Cairngorms National Park Authority

INTERNAL AUDIT REPORT - FINAL

Business Continuity Planning

April 2019

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Limited	Limited

BDO

CONTENTS

Appendices:

REPORT STATUS	
Auditors:	Gemma Rickman
Dates work performed:	28 January - 15 February 2019
Draft report issued:	22 February 2019
Final report issued:	**12 April 2019**

DISTRIBUTION LIST	
David Cameron	Director of Corporate Services
Members of the Audit Committee	

Restrictions of use

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)		
Design	🟠	System of internal controls is weakened with system objectives at risk of not being achieved.
Effectiveness	🟠	Non-compliance with key procedures and controls places the system objectives at risk.

SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II)		
High	▲	1
Medium	■	5
Low	●	1
Total number of recommendations: 7		

OVERVIEW

Background

In accordance with the 2018-19 Internal Audit Plan, it was agreed that Internal Audit would review the design and operating effectiveness of the controls in place at Cairngorms National Park Authority ('CNPA/the Authority') surrounding business continuity planning arrangements. The purpose of our review was to provide management and the Audit Committee with assurance that the Authority has appropriate arrangements in place to minimise disruption to business activities in the event of an unforeseen event.

CNPA has developed a Business Continuity Plan (BCP), which provides guidance to management in responding to significant incidents that may disrupt the Authority's operations. The BCP was most recently updated in December 2014. A supporting Disaster Recovery Plan (DRP) has also been developed. The purpose of the BCP and DRP is to ensure that CNPA is fully prepared to respond to and recover from unplanned disruptions to the business, with a goal to restore business operations to normal in the shortest time possible.

The BCP notes a number of teams formed to manage and respond to disruptive incidents. The responsibilities of each team are documented within the BCP, and are detailed below:

Continuing Functionality Team

Responsible for:

- Responding immediately to a potential disaster and calling emergency services (if not already called)
- Assessing the extent of the disaster and its impact on the business, Authority office(s), the Internet, Web site etc.

(continued overleaf)

EXECUTIVE SUMMARY

OVERVIEW

- Deciding which elements of the BCP and DRP should be activated
- Notifying the IT Manager to be prepared to recover operational systems, maintain vital services and return to normal operation
- Notifying the BC/DR Team Lead/Coordinator if the situation warrants activation of BCP and DRP and
- Ensuring employees (and stakeholders, vendors and key customers, as needed) are notified.

The names of members of the Continuing Functionality Team are detailed in the BCP, and include the Chief Executive Officer, Director of Corporate Services, IT Manager and Finance Manager amongst others.

Business Continuity/Disaster Recovery Team

Responsible for:

- Ensuring that the BCP and DRP have been prepared and documented
- Ensuring that the BCP and DRP have been distributed to all employees as well as Continuing Functionality Team and IT Manager
- Launching the BCP and DRP once approval to launch has been obtained from management
- Establishing programs to organise and conduct plan assessments, business impact analyses, risk analyses, awareness and training programs, plan exercises, plans reviews and audits, plan maintenance activities and continuous improvement of the BCP and DRP and the associated programmes
- Coordinating activities with the Continuing Functionality Team, IT Manager, building management, first responders etc.
- Reporting to the Continuing Functionality Team, IT Manager and Authority management, as needed.

The IT Manager has also been recognised as a key role, with responsibilities including establishing facilities and operational resources following an incident; restoring key services, for example the CNPA Website, critical servers and applications, and recovering technology infrastructure to business as usual.

A Business Impact Analysis is included within the BCP, which details CNPA's functions and the head count and parent process of each. CNPA has ranked its functions in terms of priority, with the IT function being the initial priority. The Analysis details the systems, applications or documents that the parent process of each function is dependent on, for example, shared drives, email, and physical and virtual infrastructure. Recovery Time Objectives and Recovery Point Objectives have also been recorded for each function.

