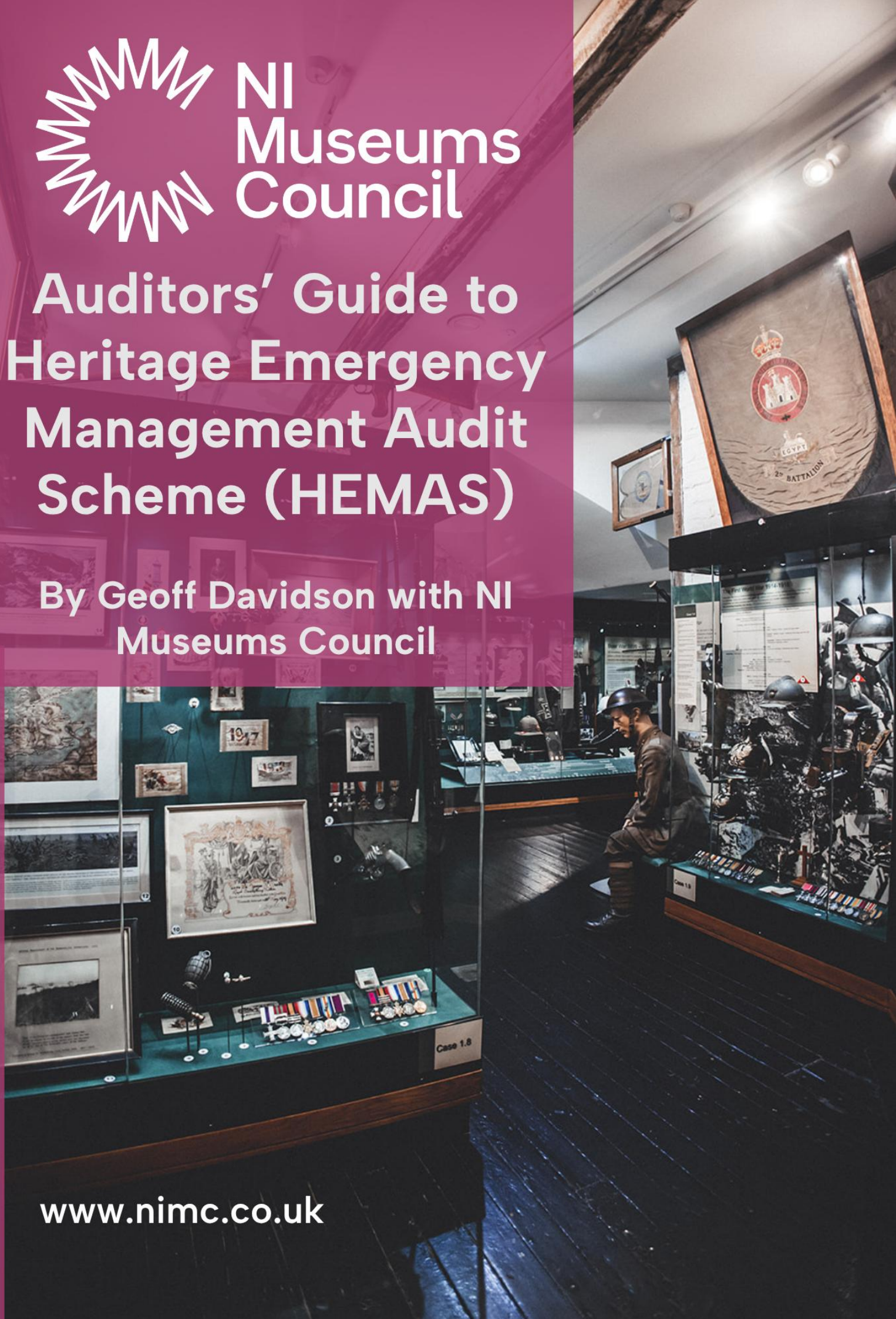
NI Museums Council

Auditors' Guide to Heritage Emergency Management Audit Scheme (HEMAS)

By Geoff Davidson with NI Museums Council



www.nimc.co.uk

NI Museums Council
153 Bangor Road
Holywood
Co. Down
BT18 0EU

devofficer@nimc.co.uk

Auditors' Guidance:
Heritage Emergency Management Audit Scheme Level 1

Introduction

This level of HEMAS is designed to introduce the process of audit allowing any heritage organisation to establish its current emergency planning and business continuity position. The scheme is designed to support the 'Plan Do Check Act' approach for continuous improvement. HEMAS Level 1 does not set out to examine management systems but seeks to establish a baseline for measuring change for those organisations who are new or unfamiliar with the concept of managing emergencies and managing the implications of a major incident.

By measuring performance and establishing an initial capacity baseline organisations can plan their improvements in critical areas and monitor progress as competence and confidence increase.

The Introduction level of HEMAS is not designed for those organisations with well developed and tested emergency and business continuity management programmes. The Introduction level audit scheme assumes that organisations have some preparation for emergencies in place based around the experiences and knowledge of individual members of staff. This background is useful and should be built upon.

The Scheme is designed to function most effectively with smaller museums and heritage organisations who are considering how to manage these important areas.

Building a culture capable of managing emergencies and recovering from adverse events will take time and effort. ISO 22301:2019 Business Continuity Management is the international standard for managing BCM and provides the template for continuous improvement. The Scheme and the principles of measurement behind it are consistent with ISO Management Systems and the intent is to allow organisations to develop a culture of continuously improving performance in critical areas when protecting Collections, buildings and long-term organisational viability.

The HEMAS Scheme is designed to provide a quantitative score for each of the audit elements. These issues are core to effective emergency management (EM) and business continuity management (BCM) in all heritage organisations. The issues addressed relate to the protection of objects, Collections and buildings.

As organisations develop EM and BCM skills the next levels of HEMAS will extend the range of issues and the depth of audit examination and will continue to provide the measurement capability necessary for continuous improvement.

How HEMAS works

There are a number of ways of measuring the performance of management systems. HEMAS is developed to measure how emergency planning and business continuity management systems are performing in heritage environments.

What is a management system?

A management system is the way we manage parts of our business in order to consistently achieve objectives we set for ourselves. These objectives can relate to a range of different management topics, including quality, environmental performance, health and safety and business continuity in the workplace. Management systems are all about improving performance by specifying repeatable and consistent steps we can consciously implement to develop an organizational culture that uses a continuous cycle of self-evaluation, correction and improvement. The EP and BCM processes improve by increasing staff awareness of how to deal with issues and effective management leadership and commitment.

The level of complexity of the system will depend on each organization's specific context. For some organizations, especially smaller ones, it may simply mean having strong leadership from senior staff, providing a clear definition of what is expected from each individual member of staff and how they contribute to the overall objectives, without the need for extensive documentation. More complex organisations will need extensive documentation and controls in order to fulfil their legal obligations and meet their objectives. HEMAS Level 1 is designed to lift EP and BCM awareness in smaller organisations and create an opportunity to move to Level 2 where the ISO principles are understood and followed.

