.

Appendix 3 identifies some of the more common perimeter types with advantages and disadvantages associated with each. Further advice and guidance can be found in BS EN 16893: 2018 Section 5.1 Building Location.

6.2 Grounds

An area that is often forgotten about when considering protective security is the grounds between the perimeter/boundary and the fabric of the venue. The area immediately surrounding buildings is referred to as the curtilage and may or may not form a part of the venue's footprint.

The grounds are an important part of a building's security and can directly impact the target attractiveness of a venue, or act as a deterrent. Wherever possible the grounds should be maintained to improve the natural surveillance for individuals using and protecting the space. Maintaining sterile areas where the space between the perimeter and the building fabric is effective, but normally unachievable. The proximity of any vegetation to the outside of the building should be reviewed, does it create an area of concealment where they could attack people or the building itself? If so, consider whether it is necessary or could be better positioned elsewhere.

External lighting plays an important part in the protection of assets as it supports the surveillance effort of security personnel and minimises the likelihood of criminals being able to conceal themselves. It also provides a positive reinforcement of operational effectiveness while allowing secondary surveillance to be undertaken by others. The use of motion sensor lighting is a positive measure and more cost-effective than continuous lighting or lighting on a timer at dusk and dawn.

Where possible the grounds should be considered during any security design stages so that areas of concealment are reduced, choke points created where individuals are funnelled, and clear lines of sight achievable by people and technology. The grounds should be considered during the security in depth process as it can work towards the Deter, Detect, Delay (through open space), and enable a response to be generated.

When there is little control of the grounds surrounding the venue (i.e. public footpaths, parks etc.) consider the 'curtilage' and areas that are in your control. As far as possible maintain and keep the area free from rubbish (highlights orderly behaviour and effective operations), avoid allowing anything to be secured or fastened to the fabric of the building, and make sure there is nothing so close that would allow easy access to spaces above the ground floor.

Tip 9:

Keep rubbish bins locked away until the day of them being emptied. Doing so may reduce the risk of them being used to access areas above the ground floor.

As far as possible, check the whole of the grounds and the venue's curtilage, looking for vulnerabilities which should include considering if a 'ram-raid' style attack is possible and whether physical features could be added that would reduce this risk.

Often archives, libraries and other venues used by ARA members are co-located with other departments or businesses without a degree of exclusivity to the grounds or spaces immediately outside their area of operation or control. That should not prevent the security risks from being considered and concerns (if identified) raised with the relevant controller of the space, preventing crimes, and reducing risks should be welcomed.

6.3 Walls and Building Fabric

Building designs have changed radically over recent times moving from more traditional brick buildings in the older buildings through to glazed curtain-walled designs in the more modern ones. Older buildings had thick walls which would require more effort to breach than modern blockwork or glazed walling.

The appearance, fabric, and condition of the external building walls will all have an impact on an adversarial mindset and any consideration they may have about the ease of ingress.

The use of modern products including blockwork and glass does not provide the robustness that traditional stone and brick walls do, and they may be identified as a vulnerability. It should also be remembered that glazing allows in light and ultraviolet/infrared (UV/IR) radiation which can damage archives, libraries, and collections. Where this type of walling exists consider the application of film on the inner face of the glazed curtain walling. This can help reduce the UV/IR risk, delay illegal entry, or reduce glass fragmentation subject to the type and thickness of the film used.

As far as possible, high-value collections or stores should not be in rooms directly accessible via an external wall. Where this is unavoidable then steps should be taken to confirm the exact composition of the wall and if necessary, increase its robustness by reinforcing the inner face[12] using modular walling systems, expanded

metal materials, or other materials that will cause a delay. This can include externally added materials, although attacking these defensive measures becomes much easier as they are exposed.

Many archives, libraries, and collections are housed in pre-existing buildings, some having listed status and therefore changes to the building fabric may be difficult. As far as possible the building fabric should not allow or facilitate the easy scaling of the building that enables criminals to access the upper floor or the roof. However, downpipes, buttresses, and ledges often exist in older buildings and therefore measures to prevent or limit easy scaling should be considered. Appendix 4 outlines some of the anti-scaling devices that can help reduce the risk from climbing adversaries.

The roof itself should always be considered an area requiring protection, especially when easily accessible. Traditional slate or tiled roofs where they are affixed to battens are easy to move, gaining access to the spaces below. The use of timber, plywood sheeting, or expanded metal sheets will increase the robustness afforded. In older buildings permission may be required and the weight of materials used needs to be considered.

Tip 10:

When roof access leads straight into stores, special collections, or areas containing assets of significance then LPS1175 SR3 rated expanded metal sheets should be used.

6.4 External Doors

Doors and other portals allow ingress into the building and egress out of them. Because of this, they are frequently targeted as a point of entry for criminals, while emergency exits provide a speedy egress from the building.

Each venue should consider its own circumstances regarding the doors being used, sometimes they fall within a listed category, sometimes they will be made of glass, or panel doors that are easily bypassed. How robust the doors are should be based on the risk to assets, ease of access to assets, and whether there are any stipulations around the type of door being used.

Where the door has historical significance, permissible steps to improve the robustness should be taken which can include changing the locks so that they are BS 3621/8621 compliant, adding bolts to the rear face, or hinge bolts. However, no adjustments may be allowed and the closest you can get to making it more secure is by using door wedges/jammers (fire safety requirements should be considered) which are not sophisticated but more effective than having nothing or accepting the risk.

[12] Ensure LPS1175 compliant, SR3 or higher (https://www.redbooklive.com/page.jsp?id=488)

Where no restrictions exist, consider the categorisation of assets immediately behind the door. If ancillary, any type of door can be used if the 'risk owner' accepts the protection levels afforded. However, if the door leads to more secure spaces and valuable assets then the layered security principle should be adopted, and a more robust door considered to maximise the delay caused.

Where higher levels of protection are assessed as being needed then a door should be installed that meets those requirements such as LPS 1175 SR3. These higher security doorsets are built to specific designs and any changes to the design could nullify its rating, although if the change is minor the protection afforded may not be impacted, it is just that it cannot be certified as meeting SR3 standards.

A venue may have assets where a higher level of protection is appropriate but because of funding or other factors, it is not able to afford purpose-built security doors. It is still appropriate to attempt to increase the level of protection afforded as high as possible and this can be achieved by using the following:

- Use a solid core timber door.
- Consider fitting a 3mm steel plate on the inner face of the door leaf.
- Add an additional mechanical locking device that conforms to BS 3621/8621 and is at least 5 levers.
- Invert the hinges so they are not exposed to the attack (outer) side of the door.
- Add two hinge bolts at 1/3 or 2/3rd height (or incorporated into the hinges themselves).
- Consider bolts or drop bars as may be appropriate.

While the above cannot be tested each measure can play a part in slowing down an attack, which may be all that is needed to deter the attacker.

The shape and style of the doorway could be such that the fitting of a security grille or roller shutter is the preferred option. While from a security perspective, an LPS1175 SR3 feature would be desirable, any metal shutter or grille can slow down an attack and may have a deterrence effect, preventing an attack in the first place.

Emergency exits will be a feature of nearly all venues, especially when opening to the public. Their design is such that there is a need for a speedy egress when there is a fire, or the alarm is activated. The construction of emergency exits has changed over recent times with a greater number of metal ones now being installed. The composition of emergency exits out into public spaces should be able to be secured by another means (for example, bolts and mortice deadlocks) rather than just a standard push bar, (subject to approval, planner, fire, etc).

The use of magnetic locking devices on external exits should be avoided as they are designed to 'Fail Safe' which means they will automatically open on the activation of the fire alarm system (FAS). Criminals are aware of this and unless a secondary locking device

exists the whole venue could become insecure by the intentional or false activation of the fire alarm.

The fitting of any locking devices or panic/emergency door bolts (containing glass/ceramic tubes) can be appropriate, as can the fitting of security-rated shutters/grilles, but approval must be sought if it is a fire exit. Equally, if an operational approach is taken to lock the doors once everybody has left the building then the organisational risk owners should document and approve it.

Tip 11:

Ensure that any method used to secure emergency fire exits have been agreed by the Fire Department and Council Planners. Once agreement given confirm that the risk owners approve it.

Each door should be considered individually as the loss, harm, or damage to assets will vary greatly and some spaces may be viewed as 'surrenderable' due to the number of other layers between that point and critical assets.

Other external access points to consider include vents, hatches, cellars etc., and how these are secured needs to be considered based on the risk to assets, including the sewer system (especially in historical buildings). If accessing them brings somebody near a 'protected space' or critical assets, assess if additional physical security measures are needed.

6.5 External Windows

Windows traditionally consist of timber frames fitted into a wall or roof, with glass panes added to allow people inside to see out, light to enter buildings, and in some cases for environmental conditioning. The concept has not changed much, although the designs and materials used have become far more sophisticated, apart from the continued use of glass.

Glass[13] is not a secure material and is prone to accidental and intentional breakages. Externally, glass is used in windows, doors, skylights, and other areas where light enters buildings (including glazed curtain walls as outlined earlier). Criminals will use windows to enter a building, especially if they can see physical security enhancements to doors and other portals. There is also an increase in attacks through windows taking place above the ground floor where physical security enhancements have been made, including at historical and cultural venues.

[13] 'Glass is a non-crystalline solid that is often transparent, brittle and chemically inert'.

Most safety glass conforms to either BS6206 or BS EN 12600 both of which use pendulum impact or drop height tests to measure performance. Toughened and laminated glass is normally measured against this standard.

EN356 standard is specifically for 'security' glazing and has eight categories of resistance against manual attack. This standard is supposed to simulate a human attacking the glazing. LPS 1270-approved glazing is tested by humans in the same way that LPS 1175 does against physical resistance to attack. EN356 is not as accurate a measure of attack resistance as LPS1270.

EN356 and P1A-P5A are tested as per BS6206 and BS EN 12600 and are viewed as low-level security glazing. P6B-P8B are tested using a mechanical hammer and axe blow and are viewed as the 'Higher' level of protection. LPS 1270 uses a range of tools as per LPS1175 and is rated between 1-8 based on the level of resistance (8 being the highest 20-minute work time within an attack duration of 60 minutes).

It should be noted that the more secure glazing is the heavier the weight and the greater the cost, which may be relevant in buildings where load bearing is an issue. Appendix 5 outlines the most common types of protective glazing used in buildings.

The protection of any window must be risk-based, the greater the risk/asset significance the more protection should be afforded. (See Appendix 6) There are also financial and operational considerations about what is used in the protection of windows, the level of protection will be based on the venue-specific circumstances that exist and the level of risk and vulnerabilities identified.

While the above relates to external windows it is equally as applicable to skylights and other glazed features on the building exterior.

6.6 Internal Physical Features

Just because the shell of the building is protected it does not mean that inner layers of security do not need to be applied. This is especially true when the archive, library or collection is in a building that is shared with others or where there is not full control.

A central reception desk where everybody reports is a great physical barrier as it forces users to engage with staff, who may then remember certain individuals especially if they do not fit an expected visitor profile. However staff need to be careful to avoid discrimination or making unfair pre-judgements, bearing in mind the stipulations of the Equality Act.

Another example of where physical and operational measures come together is the control of bags and other items used for carrying non-essential or banned items. The provision of lockers is an indirect risk reduction strategy as it lowers the likelihood of objects being stolen or illegal items being taken into the Search/Reading Room.

When the building is closed to the public and operational teams it can sometimes be easy to compartmentalise the spaces so that if somebody gained entry from outside the building, they would still have to bypass other physical barriers before they reached any of the critical assets. Therefore, by adopting a policy where doors are locked, and electronic locks are used helps create further delays before an aggressor reaches critical assets.

There should always be a clear delineation between public spaces and back-of-house areas. Physical security means of controlling who enters what areas should be introduced and can be as simple as locking all rooms where the public are not permitted, using a push button combination lock (PBCL), through to a more modern electronic access control system that provides an individual with permission to access certain areas.

With other internal and external stakeholders, an agreement should be reached as to how your specific area of responsibility can be locked down at night or when your space is closed operationally. There may be a difference in approach between general search / reading rooms and spaces designated for the use of special collections.

During the day there will be an increased use of the search/reading rooms, therefore, the physical layout of the room is important to ensure that areas of concealment are reduced and the positioning of tables and desks that staff have a clear and unobstructed view of the room. Ideally, there should be nobody with their backs to anybody invigilating or working in the space. The physical presence of a member of staff who has a clear line of sight (supported by CCTV) may be sufficient to deter a criminal act from taking place. (Of course the invigilator is also there to provide help, advice and guidance on handling of documents).

There is a need to consider other forms of attack that are not theft-driven, and this can include incidents of violence, protesters, or acts of terrorism. Irrespective of how unlikely these acts are they cannot be ruled out therefore, consideration should be made for evacuation or locking down certain areas to prevent physical ingress. The following should be considered; safe routes, are there predetermined shelter-in-place locations? How many people do they hold? Do they have escape routes if the attacker tries to gain entry?

All are sensible questions to ask and areas where professional help may be needed from the police through CTSA (Counter-terrorism Security Advisors) or DOCO (Designing Out Crime Officers) or other trusted security professionals with the knowledge and experience to assist. Advice is also available on ProtectUK, particularly the Publicly Accessible Location (PALs) guidance, concerning attack scenarios, lockdown, invacuation and evacuation procedures. [14]

6.7 Stores

Archives, libraries, and collections are stored for future retrieval, safekeeping, and protection from all threats. Collection stores can generally be split into two types, 'general' and more secure stores. This section will deal with the general storage practices while 6.8 will look at more secure storage.

The store or 'stack' can contain millions of items, many of which date back hundreds of years outlining so many aspects of life in bygone eras. While most will not have a specific financial value attached to them, they are all valuable and should be protected.

Doors leading into the stores should **at least** be constructed using:

- Solid core timber door [15]
- An additional mechanical locking device that conforms to BS 3621/8621 and is at least 5 levers.
- Inverted hinges so they are not exposed on the attack (outer) side of the door.
- Add two hinge bolts at 1/3 or 2/3rd height (or incorporated into the hinges themselves).