EXECUTIVE SUMMARY

OVERVIEW

Scope and Approach

The scope of our review was to assess whether:

- There is a clear business continuity plan in place to allow for recovery from business disruptive events;
- Roles and responsibilities in relation to business continuity are fully defined within the business continuity plan;
- The Authority has clearly defined business critical systems and processes within the business continuity plan;
- The plan is suitable to allow the Authority to recover from a significant disruption in required timescales;
- The business continuity plan is regularly tested, and the results appropriately reported to management;
- The plan is appropriately communicated to staff, and key staff are aware of their roles to instigate the plan;
- The plan is suitably located to allow it to be put into effect in the event of an emergency incident; and
- Staff contact details are kept up to date within the business continuity plan.

Our approach was to conduct interviews to establish the controls and processes in operation, and to review documentary evidence that these controls are designed as described. We then evaluated these controls to identify whether they adequately address the risks.

EXECUTIVE SUMMARY

OVERVIEW

Key Findings

Our review highlighted a number of gaps within the business continuity plan controls, which are summarised below:

- **BCP redaction and distribution**: The BCP obtained during our review is a redacted version. The information redacted includes:
  - Contact details for the Continuing Functionality Team, IT Manager, Media Coordination Team, Vendors information, emergency and key contacts, external key contacts and the emergency call-in number
  - Back up and recovery of vital records section
  - Referenced technology DR plans
  - Succession Plan
  - Equipment & specifications information.

  Management have explained that a non-redacted copy of the BCP is held on the network, although this was password-protected by a member of staff who is no longer in post, and the password is unknown to current staff.

  We note other referenced information within the BCP that has not been included, such as SLAs and details of where a disaster kit should be held.

  In addition, there is a contradiction within the BCP with regards to who should have access to the BCP. The Plan initially states that all staff must be aware of the BCP and DRP, but also explains that the plan and all additional supporting documentation shall be stored in secure locations with limited access only by Continuing Functionality Teams.
- **Action plans:** The BCP and DRP do not include clear detailed action plans for the restoration of all critical functions following a business disruption, within target timescales. In addition, there is an opportunity for the Authority to detail a range of incidents that could cause it to be evoked, along with the specific procedures to be followed for each.
- **Risk assessments and business impact analyses:** High level risks can be seen on the BCP risk register, however, there has been no risk assessment carried out to determine the business continuity risks applying to each function. Also, the current risk register is incomplete, particularly in relation to mitigating actions and risk scores. In addition, we note that the risk assessments and Business Impact Analysis have not been updated on an annual basis as required by the BCP.

(continued overleaf)

EXECUTIVE SUMMARY

OVERVIEW

Key Findings (continued)

- **Plan review and approval:** The BCP provided during our audit states that it, along with the DRP, should be reviewed on an annual basis as a minimum. However, the BCP has not been reviewed since December 2014. This has resulted in details becoming outdated, for example, members of staff are referenced who are no longer in post. The version control within the BCP states that the plan was approved by the Management Team in December 2014. However, we were unable to obtain supporting evidence, such as meeting minutes, to support this. In addition, there is no version control within the DRP which would detail the version and review history of the Plan.
- **Testing:** The BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'table top' exercise. However, these have not yet been subject to formal testing, and there are currently no plans in place to test the BCP and DRP on a regular basis.
- **Training:** There has been no training provided to staff in relation to business continuity.
- **BC/DR team membership:** The BCP details the responsibilities of the BC/DR team, however, no details are provided on the members of this team.

Conclusion

At this stage, we can provide limited assurance over the design and operational effectiveness of the controls in place in relation to business continuity planning. We recommend management implement the noted control improvements to develop the current arrangements, and ensure they operate consistently across the Authority. In particular, it is important that the Authority ensures that relevant staff members have access to a non-redacted version of the Business Continuity Plan.

RISKS REVIEWED GIVING RISE TO NO FINDINGS OF A HIGH OR MEDIUM SIGNIFICANCE

☑ Roles and responsibilities in relation to business continuity may not be fully defined within the business continuity plan.