Measurement

There are a number of ways to measure management system performance. Many relate to what is actually seen at a moment in time, such as inspections, but only an audit, taking an in-depth review of management activity, will provide a basis for improvement. It looks at what is happening as well as how it happens and identifies the process of ensuring that the required action happens each time it is required.

Audit at any level should not be something to be wary of. Used as a management tool it is directly aimed at creating the conditions for continuous improvement. We are all much more aware of the need to address emergency planning and business continuity issues following the Covid pandemic and its significant effects on every organisation. The HEMAS Audit Level 1 is kept simple and aims to address the most common EP and BC management issues identified by organisations starting on their journey. The initial use of the Scheme provides a baseline against which improvement can be planned and made. Further use of the Scheme can be used to set targets and allows a measurement of improvement which is an integral component of creating and maintaining a continuous improvement cycle. Looking at the score for individual Element issues provides a mechanism to address the opportunities for improvement. A low Audit score indicates that further action is necessary. Addressing low scores provides a better plan of improvement than working through issues identified by chance or by some form of mishap or emergency. That mishap may occur, but you will still have an action plan in place based on the needs of your Collection and activities as identified by the Audit.

To be effective the Audit must show that the conclusions reached by the Auditor are relevant, accurate and evidence based. For the Audit process to work the Auditor must see evidence of activity. This includes confirmation by reviewing records, minutes, confirmation by staff involved and seeing physical evidence of equipment, etc.

Auditors should therefore see and confirm evidence of activity when scoring each element. There may be some professional judgement involved on the part of the Auditor but to be effective in making recommendations for improvement physical evidence should be available, seen and confirmed. If a Policy or Procedure is claimed the auditor should see evidence that it exists, is relevant, current, and used. Auditor Recommendations should be the starting point for a business improvement Action Plan as it should provide guidance on how to improve management systems and how to improve the Audit score demonstrating improvement.

Managers should be aware that good intention is not a basis for improvement and action is required to make changes which will improve the level of protection for people, collections, and the organisation. Using the Audit to establish what records exist and what should exist to confirm action is important, this will be the outcome of any baseline Audit and should be included in the Auditor Recommendations.

The Level 1 Audit can be used to self-audit to provide some indication of the current baseline knowledge and performance of an organisation. Where the Auditor has limited knowledge of EP and BC management systems this may affect the effectiveness of their recommendations and organisations should consider who they ask to undertake the Audit.

Audit Cycles

Audit Cycles are important in establishing a long-term measurement protocol and while audit is important allowing a period between formal audits is necessary to demonstrate that improvements are embedded within the culture of the organisation rather than in place in advance of the audit only.

Where HEMAS is used a cycle of three years between ‘formal’ audits will allow for the introduction and embedding of recommendations within the organisation’s management system. The Scheme can be used informally at any time to quantify and confirm improvements.

Scoring

Section Scoring: HEMAS Level 1

Score each issue according to the scheme below

Inadequate Response			Adequate Response	
1	2	3	4	5
No or part control only	Controls in place are inadequate	No or irregular use of existing controls	Basic level of compliance only	Significant controls in place and used
Requires Immediate Action: The organisation is not effectively managing emergency or business continuity responses in the element. It should take immediate steps to improve performance.			**Monitor existing performance:** The organisation is managing the element. It should continue to monitor performance where it has good performance and plan to improve other areas	

The scoring system is established based on 2 responses describing 'Inadequate' or 'Adequate' levels of activity for that element. Scoring is divided to allocate a numerical value for the element which allows comparison across audit cycles for organisations and across individual locations of the same organisation. Element scoring will also indicate where they are weaknesses in EM and BCM activities and where the opportunities for improved performance are.

Inadequate Response

1 **No or part control only**

Auditor has seen no or very limited activity which indicates that the organisation is able to protect Collections during and after an emergency.

2 **Controls in place and are inadequate**

The organisation has some control measures in place, but they are unlikely to provide protection for Collections when tested in an emergency.

3 **Irregular use of existing controls**

The organisation has control measures which would offer protection to Collections but evidence that they could be applied as planned in an emergency is not available.

Adequate Response

4 **Basic level of compliance only**

The organisation has plans and tests them which will provide protection for some elements of the Collection.

5 **Significant controls in place and used**

The organisation has significant control measures in place and tests them regularly. Plans will provide protection for Collections and assist in effective recovery from adverse incidents.

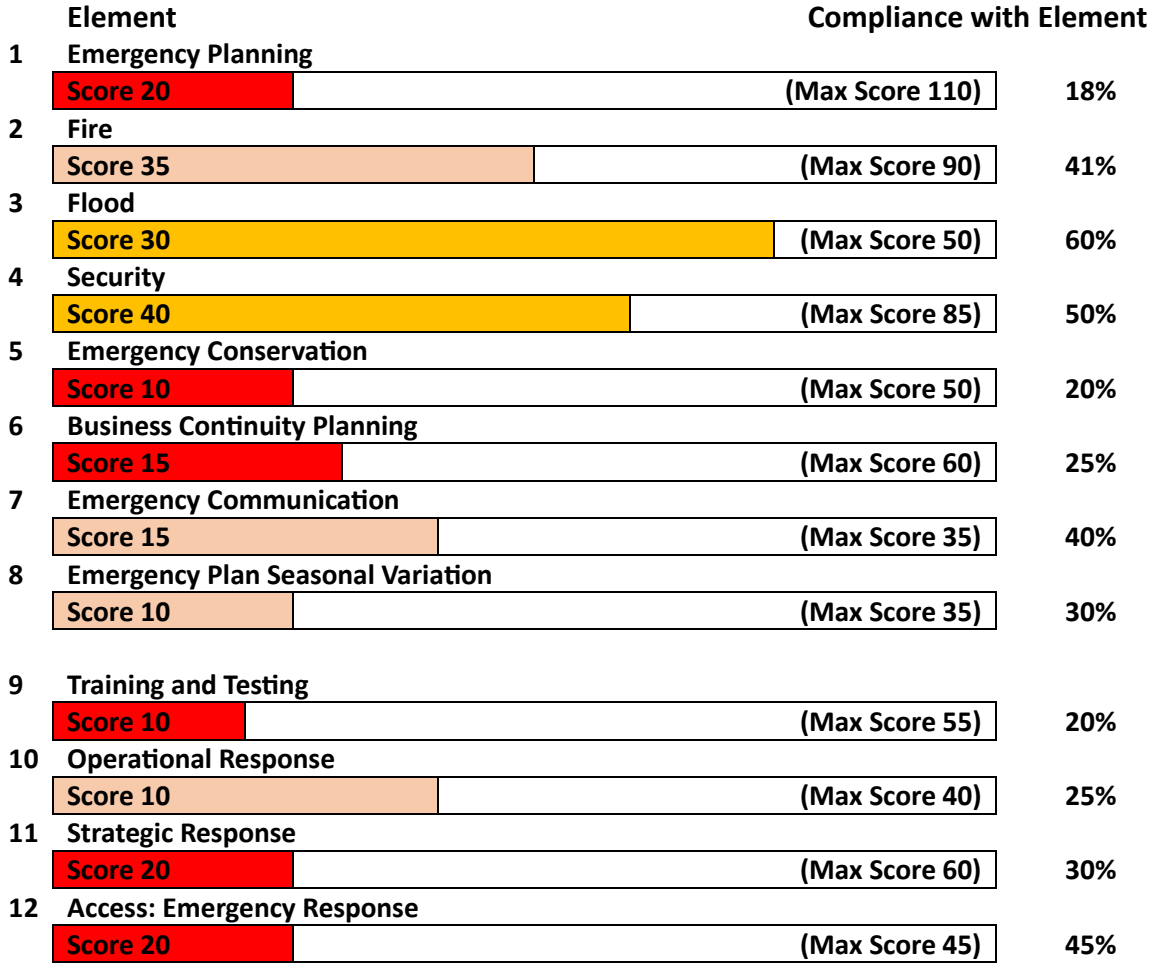
The scoring represents the Auditor's view on the organisation's performance in the Element. The recommendations are based on protecting Collections, buildings and the organisation from the threats identified. The pace at which the recommendations are considered and implemented are for the organisation to decide based on their experience and resources. At this Audit Level the recommendations are not prioritised, however, the Auditor is expressing concern which should be considered.