Where possible electronic ACS (Access Control Systems) should be used so that access control is managed, auditable, and restrictions on who enters can be applied. Where this is not possible other operational practices need to be considered.

Walls leading into the stores should be robust and provide sufficient resistance to further delay any attack and forced entry, this is also applicable to the roof.

Due to most archives and libraries containing flammable and combustible materials fire is one of the greatest risks that exists. As far as possible the store should be constructed using non-flammable materials and preferably materials that offer 4 hours of fire resistance, although any additional resistance is better than none.

The volume and nature of collections requiring storage will dictate the size of the store and the type of stacks being used.

Specific guidance can be found in standards BS 4971: 2017 Conservation and care of archive and library collections and BS EN 16893: 2018 Conservation of Cultural Heritage. An excellent reference document has also been produced by the British Library regarding the most effective use of shelving, outlining pros and cons associated with each type. As far as possible the most appropriate shelving/ containers should be used to better protect and preserve the collections [16].

Archival stores should not be used as a secondary 'junk' room due to space restrictions elsewhere, unnecessary non-archival materials, especially combustible ones, should be removed and stored elsewhere.

[14] https://www.protectuk.police.uk/evacuation-invacuation-lockdown-protected-spaces

[15] A fire door with a 120 - 240 minute fire delay rating provides the appropriate level of fire resistance as well as physical robustness.

6.8 Secure Storage Facilities

A secure storage facility should be used where there are 'Special Collections' or items of significant financial or historical value. By their nature, these documents have an increased attractiveness to criminals, especially those from organised crime groups due to the increased financial rewards.

Unless a completely secure 'bubble' can be created no 'secure store' should be positioned against an outer wall where a 'ram-raid' type attack can be carried out. The location of the secure store should be known only by those who 'need to know' and access must be tightly controlled. Providing that accessibility is not an issue, elevation from the ground floor helps create a spatial barrier (additional delay) which must be bypassed before an attack starts.

As far as possible, purpose-built LPS 1175 C5/D10 rated doors should be used to restrict access into the secure store. The walls should be constructed using multiple-thickness brick, concrete, or suitable blockwork, single layers of brick/block should be avoided wherever possible due to their vulnerability to blunt force attacks. If necessary, the walls can be suitably reinforced using LPS 1175 C5/D10 modular walling systems or expanded metal sheets.

Where this cannot be achieved any practical means of enhancing the levels of protection should be considered and can include the securing of sheet metal to the inner/outer face of the store walls, shelve placement, non-highlighting of documents or even secondary security containers within the 'secure store' such as safes and vaults.[17] Any reference to a wall in a 'secure store' also means the floor and the ceiling. Fire preventative measures similar to those outlined in 6.7 above should be considered.

Access into the store should be restricted and if a programmable ACS is not available, key control measures should be introduced. This should include the provision that the keys never leave the premises and are secured within an appropriate safe/security container when not in use.

6.9 Exhibiting and Display Cases

There will be times when a venue will want to exhibit collections, it could be that they are on permanent display in a gallery, corridor, or highlighted space and as such away from the normal levels of security that are afforded in stores. It is important that the balance between outreach and asset protection is maintained so that unnecessary risks are not introduced.

When planning an exhibition consider what is needed to protect the assets and whether they are being placed at increased risk. Areas of concealment and darkened areas should be avoided so that invigilation is not made more difficult. Consider how items are secured onto walls or plinths and think about any potential safety issues, e.g. if a stone bust fell onto a child. Pictures should be secured using mirror plates and security screws, or other suitable locking devices.

Small removable exhibits should not be positioned close to exit doors[18] and while a frequent practice, rope delineation barriers will only prevent compliant visitors from approaching exhibits, with negligible effect on non-compliant individuals or groups.

Archival items will always be displayed within a protective enclosure such as a display case. In many older venues display cases are made of wood with float glass inserts. To this day these cases exist and while providing demarcation and preventing the handling of sensitive and fragile objects they are not suitable as a physical security barrier. Even previously provided guidance regarding types of glass, thickness etc. have been superseded because of the use of more sophisticated tools in the arsenal of the criminals. Older cases may also be prone to environmental problems such as off-gassing of non-archival sealants / paints.

If the older type of display case forms a part of the experience and aesthetics, then providing it does not contain high valued articles or those of historical significance it can continue to be used providing the risk, including any environmental risk, is accepted by the owner.

A modern security display case will provide increased protection against attack, but they can still be bypassed. The guidance[19] identifies the following:

- As a minimum the glass should comply with BS5544 which is generally met by the use of 11.5mm five-ply laminated glass. (Acrylic/Perspex with a minimum thickness of 12mm is still shown as being acceptable.)[20]
- The case is to be steel framed with flanged corners to hold the glass in place. These flanges should have at least 20mm overlap around the glass to prevent a levering attack on the corners of case.
- Unglazed sides to the case will need to be of steel. MDF type materials are unsuitable.
- The case is to be secured with high-standard locks. Generally, at least two locks should be fitted to each opening in the case. Ideally, locks should be concealed and protected from direct attack.
- Lighting to be housed in a separate light box compartment secured by different locks to the main display section which will enable the lighting system to be maintained without opening the display section.
- The case to be constructed to prevent access to the collection material via the light box compartment.
- Similarly, if the case is built over a storage compartment this should be secured separately with the case constructed to prevent access to the collection material via the storage compartment.
- The case must be robust and sturdy so that it cannot be readily moved if knocked.

[16] See Appendix 1 – Point 61
[17] BS EN 1143-1:2019 refers

- Internally any shelving or display elements to be fitted to prevent collapse or movement if the case is knocked.
- Ideally hinges should be concealed and thereby protected from direct attack.

The only difference with the above advice is brought about by the improved protective elements of glass and therefore the use of LPS 1270 security rating 6-8 or EN 356 P6B-P8B rated glass should be considered especially if the case contains high-valued items (financial, historical, global significance) or is at an increased risk of being attacked due to ideological, racial, political, or environmental reason. There is a potential cost implication and increased weight placed on the steel frame, but the likelihood of a successful attack is significantly reduced. Alarms can also be fitted to cases to enhance security further.

[18] GIS Guidance Annex D stipulated within 2 metres.
[19] Collections Trust, Updated 2013; https://collectionstrust.org.uk/wp-content/uploads/2016/11/SecuritySpecification_AttackResistentDisplayCases_02.pdf
[20] GIS, Annex D: para 12

7 Technical Security Measures

For this guidance, a technical security measure is one that has a degree of automation and responds when the system detects a change in the expected circumstances causing the alarm to activate. With the advances in technology and the ability to integrate multiple systems to mutually support each other technical security systems can do so much more and further help reduce the risks being faced.

Technical security systems do not prevent ingress or cause a delay to a blunt force attack, but they can deter and ensure a timelier response to an attack that may be taking place.

This guidance will concentrate on the main technical systems that ARA members will use as well as others that can have positive benefits to the archives and libraries community and will include:

- Intruder Detection Systems
- CCTV/Surveillance Systems
- Access Control Systems
- Fire Alarm Systems
- Sprinkler System

7.1 Intruder Detection System (IDS)

An IDS, commonly referred to as a 'Burglar Alarm' is a system that sends a signal locally or to an Alarm Receiving Centre (ARC) to say that a sensor has been activated indicating an intruder or an attempt to defeat physical defences.

Any IDS installed should meet the required standards (BS 8243:2021 and BSEN 50131 (2017) and be installed by a reputable installer.

Tip 12:

Use NSI Gold or SSAIB approved installers. If covered under the Government Indemnity Scheme this is a requirement and provides a quality assurance that the installers are competent.

There will now be very few situations where an IDS does not signal to a certified ARC that operates 24/7. It was previously recommended that the signalling be sent using RedCare or similar devices. This indicated if the telephone lines had been cut or tampered with. However, with the advanced digitisation of telephone networks, this type of signalling will be obsolete in the UK by 2025. (Note: In Ireland, Grade 4 signalling should still be sought while analogue lines continue to be used.) Therefore, IDS signalling should be switched to equipment that provides DP3/4 signalling which equates to the old Grade 4 signalling. There is no change in the Grading of the alarm system which should continue to be Grade 3.[21]

Tip 13:

Check with the alarm service provider and ask them to confirm in writing the Grade of the alarm and signalling equipment. If it is not Grade 3 alarm and Grade 4/DP3 signalling request that it be upgraded to meet this standard.

It is sensible to have the earliest notification of an attack/trespassers and therefore the system should be arranged to facilitate this. A lot will depend on the type of sensors being used and how they are configured. Appendix 7 offers some guidance on which sensors may be the most suitable for use in the particular circumstances.

Modern alarm systems allow zones to be established that can remain alarmed or disarmed as needed.

Tip 14:

All secure storage facilities should be on a separate zone/loop that leaves the store alarmed when the rest of the building may be functioning as normal. .

A normal sensor configuration within a building should be based on the operational requirement (OR) and expected response that it will generate.
Generally, external doors should be fitted with door contacts or vibration sensors and be covered by a motion sensor or other sensor to provide confirmatory notification and full alarm activation. Any area leading to or around a secure store should have the ability to detect movement towards it.

As a minimum, secure stores should be fitted with contacts/vibration sensors to any portal leading into the space supported by a motion sensor in the open areas so that a full activation is achieved, irrespective of the sensors surrounding the secure store. If appropriate, vibration/shock sensors should be positioned at 2.5-metre intervals around the inside of the secure store, especially if the wall is exposed to a vulnerability such as glazed curtain walling.

[21] Grades below 3 relate to residential properties and Grade 4 systems are not installed apart from in extreme cases where there is absolute control.

General stores (stacks) could be covered by a motion sensor outside each access point, door contacts and another motion sensor should be installed inside the stacks.

Emergency exits should be fitted with sensors so that if the doors are opened during the day a notification will be received which could also include a localised sounder or a message to a designated point, enabling a timelier response. Out of hours, the sensor would revert to being a part of the overall IDS.

Not everybody should be given alarm codes or fobs to activate/deactivate the system, this is especially true for secure stores.

A URN (Unique Reference Number) must be allocated to the alarm system so that in the event of a confirmed alarm the police, subject to availability, will provide an immediate response. If there are two false alarms in any rolling 12-month period, then the police may revoke the immediate response which in all practical senses means one may not arrive for a very long time.

If appropriate, professional advice should be sought from the police or suitably qualified individuals who are preferably independent of any future sales or particular products.

7.2 CCTV (Visual Surveillance) Systems

CCTV or Visual Surveillance Systems are an effective crime prevention tool, often dissuading people from committing opportunist criminal acts and also effective for post-incident analysis and evidential purposes.

There have been great advances in the capabilities of cameras including daytime and night monitoring, the use of video analytics, and a reduction in the size of the units, making them more aesthetically pleasing. The digitisation of CCTV systems has improved the quality of images and in many cases analogue systems are becoming obsolete (poorer quality, no spare parts, and few engineers who have the necessary skills).

The storage and capture of data has also switched from VHS recorders through to cloud-based recording systems that allow remote access via laptops, tablets, or even mobile phones. In many cases, NVR (Network Video Recording) is used as opposed to DVR (Digital Video Recording) which converts analogue images into digital ones before recording. The amount of data storage needs to be considered and will be influenced by the number of cameras being used and the increasing cost associated with data storage.

There have been several changes in legislation as it tries to keep pace with technological advancements. The main legislation directly or indirectly impacting the use of surveillance equipment and the storage of data held by an organisation which is classed as 'personal data'. In the UK it is the Data Protection Act 2018 which incorporates the government's implementation of GDPR[22] (General Data Protection Regulations) which is in use in Ireland as an EU member state. Everybody responsible for using personal data must follow strict rules called the 'Data Protection Principles 'that the organisation must make sure the information is:

- used fairly, lawfully, and transparently.
- used for specified, explicit purposes.
- used in a way that is adequate, relevant, and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, ordamage.

There is other legislation which primarily affects 'Public Bodies'[23] which are defined as *"A public body is a formally established organisation that is publicly funded to deliver a public or government service, though not as a ministerial department. The term refers to a wide range of public sector entities."* That therefore means that local government organisations, the National Archives, and Arts Council England could fall into additional legislation that included:

- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Investigatory Powers Act 2016

Note that separate legislation is in force within the Republic of Ireland and for the devolved administration within Scotland.

An important consideration when using CCTV/ Surveillance cameras is the legal compliance around the reason for it being used. If the public has a right to enter a venue whether for free or as a paying visitor then there has to be a clear declaration about CCTV cameras being used and the reason why, which is normally captured in the line **"For the prevention and detection of crime."** The same is applicable for members of staff working in a venue although the way they are informed could be during an induction briefing, within a contract of employment, as well as signage.

Anybody has a right (visitor or employee) to see any video footage of them within a venue and it must be provided within a month of the request. It is acceptable to decline if the recording has already been removed due to the retention period.

There is no hard and fast rule regarding CCTV imagery retention periods, but the general advice is 30 days recording so that should anything suspicious be seen or an investigation commenced there is some historical data that can be reviewed. Archives may wish to set a longer retention period in relation to operational processes such as audit, i.e. how long it is likely to be before it is realised an item is missing and there is a need to view CCTV

[22] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/

[23] https://www.gov.uk/guidance/public-bodies-reform#:~:text=A%20public%20body%20is%20a,range%20of%20public%20sector%20entities.

footage. Where suspicious activity has been seen then the data can be downloaded and retained for future use, especially if the recording is on a continuous loop and overwriting occurs. This is equally important if accidents are captured, or any potential legal proceedings occur.

The type, size, and capabilities of any CCTV cameras that are used should always be based on what you want the cameras to do, the Operational Requirement (OR). It does not have to be a complicated task and most people will be able to have a good go at it themselves without the need for technical expertise. However, unless there is technical knowledge available within the organisation of camera capabilities and functionality it may be more cost-effective to seek professional advice first.

CCTV/Visual surveillance systems are not cheap, so careful consideration needs to be made about numbers and positioning. The following questions should be considered:

- How many cameras are needed?
- Where are they needed?
- What do I want the camera to do?
- Are there any areas where I must have camera coverage?