EXECUTIVE SUMMARY

AREAS FOR IMPROVEMENT

Ref.	Sig.	Finding Summary	Recommendation
1	▲	The BCP obtained during our review is a redacted version. The information redacted includes: - Contact details for the Continuing Functionality Team, IT Manager, Media Coordination Team, Vendors information, emergency and key contacts, external key contacts and the emergency call-in number - Back up and recovery of vital records section - Referenced technology DR plans - Succession Plan - Equipment & specifications information. Management have explained that a non-redacted copy of the BCP is held on the network, although this was password-protected by a member of staff who is no longer in post, and the password is unknown to current staff. We note other referenced information within the BCP that has not been included, such as SLAs and details of where a disaster kit should be held. In addition, there is a contradiction within the BCP with regards to who should have access to the BCP. The Plan initially states that all staff must be aware of the BCP and DRP, but also explains that the plan and all additional supporting documentation shall be stored in secure locations with limited access only by Continuing Functionality Teams.	We recommend that CNPA ensures a non-redacted BCP can be fully accessible on the network and held remotely by key staff members, with all omitted information included. Consideration should be given to who can access the full BCP, and whether staff members who are not members of the Continuing Functionality Team and BC/DR Team only have access to information that is not considered confidential. For example, a summary card of the key high level initial steps to be taken during a major incident could be provided to staff, with the full BCP being provided to only the Continuing Functionality and BC/DR Teams.

EXECUTIVE SUMMARY

AREAS FOR IMPROVEMENT			
Ref.	**Sig.**	**Finding Summary**	**Recommendation**
2	🟧	The BCP and DRP do not include clear detailed action plans for the restoration of all critical functions following a business disruption, within target timescales. In addition, there is an opportunity for the Authority to detail a range of incidents that could cause it to be evoked, along with the specific procedures to be followed for each.	We recommend that clear action plans are developed for each business critical system or function. The action plans should document the process to be followed in the event of disruption, actions to be taken and procedures to be followed to restore the function, and should be designed to achieve intended recovery times. In addition, we recommend that the Authority documents a range of incidents that could cause the BCP to be evoked, along with the procedures to be followed for each in a ‘check list’ format. Example incidents could include fire evacuation, a serious medical emergency, severe weather, terrorist threat, power failure and loss of gas supply.
3	🟧	High level risks can be seen on the BCP risk register, however, there has been no risk assessment carried out to determine the business continuity risks applying to each function. Also, the current risk register is incomplete, particularly in relation to mitigating actions and risk scores. In addition, we note that the risk assessments and Business Impact Analysis have not been updated on an annual basis as required by the BCP.	We recommend that risk assessments are carried out to assess the business continuity risks applying to each function, and should be fully documented within the BCP risk register. We also recommend that the risks assessments and the business impact analysis are assessed and reviewed on a regular basis, to ensure these remain relevant and accurate.

EXECUTIVE SUMMARY

AREAS FOR IMPROVEMENT

Ref.	Sig.	Finding Summary	Recommendation
4	🟧	The BCP provided during our audit states that it, along with the DRP, should be reviewed on an annual basis as a minimum. However, the BCP has not been reviewed since December 2014. This has resulted in details becoming outdated, for example, members of staff are referenced who are no longer in post. The version control within the BCP states that the plan was approved by the Management Team in December 2014. However, we were unable to obtain supporting evidence, such as meeting minutes, to support this. In addition, there is no version control within the DRP which would detail the version and review history of the Plan.	We recommend that the BCP and DRP are reviewed and approved on a regular basis. It is best practice for a BCP and DRP to be reviewed on an annual basis, however the Authority should consider the most appropriate review period for the organisation, and this frequency should be documented within the BCP. In addition, we recommend that version control is added to the DRP.
5	🟧	The BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'table top' exercise. However, these have not yet been subject to formal testing, and there are currently no plans in place to test the BCP and DRP on a regular basis.	We recommend that CNPA develops a testing plan/schedule for BCP which should be reviewed regularly to ensure a strategic approach to testing is developed and implemented. This plan should ensure that varying categories of events are scheduled to be tested on a regular basis based upon likelihood and overall risk. A formal testing schedule should also be developed for the DRP. We note that the BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'table top' exercise. However, from discussions with management, it is understood that this is not achievable due to the size of the organisation. Therefore, Management should decide on the most suitable frequency of testing, and this should be detailed within the BCP. In addition, we recommend that the outcomes, lessons learned and required actions are formally documented, and thereafter reflected within the plan for each test.