By scoring each element a numerical value can be developed which provides a baseline for measuring improvement with time as the Scheme is used in the future. The use of a Scheme reduces the risk of a subjective response and allows for fair comparison across a longer audit timescale even where auditors have changed. Totalling all the individual results gives a single number quantitively indicating performance and allowing easy, if non-specific, comparison across different and differing sites.

The Scheme can also be used to monitor changes as EM and BCM programmes are developed and introduced giving a measure of the benefit achieved by the improvements made.

The scoring system can also be for graphical presentation or dashboard of results so that individuals and stakeholders can easily and quickly understand how the organisation is performing. How you do this is up to you and how you normally present information to staff and stakeholders.

Audit Numerical Results (Example)



Audit Level:
HEMAS 1 Introduction

Score 215	(Max Score 685)

Compliance
30%

	Audit Element	Score	Max Score	% Comp with HEMAS 1
1	Emergency Planning	20	100	20%
2	Fire	35	90	45%
3	Flood	30	45	65%
4	Security	40	85	50%
5	Emergency Conservation	10	45	20%
6	BCM Planning	15	60	25%
7	Emergency Comms	15	35	40%
8	Seasonal Variation	10	25	40%
9	Training and Testing	10	55	20%
10	Operational Response	10	40	25%
11	Strategic Response	20	60	30%
12	Access: Emer. Resp.	20	45	45%
	HEMAS 1 Introduction	235	685	35%

HEMAS Level 1: Introduction

HEMAS: Audit Scheme Element 1

Emergency Planning

Issues:

This Section of the Audit looks at your emergency planning process and your ability to respond to and mitigate the effects of an emergency. It is not possible to plan for every possible emergency and it is unwise to try. It is much better to have a core plan in place which can be amended in real time by trained staff to suit any emergency and the threat it presents. Your plans need to be flexible and allow staff the freedom to respond efficiently and effectively. Conversely, where staff are not familiar with the plan and have not trained in how to use it their response is likely to be hampered by indecision as they either apply 'common sense' based on their own experience or adhere to a plan they consider to be the only appropriate response even where it is not effective.

Creating a core plan with trained, competent staff using it to guide their response will be more successful than having a single plan requiring senior managers to agree any change.

What the Auditor is looking for:

1.01 Most organisations have some form of emergency plan. To be effective it should be documented, relevant and subject to regular review. The auditor should be able to read and follow the guidance.

1.02 Has the organisation considered a range of potential emergencies which can affect the Collections, buildings, and activities? Auditors will need to see evidence of this including meeting minutes or lists which have been discussed with staff and advisers. It should be remembered that this is a list of possible emergencies not just those that are most likely – this list should not be 'most probable' but take a much wider look at the threats to Collections. A risk assessment later can address the likelihood of an event. Fire is a major threat; flooding is a more likely threat to objects, and both are normally identified. A pest infestation within a collection can be devastating and is a real threat.

1.03 The Plan should be appropriate to the needs of the organisation and should refer to how the organisation will look after staff, volunteers, visitors, collections and collections information including the collections management system.

1.04 There is a tendency to assume that staff know how to call the emergency services. There should be evidence that people know what information is required by the emergency call handler to ensure that the response is appropriate from the initial contact. The Auditor should ask members of staff.

People should know when and how to declare an emergency. There are variations in the level of emergency as some can be addressed from within the organisation's resources, some will require support from outside the organisation and others will require a blue light response from emergency services. The organisation should have established the criteria for declaring an emergency through to major incident and this will dictate the speed of response.

1.05 For the plan to be effective those members of staff involved should have easy access to the plan or have their own copy. To be effective the approach to an emergency must be consistent with everyone involved knowing what to do and also what others are to do. In an emergency people may have difficulty in remembering what their response is and having a copy of the plan works

as a reminder in such circumstances. Organisations may have hard copy plans or use smart phones. The Auditor should be able to see the Plan used by members of staff.

1.06 In an emergency staff and senior members of the emergency services should be able to have access to a copy of the plan easily. Having it locked in a cabinet or requiring system access to get to it will slow the response. Speed of response is essential, so the location of the plan is important especially where people are coming onto site outside normal opening hours.

1.07 The plan should clearly identify the individuals who make up the Incident Response Team. It is important that this Team is controlling the incident responses and that others know that the response is effectively coordinated by this Team. Where individuals act on their own, they put themselves and others in danger and will adversely affect the working of the plan.

1.08 The plan should identify and explain the role of each of the Incident Response Team members to minimise duplication and ensure that activities are coordinated.

1.09 In an emergency you may need to contact staff, suppliers, or others in a hurry. To minimise the time taken to contact the appropriate people a list of names and contact details should be included in the Plan. It is important that those asked to respond are the right people for the incident, asking people to respond who are not required will simply create a group of onlookers who will then have to be managed by the Incident Team.

1.10 It is helpful to know how long it will take for individuals asked to respond to arrive on site when responding to an incident.

1.11 Those people who have agreed to play a part in an emergency response will know that they might be asked to respond. They should be aware of how they will be contacted and have agreed to monitor that communication route.

1.12 The organisation should have a list of equipment that can be available in an emergency and where it is located. People unfamiliar with the equipment may not know what it available and miss the opportunity to use it.

1.13 Equipment which could be of use in an emergency may be located where it is used by others. Incident responders need to be aware of where it is and how to get it.

1.14 Organisations should have identified priority objects which they need to move or protect in the event of an emergency. It is not realistic to believe that every object is equally valuable and needs to be safe. Some objects should be identified as critical to the Collection and their protection should be described in the Emergency Plan. This may mean removal to a safe place or protection in-situ.

