CAIRNGORMS NATIONAL PARK AUTHORITY
Audit & Risk Committee Paper 2 Annex 1 06/09/19

Cairngorms National Park Authority

INTERNAL AUDIT REPORT

Risk Management

August 2019

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Substantial	Substantial

BDO

CONTENTS

Appendices:

REPORT STATUS	
Auditors:	Sean Morrison
Dates work performed:	02 July 2019 - 07 August 2019
Draft report issued:	16 August 2019
Final report issued:	**19 August 2019**

DISTRIBUTION LIST	
David Cameron	Director of Corporate Services
Audit Committee	Members

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	●	There is a sound system of internal control designed to achieve system objectives.
Effectiveness	●	The controls that are in place are being consistently applied.

SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II)		
High	▲	
Medium	■	
Low	●	3
Total number of recommendations: 3		

OVERVIEW

Background

It was agreed with management and the Audit & Risk Committee within the 2019-20 Internal Audit Plan that Internal Audit would review the key controls in place within Cairngorms National Park Authority (CNPA) in relation to risk management. The purpose of our review is to provide independent assurance to management and the Audit & Risk Committee that the controls in place in relation to risk management are well designed and operating effectively.

BDO previously conducted a risk management audit at CNPA, in August 2016. The audit provided moderate assurance over the design and operational effectiveness of the risk management controls in place, with four recommendations made, two of which have been fully implemented as reported within the 2018-19 follow up audit.

Since the previous audit CNPA has created a risk management strategy. The strategy was developed in the first half of 2018, and approved by the Board in June 2018. The strategy outlines the key responsibilities for risk management within CNPA and in particular the tone from the top in relation to risk management. The strategy also notes the risk appetite adopted, and risk management reporting requirements. The strategy is the key internal guidance document for risk management, and is made available to staff via the organisation's public network folders and was communicated internally through the Management Team and Operational Management Group meetings.

The Audit & Risk Committee terms of reference outlines that it is the Committee's responsibility to oversee the risk management and corporate governance arrangements within the organisation. The terms of reference for the Management Team (MT) outlines the group's risk management responsibilities, including the responsibility to develop policy on risk, oversee the strategic risk register, agree mitigation plans and lead on implementation of risk mitigation actions.

EXECUTIVE SUMMARY

OVERVIEW

The Operational Management Group's (OMG) remit details that they are responsible for managing risks to delivery, and reporting new and significant risks to the MT for action. Risk management responsibilities for individual staff are reviewed and considered as part of the annual job evaluation process.

The Board considered and approved the current format of the risk register in June 2018. The risk register format was developed by management to support the delivery of the 2018-2022 Corporate Plan. The strategic risk register format is illustrated at Appendix IV of this report. The risks identified within the risk register are aligned to the strategic priorities outlined within the Corporate Plan and are categorised into key themes, which are as follows:

1) Governance

2) Resources/Resourcing

3) Staffing

4) Technical

5) Reputation

6) Partnerships

Risks are assessed by CNPA to consider the likelihood of the risk occurring and the impact on the organisation if the risk were to crystallise. The risk register records the risk scoring, with both likelihood and impact categorised on a scale of 1 to 5 during the risk assessment process on a gross and net basis. The target risk score is to reduce the likelihood multiplied by impact score of each risk (net score) to below 10 by applying relevant risk treatments. The trend score for the risk is also recorded on the risk register, which notes the three most recent quarters scoring. The risk register also details the risk description, reference to the Corporate Plan, risk owners, mitigating controls and comments on the risk environment. The risks recorded in the risk register are separated between cross-over risks and specific service area risks.

Risks are identified through a range of channels within the organisation. Most typically they are identified via discussion for inclusion on the risk register at the OMG and MT meetings, and escalated to the Audit & Risk Committee and the Board on a quarterly basis for approval to include within the register. Both the Audit & Risk Committee and the Board are also presented with the opportunity to highlight emerging risks at their respective meetings.

EXECUTIVE SUMMARY

OVERVIEW

CNPA's risk management processes are supported through reporting arrangements at a strategic and management level. The strategic risk register is reviewed by the Board twice a year, alongside Corporate Plan performance reports prepared by the Director of Corporate Services. This provides the Board the opportunity to assess the content of the risk register, and as previously noted, to identify gaps within the register.