The main uses of any surveillance system is to act as a deterrent, monitor suspicious activities, and to provide evidence of events whether illegal or operational. Unless there is live monitoring then most CCTV systems are used 'post-incident' to review what has happened and/or to share with others for investigations. Where there is live monitoring, technology can greatly assist and provide an 'alarm'[24] state if somebody enters a certain area (trip lines) or people get too close to objects (geo-fencing).

External cameras may or may not be permitted and permission/approval may be needed from the planning department. Equally, the benefits of having external cameras versus the cost of installation may be prohibitive. There is no wrong or right answer it will be specific to the individual venue, approach to risk management and level of resourcing. Externally it is recommended that the following areas be covered using CCTV cameras:

- Whole exterior of the building (If financially viable)

OR

- Any 'choke' points where visitors are forced to walk through to reach the venue (i.e., narrow passageway, gates, etc.)
- Access points into/out of the venue
- Any pre-identified vulnerable areas
- Scaling points
- Walls behind which are critical assets.

Internally there are certain areas where the positioning of cameras is recommended, and these include:

- Main public entrances
- Search/Reading rooms
- Entrances to stores (general)
- Inside and outside secure stores
- Loading/delivery bays (documents /collections, not retail)
- Retail spaces
- Reception desks
- Server/plant room doors

A point to note regarding CCTV in secure stores. There may be individuals who question the need for cameras in stores and see this as a comment on their integrity and trustworthiness. From a security risk management perspective, it is nothing of the sort. Having cameras that can identify who enters the store and their activities can go a long way in protecting individuals and ensuring additional care is taken in the safeguarding of critical assets.

As can be seen, there are many areas where surveillance coverage is recommended, this does not include the general area coverage which will be for the venue to prioritise locations and number of cameras. Guidance on the design of CCTV systems is provided by the Home Office and valuable information regarding CCTV systems can be found in Appendix 1.

Apart from the most basic of CCTV systems the advice and guidance of security professionals may be appropriate to prevent the overspecification or unnecessary purchase of equipment.

7.3 Access Control Systems (ACS)

Access control systems as defined in this document relates to the means of operating or checking an authority of a person to access into certain areas. They can play a role in securing physical spaces and ensuring the safety of individuals and assets.
Traditional methods using keys still have their place, especially when dealing with listed buildings where the addition of anything on doors will not be permitted. However, keys have their drawbacks in the sense that they can be:

- Copied
- Lost
- Difficult to manage.
- Difficult to audit.

Modern ACS can be programmed to permit individuals to enter certain areas and during certain times. They can provide auditable information about who has entered what space, when, and if they have attempted to enter other spaces. Systems can now be programmed to ensure dual verification which can include the presentation of a card and a pin number, biometrics, retinal scanning, voice recognition, etc.

A useful guide encompassing many aspects of access control is 'A Specifier's Guide to Access Control Systems' was produced by the British Security Industry Association (www.bsia.co.uk) and remains an appropriate reference point.

[24] This is where that camera provides an indication of activity either through filling the screen or a visual indication to the operator.

The following are areas where it is appropriate to use ACS, although different permissions may be required and there will be venue variations:

- Staff entrance/exit point [25]
- Line between public and back-of-house spaces
- Server rooms
- Stores
- Secure stores (Special Collections)
- Search/Reading rooms[26]

The ACS can be fully integrated with the IDS, CCTV, and other technical security systems and although not suitable for every venue it should be seen as a security, operational, and management tool.

The standard requirements covering the use of ACS is outlined in BS EN 60839 (Parts 1, 2, 31, and 32)

Care has to be taken when selecting the type of locks being used in any ACS as there are legal obligations regarding fire life safety and security considerations as well as the protection of assets. ACS that is linked to 'maglock' devices means that in the event of a fire all locks 'fail-safe,' by disconnecting power to the lock and the door becomes insecure. Therefore, 'maglock' type devices should never be used in stores, especially secure storage areas containing 'Special Collections.' Electronic 'strike' locks generally 'fail-secure' which means they are better for security, and they are a lot more discreet than bulkier maglocks.

Where needed professional advice should be sought, although additional supportive information is provided in Appendix 1 – Signpost Document.

7.4 Fire Alarm Systems (FAS)

Fire continues to be the biggest danger facing archives, libraries, and cultural venues, once items have been destroyed by fire the contents are gone forever unless a digital surrogate has been created. As such it is appropriate that steps are taken to reduce the risk as low as is reasonably practicable and FAS plays a vital role in achieving this.

The UK Regulatory Reform (Fire Safety) Order 2005 stipulates that all buildings other than private homes must have adequate fire safety measures in place, which may or may not include automatic fire detection systems. In Ireland a similar law exists in the form of Fires Services Act (1981 and 2003). Both place a legal duty on anyone in control of the premises to undertake a fire risk assessment and put in place and maintain general fire precautions. Following the Grenfell Tower disaster, additional guidance and requirements will be placed on the 'Responsible Person' under Section 156 of the Building Safety Act 2022[22] which in the UK came into force on 1 October 2023.

BS 5839 is the recognised standard used in the design, installation, and maintenance of FAS in the UK while in Ireland the Irish Standard I.S. 3218: 2013 applies. FAS consists of different parts that detect and then notify of a fire. Detectors are normally a mixture of smoke and/or heat detection and the alarm is the notification back to an approved ARC (Alarm Receiving Centre) and where subject to the existence of a URN notifies the local fire service.

Alarm systems are graded using letters and numbers, where the lower the number represents the most protection Appendix 8 provides guidance on the meaning of each category.

It has traditionally been recommended that cultural venues (especially those containing items from National Collections) should be equipped with an L1/P1 system to reduce the loss and damage to documents. The P1 categorisation is more important where large collections and amounts of combustible materials exist, they risk increasing the spread of fire.

Any fire alarm system and fire prevention actions taken at any venue should be based on a Fire Risk Assessment (FRA), which is a legal requirement if more than five staff are employed or the venue is open to the public. Due to liability issues if you are anything other than a very small venue that does not open to the public it is recommended that professional advice and guidance be sought.

7.5 Sprinkler System

There appears to be a continued concern by some museums, archives, and libraries about using sprinkler systems as a firefighting tool, this is despite the increased reliability and effectiveness of the systems. The Fire Protection Association stated, *"the National Fire Chiefs Council found that in 94% of fire incidents, the system functioned as expected and in 99% of cases the controlled or extinguished the fire."*

The decision to use sprinkler systems will be an individual matter for venues. However, from a risk management perspective, it is easier to suffer the pain of drying and repairing documents than having no documents at all.

There is very little legislation regarding the use of sprinkler systems that does not relate to residential properties. There is a reference to commercial buildings with a single expanse (non-compartmentalised) of 20,000 metres or more requiring a sprinkler system. However, it is further confused because buildings that pre-date 2007 are not required to have them installed.

Each venue will have to consider the benefits (primarily controlling and extinguishing fires before the arrival of the fire service) against the negatives (cost of installation, water damage etc.) and reach a decision.

There are several de-oxygenating or 'misting' systems that exist and can be applied. However, careful consideration has to be taken regarding any health and safety legislation and concerns. Where necessary professional advice should be sought. See also BS EN 16893:2018 section 6 (Fire protection and prevention).

[25] Using only an electronic access card is not recommended unless there is somebody on-site 24/7 entry and final exit points should also be covered using a secondary locking device in case of a system failure.
[26] Not that members of the public have cards but where a member of staff permits ingress.

8 Operational Security Considerations

Operational security considerations are how an organisation delivers and implements the security governance that have been created. In many cases, the operational aspects are what the public will see, which can also mean those conducting hostile surveillance will see and evaluate the effectiveness of operations.

The levels of alertness demonstrated, and awareness shown by all members of staff against possible hostile threats will be recognised by those with adversarial intent, whether internal or external. The greater the alertness and vigilance of staff the less likely hostile actors are to think that the venue is an easy target.

Operational security will very much depend on:
- The organisational approach to security.
- The quality of the governance that exists.
- The nature and profile of the venue.
- The assets held within.
- Funding resources (staff etc.)
- The number of staff on duty.

Considering the following operational security activities will support the robustness of any layered security approach adopted by the venue and help reinforce the concept of, *"Security is everybody's responsibility"*.

8.1 Security Responsible People

Not every venue has the luxury of dedicated security personnel, but every organisation should have an identified Security Responsible Person (SRP). This individual should be an influencer, effective listener, be calm under pressure, and have a degree of understanding about security and the protection of assets.[30] The SRP should be the conduit where operational concerns can be raised to the Leadership Team and directions can be delivered to the operational teams.

The selection of an SRP is important, and they must have a position within the organisation or the character where all parts of the organisation feel comfortable discussing things with them. They need to have a proactive approach to work and be a problem solver who is has the moral courage to defend a position that may not be agreed with by senior managers, if justified.

Where there is in-house security there are advantages and disadvantages. The primary advantage is that a focal point already exists. The disadvantage is that in many cultural venues, the security team are seen as 'enforcers' of rules and not as a part of the wider effective functioning of the organisation. Security teams are not a police force and should not be run as such, there is more to the protection of assets than the prevention of crime.

An effective head of security (who can be the SRP) should be an enabler of organisational objectives that underscore the reason for the organisation's existence. They need to understand the functioning and activities of each department and by understanding this they will be able to better protect the assets, but from an informed position as opposed to working in a silo.

Security staff often come from a policing or military background with an expectation that they know and understand 'security', but that is not necessarily the case, especially when it comes to understanding the specific threats and risks those holders of collections face. There may be a need for the security team to be upskilled and for the head of security to receive specialist training that will enhance their capabilities to support the organisation.

The SRP should be responsible for updating the security governance and presenting the annual report to the Leadership Team. They should also be seen as the focal point for external liaison especially with the police or other governmental departments. Where there are VIP visits, they should be the point of contact for any security arrangements that are or need to be made. There is a common occurrence that those responsible for events take over everything without the specialist knowledge or experience that the SRP brings. An effective SRP is a great asset to any organisation and should be viewed as such by all and they should be supported by senior managers to help achieve their aims.

8.2 Opening and Closing Activities

This activity is so important for ensuring the integrity and protection of the organisational assets. Irrespective of whether you are a single venue or a site of multiple occupancy there will normally be a time when the archive, library etc. is closed to staff, researchers, or the public and locked securely. If the venue is closed and locked, then for operations it has to reopen at some point.

The importance of this activity is heightened because there are several ways that mistakes can be made which increase the risk to the organisation and its assets. These include:
- Doors being left insecure.
- People can be locked into premises.
- Alarms not being set correctly.
- Windows being left open.
- Heaters being left on.
- Taps being left running.

[30] If additional training is needed to upskill this should be identified as outlined in Section 9.

By adopting a structured approach to opening and closing the likelihood of any of these events occurring is reduced.

Where areas are controlled due to their contents and significance/value of documents (i.e. Special Collection stores, 'Stacks') then separate opening and closing procedures may further exist. This will be for venues to consider based on their individual circumstances.

Hostile reconnaissance may be carried out by organised crime groups, protesters, or terrorists will seek to establish a pattern of life which includes observing opening and closing times, who does it, where do they go to or come from. If somebody continuously locks the venue and goes straight to the pub every night, this is information that could be exploited.

Opening and closing activities will normally involve physical and technical measures (setting alarms and locking doors) and require a degree of education to ensure mistakes aren't made.

It should also be remembered that there may be a need to include multiple opening and closing instructions. For example, opening activities for staff at 0900hrs, and then at 1000hrs for the public. The procedure can have multiple stages depending on the nature of the organisation. Appendix 9 shows a basic Opening and Closing Procedure for a venue.

8.3 Access Control Activities

Despite there being a desire across the cultural sector to be more open and allow greater access across the venues there is still a need to protect staff and assets. One of the best ways of achieving this is by having robust access control measures in place that identify different spaces within the venue and who has permission to enter them. Access into more sensitive areas should be controlled and limited on a 'needs' basis and not just because they hold a certain position within the organisation or are involved in security activities. When considering which areas require what level of control it is helpful to consider the following Table 2.

Many organisations have electronic access cards[31] that also double up as a form of identification which allows control of access through zoning and granting of permissions. They also allow challenges to be made if somebody who is unknown or not wearing a pass is seen in anywhere other than a 'General' area.

However, smaller venues may not have the resources, need, or desire to warrant installing such systems and then have to rely on effective operational practices or using physical barriers such as PBCL (Push Button Combination Lock), signage, or even ropes to delineate private areas. Whatever method is used it should be documented and outlined as a procedure. Appendix 10 provides a basic access control procedure where access control cards are not used.

Access control must be layered and proactively managed including the requirement that when somebody leaves the organisation their keys, passes, and identity documents must be surrendered and where applicable they should be removed from any ACS.

8.4 Collections Management Activities

Assets can only be protected if they are known, accounted for and correctly managed. This guidance highlights the importance of proactive prevention and protection but if we don't know what assets exist, where they are, or the criticality of them, then their protection becomes much harder. For guidance on overall approaches to Collections Management Policy, see the Collections Trust. [32]

It is critical, irrespective of whether recorded in ledgers, spreadsheets, or by using software that all collections

[31] Section 7.3 refers
[32] https://collectionstrust.org.uk/wp-content/uploads/2016/10/Collections-Management-Policies.pdf

Zone	Description	Level of Control
General	Areas where the public/visitors can enter and use the facilities with few restrictions. Including public libraries, cafes, and toilets.	**Low**
Controlled	Areas where there should not be general access for members of the public/ visitors and where some restrictions should apply. Including staff offices, search/reading rooms, and cleaning cupboards (due to contents).	**Raised**
Sensitive	These are areas where access should be controlled and restricted to those with an operational need to enter. Including 'stacks', stores, operational rooms, and finance offices.	**High**
Critical	These are areas where access should be severely restricted and permitted to only those with a specific operational need to enter that area. Including special collection stores, secure storage facilities, and server rooms.	**Very High**

Table 2 – Access Control Zoning Scale

(assets) are documented as fully as possible and accounted for when in storage, on display, or loan. It means that there are processes that are auditable by third parties and the likelihood of items being misplaced, lost, or stolen are reduced. Archives face a significant challenge in this area given the scale of holdings and legacy practices. While it is unrealistic in most cases to expect every piece of paper to be catalogued, the organisation should identify a clear approach to documentation and as far as possible eliminate black holes such as unaccessioned or entirely unlisted boxes of material. There should be measures in place to regularly audit or stock-take holdings and to prioritise any specific areas of concern.