1.15 If a critical object is to be moved the organisation should have a plan to move it including identifying handlers and equipment. The Fire Service will assist but, without object handling training in advance, their capacity is limited. They may have other tasks at the time you want to move objects.

1.16 Moving objects in the event of an emergency may be necessary and may be difficult. If the organisation has planned for this, it should also have planned where the objects will be moved to and stored. Leaving them exposed in an unsafe place is never appropriate.

1.17 Buildings can be reoccupied when it is safe to do so. The Emergency Plan should identify who can confirm that the building is safe. There may be circumstances when the Fire Service will not advise on access and the organisation may need to identify an appropriate person who can advise on the building and the implications of any damage to it.

1.18 For any response plan to work effectively each person involved must have practiced their role. Regular tests of the Plan should be conducted. Additional tests may be appropriate where there are staff changes or for new spaces or activities.

1.19 To remain current and valid the Emergency Plan should be regularly reviewed especially after an incident or test where issues have been identified. Two tests per annum should be the minimum.

1.20 The Plan is important and should be authorised by a senior manager to ensure that it has organisational authority allowing staff to act appropriately.

1.21 The Plan is an important document that establishes how the organisation will respond to a major incident. Once authorised it should be available to those who are also involved in the response, e.g. emergency responders.

1.22 It is possible that organisations will share space with others, and it is important that links between plans are regularly reviewed and understood.

HEMAS: Audit Scheme Element 2

Fire

Issues:

As well as a major threat to people fire is a very significant threat to every Collection and historic building. Not only will the fire cause damage where it is in contact with or close to any object but the effects of smoke will continue far beyond the seat of the fire. The materials used to control and extinguish the fire will also cause damage to objects.

Considering the effects and implications of a fire are important and will guide discussions on the risks involved. The Fire Service will advise and work with any organisation where collections are important to the history of the country. Where the Fire Service is aware of the collection or building and has been involved in the emergency preparations they can respond quickly and effectively. This will reduce response times and ensure that any specific needs of a Collection are addressed. Working regularly with the Fire Service increases their familiarity with the location and Collections and improves working relationships and outcomes in the event of an emergency.

What the Auditor is looking for:

2.01	The emergency services should know that the organisation exists. If they don't know about you, they cannot assess how to address a major incident and responses may be delayed.
2.02	The Fire Service should know exactly where the organisation is based and the location of all the buildings to which the Emergency Plan applies. They need to be able to go directly to the site.
2.03	The Fire Service is keen to have an effective response to an emergency. Regular site familiarisation visits are a positive means to ensure that your Collection is known and understood. Annual visits by each responding watch are appropriate.
2.04	When the Fire Service arrive, they will need to know of the location of any materials which may pose a risk to firefighters. The organisation should identify all fuels, flammable liquids and gases and hazardous materials in advance and have shared this information with the Fire Service as well as having a site plan showing the locations of such materials.
2.05	If certain objects require a specific response this should be discussed in advance with the Fire Service during the site-specific risk assessment or familiarisation visits. Staff should also know that they should discuss this with the senior officer when they arrive on site.
2.06	The Fire Service will conduct a site-specific risk assessment when they are aware of the organisation. This is a primary means of communicating relevant information with Fire Officers responding to any incident and should be updated when circumstances change.
2.07	If the fire detection system includes a mechanism to automatically call the Fire Service staff should confirm the alarm by dialling 999 as well. Where the organisation relies on a telephone call to the Fire Service staff all should be aware of the need to ensure that they answer the Emergency Operator's questions about the incident. The Emergency Operator will want the individual to stay on the line to gather information for responding Officers.

2.08 Every Collection will have specific needs and require appropriate responses, and the organisation should take an opportunity to fully discuss this with the Fire Service, including access, extinguishing medium and salvage potential.

2.09 Where an organisation has identified its priorities a plan of their location indicating priority objects or materials should be available to the Fire Service. This will help as Senior Officers can decide if access to areas holding priority objects is possible.

2.10 If there are objects where the use of firefighting techniques or materials would have an adverse effect, they should be identified in the Plan. Such requirements should be discussed with the Fire Service in advance of any incident.

2.11 The Fire Service should be offered the opportunity to join in some of the Plan tests. This provides a training opportunity for Officers in a different environment and allows discussion of any needs of collections and responses in controlled circumstances.

2.12 The organisation should have a Fire Plan for its building which provides the Fire Service with information about the building itself. This should include internal evacuation routes, assembly points, exit doors, access routes through the building, hydrants, fire extinguishers, fuels, service isolation controls and fire alarm panels.

2.13 The organisation should have a current fire risk assessment for the buildings, contents, and activities.

2.14 A Fire Safety Policy is important as it addresses the overall management and control of fire risks across all areas of the organisation and should link to the Emergency Plan.

2.15 The organisation should have a fire detection and alarm system. Staff, visitors, and Collections should be protected.

2.16 All detection and alarm should be maintained, inspected, and tested in compliance with the manufacturer's specification. They must work when required and should not cause false alarms to maintain confidence.

2.17 Regular testing of the alarm system is important, and a record of all tests should be competed and regularly reviewed. This creates opportunities to identify any failures within the system.

HEMAS: Audit Scheme Element 3

Flood

Issues:

Water ingress in the event of a flood is an unusual event but likely to become more frequent with climate change. It is more likely that water ingress will arise from 'accidental' circumstances such as physical damage, frozen and thawing pipes, clogged gutters or downpipes or a damaged wall or roof allowing a route for water entry. Water does not mix with Collections and the consideration of this specific risk should be part of every emergency plan.

Water ingress is more likely than fire and should always be regarded as a high-risk threat.

What the Auditor is looking for:

3.01	The organisation should review the Department for Infrastructure Rivers and Flooding Strategic Flood maps to identify any areas where river, high tide and weather-related flood present a risk to premises.
3.02	The organisation should be aware of the locations and routes of all water carrying pipes through its buildings, and particularly those through areas where priority objects are present.
3.03	The organisation should be aware of areas where rainwater could enter any buildings from gutters, downpipes, and roof valleys.
3.04	Where rain risk areas have been identified they should be inspected regularly to ensure that the water can be removed quickly and efficiently. Inspection frequency should be risk based and reflect weather patterns.
3.05	The organisation should have identified areas where external flood water could enter a building. The water may be outside your site but have an impact within it.
3.06	The organisation should have considered how to react in areas where flooding is likely. This reduces the time taken to respond to a flood event.
3.07	Where the risk of flood is identified and considered possible the organisation should consider how it will divert water flow to protect buildings.
3.08	Objects at particular risk from water damage should be located or stored in an area where they are unlikely to be affected. This may mean they are stored or exhibited above floor level.
3.09	The organisation should have considered how to deal with objects are wet or waterlogged. Wet objects will deteriorate quickly without a rapid response. To prevent further damage the organisation should be aware of the need to act quickly to provide safe storage and restoration space.
3.10	Flooding will require an immediate response for the organisation. The organisation should identify organisations who can assist in that response, e.g. provision of pumps, fans, etc.