The Audit & Risk Committee review the risk register twice a year, in the periods where a full review is not conducted by the Board. The Committee consider the content of the register and identify additional risks for the risk register. The Committee are also provided with risk management cover reports prepared by the Director of Corporate Services, providing an executive summary of the organisation's risk environment. Risk interrogation reports are also presented to the Audit and Risk Committee during the risk register reviews, which provide a deep dive into a specific risk within the register.

Senior management review the risk register at the monthly OMG meetings to discuss the content of the risk register, and the actions being taken to mitigate the risks.

Risk management training is available to staff upon request, and is included within the induction process for Board members. The Director of Corporate Services provides one to one guidance on the risk management processes to any new members of the organisation who are in a position to be responsible for risks.

Scope and Approach

The scope of our review was to assess whether:

- A suitable risk strategy and policy is in place.
- The structure, roles and responsibilities for risk management are clear, including the respective roles and responsibilities of the Board, Audit & Risk Committee, and Management.
- CNPA has robust systems for identifying and evaluating all significant strategic and operational risks.
- Mitigating controls, net risk and target risk are sufficiently identified and agreed.
- Reporting arrangements in place for risk management are appropriate.
- Appropriate risk management training is being provided.

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

Good Practice

We noted a number of areas of good practice being demonstrated at the Authority in relation to risk management. These included:

- A risk strategy has been developed for the organisation, which was reviewed and approved by the Board in June 2018.
- Roles and responsibilities for risk management of the Audit & Risk Committee and management have been clearly defined.
- A strategic risk register is in place and contains mitigating controls and actions, which are identified and agreed by management.
- Effective reporting arrangements are in place for risk management, including review of the strategic risk register and risk reports twice per year by both the Audit & Risk Committee and the Board.
- Risk management training is available to staff when requested, and is provided to Board members during their induction process.
- Risk interrogation reports are presented to the Audit & Risk Committee.

Key Findings

Not withstanding the areas of good practice noted above, we have noted areas where further improvements can be made to the risk management processes, summarised below:

- **Risk Management Procedure -** We recognise that CNPA have developed a risk management strategy which has information on risk appetite, direction and roles and responsibilities. However, the document lacks some of the following information that we would expect to see within a risk management guidance document:

1. Risk management process, including identification, assessment, analysis, response, mitigation and escalation.
2. Risk register format.
3. Risk prompts and tools.
4. Risk impact and likelihood descriptions.

EXECUTIVE SUMMARY

OVERVIEW

- **Risk Identification -** We recognise that the Authority management and Board members have created a detailed risk register, and that opportunities are there for unrecorded risks or gaps to be identified. However, there is no periodic risk identification exercise undertaken utilising best practice prompts, such as PESTLE and SWOT.
- **Mitigating Controls -** The CNPA risk registers do not clearly outline whether mitigating controls are preventative or remedial.

Conclusion

We are able to provide substantial assurance over the design and operational effectiveness of the controls in place relating to risk management at CNPA.

EXECUTIVE SUMMARY

RISKS REVIEWED GIVING RISE TO NO FINDINGS OF A HIGH OR MEDIUM SIGNIFICANCE	
☑	Cairngorms NPA may not have set out clearly its strategic direction and objectives in relation to risk management (including policy, roles and responsibilities, objectives and communication).
☑	Cairngorms NPA may not have adopted a systematic process in identifying, evaluating and measuring its key strategic and operational risks.
☑	Cairngorms NPA may not have adequate reporting to its committees and the Board in relation to risk management activities.
☑	Cairngorms NPA may not be providing appropriate risk management training.