The question of whether and how to mark documents (e.g. via application of an ink stamp) is contested, however this should be considered as a matter of organisational policy. From the perspective of police attempting to reunite recovered documents following apprehension of a thief, the lack of any marks of ownership presents serious problems.

When material is uncatalogued, processed, or adequately managed it places the organisation at risk of unacceptable losses and potential reputational damage. Staff managing collections should not 'accept' the situation and must raise it with management to ensure that appropriate resources are allocated to remove any backlog and targets set for reducing it. This is especially important if donations, gifts, or bequests are a regular occurrence. There should be no reason why any new acquisition is not recorded and managed to an agreed level, even if this is a matter of basic inventory or box-listing in the first instance.

In relation to collection development, the archive must exercise due diligence in relation to title, e.g. to ensure that it does not inadvertently become the recipient of stolen property. Collections on deposit or long-term loan present particular challenges, and the archive should ensure that any collections are subject to a robust agreement with the owner to protect the archive against any claims relating to loss or damage. The Government Indemnity Scheme may be able to provide insurance cover for deposited collections once assessed and valued in accordance with the rules of the scheme.

Tip 15:

Subject to the organisational requirements a separate 'Collections Management Policy' for the safe management of Collections can be prepared with clearly defined practices included. This CMP should have Senior Leadership approval and sign-off.

If material is unregistered and unrecorded the making of any transfer or disposal becomes difficult to manage and risks of misappropriation and loss are increased. The process for transferring or disposing of collections must be articulated in a procedure. Uncatalogued collections should not be made accessible for use in a reading room: all documents should be provided with a unique, recorded reference number in advance of making them accessible.

The management of all collections should only be undertaken by those with the necessary skills and knowledge of the task to be undertaken. In an archive, professionally-trained staff should assume responsibility and untrained third-party involvement should be kept to a minimum.

Any internal movements of collections to or from search/reading rooms, conservation workshops, or off-site storage facilities should be recorded using appropriate means. This may include a tracking note in the online catalogue system, a physical slip on the shelf / in the box, an issue book / spreadsheet, or all of these measures. When deciding on these measures, the organisation should consider what its needs might be in terms of future retrieval of this information.

The use of RFID (Radio Frequency Identification) has long been used by retailers around the world to track movements and to raise an alarm if an item is being removed from a certain area. As technology develops the devices have become more discreet and in certain cases adapted for the cultural sector, including archives and libraries. However, care must be taken especially with 'Special Collections' that damage is not caused to the object because of the placement, or adhesives used to secure them.

The tagging and documentation of unbound folders/folios can become very difficult and careful considerations need to be made. The weighing and counting of folios are an option and if seen can act as a deterrent but both have vulnerabilities that can be exploited. An alert and proactive invigilator is key to the successful secure management of a reading room and organisations should avoid complex processes which might distract them from their main task.

If an item in the collection is believed to be lost, stolen, or misplaced a procedure must exist to report it and for actions to be taken. There can be different procedures for general collections and those from 'Special Collections' due to the increased impact historically, financially, and reputationally the loss could have on the organisation and individuals. There should be no reason to delay reporting the incident, if retrieved then the report can be closed, and any lessons learnt documented to prevent others from facing the same risk. Confidential networks exist within the professional archives and rare books

[33] E.g. the ILAB missing books register, https://missingbooksregister.org/

Tip 16:

Any procedures should provide all the necessary information including who to report to and the escalation process. It is useful to document different 'Stages' so that a process can be followed, and activities/actions confirmed.

The last 2 'Stages' should include 'Final Outcome' followed by 'Lessons Learned'.

Managers should be supportive of the process and encourage transparency. If people feel they will be victimised or targeted, they are less likely to be honest about what is reported.

Adopting a transparent process is far more defendable in a court of law, and in the court of human opinion where trial by media is a constant threat to organisational reputation.

communities for the sharing of relevant information and there are also partnerships with the trade for recording stolen items. [33]

8.5 Transportation of Collections / Loans

Whether transporting items from a 'stack' to a search/reading room, between archival buildings or to an overseas borrower, the protection of the item needs to be considered. This reverts to the criticality of the item and any particular risk associated with its movement.

Tip 17:

Special handling instructions for individual items or collections should be determined with the assistance of trained conservators and this could be based on:

- Risk rating
- Fragility
- Any specialist equipment needed.
- Packaging
- Third party instructions
- Conditioning

This ensures clarity and transparency for all.

[34] Care must be taken with the handling of sensitive personal data and the Data Protection Act/GDPR legislation must be followed.

Where couriers are used it is important to use providers or staff who are trained and have the appropriate skills to successfully transport collections, especially when travelling overseas. Fragile items and those with a high value should be transported in vehicles that provide appropriate levels of protection. The guidance provided by the Government Indemnity Scheme is valuable[34] and must be followed by institutions wishing to be covered by the scheme. This guidance is sensible for the transportation of any fragile or high-valued collection items.

Transportation procedures should ensure that the means chosen complies with insurance cover. This is likely to rule out the use of Uber or untrained staff. Even a very short journey can introduce unnecessary risks if corner-cutting assumptions are made.

Where there is a risk of exposure to the elements of environmental conditions then steps should be introduced to reduce the risk as low as reasonably practicable. This could include archival packaging within a waterproof container or use of a climate-controlled vehicle with environmental monitoring.

8.6 Search/Reading Room Activities

By their nature archives and libraries allow greater 'hands-on' access to documents and other items in the collections than most other cultural venues because of the need to allow custody to temporarily pass onto third parties. As such the risk of theft and damage (intentional and accidental) is increased. Where physical measures are reduced, they have to be compensated using the other available measures, especially for 'Special Collections.'

As with most things good governance plays an important part in reducing the risks. There should be procedures that help the staff understand the expectations and permissible activities but there should also be a type of contract/agreement with anybody wanting to enter and use the services that exist. The Reader contract should identify the following:

- Acceptable conduct
- Permissible items (into the search/reading room)
- Limits on the permissible number of collections/documents at any given time
- The need for identification to be shown/verified before and during visits.
- Video recording is taking place for the prevention and detection of crime.
- Special Collections may have additional measures that are found locally and may need to be acknowledged.
- The venue has a right to search the individual and anything they are carrying.
- The venue can revoke an individual's right of entry without advanced notice.
- The venue has the right to exclude individuals if they are found to breach any rules.
- The police will be notified of any identified or suspected criminal activity.

- The venue accepts no liability for the loss or damage to the user's personal possessions, however caused.

The contract/agreement should be signed confirming understanding and acceptance of the rules. There should be proof of identity which should include the following:

- Government issues photographic identification (passport, driving licence)
- Private address confirmation (if a non-institutional researcher/visitor).
- Institutional organisation address and confirmation letter of association between the researcher and the institution.
- Passport style photographs (that can be added to any pass or permit and allow a verification that the individual presenting the token is actually the person shown in it.)[35]

If an organisation is excluding personal possessions from search/reading rooms then providing a lockable container is good practice, as is it having a transparent front.

Apart from general library spaces, it is expected practice that appointments are made and where necessary specific seating arranged so that the higher the criticality of the material the closer the reader is to an invigilator. Access should be restricted until the reader has been verified and the material can be issued. It is not acceptable for there to be no invigilation when the search/reading room is occupied.

Tip 18:

If the search/reading room is left unattended at any point, then from a security risk management perspective all readers should be asked to leave the room (even temporarily) until the invigilation can resume. Best practice is to ensure that two members of staff are on duty at any time when the facility is open.

If it is going to be unattended for anything more than a few minutes (5-10 minutes) readers should be informed and any personal possessions can be removed, if desired before the room is locked.

[35] Care must be taken with the handling of sensitive personal data and the Data Protection Act/GDPR legislation must be followed.

Invigilation is a key means of protecting assets in search/reading rooms and ensuring general good practice in relation to handling of collections. Good invigilation requires the member of staff to be situationally aware, vigilant, and alert to what is happening at any given time. It is also hugely beneficial if the invigilator has been trained in understanding the different threats that exist, how they can manifest themselves, and appropriate actions that can be taken to help reduce the risks.

As previously explained the physical layout of the search/reading room can help reduce the security risks, as can the use of CCTV cameras.

Tip 19:

Do not rely on monitoring the CCTV camera as a means of observation and invigilation. The monitor should be viewed as 9 parts deterrence and 1 part proactive use.

The reason for this is that cameras do not have the ability to look beyond a preset focal point and by watching a monitor, the broader observation of activities can be missed.

Another good way of invigilation and to reduce the likelihood of boredom is to undertake a patrol of the area where you are working. A patrol is not an aimless wandering around a given area. It is a purposeful activity that is looking for threats and vulnerabilities. It also causes anybody with ill intent to think again about whether they have been observed or compromised.

8.7 Fire Risk Management

Fire is probably the most serious threat to archives, libraries, and holders of special collections because it destroys documents and buildings while endangering life. Therefore, a strategy to reduce the risks posed by fire is critical.

It is in everybody's interests to proactively reduce the fire risks from both a life safety and the protection of collections perspective. Everybody must know and understand the actions to take when the fire alarm is activated.

All staff should be encouraged to be proactive in fire risk reduction activities. This can include:

- Checking emergency exits are not blocked.
- Knowing evacuation routes out of specific areas.
- Knowing where the muster/assembly points are.
- Knowing where fire extinguishers and how to use them (if safe to do so).
- Reporting the collection of combustible materials close to the building shell.

- Reporting unsafe storage of combustible materials within the venue.
- Inappropriate storage of materials in collection stores.
- Reporting damaged or faulty fire prevention equipment.
- Closing fire doors that have been propped open.
- Ensure they fully understand the emergency fire procedure.

There are legal and moral requirements for all businesses/organisations to appoint a 'Responsible Person' to reduce the risks, checks should be made to ensure the 'Responsible Person' is known and if non-existent, one should be appointed. Every organisation has a duty of care to ensure that whatever fire risk management activities exist they are known and understood by all staff.

The organisation should also ensure that there is sufficient equipment and other resources to help reduce the fire risks and not increase the risks to life or property by their omission.

When you have control of the procedure anything created must be easy to read, brief, and directive. Appendix 11 provides a basic Fire Procedure for a location that does not have an automated FAS (Fire Alarm System).

8.8 Incident Reporting

To minimise the risk of loss, harm, or damage to collections, visitors, and staff there must be clearly defined guidance on when actions or activities are to be reported. Each location may have different incident types that it sees as a priority, or which are dictated by the threats and the risks they pose but the use or creation of a basic incident reporting system can help all organisations.

The following are incidents, whether real or suspected that organisations should consider reporting:

- Suspected theft
- Unauthorised access
- Suspicious behaviour
- Loss of collections
- Damage to collections
- Crime affecting the building.
- Acts of Violence/Intimidation
- Policy breaches
- Fire
- Protests
- Lost children
- Vulnerable adults

Some incidents have the potential of impacting an organisation's reputation which in turn could affect their financial viability. This can lead to a reluctance by organisations to report certain incidents, including to the police. However, case after case shows that in the modern world of social media, there is nearly always data leakage, whether accidental or intentional.

Therefore, it is recommended that a clear policy is developed outlining the organisational strategic approach to incident reporting including which incident types should be reported and to whom. This is particularly important when considering whether criminal matters are reported to the police. This should be signed off at the Leadership Team level and cascaded to all staff, so they are aware of the direction given and do not deviate from the policy.

An important aspect of all incident reporting is to learn from the event and reduce future risk exposure.

Tip 20:

Any decision not to report a crime or suspected crime to the police has to be risk assessed, as the consequences of failing to report could be far greater than any adverse inference which can and should be managed through any Crisis Management Plan and its communications strategy.

9 Education and Training

One of the most important security risk management tools for organisations that allow public access into their venues is the training and education of staff and visitors alike. It is important to ensure that where there is an expectation on staff to act or deliver services in a certain way that they are given the tools, through learning, to do so.

As was explained earlier, [36] staff do not automatically know and understand an organisational security risk management requirement and so there is a need to help them understand:

- What exists.
- Why it exists.
- What individuals are to do.

AND

- How to do it.

The sooner you start educating staff about the protection of assets the quicker a security culture can start to be established. The induction phase is the ideal starting point. If during induction there is very little mention of 'security' then the subconscious view will be that it is not an important matter and so there is no need to worry about it, ***'it is somebody else's job'.***

It is also important to recognise that staff have been culpable of security breaches such as theft and this can be difficult to prevent, given the need for privileged access in the course of their work. In a healthy security culture staff should be aware that no-one is above suspicion and be ready to accept spot-checks, ID challenges and restrictions on unnecessary access. There are multiple ways of educating and training staff to ensure they play a proactive part in the protection of the organisational assets and collections. Some are included in example 9 below:

Example 9:

Security education and training delivery methods:

- Presentations (Induction)
- Briefings (Internal stakeholders)
- Toolbox talks
- On-line learning
- Shadowing
- Reading material.
- Posters
- On-the-job training
- Specialist programmes

[36] Section 3.1.6

Educating and training should not be viewed as a one-time fix, it is a continuous process and needs to evolve with the threats and risk landscape. This results in 'proactive prevention' which is more beneficial and presents a greater value for money than a 'reactive response'.

Not all programmes have any additional costs associated with them and the level and types of training should be dictated by a training needs analysis that identifies who needs what training, when, and what is the priority. If by not receiving training a new member of staff cannot do their job, then there is a cost implication until they can.

If the venue has an in-house security professional or identifiable SRP (Security Responsible Person) they can and should play a proactive part in educating other staff. It makes their job easier if others are playing a proactive part in the protection of assets.