HEMAS: Audit Scheme Element 4

Security

Issues:

Emergency planning should include all threats to Collections and buildings, and this should include security threats. The potential for theft is obvious but you should also consider arson, vandalism, and protest. The security threat from those seeking publicity or their aims should be considered.

What the Auditor is looking for:

4.01	The Police should know of the Collection and location of all the buildings so that they can monitor and respond quickly to any incident.
4.02	The Police Crime Prevention Officer will provide guidance and advice on crime prevention and organisations should discuss crime regularly with them. The CPO will have local experience and can connect with other Police Services on issues
4.03	The CPO can provide up to date information on a range of issues beyond theft and vandalism including targeted museum crime, protests and disruptions and should be involved regularly by the organisation.
4.04	Crime Prevention Officers and insurers will give advice on security arrangements and how they can be improved. Where new acquisitions or exhibitions are planned their guidance should be sought.
4.05	Advice on arson prevention and protection should be sought from the Fire Service.
4.06	Insurers are a very significant source of advice on security arrangements and have an interest in protecting objects. Insurers also provide information on a range of security issues on-line.
4.07	Organisations should complete regular environmental visual assessments (EVA) to identify access points and in particular areas where any attempt to gain access is obstructed by trees, hedges and fences. The EVAs should be carried out regularly as winter conditions present greater opportunities for criminals with some areas in darkness.
4.08	Every organisation should have a system in place to monitor visitor access to rear of house areas. These visitors should be identified with badges or passes. Staff should challenge unaccompanied persons and those without a pass or badge.
4.09	A security alarm system is important. Vandalism rather than theft may be the aim of an intruder, and a system will detect both.
4.10	Security alarm systems should be maintained and tested regularly in compliance with the manufacturer's recommendations.
4.11	Organisations should consider how they will respond to a security incident. Staff should know how to respond to particular types of incidents. Guidance is available from the Police Crime Prevention Officer on how to respond.
4.12	Information on museum and visitor attraction security is readily available from a variety of sector organisations. It is important to keep up to date in an ever-changing area as what is attractive to

criminals does change. While opportunist theft or vandalism is an issue a great deal of material is stolen to order irrespective of the scale of the organisation.

4.13 A Security Policy addresses the overall management of security risk including people, objects, buildings, and IT systems.

4.14 As areas such as IT security where risk changes quickly it is important that the Security Policy is regularly reviewed to ensure that is current and effective.

4.15 A security risk assessment is a means of establishing what threats there are to a Collection and how the risk can be reduced. It provides a format for considering security and its management which can be reviewed and improve security performance.

4.16 Temporary exhibitions present a range of issues from installation and opening through to breakdown and exit. These are often new security threats to the organisation and a separate risk assessment should be undertaken linking to the existing organisational assessment to identify and control risks.

4.17 The Security risk Assessment should be reviewed regularly and after any incident. The review provides an update opportunity and should not rely on any loss or damage but the potential for loss.

HEMAS: Audit Scheme Element 5

Emergency Conservation

Issues:

In the event of a major incident resulting in objects requiring conservation the response time is of vital importance. It is critical that organisations consider conservation before an incident occurs. Where objects are removed from a building and left for several days awaiting conservation damage will happen and some will be permanent. Organisations should plan for this!

What the Auditor is looking for:

5.01	Organisations should have identified and noted those priority objects that it wants to move in an emergency. All the objects in a Collection cannot be moved and consideration should be given to establishing a process which identifies those objects that can be moved.
5.02	Where objects cannot be moved and are on a priority listing the organisation should have considered how they will be protected in-situ.
5.03	Objects may need to be protected quickly after an incident. It is important to have identified a suitable conservator who can assist in triaging objects when they have been moved from their normal position following an incident.
5.04	Organisations should know how and when to contact emergency conservators including outside normal working hours and days.
5.05	Where emergency conservation is needed a range of materials will be required by the conservators. The organisation should discuss the materials necessary with conservators.
5.06	Organisations should consider what conservation materials to have on site and know where they can access other materials when required.
5.07	Objects requiring conservation will have a range of needs and conservators can provide advice and guidance on how to categorise damage and response to ensure the objects have appropriate treatment.
5.08	Where objects require conservation suitable spaces for triage, storage and conservation should be identified in advance and easy to access. The spaces should be secure.
5.09	Where objects have been removed for conservation organisations should recognise that this may mean that this conservation space may be in use for some considerable time. Security risk assessments and arrangements and control measures should be updated for the spaces and anticipated occupancy.
5.10	Some objects may have to be held in storage for a long time before conservation can start, the organisation should consider the security requirements for prolonged storage of objects.

HEMAS: Audit Scheme Element 6

Business Continuity Planning

Issues:

Business Continuity Management (BCM) is about identifying those parts of your organisation that you can't afford to lose – such as IT systems, objects, premises, key staff – and planning how to maintain these when an incident occurs. Any incident, large or small, whether it is natural, accidental or deliberate, can cause major disruption. By planning rather than waiting for it to happen, you will be able to get back to business in the quickest possible time. Response delays could mean you lose valuable opportunities and visitors, suppliers and stakeholders lose confidence.

What the Auditor is looking for:

6.01	Organisations tend to think that they know what their critical activities are. To establish what is critical it is important that they review all their activities – including finance, operations, collections, etc. to establish what services are critical to maintaining the organisation.
6.02	Once critical activities have been identified the organisation should consider what and how the critical activities can be affected.
6.03	When critical activities and how they are affected have been established the organisation should develop 'work around' plans to deal with interruptions.
6.04	Many organisations are in similar positions and may be open to discussions on mutual aid opportunities. Insurers should be informed on the arrangements.
6.05	Staff in business-critical areas may not have stand-in cover. Consideration should be given to developing and maintaining critical skills across the organisation. This rarely means that all of an individual's work must be duplicated and is most likely a specific task which others can learn and practice.
6.06	Where space in a business-critical area is compromised or unusable the organisation should have identified alternative workspace to ensure that the activity can continue. This should include access to equipment including IT.
6.07	IT systems are used extensively across all parts of most organisations. Where a system within a business-critical area is lost the organisation should have plans for restoration and recovery.
6.08	Organisation should consider how they will communicate business continuity changes to staff and stakeholders. As such changes are likely to attract external attention communication plans should include media outlets to prevent inaccurate information. Changes may be to locations, access, buildings, and their use, opening times, deliveries etc.
6.09	BCM is important as it manages responses to circumstances which will change frequently. The BC plan should be reviewed regularly.
6.10	New threats can be identified early by reviewing the 'threat level' information provided on the websites of insurance companies, Business Continuity Institute and the national risk register maintained by Government.
6.11	Social media is an important communication opportunity for staff and visitors. Organisations should have systems in place to manage social media and should control outward facing communication.