EXECUTIVE SUMMARY

AREAS FOR IMPROVEMENT

Ref.	Sig.	Finding Summary	Recommendation
6	🟧	There has been no training provided to staff in relation to business continuity.	We recommend that the Authority implements business continuity training for all staff. Regular refresher training should be provided going forward, and the Authority should ensure it records all training for each staff member, and obtains sufficient evidence of attendance/completion.

All our findings and recommendations are set out in the following pages and include those of low significance which have not been summarised above.

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: The plan may not be suitably located to allow it to be put into effect in the event of an emergency incident.

RISK: The plan may not be suitable to allow the Authority to recover from a significant disruption in required timescales.

RISK: The plan may not be appropriately communicated to staff, and key staff may not be aware of their roles to instigate the plan.

RISK: Staff contact details may not be kept up to date within the business continuity plan.

Ref.	Finding	Sig.	Recommendation
1	It is expected that the BCP is communicated to staff in order to ensure that they are aware of their responsibilities, and the processes to follow, in the event of a business disruptive event. The BCP obtained during our review is a redacted version. The information redacted includes: - Contact details for the Continuing Functionality Team, IT Manager, Media Coordination Team, Vendors information, emergency and key contacts, external key contacts and the emergency call-in number - Back up and recovery of vital records section - Referenced technology DR plans - Succession Plan - Equipment & specifications information. Management have explained that a non-redacted copy of the BCP is held on the network, although this was password-protected by a member of staff who is no longer in post, and the password is unknown to current staff. We note other referenced information within the BCP that has not been included, such as SLAs and details of where a disaster kit should be held. *(continued overleaf)*	▲	We recommend that CNPA ensures a non-redacted BCP can be fully accessible on the network, and a hard-copy held remotely by key staff members, with all omitted information included. Consideration should be given to who can access the full BCP, and whether staff members who are not members of the Continuing Functionality Team and BC/DR Team only have access to information that is not considered confidential. For example, a summary card of the key high level initial steps to be taken during a major incident could be provided to staff, with the full BCP being provided to only the Continuing Functionality and BC/DR Teams.

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: The plan may not be suitably located to allow it to be put into effect in the event of an emergency incident.

RISK: The plan may not be suitable to allow the Authority to recover from a significant disruption in required timescales.

RISK: The plan may not be appropriately communicated to staff, and key staff may not be aware of their roles to instigate the plan.

RISK: Staff contact details may not be kept up to date within the business continuity plan.

Ref.	Finding	Sig.	Recommendation
1 (cont.)	In addition, there is a contradiction within the BCP with regards to who should have access to the BCP. The Plan initially states that all staff must be aware of the BCP and DRP, but also explains that the plan and all additional supporting documentation shall be stored in secure locations with limited access only by Continuing Functionality Teams. There is a risk that CNPA will be unable to recover from any disasters or incidents affecting its business activities, due to the limited information within the BCP that is available to staff.	▲	

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
A hard copy of the BCP which includes all contact information held in the redacted version of the plan was issued to all key staff for them to hold remotely. We have a copy of this hardcopy version and have evidenced that key staff still have access to this document. Notwithstanding this note to this finding, we accept the recommendation. We also note that the BCP should not have been redacted and non-redacted version password protected. This is contrary to CNPA policy, which requires that documents should be held in file locations which carry appropriate levels of access security relevant to their content. The full version should therefore have been held in a folder with appropriate access control.	***Responsible Officer: Director of Corporate Services*** ***Implementation Date: By end of July 2019***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: The plan may not be suitable to allow the Authority to recover from a significant disruption in required timescales.

RISK: The Authority may not have clearly defined business critical systems and processes within the business continuity plan.