It doesn't always need to be anything formal, it can be as simple as walking and chatting with staff, attending morning briefings, or anything that encourages engagement with 'security' and encourages dialogue, especially if there is misunderstanding or concerns. This approach recognises that the operational teams are far more likely to see an operational vulnerability than a security person and the continual engagement will encourage and empower them to speak up. (Another strong indicator of a robust security culture.)

For staff to play a proactive part in the protection of the organisation's assets it is helpful for them to understand what threats exist, how they manifest themselves, and the proactive actions that every member of staff can take to help reduce the risks. More recently cultural venues, especially those with a larger footfall are requesting training that includes situational awareness/ behavioural analysis and surveillance detection which is a proactive step as pre-attack surveillance is undertaken by organised crime groups, protesters, and terrorists.

The UK's NPSA - National Protective Security Authority (formerly CPNI – Centre for the Protection of National Infrastructure) and Counter-Terrorism Policy (CTP) has pages of free resources dedicated to the learning of security risks that exist and steps that individuals and organisations can take to reduce the risks that are face. While there is a counter-terrorism theme to the training, the cross-over into organised crime, protesters, and personal safety is very evident and therefore a beneficial and cost-effective service for organisations to draw upon.

Some commercially available providers specialise in the delivery of programmes dedicated to the protection of

cultural heritage and over the last five years there has been a change in attitudes whereby this training is being provided to all staff as well as to people with specialist operational requirements.

There are times when a venue may have externally-provided security guards. All guards are required by law to be licensed and to display a current and valid SIA (Security Industry Authority) badge. That is a baseline requirement for delivering 'frontline' security services. There is a misconception that contract security staff understand 'security' and the protection of assets, they don't necessarily, at least not at the start. A security service provider is just that, they provide guarding services and will normally work within a pre-determined contractual basis. Therefore, most will lack the knowledge and skills required for working effectively in a cultural setting, they too will require education and training.

The following table contains some examples of protective training and education programmes that may be of benefit to ARA member organisations and while the list is not exhaustive it indicates available options:

Tip 21:

Tip 21: During the writing up of any contractual agreement or tender scope, clearly specify any training you want them to have already received and what they must undertake within a certain timeline and frequency. That way the continuous learning and developing process is shared with those being paid to protect your assets.

Programme	Recipient
• Understanding threats, risks, & vulnerabilities	• All staff (Including contractors)
• Situational awareness/behavioural analysis	• All staff
• Advanced situational awareness/behavioural analysis	• Security team, those with protective responsibilities.
• Surveillance detection	• All staff
• Advanced surveillance detection	• Security team, those with protective responsibilities.
• Bag searching	• Security teams.
• Risk assessing	• Managers
• Protective invigilation	• Invigilators
• Conflict avoidance	• All staff
• Incident responses	• All relevant staff
• Crisis Management	• CMT, wider staff, external partners
• Challenging procedure	• Front-of-house staff or those with public engagement
• Preventing Workplace Violence	• All staff
• Personal safety and security	• All staff (especially public-facing and lone workers)
• Use of technical security equipment	• Anybody who has to use it during their working day.

Table 3 - Suggested protective training programmes

There is a need to train visitors to the venue so that they comply with the rules and requirements that exist to protect the collections. A lot of this education relates to the clear communication of rules, for example, the signing of a contract by 'Readers'.

Unless a reason for doing something in a certain way is known a visitor may do something that is non-compliant, normally this is unintentional, but it can lead to disagreements which can escalate. By sharing this information in advance and having good customer services (should be the first lesson for any public-facing security activity) risks are greatly reduced. Notices and signage are a great tool to advise and educate people such as:

- No entry
- No food or drink in the search/reading room
- Violence against staff will not be tolerated.
- Emergency Exit
- Restricted access
- CCTV is in Operation
- No bags are allowed beyond this point.
- Security personnel operate in this area.

All the above are very basic but they educate people about expected behaviours and therefore help reduce the risk. It also means that any challenges for non-conformity are justified.

Another way in which visitors are educated is when there has to be a member of staff intervening because an activity risks harm to collections, individuals, or staff. The calm intervention and explaining why certain activities are not permitted is a form of education as well as a polite challenge.

The final point regarding training is the one that most organisations find difficult to implement and that is Emergency and Crisis Management training. A critical part of protective governance is the emergency and crisis management plans but apart from a fire evacuation (required by law), most plans are not tested. That means the effectiveness of a salvage plan or the crisis management plan in dealing for example with a death, or terrorist incident is unknown. It is important that plans are tested, not to evaluate the effectiveness of individuals but to establish any gaps in the plans and actions that can be taken to reduce the risks and make them more effective. This includes gaps in link up to other parts of an organisation (e.g. in a university context), or with external agencies (e.g. fire brigade or policing).

The plans should be reviewed and tested annually or following a significant event including a significant change in personnel or plan content. The use of briefings of different groups is a good way to educate and prepare them for the next stage which may be a tabletop exercise where a scenario is developed, and the plan has to adapt and deal with whatever situation is presented. It should always be remembered that one of the most beneficial parts of any training is the debrief and 'lessons learned' as they help identify gaps or areas for improvement. It is advisable to only move up to a full test, potentially involving external partners, once tests using tabletop exercising has been done as this allows gaps to be identified and closed before moving onto a full exercise. These can be done in-house or with external partners. Where terrorist-related exercises take place additional support may be available from CTSA or police DOCOs.

10 Terrorist Threat Considerations

The threat from terrorism against individuals and organisations in the United Kingdom and the Republic of Ireland is nothing new and has been with us in its modern form since the 1970s, although the use of terror for political purposes goes back centuries. Therefore, when undertaking a risk assessment, the threat from terrorism should already be considered and effective steps taken to manage and mitigate any identified risks.

The tactics used by terrorists continue to evolve. For example, recent years have seen a greater use of indiscriminate attacks where the public or specific groups are seen as legitimate targets. As the government have introduced successful interventions (inability to purchase explosive components, restricted access to firearms etc.), terrorists have adapted their attack methodology using vehicles and bladed weapons.

The addressing of the terrorist threat has also changed dramatically with the creation of Counter Terrorism Policing, [39] NaCTSO [40] (National Counter Terrorism Security Office) and their teams throughout the United Kingdom. These organisations work closely and at times jointly with MI5 – Security Service and the Joint Terrorism Analysis Centre (JTAC) [41] who are responsible for establishing the national threat levels from terrorism. In the Republic of Ireland the Garda Síochána (police) has responsibility for countering the terrorist threats that exist.

The terrorist threat levels indicate the likelihood of an attack taking place and falls within certain categories:

- **LOW** means an attack is highly unlikely.
- **MODERATE** means an attack is possible, but not likely.
- **SUBSTANTIAL** means an attack is likely.
- **SEVERE** means an attack is highly likely.
- **CRITICAL** means an attack is highly likely in the near future.

The threat levels should not be taken out of context, the likelihood of most ARA members being involved in or directly impacted by acts of terrorism are extremely low. These levels do not relate to specific sites, venues, or sectors and so the undertaking of an effective risk assessment that includes considering the terrorist threat in your local context is really important.

An important aspect of assessing the risk to your venue is understanding how attractive you are to a terrorist. Are you such a 'target rich' venue that they would attack you as opposed to others, or would they attack others because of their greater newsworthiness and higher profile, especially if the likelihood of success is the same?

[39] https://www.counterterrorism.police.uk/
[40] https://www.protectuk.police.uk/
[41] https://www.mi5.gov.uk/joint-terrorism-analysis-centre

Example 10:

Security education and training delivery methods:

Venue 1: is in the Yorkshire Moors and has an average of 100 visitors per day. Its archives relate to the mining activities of the immediate area dating back to 1800. Access is via car or a bus that runs every hour.

Venue 2: Is in the centre of Manchester and has a worldwide reputation for its collection of Jewish and Christianity literature dating back over 1000 years. It has 5,000 daily visitors and is located close to Manchester Piccadilly railway station.

Which is more attractive to a terrorist?

The target selection will also depend on the likelihood of success and the amount of exploitation it can achieve, increasingly through social media. Using the above example **Venue 2** could be a more attractive target based on accessibility, justification, number of targets, and the potential for secondary targets if a marauding attack were to occur. Please see ProtectUK guidance for further guidance to assess the risk.[42] Many of the measures that have already been outlined within this guidance can go a long way to reducing the risks that exist to your venue.

Archives have a symbolic value as representing the heritage and recording the history of particular regions or groups; they also have a practical role as trusted sources of knowledge at a time of widespread online misinformation. This may mean that their collections could be targets as well as their buildings, staff and visitors.

Irrespective of how low the likelihood of an attack, the potential consequences will always be assessed as critical and so effective planning and threat consideration should take place. There is already a legal and moral duty of care supporting this approach. Potential changes to legislation brought about by Martyn's Law (Protect Duty) may make it a legal requirement to put protective measures in place against terrorist acts.[43] Additional changes to operational practices and procedures may be required alongside a clear assessment of the risks posed by the terrorist threat.

Tip 22:

Acts of terrorism should already feature in your risk assessment and be included within the Crisis Management Plan. Where they don't exist the Security Responsible Person should ensure the development of appropriate procedures in different scenarios identifying what and how the risk can be reduced and if any additional resources are needed.

There is no reason to wait for the finalisation of legislation to do the right thing to protect staff and visitors to your venue.

The attack methodology and measures to mitigate them require specialist knowledge and experience which unfortunately most ARA members will not have. Therefore, external expertise may be needed.

The first port of call should be the ProtectUK website (and NPSA website for technical guidance). Sites that are already engaged with Counter-Terrorism Security Advisors (CTSAs) should continue to do so, however, they do not have unlimited resources and may not be able to provide anything other than redirecting you to free advice and guidance [44] or a DOCO (Designing out Crime Officer) from the local police service.

Care should be taken if using commercial organisations who declare that they will make you Protect compliant as it is presently impossible due to the legislation not being finalised. However, some specialist commercial advisors have the skills, knowledge, and expertise to support, they may also have the cultural sector-specific experience to offer a more balanced approach.

Appendix 1 – Signpost Document provides a complete section dedicated to the support and guidance available from the government to reduce the risks being faced from terrorism and a range of other threats. This is a rapidly-evolving area so the guidance is likely to change.

[42] https://www.protectuk.police.uk/threat-risk/security-risk-management
[43] Legislation has not been finalised and therefore any information is currently indicative.
[44] Contained in Appendix 1

11 Cyber/IT Threats

The threat from cyber-crime is ever increasing and above all other crime types is the most prevalent. If successful it can be one of the most harmful to ARA members especially where records are born-digital or have been digitised.

MI5 describe 'cyberspace' as: *"the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure, and services."*

Most individuals and organisations rely on the cyber world to conduct their private and professional business. Archives, libraries, and other cultural venues are not immune from being targeted by hostile actors who can include governments, organised crime groups, 'hacktivists,' and terrorists.

The motive for attacking can be wide-ranging but in the cultural heritage world it can include:

- Causing reputational damage
- Obtaining sensitive data
- Fraud
- Denial of services
- Financial gain – blackmail
- 'Because they can'

The impact can be far-reaching from interfering with environmental control systems through to complete denial of access and the unauthorised disclosure of material. Access to analogue collections can also be significantly disrupted, particularly if digital catalogues are unavailable. All of these can have a significant financial, operational, and reputational impact on the organisation, as well as potential legal consequences for any data breach imposed by the Data Commissioner, including a fine of up to £17.5 million or 4% of the annual global turnover. Therefore, seeing the cyber infrastructure as an asset and a potential threat is a sensible way of considering it.

As with traditional security methods, protection from Cyber/IT threats doesn't just happen. The condition has to be created to ensure it is effective and while there is often a need for specialist support there are plenty that all organisations can do to reduce the risks they face.

It is important to understand there are different parts to an IT network and each can be attacked by different actors. The **Hardware** includes the server, computers used by organisations, the means of transmitting the data and devices that connect computers to the server and other devices. The **Software** relates to programmes that are being used, drivers, and operating systems. The final part is the **Human** interaction!

Increasingly, organisations are moving to cloud storage, which has cyber security benefits e.g. in relation to the distribution of assets. However you still need to understand the provider's security policy and approach to backup / restitution in the event of system penetration. This should be covered in the contract agreement. You should also understand how to manage the interaction between the cloud system and in-house systems as this can present a vulnerability. For example, should you ensure that there is rigorous password management for accessing cloud systems and avoid generic logins.

Steps should be taken by all organisations to minimise the risk as **low as reasonably practicable**. One of the first considerations is whether the organisation develops a Cyber Security Risk Management Policy (or included within a broader Security Risk Management Policy), providing the organisation with a clear understanding of the organisational expectations regarding cyber security.

Access to Hardware

Unauthorised access to organisational devices must be limited. Server rooms should have restricted access, preferably as a part of an Access Control System, and be covered externally and internally with CCTV (subject to resource availability). Desktops and other devices used by the organisation should have USB ports disabled unless there is a clear operational need, which should be documented and approved.

No personal hardware should ever be used or connected to the organisational IT infrastructure, the levels of protection cannot be guaranteed, and the organisation's system could become infected.

When travelling overseas there are certain countries where it is not advisable to take any laptop or other electronic devices connected to the IT infrastructure due to the increased threat levels, including from 'state' actors. If you do have to travel with a laptop, consider using a USB Port locking device and storing it in a safe when not in use.

Access to Software

In most cases, the software providers are responsible for ensuring the protection of the software. However, many organisations have suffered significant losses, and fines, because they did not keep their software updated. It is recommended that system updates are scheduled alongside data backups (if not cloud based). If you are accessing software as a service in the cloud, you need to understand the implications e.g. that you are using external hardware to do so.

A structured approach to who has access to software should be incorporated into any policy and this should include the issuing of passwords. Only system administrators should be allowed to add software to organisational systems and an audit trail should be provided.