6.12 Unplanned and uncontrolled information to parties outside the organisation will create major issues. The organisation should use a single point of contact for all comment and a mechanism to ensure that all communications reviewed before release.

HEMAS: Audit Check Element 7

Emergency Communication

Issues:

Communication is vital to managing emergencies. Effective communication will allow organisations and managers to speak directly to everyone who is involved.

What the Auditor is looking for:

7.01	The organisation must be able to quickly contact every person involved in an emergency response. A contact list should be available to staff involved in any emergency.
7.02	For the call-out list to be effective the organisation should review it regularly to keep it up to date.
7.03	The contact list should include contractors and service providers who may be needed, including those you may need only in an emergency. There should be one contact list for the organisation to prevent vital details becoming lost in instances where staff and contractors' lists are kept separate.
7.04	The contacts list should be tested regularly to ensure it is current and familiarise personnel with such calls.
7.05	As emergencies are predictable, however unexpected, it is possible to plan how the organisation will communicate effectively with staff, stakeholders, and the media.
7.06	Plans to communicate with all staff on BCP should be tested regularly, e.g., changes of location, change in opening times. The testing should be announced in advance so that staff know how to respond and that failure to receive the message scan be reported.
7.07	Social media is a useful tool in BCP. As it is so important organisations should have planned how they are going to use it for maximum benefit.

HEMAS: Audit Check Element 8

Emergency Plan Seasonal Variation

Issues:

We live in a temperate zone where temperature and relative humidities will vary considerably throughout the year. Climate change is having an impact on those variations which are likely to become more pronounced with time. The frequency and duration of these variations is likely to increase and will prove challenging. In recognising that such variation will occur it is important that seasonal variation is part of the continuity and emergency planning of an organisation.

What the Auditor is looking for:

8.01	The organisation should consider seasonal variation in climatic conditions and the impact on Collections and storage across the year. Seasons are blurred and unexpected weather should be expected!
8.02	Longer periods of cold and warm weather outside what we expect may be challenging for conditioned storage. Organisations should consider the implications of protracted cold and hot conditions.
8.03	Longer periods of high and low humidity will also be challenging for conditioned storage and for some objects in unconditioned storage. Organisations should consider the implications for Collections.
8.04	Most organisations will check that their buildings are weatherproof. Climate change may be causing an increase in the number of storms being experienced. Organisation should be aware of this and plan accordingly.
8.05	Wet weather as well as flooding should be considered. Prolonged rain and wet conditions can have an impact on buildings and collections.
8.06	Buildings use gutters and drains to remove water quickly and effectively. To be effective they should be regularly checked and maintained.
8.07	Where measures are in place to minimise the risk of damage the organisation should check them regularly to ensure that they will work as planned when required.

HEMAS: Audit Check Element 9

Training and Testing

Issues:

Training is about creating and improving organisational resilience. People involved in incident responses have an opportunity to learn from practices and testing of the plans without the stress of a real time incident happening around them. Regular testing promotes confidence in the plan and increases the probability that the expected outcome will occur. Follow up debriefing on what happened and why will also improve the plan and create a feeling of ownership.

What the Auditor is looking for:

9.01	The organisation should review the Emergency Plan to establish who requires training and how often to ensure that the plan functions effectively.
9.02	The training review should give rise to a training programme for staff involved in incident responses. Performance against the programme should be monitored.
9.03	The organisation should have a training schedule for regular training ensuring that the training is regular and happens.
9.04	All staff identified the Plan should be trained and they should also be trained in any role where they act as stand-in for others.
9.05	The organisation should identify non-operations staff who may plan a part on the incident responses. They should be included in training, e.g. stand-in staff, conservators.
9.06	Emergency responders may be involved in testing the plan and can provide important feedback on their activities and how they interact with the site.
9.07	The only way to establish if a plan works is to test it regularly. Tests should address a range of incident types.
9.08	Tabletop exercises provide a quick, and once started, challenging opportunity for staff to react to a scenario. It requires staff to demonstrate skills without considerable time demands. They do not recreate the demands of a real incident.
9.09	Live exercises provide the most realistic test outside a real incident. Real time testing provides the closest opportunity where time is limited, and the demands of the test are significantly greater than for a table top exercise. Organisations should plan for a mixture of tabletop and live exercises with one live exercise every year
9.10	The emergency services are often interested in assisting testing. The training opportunity for services such as the Fire Service are often welcome. The emergency services appreciate involvement with heritage and museum venues and will provide ideas and assist in live exercises..

9.11 To get maximum benefit from training and testing organisations should carryout formal debriefing and reviews with staff immediately after the exercise. The debrief allows staff to identify opportunities for improvement in the plan based on their experiences and knowledge.

HEMAS: Audit Check Element 10

Operational Response

Issues:

Emergency plans work best when everyone involved understands the plan, their role within it and the equipment they need to use. To reduce the potential for inappropriate actions, inadvertently duplication or equipment being unavailable the plan should specifically identify the actions and equipment required. While some variation to a Plan is to be expected the 'single song sheet' approach is the most effective means of managing a response.

What the Auditor is looking for:

10.01	Organisations should identify their criteria for declaring different types of emergencies up to major incidents. Staff need this to be clearly set out as there is often an initial reluctance to be the first to declare an emergency.
10.02	The person declaring a major incident should not be a named individual as they may not be present at the time. Staff need to be aware of the criteria for declaring a major incident and understand that it is the criteria that are important when declaring a major incident not the presence of any particular individual. When the criteria are met anyone should be able to declare a major incident.
10.03	The Emergency Services have well practiced and successful protocols for managing major incidents. It is important that organisations are familiar with these protocols and understand how to communicate effectively during after the incident. Emergency responders will be happy to discuss their protocols with organisations.
10.04	The emergency services will expect to have a single member of staff to talk to when they arrive on site to ensure effective communication. The organisation should ensure that named individuals are available to meet with emergency responders as soon as possible on arrival.
10.05	Every organisation has equipment that may be useful in an emergency response. The location of and how to access to the equipment should be known to responding staff.
10.06	Where equipment can be used for an emergency response staff using it should have regular training in how and where they can use it.
10.07	Equipment used for emergency response should be available for use when needed. An inspection and maintenance programme should be established, documented, and followed.
10.08	Staff responding to an incident should be aware of who to contact and how to contact them. Having contact information for critical stakeholders readily available ensures effective and timely communication. All staff should know that all communications outside the organisation must be controlled and is the responsibility of named senior staff only.

HEMAS: Audit Check Element 11

Strategic Response

Issues:

It is important that organisations recognise that an operational response must be supported by a strategic response. Incidents do not finish when the emergency services have left the site and it is certain that following a major incident the work to restore Collections and buildings will take considerably longer to complete. Considering the long-term nature of the response a Strategic or Business Recovery Management teams should be part of the response.