Ref.	Finding	Sig.	Recommendation
2	Effective BCPs require clear action plans for business continuity events in order that business functions can be recovered within the target timescales. The BCP and DRP do not include clear detailed action plans for the restoration of all critical functions following a business disruption, within target timescales. In addition, there is an opportunity for the Authority to detail a range of incidents that could cause it to be evoked, along with the specific procedures to be followed for each. There is a risk that the Authority has not considered all potential incidents, and how it would react to these.	🟧	We recommend that clear action plans are developed for each business critical system or function. The action plans should document the process to be followed in the event of disruption, actions to be taken and procedures to be followed to restore the function, and should be designed to achieve intended recovery times. In addition, we recommend that the Authority documents a range of incidents that could cause the BCP to be evoked, along with the procedures to be followed for each in a ‘check list’ format. Example incidents could include fire evacuation, a serious medical emergency, severe weather, terrorist threat, power failure and loss of gas supply.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Recommendation agreed.	***Responsible Officer: Director of Corporate Services to coordinate team.*** ***Implementation Date: End November 2019***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: The Authority may not have clearly defined business critical systems and processes within the business continuity plan.

Ref.	Finding	Sig.	Recommendation
3	It is important that a risk assessment of all functions is carried out as part of the business continuity planning process to allow full consideration of the business continuity risks applying in each area. It is also important to understand the business critical functions and the impact which the crystallisation of business continuity risks may have on the Authority in terms of welfare, legal, financial and reputational impacts. High level risks can be seen on the BCP risk register, however, there has been no risk assessment carried out to determine the business continuity risks applying to each function. Also, the current risk register is incomplete, particularly in relation to mitigating actions and risk scores. In addition, we note that the risk assessments and Business Impact Analysis have not been updated on an annual basis as required by the BCP. There is the risk that business continuity risks affecting particular functions have not been fully assessed, and risks affecting critical functions are not fully understood. There is also the risk that the impact of downtime and that the timescales required for recovery have not been regularly reviewed for suitability.	🟧	We recommend that risk assessments are carried out to assess the business continuity risks applying to each function, and should be fully documented within the BCP risk register. We also recommend that the risks assessments and the business impact analysis are assessed and reviewed on a regular basis, to ensure these remain relevant and accurate.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Recommendation accepted. We will incorporate a requirement for risk assessments, impact analysis and associated plans to be reviewed at least every 30 months.	***Responsible Officer: Director of Corporate Services to coordinate team*** ***Implementation Date: By end July 2019***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Staff contact details may not be kept up to date within business continuity plan.

RISK: The plan may not be suitable to allow the Authority to recover from a significant disruption in required timescales.

Ref.	Finding	Sig.	Recommendation
4	It is expected that the BCP and DRP are reviewed and approved on a regular basis, to ensure the plans remain suitable to recover the Authority from a disruptive incident. The BCP provided during our audit states that it, along with the DRP, should be reviewed on an annual basis as a minimum. However, the BCP has not been reviewed since December 2014. This has resulted in details becoming outdated, for example, members of staff are referenced who are no longer in post. The version control within the BCP states that the plan was approved by the Management Team in December 2014. However, we were unable to obtain supporting evidence, such as meeting minutes, to support this. In addition, there is no version control within the DRP which would detail the version and review history of the Plan. There is a risk that information within the BCP is outdated and therefore inaccurate.	🟧	We recommend that the BCP and DRP are reviewed and approved on a regular basis. It is best practice for a BCP and DRP to be reviewed on an annual basis, however the Authority should consider the most appropriate review period for the organisation, and this frequency should be documented within the BCP. In addition, we recommend that version control is added to the DRP.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed. We will incorporate a review of the BCP and DRP at least every 30 months and to support that longer than best practice review period we will incorporate a standard HR check of any need to update documents within all staff resignation and appointment processes.	***Responsible Officer: Director of Corporate Services to coordinate team*** ***Implementation Date: By end November 2019 for incorporation of agreed review periods and associated HR policy adaptations***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: The business continuity plan may not be regularly tested, and the results appropriately reported to management.			
Ref.	Finding	Sig.	Recommendation
5	In order to gain assurance that the BCP and DRP are effective in the event of a business disruption, it is important that the plans are tested on a regular basis. The BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'table top' exercise. However, these have not yet been subject to formal testing, and there are currently no plans in place to test the BCP and DRP on a regular basis. There is the risk that the BCP and DRP may not be effective, and that this will only become apparent when a disruption to a business critical process occurs.	🟧	We recommend that CNPA develops a testing plan/schedule for BCP which should be reviewed regularly to ensure a strategic approach to testing is developed and implemented. This plan should ensure that varying categories of events are scheduled to be tested on a regular basis based upon likelihood and overall risk. A formal testing schedule should also be developed for the DRP. We note that the BCP states that testing of the BCP and DRP should be annual, with consideration given to a daily 'table top' exercise. However, from discussions with management, it is understood that this is not achievable due to the size of the organisation. Therefore, Management should decide on the most suitable frequency of testing, and this should be detailed within the BCP. In addition, we recommend that the outcomes, lessons learned and required actions are formally documented, and thereafter reflected within the plan for each test.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.	***Responsible Officer: Director of Corporate Services to coordinate team*** ***Implementation Date: By end November 2019 for incorporation of testing schedule***