It is important to ensure firewalls and anti-virus programmes are installed on all computers and kept up to date. There may be occasions when air gapped systems are required to protect the network and data being worked on, e.g. in digital archiving projects.
Access to publicly accessible Wi-Fi should be risk-assessed and if appropriate disabled. Private VPNs can offer a degree of protection, but they require updating and ensuring that they remain fit for purpose.

Human Interaction

Most threats, breaches, and infections are caused by human activity, which can be accidental or intentional. There should be clear guidance provided on the opening of attachments, downloading emails, or clicking online links all of which can be routes for introducing infections.

It is important that the Cyber Security Policy is read by all staff and that they understand and continue to understand the dangers associated with cyber threats and their potential impact. The policy should also state that connecting to publicly accessible Wi-Fi should not be allowed for any organisational device. Passwords should be a mixture of alphanumerical characters and should not be used for multiple devices or programmes, especially if mixing personal and private. Training, reinforced by exercises such as a mock "phishing" campaign, should be provided to reduce the risks faced.

Make sure that when leaving the desk for a short period that the computer is locked, if leaving for an extended period of time [45] close the computer down. If you see anything unusual on your monitor or the system appears to have slowed down, turn off the computer and report it, there could be a virus.

Staff are to be reminded about not sending insecure videos to organisational emails or opening private emails on the organisational computer, depending on the local policy.

The list of threats and issues are continuous and ever-changing, the capturing of a 'Do and Don't' list within an IT Cyber Security Policy will go a long way to reducing the human errors that can impact an organisation.

It is important that any Crisis Management Plan considers the impact of a cyber-attack on the organisation and that steps are taken to introduce measures that will reduce the adverse impact and ensure a speedier recovery and resumption of operational activities.

The threat posed by cyber-attacks is such that the organisational appointment (subject to other factors) of an IT manager may be an appropriate action to take. It could be that the management of the IT system is outsourced to a third party, where this is being considered suppliers approved by the National Cyber Security Centre (NCSC) [46] should be selected, (a link is included within Appendix 1). An organisational risk management and assessment approach such as Cyber Essentials is recommended, especially for standalone organisations.

Where advice and guidance is needed then the NCSC has developed a one-stop-shop for all cyber security advice, guidance, and training. While there may be commercial providers of information and data regarding the threat to infrastructure posed by the cyber threat it is not felt necessary or appropriate to include them in this guidance when such an excellent one is freely available.

[45] Organisations to decide what is viewed as an 'extended period of time' and ensure it is documented.
[46] https://www.ncsc.gov.uk/

12 Conclusion

This guidance document has been prepared to support ARA members in protecting their venues from the current security threats and risks that exist. While there will be areas of the guidance which have not changed significantly from the 2003 Resource document it does consider many of the new and emerging threats that may not have been a feature when the original guidance was created.

There are also changes in security practices and standards which have hopefully been captured in a way that all ARA members will be able to follow, irrespective of size, nature, or geographical location.

This document (and Appendices) are designed to help you make informed decisions about how to manage the security threats and risks you face. There is nothing to say that everything within this will suit your particular circumstances or is relevant. But hopefully, it will provide appropriate indications as to security good practices that can be implemented.

More detailed aspects of protective security is provided within **Appendix 1 – Signpost Document** that includes direct links to websites and other sources of information. To make the Appendix more readable and easier to follow, the sections correspond to those within the guidance main body.

Where gaps in guidance exist or changes in legislation occur the document will be updated and shared amongst the members.

Appendix List

Appendix 1
'Signpost Document'

The purpose of this Appendix is to provide the member with electronic links to detailed information relating to the particular area of discussion. Not all areas have links, that does not mean that they did not exist only that they were not appropriate as a point of reference.

This Appendix is a 'living document' meaning that when the ARA members identify suitable links, they can inform the ARA Security and Access Group which will consider its inclusion without affecting the whole guidance document.

Governance Development

1) **Understanding governance:**
https://www.cgi.org.uk/professional-development/discover-governance/looking-to-start-a-career-in-governance/what-is-governance

2) **Understanding governance:**
https://governancetoday.com/GT/GT/Material/Governance__what_is_it_and_why_is_it_important_.aspx

3) **NPSA - Passport to Good Security:**
https://www.npsa.gov.uk/managing-my-asset/leadership-in-security/board-security-passport

4) **British Library – Collection Security Governance:**
https://www.cerl.org/_media/services/seminars/vaticanpresentation2.pdf

5) **NPSA - Protective Security Management System:**
https://www.npsa.gov.uk/protective-security-management-systems-psems

Emergency Planning

6) **Scottish Council of Archives – Emergency Planning Guidance:**
https://www.scottisharchives.org.uk/resources/preservation/emergency-planning/

7) **Scottish Council of Archives – Emergency Plan Template:**
https://www.scottisharchives.org.uk/wp-content/uploads/2020/05/TEMPLATE-2-Planning-Matters-Emergency-Plan.pdf

8) **Cabinet Office – Emergency Preparedness:**
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61028/Emergency_Preparedness_chapter5_amends_21112011.pdf

9) **Government Communications - EP Framework:**
https://gcs.civilservice.gov.uk/publications/emergency-planning-framework/

10) **Government Communications – Local Planning:**
https://www.gov.uk/local-planning-emergency-major-incident

11) **Government Communications - Preparing for Emergencies:**
https://www.gov.uk/government/publications/preparing-for-emergencies/preparing-for-emergencies

12) **Safety Culture – Crisis Management Planning:**
https://safetyculture.com/checklists/crisis-management-plan/

13) **Protect UK- Managing Risk & Business Continuity:**
https://www.protectuk.police.uk/advice-and-guidance/risk/managing-risk-and-business-continuity

14) **Collections Trust – Emergency Planning for Collections:**
https://collectionstrust.org.uk/spectrum-resources/risk-management/

Threat, Risk, & Vulnerability Assessments

15) **Collections Trust – Security Risk Assessment:**
https://collectionstrust.org.uk/accreditation/organisational-health/assessing-and-managing-risk/security-risk-assessment/

16) **Collections Trust – Security Audit:**
https://collectionstrust.org.uk/resource/the-security-audit/

17) **Scottish Archives – Risk Assessment & Management:**
https://www.scottisharchives.org.uk/wp-content/uploads/2020/05/TEMPLATE-1-Planning-Matters-Risk-Assessment-and-Management-.pdf

18) **NPSA – Protecting Your Assets:**
https://www.npsa.gov.uk/protecting-your-assets

19) **Protect UK – Security Risk Management:**
https://www.protectuk.police.uk/threat-risk/security-risk-management

20) **Health & Safety Executive – Managing Risk:**
https://www.hse.gov.uk/simple-health-safety/risk/index.htm

21) **Safety Culture - Risk Assessment:**
https://safetyculture.com/topics/risk-assessment/

22) **Collections Trust – Museum Security Toolkit:**
https://collectionstrust.org.uk/resource/the-museum-security-toolkit/

23) **CPNI – Personnel Security Risk Assessment:**
https://www.npsa.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf

Security in Depth – Security Designs

24) **NPSA – Protective Security:**
https://www.npsa.gov.uk/protective-security

25) **NPSA - Build it Secure:**
https://www.npsa.gov.uk/build-it-secure-0

26) **RIBA - Plan of Work:**
https://www.architecture.com/knowledge-and-resources/resources-landing-page/riba-plan-of-work

27) **NPSA - Security Considerations in the Planning Process:**
https://www.npsa.gov.uk/security-considerations-planning-process

28) **NPSA - Operational Requirements:**
https://www.npsa.gov.uk/operational-requirements

29) **Collections Trust – Advice for Architects & Planners:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/AdviceForArchitectsAndPlanners_02.pdf

Physical Security Considerations

30) **NPSA – Beyond the Perimeter:**
https://www.npsa.gov.uk/beyond-perimeter-0

31) **NPSA - Perimeter:**
https://www.npsa.gov.uk/perimeter-0

32) **NPSA - Fences & Gates:**
https://www.npsa.gov.uk/fences-and-gates-0

33) **Collections Trust – Security in Museums & Galleries – Buildings & Perimeter:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/PracticalGuide_Buildings_and_Perimeters_01.pdf

34) **NPSA – Building Services & Internal Spaces:**
https://www.npsa.gov.uk/building-services-internal-spaces

35) **BRE - Loss Prevention Standard (LPS1175):**
https://www.redbooklive.com/download/pdf/LPS1175.pdf

36) **Secure by Design – Building Regulations for Security:**
https://www.securedbydesign.com/guidance/building-regulations

37) **Secure by Design (Commercial Buildings – Generic guidance):**
https://www.securedbydesign.com/images/COMMERCIAL_GUIDE_23.pdf

38) **NPSA - Doors:**
https://www.npsa.gov.uk/doors-0

39) **BRE - Accredited Doorset Suppliers:**
https://www.redbooklive.com/search/productsearch.jsp?id=688&results_pp=10&searchgroupid=50&searchgrouptypeid=5&searchgroupsectionid=497&productType=0&productName=&securityRating=&companyName=&certNo=&standardInfo=&addressPostcode=&countryId=0

40) **Collections Trust - Solid Core Door (2013):**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/SecuritySpecification_SolidCoreDoors_02.pdf

41) **Collections Trust – Internal Window Grilles:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/SecuritySpecification_InternalWindowGrilles_02.pdf

42) **NPSA – Protecting from Forced Entry:**
https://www.npsa.gov.uk/protection-forced-entry

43) **NPSA - Windows:**
https://www.npsa.gov.uk/windows

44) **Commercial site – Toughened & laminated Glass Explained:**
https://stevenage-glass.co.uk/toughened-and-laminated-glass-explained/

45) **AMNH – Light Impact in Museums:**
https://www.amnh.org/research/science-conservation/preventive-conservation/agents-of-deterioration/light-ultraviolet-and-infrared

46) **NPSA - Catalogue for Security Equipment:**
https://www.npsa.gov.uk/cse-categories

47) **NPSA – Blast Mitigation for Curtain Wall Systems:**
https://www.npsa.gov.uk/system/files/documents/c9/3c/WIP%20GN%20Mitigation%20measures%20for%20stick%20curtain%20walling%20systems-%20Version%201%20May%202021.pdf

48) **BRE – LPS 1270 – Security Glazing:**
https://www.redbooklive.com/download/pdf/LPS1270.pdf

49) **BRE – Security Glazing Supplier List:**
https://www.redbooklive.com/search/productsearch.jsp?id=688&results_pp=10&searchgroupid=50&searchgrouptypeid=5&searchgroupsectionid=363&productType=0&productName=&securityRating=&companyName=&certNo=&standardInfo=&addressPostcode=&countryId=0

50) **Master Locksmith Association (MLA):**
https://www.locksmiths.co.uk/

51) **NPSA – Catalogue of Security Equipment:**
https://www.npsa.gov.uk/cse-categories

52) **Architectural Armour - Security Glazing Data Sheet:**
https://www.architecturalarmour.com//content/Tech%20Spec/PDFs/LPS%201270.pdf

53) **NPSA – Internal Glazing:**
https://www.npsa.gov.uk/internal-glazing

54) **CPNI (NPSA) - Improving Blast Resistance of Glazing:**
https://www.npsa.gov.uk/system/files/documents/89/49/Improve-the-blast-resistance-of-glazing.pdf

55) **Collections Trust – Security Specifications for Display Cases:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/SecuritySpecification_AttackResistentDisplayCases_02.pdf

56) **ASIS & AAM – Suggested Practice Display Cases:**
http://www.securitycommittee.org/securitycommittee/Guidelines_and_Standards_files/Final%20Exhibit%20Suggest%20Practices%20ASIS%20Format.pdf

57) **Home Office – Firearms Security Handbook:**
https://www.nationalcrimeagency.gov.uk/who-we-are/publications/489-home-office-firearms-security-handbook-2020/file

58) **Arts Council England – Government indemnity Scheme Guidance:**
https://www.artscouncil.org.uk/sites/default/files/download-file/GIS_National_guidelines_2016.pdf

59) **Christie's – Everything you need to know about hanging art:**
https://www.christies.com/features/How-to-hang-artworks-8182-1.aspx

Collections/Archives Stores

60) **American Alliance of Museums – Collections Space Security:**
https://www.aam-us.org/wp-content/uploads/2018/01/suggested-practices-for-museum-collections-space-security.pdf

61) **British Library - Archive Store Furniture:**
https://www.bl.uk/britishlibrary/~/media/bl/global/conservation/pdf-guides/library-and-archive-storage-furniture-guide.pdf

62) **Collection Trust – Creating & Improving Stores:**
https://collectionstrust.org.uk/resource/creating-and-improving-stores/

63) **Collection Trust – Store & Preserve:**
https://collectionstrust.org.uk/tapping-our-collections-potential/framework/store-and-preserve/

Technical Security Measures

64) **Home Office (NPSA) Perimeter Intruder Detection Systems Guidance:**
https://www.npsa.gov.uk/resources/perimeter-intrusion-detection-systems-guidance-document

65) **NSI (National Security Inspectorate) – Home Page:**
https://www.nsi.org.uk/

66) **SSAIB – Home Page:**
https://www.ssaib.org/

67) **Collections Trust – Fire and Intruder Alarm Systems:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/PracticalGuide_FireAndIntruderAlarmSystems_02.pdf

68) **BT RedCare – Alarm Signalling is Changing:**
https://www.redcare.bt.com/assets/documents/installation-support/bt-redcare-installer-handbook.pdf

69) **CSL Group – Alarm Signalling Standards Explained:**
https://www.csl-group.com/uk/getfile/442/

70) **Home Office – Fire Safety Building Safety Act 2022:**
https://www.gov.uk/government/publications/check-your-fire-safety-responsibilities-under-section-156-of-the-building-safety-act-2022/fire-safety-responsibilities-under-section-156-of-the-building-safety-act-2022

71) **UK Government - Regulatory Reform (Fire Safety) Order 2005:**
https://www.legislation.gov.uk/uksi/2005/1541/contents/made

72) **HSE - Introduction to Fire Safety:**
https://www.hse.gov.uk/fireandexplosion/fire-safety.htm

73) **Business Watch - Fire Alarm Categories:**
https://www.businesswatchgroup.co.uk/fire-alarm-categories-and-grades/

74) **World's Monuments Fund – Fire Protection for Heritage Places:**
https://www.wmf.org/fire#:~:text=Detection%20systems%20should%20be%20installed,fire%20suppression%20system%2C%20or%20both.