What the Auditor is looking for:

11.01	The longer-term implications of a major incident should be considered by the organisation as it deals with Collections, systems, and buildings. Object treatment, short- and long-term storage, security, potential effects on future exhibitions and programmes and implications for loans need to be addressed.
11.02	A major incident management team should have been identified who will support the incident responders and continue to manage the effects of the incident when the responding team has completed their work and stood down. As all incidents have a longer life than the immediate response it is important that a team is in place to address the strategic and business recovery issues presented by the longer-term implications of an incident. Ideally this team will include some members of the response team once their immediate tasks are complete to provide continuity and knowledge of how the incident progressed.
11.03	The strategic management team should have a dedicated means of communicating during and after an incident. This allows for decisions to be made quickly across the short and longer-term aspects of the incident. This team should not be communicating across open systems as their involvement and decisions are covering a much greater remit than responders. The organisation may consider social media as an appropriate comms mechanism.
11.04	Members of the incident management team should be aware of their role. They are not there to manage the incident response and should understand their support and strategic role. Any involvement with responders working within the remit of the agreed emergency plan is likely to create confusion and delay actions.
11.05	The incident management team should be the responsible for all communication with stakeholders and should have up to date contact details for them. The team should have nominated a single person, and deputy, to do this. They should also ensure that stakeholders are aware that this person will be the only point for communications. This prevents duplication which can distort messages and prevents other team members being distracted by stakeholders.
11.06	All incidents are newsworthy and will attract media attention. The organisation should have a plan to deal with media enquiries. An initial holding statement should be agreed in advance to provide time for a further statement when circumstances are better understood. All staff should understand that the nominated person will be the only spokesperson, and all enquiries should be directed towards them.
11.07	For many organisations their insurers will play an important role in the incident and recovery. Contact details for insurers should be readily available to this team. Where possible the

organisation should be able to contact a named insurance representative who is aware of their business activities.

11.08 It is likely that there will be a need for unplanned expenditure in the immediate recovery period. As this is will be an immediate demand it is important that a protocol for expenditure is in place before any incident. The protocol should be known to all the Management Team so that responses are not delayed.

11.09 Staff responding to an incident will often on site at unsocial hours and organisations should recognise that refreshments are important and plan to provide them and a safe place to take refreshment.

11.10 Incident responders will be focussed on their work and are often unaware of the passage of time. They will also have an emotional connection to Collections and buildings and may be reluctant to leave when they consider their work is not complete. They are less effective when tired and the Management Team should consider how they manage rest breaks for the Incident Response Team during the incident. The Fire Service are experienced in staff rotation during an incident and may be able to offer guidance.

11.11 Where staff have been involved in a response it is entirely predictable that they will be tired. The Incident Management team should consider how responders can get home safely. The safety of the responders is the responsibility of the organisation and does not end when they leave under such circumstances.

11.12 Incident responders should not be responsible for external communications at any time. The organisation should have a plan for communicating beyond stakeholders and will need to keep visitors and guests informed of any changes including access, closures and re-openings, alternative venues, bookings, etc.

HEMAS: Audit Scheme Element 12

Major Incident Recovery

Issues:

It is important that organisations have a realistic expectation that they will recovery effectively and efficiently following a major incident. The health of collections and the organisation is at risk unless the recovery process allows a return to business and maintains collections in good condition or held for planned conservation. It is important that every opportunity to learn lessons from an incident are learnt as they will create opportunities for improvement.

Staff plan the leading role in responding to an incident and ensuring their well-being is important.

Recovery can be broken into a number of areas, people, equipment, materials environment, and the auditor should see evidence of activity in each area to ensure that the organisation can maximise the learning opportunities and prepare for any future incidents.

Incidents do not follow a schedule and can happen at any time including soon after a major incident.

What the Auditor is looking for:

12.01	The organisation should have a plan to debrief people following an incident when their memory and thoughts are fresh. Debriefing should be in small groups to encourage discussion and keep the discussion focussed on the incident. The need for debriefing should be established the Major Incident Plan. Notes of the debriefing should be available for review.
12.02	Individuals involved in a major incident will have experienced something outside their normal experience. It is important to recognise the impact of major incidents, and the organisation should have a plan to bring small groups together to discuss their concerns. The organisation should identify a route to provide any additional support needed by staff.
12.03	The small groups do not run themselves and the organisation should identify a facilitator who is trusted by staff to lead the group and encourage open and honest discussion.
12.04	It is important that the learning opportunities from debriefing and discussion groups are not lost, and management teams should collate them and produce recommendations and an activity timeline. Staff are more likely to continue to provide feedback where they see it is valued. The auditor should see documentary evidence of the recommendations.
12.05	The incident management team should be the responsible for all communication with stakeholders and should have up to date contact details for them. The team should have nominated a single person, and deputy, to do this. They should also ensure that stakeholders are aware that this person will be the only point for communications. This prevents duplication which can distort messages and prevents other team members being distracted by stakeholders.

12.06 The emergency services who responded will also have prepared a report on the incident and it is important the organisations discuss the incident, how the response was managed and any learning opportunities with those who responded.

12.07 The organisation should establish what equipment is critical in meeting the needs of its collections and delivering activities. Where this equipment has been affected by the incident the organisation should know how to return it to service as quickly as possible or arrange for alternatives.

12.08 The organisation should know how to return equipment to service by having plans to clean, maintain and inspect prior to a return to service.

12.09 Organisations should review the effectiveness of equipment involved in an incident to confirm that it is meeting its aims. The review will influence future specification for replacement equipment.

12.10 Materials will be consumed during the response and in the time immediately follow an incident. The organisation should be aware that the materials should be replaced as soon as possible to be available if required.

12.11 Following an incident the organisation should include a review of the effectiveness and quantity of the response materials that it holds. This review should be included in the major incident review and should be documented along with any recommendations on emergency response materials.

11.12 It is likely that any major incident response will involve material not normally used on the site, e.g. firefighting chemicals, smoke residue or water ingress from flooding. The organisation should be aware of the potential for such substances and plan to deal manage them and any potential environmental runoff.

12.13 As the potential for unplanned material is recognised the organisation should have considered the risk and have risk assessments in place to control the risk to staff, volunteers, and collections.

HEMAS: Audit Scheme Element Appendix A (Museum Accreditation)

Security

Issues:

Security is a component of Museum Accreditation, and this element addresses the management of museum security. The Section follows the requirement of Section 3.1 'Secure occupancy of all premises containing collections' and 3.2 'A risk assessment of security arrangements' of the Museum Accreditation Guidance. The substance of this element is contained in the Arts Council England 'Security in museums and galleries: the Security Audit'.

As this component is contained within an existing ACE document it is a stand-alone Appendix with no further explanation for the auditor.

HEMAS: Audit Scheme Element Appendix B

Cyber Security

Issues:

Cyber security is highlighted as a major threat to all organisations and museums are not immune to the threat. This Section addresses practical security arrangements for museums based on the guidance of the National Cyber Security Centre specifically for small business.