DETAILED FINDINGS AND RECOMMENDATIONS

<table>
<tr><th colspan="4">RISK: The plan may not be appropriately communicated to staff, and key staff may not be aware of their roles to instigate the plan.</th></tr>
<tr><th>Ref.</th><th>Finding</th><th>Sig.</th><th>Recommendation</th></tr>
<tr><td>6</td><td>Training is essential in ensuring that staff are aware of the required actions to be taken in responding to a business disruptive event.
There has been no training provided to staff in relation to business continuity.
There is a risk that staff are not aware of current business continuity procedures or their roles in instigating the plan.</td><td>🟧</td><td>We recommend that the Authority implements business continuity training for all staff. Regular refresher training should be provided going forward, and the Authority should ensure it records all training for each staff member, and obtains sufficient evidence of attendance/completion.</td></tr>
<tr><th colspan="3">MANAGEMENT RESPONSE</th><th>RESPONSIBILITY AND IMPLEMENTATION DATE</th></tr>
<tr><td colspan="3">Agreed.</td><td><em>Responsible Officer: Director of Corporate Services to coordinate team</em>
<em>Implementation Date: By end February 2020</em></td></tr>
</table>

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Roles and responsibilities in relation to business continuity may not be fully defined within the business continuity plan.

RISK: The plan may not be appropriately communicated to staff, and key staff may not be aware of their roles to instigate the plan.

Ref.	Finding	Sig.	Recommendation
7	It is important that key teams or roles are identified in managing and responding to a business disruptive incident. The BCP details the responsibilities of the BC/DR team, however, no details are provided on the members of this team. There is a risk that the responsibilities of the BC/DR team may not be rolled out in the event of an incident, due to the membership of the team being unknown.	🟢	We recommend that the Authority documents each member of the BC/DR team within the BCP.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.	*Responsible Officer: Director of Corporate Services to coordinate team* *Implementation Date: By end November 2019*

APPENDIX I - STAFF INTERVIEWED

NAME	JOB TITLE
David Cameron	Director of Corporate Services
Sandy Allan	IT Service Manager

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.

APPENDIX II - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of internal controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
Substantial 🟢	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 🟦	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited ⯃	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 🔺	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation’s overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation’s overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation Significance	
High 🔺	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 🟧	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 🟢	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX III – TERMS OF REFERENCE

BACKGROUND

As part of the 2018-19 Internal Audit Plan, it was agreed that we would carry out a review of the business continuity planning arrangements in place and compare them with good practice. The review will cover operational and IT environments and include examining procedures for emergency response handling; business impact analysis; disaster recovery; contingency planning; and business resumption.

PURPOSE OF REVIEW

The purpose of the review is to provide assurance that the Authority has appropriate arrangements in place to minimise disruption to business activities in the event of an unforeseen event. Therefore, the review will assess the design and the effectiveness of the Authority's business continuity arrangements.

KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- roles and responsibilities in relation to business continuity may not be defined within the business continuity plan;
- the Authority may not have clearly defined business critical systems and processes within the business continuity plan;
- the plan may not be suitable to allow the Authority to recover from a significant disruption in required timescales;
- the business continuity plan may not be regularly tested, and the results appropriately reported to management;
- the plan may not be appropriately communicated to staff, and key staff may not be aware of their roles to instigate the plan;
- the plan may not be suitably located to allow it to be put into effect in the event of an emergency incident; and
- staff contact details may not be kept up to date within business continuity plan.

www.bdo.co.uk