75) **National Archives (USA) – Fire Protection in Cultural Institutions:**
https://www.archives.gov/preservation/emergency-prep/fire-prevention.html

76) **UK Fire - Cultural Heritage Fire Safety:**
https://ukfiremag.co.uk/cultural-heritage-fire-safety/

77) **NEDCC – Fire Detection & Sprinkler Systems for Cultural Heritage:**
https://www.nedcc.org/free-resources/preservation-leaflets/3.-emergency-management/3.2-introduction-to-fire-detection-and-automatic-sprinklers-for-cultural-heritage

78) **Fire Protection Association: When to Use Sprinkler Systems:**
https://www.thefpa.co.uk/advice-and-guidance/advice-and-guidance-articles/when-are-fire-sprinklers-required-in-commercial-and-residential-buildings-#:~:text=UK%20legislation%20surrounding%20fire%20sprinkler,have%20a%20sprinkler%20system%20installed.

79) **British Automatic Fire Sprinkler System Association – Home Page:**
https://www.bafsa.org.uk/

80) **NPSA – CCTV (72 links to guidance):**
https://www.npsa.gov.uk/cctv

81) **Home Office – CCTV Operational Requirement Manual:**
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf

82) **Surveillance Camera Commissioner – Standards for the Surveillance Camera Industry:**
https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry

83) **NSI - Standards for CCTV Design, Installation and Maintenance:**
https://www.nsi.org.uk/wp-content/uploads/2012/10/NCP-104.3-Code-of-Practice-Design-Installation-and-Maintenance-CCTV-Nov-2017.pdf

84) **Information Commissioners Office: Video Surveillance Guidance:**
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/

85) **Protect UK – CCTV Guidance (PALs):**
https://www.protectuk.police.uk/cctv

86) **Collections Trust - CCTV Systems:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/PracticalGuide_CCTVsystems_02.pdf

87) **National Records Scotland – CCTV in NRS:**
https://www.nrscotland.gov.uk/record-keeping/legislation/primary-information-legislation/cctv-in-nrs

88) **Scottish Government: - A guide for Public Space CCTV:**
https://www.gov.scot/publications/national-strategy-public-space-cctv-scotland/

89) **British Museum – CCTV Policy:**
https://www.britishmuseum.org/sites/default/files/2019-12/CCTV_policy_231219.pdf

90) **NPSA - Control Access:**
https://www.npsa.gov.uk/content/control-access

91) **BSIA - Access Control Guidance:**
https://www.bsia.co.uk/zappfiles/bsia-front/pdfs/132-specifiers-guide-access-control-systems[1].pdf

92) **NSI – Codes of Practice Access Control Systems:**
https://www.nsi.org.uk/wp-content/uploads/2012/11/NCP-109.2-Code-of-Practice-Access-Control-Systems-Oct-16.pdf

93) **NEPAD (Commercial) - Guide to Physical Access Control Systems 2023:**
https://www.nedapsecurity.com/the-ultimate-guide-to-physical-access-control-systems/

Operational Security Considerations

94) **Museums Galleries Scotland – Government Indemnity Scheme (explained):**
https://www.museumsgalleriesscotland.org.uk/advice-article/government-indemnity-scheme/

95) **Collections Trust – Access to Collections:**
https://collectionstrust.org.uk/wp-content/uploads/2016/11/Access-to-Collections-2022.pdf

96) **Consortium of European Research Libraries – Information for the Security Network:**
https://www.cerl.org/collaboration/security/otherinformation

97) **Protect UK- Insider Threat:**
https://www.protectuk.police.uk/advice-and-guidance/security/reducing-insider-risk

98) **ARCL/RBMS – Guidelines for the Security of Special Collection Materials:**
https://www.ala.org/acrl/standards/security_theft

99) **NPSA – Employee Risk (Insider Threat):**
https://www.npsa.gov.uk/system/files/documents/npsa-holistic-management-of-employee-risk-homer-executive-summary_0.pdf

100) **National Archives – Managing Digital Records (non-EDRMS):**
https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-digital-records-without-edrms/

101) **Trident Manor Limited (Commercial site) – Cultural Protection Services:**
https://www.tridentmanor.com/consultancy-services/cultural-heritage/cultural-protection-services/

102) **Local Government Association – Protecting & Improving local Arts & Cultural Services:**
https://www.local.gov.uk/parliament/briefings-and-responses/protecting-and-improving-local-arts-and-cultural-services

103) **Collections Trust – Spectrum:**
https://collectionstrust.org.uk/spectrum/

104) **Collections Trust – Spectrum Approved Software:**
https://collectionstrust.org.uk/software/

105) **Royal Armouries – GIS (Annex E) Transportation Guidance:**
https://royalarmouries.org/wp-content/uploads/2018/04/Transport-Guidelines-Jan-2016.pdf

106) **National Archives – Preservation Policy:**
https://cdn.nationalarchives.gov.uk/documents/preservation-policy-june-2018.pdf

107) National Archives – Things Allowed into Search rooms:
https://www.nationalarchives.gov.uk/about/visit-us/researching-here/can-take-reading-rooms

108) NPSA – Business Continuity:
https://www.npsa.gov.uk/content/business-continuity

Security Education & Training

109) ARA (UK & Ireland) – Training Events:
https://www.archives.org.uk/training

110) Trident Manor Training Academy – Cultural Protection Training (Commercial site):
https://tridentmanor-ta.com/cultural-heritage/

111) International Council of Archives – Training Programme:
https://www.ica.org/en/training-programme

112) Scottish Council of Archives – CPD Modules for Archivists:
https://www.scottisharchives.org.uk/education/archivists/10-20-30/

113) NPSA – Employee Vigilance Campaign:
https://www.npsa.gov.uk/security-campaigns/employee-vigilance-campaign

114) NPSA - Workplace Behaviour Campaign:
https://www.npsa.gov.uk/security-campaigns/workplace-behaviours-campaign

115) Collections Trust (British Museum) - An Introduction to Loans:
https://collectionstrust.org.uk/resource/loans-part-one-an-introduction-to-loans-british-museum-collections-skills-film/

116) Collections Trust – Online Training Programmes:
https://collectionstrust.org.uk/events/nationwide-event-listings/online-training-sessions-for-organisations/

117) NPSA – Security Consideration Assessment:
https://www.npsa.gov.uk/security-considerations-assessment-sca

118) NPSA - Insider Risk Mitigation:
https://www.npsa.gov.uk/insider-risk-mitigation-digital-learning

119) National Archives Training Programmes:
https://www.nationalarchives.gov.uk/information-management/training/

120) Protect UK - ACT (Actions Counter Terrorism):
https://www.protectuk.police.uk/group/84?type=catalog

121) NPSA - SCaN Training – Situational Awareness:
https://www.npsa.gov.uk/see-check-and-notify-scan

122) NPSA - Security Messages for New Joiners:
https://www.npsa.gov.uk/security-messages-new-joiners

123) Counter Terrorism Policing – Run, Hide, Tell Video:
https://www.youtube.com/watch?v=gx0d6W-QeUQ

Terrorist Threat Considerations

124) Counter Terrorism Policing – Home Page:
https://www.counterterrorism.police.uk/

125) Protect UK – Home Page:
https://www.protectuk.police.uk/

126) NPSA – Countering Terrorist Threats Guide:
https://www.npsa.gov.uk/recognising-terrorist-threats-guide-0

127) MI5 - Counter-Terrorism:
https://www.mi5.gov.uk/counter-terrorism

128) Protect Uk – Stay Safe:
https://www.protectuk.police.uk/advice-and-guidance/response/stay-safe-film

129) Protect UK - Marauding Terrorist Attacks:
https://www.protectuk.police.uk/advice-and-guidance/response/marauding-terrorist-attacks-mta

130) Protect UK – A Guide to Personal Security:
https://www.protectuk.police.uk/advice-and-guidance/awareness/blue-book-guide-personal-security

131) Protect UK – Countering Vehicle as a Threat:
https://www.protectuk.police.uk/advice-and-guidance/awareness/countering-vehicle-weapon-best-practice-guidance-goods-vehicle

Cyber/IT Threats

Note:
Having reviewed various sites it has been decided that for ARA members it is inappropriate to list anything other than the excellent government site below that basically provides a 'one-stop-shop' for all advice and guidance regarding cyber/IT threats and ways to protect organisations.

ARA members' IT infrastructure is being attacked daily and rather than add any confusion to what is an ever changing and evolving threat landscape, a single source that is centrally funded is provided.

132) NCSC – National Cyber Security Centre – Home Page:
https://www.ncsc.gov.uk/

Appendix 2
Risk Assessment Scales & Descriptors

These tables are designed to provide the client with an understanding of the parameters and criteria used to assess threats and the risks they pose to a venue. In order to be user-friendly and provide a legacy framework for future risk assessment processes, a basic format and descriptive process are used. This process is primarily quantitative in nature as opposed to a more complex combined qualitative and quantitative assessment, carried out by risk management professionals.

The risk assessment and the descriptors used to complete it are moveable parameters based on the threats and risks that exist or those that can be reasonably expected. Should circumstances change that impact the nature of any threat or risk to the proposed venue or exhibition, then a complete review of the risk assessment should be undertaken. This is necessary to ensure that the risk mitigation measures remain appropriate, balanced, and relevant.

Assessment of Threat Ratings (HIC – Historic, Intentions, Capabilities - Principles)

Rating	Threat Description
Very High	Currently active threat source with a proven intent and high level of experience and capabilities.
High	Historically, significant active threat source with current and demonstrated intent and capability.
Moderate	Historically active threat source. Stated or expectant intention and a credible capability.
Low	Historically minor incidents involving the threat source. An assumed intention but with limited capability.
Very Low	No historical incidents involving the threat source. Limited or unknown intentions and unknown capabilities.

Risk Likelihood Descriptor

Rating	Risk Likelihood Description
Very High – 5	There is an expectation that the risk event will occur.experience and capabilities.
High – 4	There is a probability that the risk event will occur at some point.
Moderate – 3	There is an increased likelihood that the risk event will occur at some time.
Low - 2	There is a possibility that the risk event will occur at some time.
Very Low – 1	The risk event is highly unlikely to occur.

Risk Impact Consequence Matrix
(variable scales, organisation specific based on risk acceptance/tolerance)

Rating	Threat Description			
Critical - 5	Complete loss of operational capabilities for an extended period or permanently.	Loss of life and serious injuries requiring hospitalisation	The proactive adverse media campaign, nationally and internationally. Serious reputational damage with long recovery times.	Financial losses **Not assessed by Trident Manor, this rests with the risk owner**
High - 4	Full operational loss of functions for a short period or partial loss over an extended period.	Single or multiple serious injuries requiring hospitalisation	The extended media campaign, national or international, has long-term reputational damage.	Financial losses **Not assessed by Trident Manor, this rests with the risk owner**
Moderate - 3	Significant disruption to operations (no timeline).	Injuries requiring hospitalisation.	Wider adverse media coverage, short-term impact and reputational damage.	Financial losses **Not assessed by Trident Manor, this rests with the risk owner**
Low - 2	Minor disruption to a single area of operation for a moderate period (1 – 4 hours).	Other injuries at the venue without hospitalisation but requiring first aid.	Local levels of adverse media coverage with a degree of reputational damage.	Financial losses **Not assessed by Trident Manor, this rests with the risk owner**
Very Low - 1	Minor disruption to a single area of operation for a short period of time (>1 hour).	Minor injuries. Local treatment without hospitalisation	Limited levels of adverse media coverage. Minor reputational damage.	Financial losses **Not assessed by Trident Manor, this rests with the risk owner**

Risk Likelihood Matrix

Likelihood \ Consequences					
	20-25	16-19	16-19	10-15	10-15
	16-19	16-19	10-15	10-15	10-15
	16-19	10-15	10-15	10-15	5-9
	10-15	10-15	10-15	5-9	5-9
	10-15	10-15	5-9	5-9	1-4

Achieved by multiplying the Likelihood score with the Consequence one to generate a quantitative score that can be assigned to the below 'Action Timeline'.

Action Timeline

Final rating	Action timeline
Extreme	Immediate
High	Urgent
Moderate	As soon as possible
Raised	When possible
Low	Accept risk

Example Risk Assessment:

Threat General	Threat Specific	Likelihood	Consequence	Risk Score Likelihood x Consequence
Criminal	Burglary - Organised Crime Groups	1	3	3
	Burglary - Opportunistic	2	3	6
	Theft - Opportunistic	2	2	4
	Theft - Insider Threat	3	3	9
Social	Drugs	3	3	9
	Organised Protests	3	4	9
	Industrial Disputes - strikes, riots	2	3	6
	Extreme precipitation - rain, snow, ice, hail	3	4	12
	Flood - rivers rising, surface water runoff, storm surge	2	4	8
Accidental or Human Error	Fire	3	5	15
	Damage	3	3	9
	Complex attack	1	5	5
Terrorism	Bladed weapon attack	1	5	5
	Vehicle as a Weapon	1	5	5

Appendix 3
Perimeter Materials

Type	Advantages	Disadvantages
Natural Topographic		
Open Space	• Limited cost	• No demarcation • No barriers • Risk acceptance • Lack of control • Reduced protection
River/lake	• Can be difficult to cross, especially with a vehicle. • Low cost • Aesthetically pleasing • Creates stand-off	• Limited control • Climate change • Maintenance still required • Potential for flooding • Potential for drying up
Cliff/ escarpment	• Difficult to scale • Limited vehicle access • Possibly low maintenance • Low design cost • Creates stand-off	• Prone to climate change • No control • May require underpinning
Perimeter using natural materials		
Bund	• Potentially cheaper than fences • Easy to maintain • Aesthetically pleasing	• Prone to climate change • Maintenance still required • Might not be recognised as a boundary /perimeter • Easily by-passed with basic
Water feature	• Creates stand-off • Can be difficult to cross, especially with a vehicle. • Low cost • Aesthetically pleasing • More controlled than natural waterways	• The cost of designing and implementing might be more expensive than adding a fence. • Maintenance still required
Hedges	• Environmentally friendly • Aesthetically pleasing • Low profile • Possible cost saving • Provides a demarcation line between public and private spaces.	• Quite easy to breach • Maintenance costs • Potentially provides areas of concealment and cover from view. • Takes time to grow.