What the Auditor is looking for:

Data Security

B.01	Has the organisation reviewed their activities to establish what activities involve data which is critical to their operation. Whilst Collections information is critical there are other business areas where the loss of data or access to date could be critical to the life of the organisation.
B.02	There should be evidence that the business-critical data is regularly backed up. This should be a part of a regular managed routine whether to the Cloud or other device. The frequency of backup should be established and frequent enough to prevent significant loss in the event of an attack.
B.03	Backed up data should not be retained on the same computers or system to prevent loss should a system be attacked.
B.04	To maintain control of backed up critical data access to it should be permitted for named personnel only. Staff should not have access to critical data without permission.
B.05	The organisation should have reviewed the frequency of backup required for data and created a routine which staff follow. Procedures for backup should be seen and evidence that they are followed identified.

Protecting the Organisation from Malware

B.06	Most software comes with antivirus protection built in by the designer. It should be switched on.
B.07	Where business critical data is held on a system antivirus software should be installed.
B.08	Staff should be aware that they cannot download apps or software. Permission should be given to authorised personnel only to prevent viruses being downloaded.
B.09	System Administrators should be appointed to give permission to download as they have greater understanding of the security risk involved.
B.10	Staff access to data and systems should relate to their role. Staff should not have access to areas outside their role to maintain the security of the system.
B.11	Staff using smartphones and tablets should be aware that they should not download Apps unless they are sure that the source is trusted by the organisation.
B.12	All the Firewalls available for the system should be switched on.

Keeping all IT Equipment Up to Date (Patching)

B.13 Vendors, suppliers, and developers will develop patches to improve security throughout the life of their product. The organisation should be awe of this and keep up to date with patches.

B.14 To ensure that patches are not missed the organisation should have automatic updates for patches.

Control of USB Devices

B.15 USBs offer a significant opportunity to download viruses to a system. Where possible, access to connect a USB should be prevented. This might include placing equipment where access is controlled or covering ports.

B.16 Where USBs are used by the organisation, they should be secure with password protection and approved by administrators.

Keeping Smartphones and Tablets safe

B.17 Password protection should be switched on a for all smartphones and tablets to protect systems.

B.18 Where biometric protection is available, e.g. fingerprint recognition, it should be enabled on all devices.

B.19 The organisation should be able to track, lock and wipe any device that cannot be accounted for.

B.20 Devices should be set to allow for regular security updates.

B.21 Evidence of regular App updates should be seen

B.22 All device users should be aware that unknown Wi-Fi hotspots may not be safe. They should make use of their provider 3G and 4G networks.

Using Passwords to Protect Data

B.23 Passwords and biometrics where available should be enabled on all devices

B.24 2-Step verification is an added security measure and should be enabled for all critical accounts

B.25 Staff should be aw are that choice of passwords can become predictable and should know how to work around such issues.

B.26 Even where staff ae working on the same system they should be aware that passwords should never be shared.

B.27 Where a number of separate passwords are required, it may be difficult to remember them and it is possible that some may be shared across a number of systems or accounts. The organisation should be aware of this and provide guidance on how to manage overload including password managers on a separate system.

B.28 New equipment may be protected by a manufacturer's default password. This should be changed as soon as possible and before it enters service.

Avoiding Phishing Attacks

B.29 Where accounts can be accessed by those not working directly with them, they should be configured to provide protection preventing or controlling phishing expeditions.

B.30 As Administration accounts provide significant controls over the system browsing from such accounts should be always prohibited.

B.31 All organisations are liable to attack and should ensure that staff are aware of that potential. Opportunities should be taken to discuss with staff how such attacks may be launched with emphasis on unusual, out of character and suspicious requests.

B.32 Where staff do receive a request that consider to be suspicious, they should know how to deal with it and how to get assistance.

Reporting Attacks

B.33 Staff should be aware that they should raise their concerns as soon as they suspect that they are a victim of a phishing attack. Attacks will happen and despite vigilance some will succeed, and it is vital that staff understand that an alarm must be raised as soon as possible to limit damage

B.34 To provide information on phishing all attacks should be reported on the Action Fraud website.

Checking your Digital Footprint

B.35 Digital footprints are the information that can be gleaned for websites and social media about an organisation. This can be used for phishing by an attacker without having to gain access to systems. The organisation should regularly review its public facing information considering what viewers need to know and what detail is unnecessary but may be useful to attackers.

B.36 The organisations should help staff understand how sharing their personal information can affect them and your organisation. This is **not** about expecting people to remove all traces of themselves from the Internet but Instead managing their digital footprint, shaping their profile so that it works safely for them and the organisation.

B.37 Many organisations have partners, share information, and need to be aware that the information can end up elsewhere and available to others

HEMAS: Audit Scheme Element Appendix C

Access: Emergency Response

Issues:

Arrangements for staff, volunteers and visitors should covers evacuation procedures, meeting points, social media response and information sharing for those with a disability. In terms of disability access, what arrangements should address evacuating wheelchair users and less ambulant visitors (prams and buggies also fit into this need).

Staff, volunteers and visitors with sensory needs or disabilities, measures in place for clear emergency guidance both audible, for blind/visually impaired people, visual for D/deaf people and for those with learning and neurodivergent disabilities.

What the Auditor is looking for:

C.01	Organisations should have a programme in place to regularly establish the access needs of staff, volunteers, and visitors. The auditor should be able to review the access requirements of various groups and the adjustments required.
C.02	The organisation should have reviewed access needs and developed Personal Emergency Evacuation Plans (PEEPs). The plans should be documented and regularly reviewed. The auditor should see a range of plans.
C.03	The PEEPs should address the range of disabilities identified during the review of access needs. The auditor should see a range of PEEPs.
C.04	The PEEPs are personal to the individual or group with similar needs and should be shared so that the user is aware of what the response will be. The auditor should confirm that the pans are shared.
C.05	There is a standard for emergency signage which should be followed, the organisation should discuss the effectiveness of the sign intent with user groups.
C.06	People with mobility issues are likely to be on the site regularly and the routes and assembly points will be required. The organisation should review the routes and points to ensure that they are available and usable for people with disabilities. This is also important for temporary exhibitions or changes which may have implications for evacuation routes.
C.07	PEEPS should be reviewed with disabled users and staff to ensure that the plan is possible and makes sense to those who need to use them including staff or volunteers who may be called to assist disabled users.
C.08	Regular practice of emergency plans is important and to be realistic disabled people should be included in practices. They can provide feedback on the effectiveness of the PEEPs to those planning evacuations.
C.09	Organisations will plan for special and temporary events and their planning should include the planning for the needs of disabled people in any evacuation. Evacuations will involve visitors who may not be familiar with the premises and consideration should be given to providing a refuge or safe point for visitors who may become temporarily separated during the evacuation. It is important that staff are aware of any refuge point so they can direct others there.

C.10 Every major incident should be reviewed to establish all the learning and improvement opportunities. The ability to evacuate people with disabilities should be included in all reviews and should apply every time irrespective of the involvement of people with disabilities.