Type	Advantages	Disadvantages
Manufactured Perimeter Fences		
Timber fence panels	• Easy to install • Cheaper than other fences • Provide cover from view • An effort is required to scale them.	• Easy to scale • Easy to destroy • Cover from view • Requires maintenance • Longer-term costs and efforts may not be value for money.
Chain link fence	• Relatively easy to install • Clear delineation • Cheaper than other security fences • Requires scaling and presents a barrier for an undetermined attacker.	• Questionable cost-effectiveness. • Easily cut • Easily scaled • Not aesthetically pleasing. • Some maintenance requirements
Steel palisade fence	• Effective delineation • Moderately robust security fence • Deterrence effect on most casual criminals/trespassers	• More expensive than chain link. • Not aesthetically pleasing
Security grade fencing	• Effective delineation • Robust security fencing • Difficult to scale or cut	• Expensive compared to other fence types. • Not conducive to a cultural setting.
Brick wall	• Relatively easy to install • Cheaper than some fences • Provide cover from view • An effort is required to scale them	• Easy to scale if not high enough. • Cover from view not an aid to natural surveillance • Costs and installation time could be higher than other fabricated fences.

Appendix 4
Anti Scaling Products

Type	Advantages	Disadvantages
Signage	• Cheap • Easy to install	• Requires third parties to be compliant. • No real deterrence • Not prevention
Anti-climb paint	• Relatively cheap • Easy to apply • Moderately effective against casual trespassers. • Environmentally friendly • Potential staining of clothing and skin.	• Potential for injury liabilities (use of signage mitigates most of that risk) • No physical barriers
Roller barriers	• A visible deterrent • A physical barrier that has to be bypassed • Non-injurious • Creates a time delay.	• Increased cost • Not aesthetically pleasing
Wall spikes	• A visible deterrent • A physical barrier that has to be bypassed • Non-injurious • Creates a time delay.	• Increased cost • Not aesthetically pleasing • Injurious
Downpipe cover	• Reduces the risk of downpipes being used for scaling. • Non-injurious • Aesthetically acceptable	• Cost • Maintenance still requiredus
Spiked collars	• Effective anti-climbing devices • Visible deterrent	• Injurious • Aesthetically horrible • Potential for liability
Barbed/coiled Razor Wire	• Partially effective anti-climbing products • Visible deterrent	• Quite easy to breach • Maintenance costs • Aesthetically horrible • Injurious • Potential for liability

Appendix 5
Protective Glazing Options

Type	Advantages	Disadvantages
Toughened safety glass	• Cost • Aesthetically acceptable	• Vulnerable to attack with basic tools • No visual deterrent (could increase the target attractiveness)
Laminated safety glass	• Cost • Aesthetically acceptable • More robust than toughened glass	• Vulnerable to attack with basic tools • No visual deterrent (could increase the target attractiveness)
Toughened/ laminated safety glass with ASF [1]	• An additional layer of robustness is added that will delay any ingress by a few seconds for the toughened glass and slightly longer for the laminated glass. • Additional cost over the use of safety glass.	• Questionable benefit if tools are used. • Cost-benefit of the delay versus the additional installation cost
Wired Glazing	• Visible deterrent for opportunist criminals • More robust than toughened glass	• Not aesthetically pleasing
Security Glass	• Robustness • Known delay	• Cost • Weight

[1] Anti-shatter film, min 200 microns, security function

Appendix 6
Glazing Protection Measures

Type	Advantages	Disadvantages
Narrow windows (150mm)	• Not easy to climb through • Reduced costs	• May not be aesthetically pleasing.
Using window locks	• Helps to reduce the risks of surreptitious entry. • Helps reduce the risk of items being dropped or lowered out of the window. • Cost effective.	• Limited benefit if the pane is attacked.
Metal bars [1]	• Visual deterrent • A degree of robustness from opportunistic adversaries • Reasonably cost-effective • Can be installed inside or outside the glass.	• Susceptible to cutting • Can be pulled from fixings if a vehicle is used. • May not be approved by planners • Possibly not accepted aesthetically
Shutter/Grille (not security rated)	• Visual deterrent • A degree of robustness from opportunistic adversaries • Reasonably cost-effective	• Susceptible to cutting • Can be pulled from fixings if a vehicle is used. • May not be approved by planners • Possibly not accepted aesthetically
Timber shutters with locking bar	• Potentially cheaper than the above. • Aesthetically pleasing	• Susceptible to cutting • Susceptible to direct force attack • Weaker than the above. • May not be approved by planners • Possibly not accepted aesthetically
Timber shutters with steel inserts and metal locking	• Aesthetically pleasing • Increased robustness over standard timber shutters	• May not be approved by planners • Possibly not accepted aesthetically
Security rated (SR3) Shutter/ Grille	• Robust • Visual deterrent • Can be installed inside or out.	• Cost • May not be approved by planners. • Possibly not accepted aesthetically
Secondary security glazing (SR3)	• Discreet • Robust • Aesthetically pleasing • Normally acceptable to planners if demountable. • Environmentally supportive	• Cost

[1] Securely affixed to the masonry or designed in.

Appendix 7
Intruder Sensor Selection

Sensor	Advantages	Disadvantages
PIDS (Perimeter Intruder Detection System) – Fence mounted	• Will give the earliest notification of somebody scaling a fence.	• Not normally practicable for a cultural setting. • Expensive with limited cost benefit, especially if no immediate response is available. • Ongoing maintenance costs
PIDS (Perimeter Intruder Detection System) – Buried	• Will give the early notification of somebody walking over an area. • Discreet	• Not normally practicable for a cultural setting. • Expensive with limited cost benefit, especially if no immediate response is available. • Ongoing maintenance costs and difficulties if faults or damaged. • Prone to false activations especially if cattle are in the area.
PIDS - Microwave Beams	• Effective in most weather types • Effective up to 200 metres • More effective than IR beams	• Expensive • Hard-wired power is required. • Vegetation can still create false alarms
PIDS - Infrared	• Less expensive than microwave	• Still expensive with a questionable cost/benefit. • Impacted by weather • Precise installation/alignment needed • Prone to false alarms caused by animals and vegetation
Motion sensor with light combination	• Low costs • Provides a clear illumination of an area • Can be powered from inside a property	• False alarms • Not normally linked to an IDS and therefore passive
Door/window contacts	• Discreet • Effective if a door/window is opened. • Cheap • Good as an initial notification • Can be hard-wired or wireless[1]	• Can be damaged and/or cables removed • Potential to bypass.

[1] Wireless sensors are only acceptable to Grade 2 systems and therefore would not be appropriate for the standard requirements of Grade 3 and Grade 4 (DP3/4) signalling.

Continued overleaf

Appendix 7 *Continued*

Sensor	Advantages	Disadvantages
Vibration/shock sensors	• Can provide an initial notification of a forced entry attack. • Can be used on/in display cases • Cost effective • Versatile • Can be used on doors to provide a confirmed alarm • Very effective when fastened to walls of secure storage facilities.	• Not normally practicable for a cultural setting. • Expensive with limited cost benefit, especially if no immediate response is available. • Ongoing maintenance costs
Acoustic (break glass)	• Discreet • Can provide the initial notification of windows/ glass being broken. • Cost effective	• Only works with glass • Not very versatile
PIR (motion sensors)	• Wide choice • Cost-effective • Good for spatial coverage • Discreet • Anti-masking capabilities • An ability to undertake a walk test to confirm if working.	• Can be accidentally obscured thereby reducing effectiveness
Dualtech sensors	• Less prone to false alarms • Good for spatial coverage • Wide choice • Cost effective • Good for spatial coverage • Discreet • Anti-masking capabilities • An ability to undertake a walk test to confirm if working.	• Can be accidentally obscured thereby reducing effectiveness

Appendix 8
Fire Alarm System Categories & Meanings

Grade	Advantages
M	**Manual:** The least sophisticated of systems that rely on the venue's occupants to detect a fire and warn others. When a fire is discovered, the alarm must be activated manually to alert everybody else in the building to the danger. (This can include break-glass devices, tannoy's, or verbal calling. Manual fire alarm systems can be effective in certain circumstances but due to reliance on people, errors can occur. These systems are not recommended for larger spaces or those with a lot of visitors
Grade	**Advantages**
L1	**Life 1:** The most comprehensive fire alarm system, which includes detectors in all areas of a building where a fire could feasibly start. Detectors are linked up to a centralised alarm system which alerts the whole building should a fire break out. This enables all occupants to have the earliest notification of a fire being detected and maximises the chances of escaping. Suitable for venues where there is a large footfall.
L2	**Life 2:** Life 2: Systems that fall into this category feature smoke detectors in all rooms forming part of an escape route. Detectors will also need to be installed in all high-risk rooms, such as kitchens, boiler rooms and areas with heavy plant machinery. L2 systems are effective at providing an early warning to occupants beyond the source of the fire and those working in high-risk areas.
L3	**Life 3:** A system features detectors in all escape routes and rooms that open onto an escape route. This ensures that all inhabitants of the building are given enough warning before being impeded by flames, smoke, or toxic fumes. This category is normally used in office blocks and commercial buildings that have flights of stairs.
L4	**Life 4:** This system has detectors in escape routes only and can include corridors and stairs. This category is for the lower levels of risk such as single-storied buildings.
L5	**Life 5:** This is where detectors are installed in a specific area because of the activities taking place in there or items stored in that space.
P1	**Property 1:** This grade of system installs detectors across the whole building to protect the building and contents as far as reasonably practicable. This grade of system lowers the risk of damage and disruption, which in turn, reduces losses that a fire could inflict.
P2	**Property 2:** In this system, detectors are installed in high-risk areas only, providing early detection for the most likely sources of a fire. This will help to minimise any damage to the property and contents, but not as well as a P1 system.

Appendix 9

Example - Opening and Closing Procedure

Opening and Closing Procedures –

Summary
The protection of ### Limited assets and information is of critical importance to our continued existence and ongoing reputation. Therefore, it is important that we are proactive in taking steps to protect our information and assets.

The following procedure will be adopted by all staff involved with opening or being the last to leave the office at night. Failure to follow these actions will be viewed as a security breach; if recklessness is shown then it will be considered a serious security breach and disciplinary action may be taken.

Opening

1. Disengage the mortise lock.
2. If the lock is not engaged find out who was the last to leave. Report to the Office Manager.
3. If the lock was engaged and was found insecure inform the MD immediately.
4. Within 20 seconds present the alarm fob to the control panel to turn off the alarm.
5. Open the filing cabinets ready for daily use.

Operational Hours

1. It is acceptable to put the door 'on the latch' during office hours. However, it should never be left in that state if the office is unattended, irrespective of the time frame.

Closing

1. All classified and sensitive materials should be cleared from desks and locked away.
2. The secure store door should be checked and the alarm set.
3. All windows are to be closed.
4. Shared cabinets must be locked.
5. The alarm fob is to be presented to the control panel and a 20-second sounder should be heard. (If no sounder is heard then the alarm has not been set (check 2. above) and the process must be retried. If it still does not set call the Office Manager.)
6. When the sounder is heard leave the office and turn the key in the mortise lock (this fully arms the intruder alarm system).

If anybody has any questions about this process, they should be raised with Office Manager in the first instance.

Appendix 10
Example - Access Control Procedure

Access Control Procedure –

Summary
The protection of ### Limited's assets and information is of critical importance to our continued existence and ongoing reputation. Therefore, it is important that we are proactive in taking steps to protect our information and assets.

The following procedure will be adopted by all staff to ensure that access to the venue is controlled and limited to those who have a right to access.

Public Space and Reception

- Visitors are allowed free access to the public space on the ground floor including the café, seating area, and toilet facilities.

Staff Working Areas

- Anybody wanting access to the staff working areas must speak with the reception desk and confirm an appointment has been made. (If no appointment has been made then approval from the office manager must be sought before progressing further.)
- The reception desk will contact the named individual.
- The individual will ensure that the conference room is clear of all sensitive materials or anything that relates to other clients. They will then go to the reception area and bring their guest into the conference room.
- Nobody other than staff members are to be brought into the working area due to client confidentiality and sensitive discussions by other members of the team.
- Following the meeting the visitor is to be escorted back to the reception desk and signed out.
- Where there is a need to vary this procedure agreement must be sought from Management.

Secure Storage Area

- The Office Manager controls access into the secure storage area. All movements in and out of the store are to be recorded.
- Access is only permitted if accompanied by the Office Manager or if unavailable the Managing Director.
- Items removed from the secure store must be signed out and returned at the end of each day.

If anybody has any questions about this procedure, they should be raised with **Office Manager** in the first instance.

Appendix 11

Example - Fire Procedure (no fire alarm)

Opening and Closing Procedures –

Summary
Fire is the biggest danger to life and the preservation of archives, collections, or other flammable documents.

- On finding a fire shout repeatedly '**FIRE, FIRE, FIRE**' to make others aware.
- Dial or have somebody dial **999/911 immediately**. Provide as much information as possible.
- If a small fire and you have been trained in using firefighting equipment attempt to extinguish the fire. **On no account should you put yourself or others in danger to do so.**
- **EVACUATE** the building by the safest route.
- Leave personnel possessions when evacuating.
- Go to the **Assembly area. [specify]**
- Account for all staff and advise those who are off-site to remain so until informed otherwise.
- Do not return to the building until the **Fire Service** has given the **'all clear'**.
- Consider whether there is a need to implement the **Salvage Plan**.

Any questions about this procedure should be raised with the Responsible Person, **Sue Gaines, Health & Safety Manager.**