DETAILED FINDINGS AND RECOMMENDATIONS

<table>
<tr><td colspan="4"><b>RISK: Cairngorms NPA may not have set out clearly its strategic direction and objectives in relation to risk management (including policy, roles and responsibilities, objectives and communication).</b></td></tr>
<tr><td><b>Ref.</b></td><td><b>Finding</b></td><td><b>Sig.</b></td><td><b>Recommendation</b></td></tr>
<tr><td>1</td><td><b>Risk Management Procedure</b>
Effective risk management policies and procedures outline the key objectives, responsibilities, strategies and processes for managing risk across the organisation.
We recognise that CNPA have developed a risk management strategy which has information on risk appetite, direction and roles and responsibilities. However, the document lacks some of the following information that we would expect to see within a risk management guidance document:
• Risk management process, including identification, assessment, analysis, response, mitigation and escalation.
• Risk register format.
• Risk prompts and tools.
• Risk impact and likelihood descriptions.
There is a risk that if key personnel with risk management responsibilities within the organisation where to leave, such as the Director of Corporate Services, that staff would be unaware of the risk management processes to be followed within the organisation, due to the risk management strategy gaps identified above.</td><td>🟢</td><td>We recommend that a risk management procedure is developed or that the risk management strategy is updated to include the following best practice areas:
• Risk management process, including identification, assessment, analysis, response, mitigation and escalation.
• Risk register format.
• Risk prompts and tools.
• Risk impact and likelihood descriptions.</td></tr>
<tr><td colspan="3"><b>MANAGEMENT RESPONSE</b></td><td><b>RESPONSIBILITY AND IMPLEMENTATION DATE</b></td></tr>
<tr><td colspan="3">Agreed</td><td><b><i>Responsible Officer:</i></b>
<b><i>Director of Corporate Services</i></b>
<b><i>Implementation Date:</i></b>
<i>31 May 2020</i></td></tr>
</table>

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Cairngorms NPA may not have adopted a systematic process in identifying, evaluating and measuring its key strategic and operational risks.

Ref.	Finding	Sig.	Recommendation
2	**Risk Identification** A formal periodic risk identification process ensures that a risk register contains up to date risks and mitigates the possibility of there being gaps within the risk register. We recognise that the Authority management and Board members have created a detailed risk register, and that opportunities are there for unrecorded risks or gaps to be identified. However, there is no periodic risk identification exercise undertaken utilising best practice prompts, such as PESTLE and SWOT. To mitigate the risk of the risk register having any gaps it would be beneficial for a more rigorous periodic risk identification exercise to be conducted.	🟢	We recommend that on a periodic basis, for example every two years to align with the start and mid-point of the Corporate Plan cycle, for management to carry out a full scale risk identification process for the risk register.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed	***Responsible Officer:*** ***Director of Corporate Services*** ***Implementation Date:*** *31 May 2020*

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Cairngorms NPA may not have adopted a systematic process in identifying, evaluating and measuring its key strategic and operational risks.

Ref.	Finding	Sig.	Recommendation
3	**Mitigating Controls** Best practice risk management processes encourages the splitting of mitigating controls between preventative (affecting the likelihood of an event occurring) and remedial (affecting the impact once the event has happened). The CNPA risk registers do not clearly outline whether mitigating controls are preventative or remedial. There is a risk that risk owners have not considered or are not fully aware of the actions to be taken to prevent an event from occurring and those actions to be taken to mitigate the impact of an event once it has crystallised.	●	We recommend that management consider detailing both preventative and remedial controls within the risk register.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed	***Responsible Officer:*** ***Director of Corporate Services*** ***Implementation Date:*** *30 November 2019*

OBSERVATIONS

Risk Training

CNPA management are currently discussing the facilitation of an Audit & Risk Committee workshop to be conducted by BDO. It is expected that this will be an opportunity to provide the members with best practice guidance on risk management, and in particular the Authority are interested in receiving risk appetite advice.

Prior Audit Findings

The 2016 BDO risk management audit has two recommendations outstanding as of the most recent follow up audit conducted for the 2018-19 audit year. These recommendations have been noted below, and require a revised timetable for completion to be agreed:

1. Project risk registers to be completed in a consistent manner for all projects.
2. Staff are required to confirm whether they are aware of the organisation's risk management approach.

APPENDIX I - STAFF INTERVIEWED

NAME	JOB TITLE
David Cameron	Director of Corporate Services

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 preparation of the 2019-20 Internal Audit Strategy and plan, it was agreed that internal audit would review the risk management framework in place within Cairngorms NPA and compare this with good practice, using our risk management maturity model.

PURPOSE OF REVIEW

The purpose of this review is to provide the Audit and Risk Committee with a level of assurance around the current risk management arrangements, and to provide management with advice and recommendations for improving the arrangements further. It will also inform Management and the Audit and Risk Committee of improvements in risk management process maturity.

KEY RISKS

Based upon discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

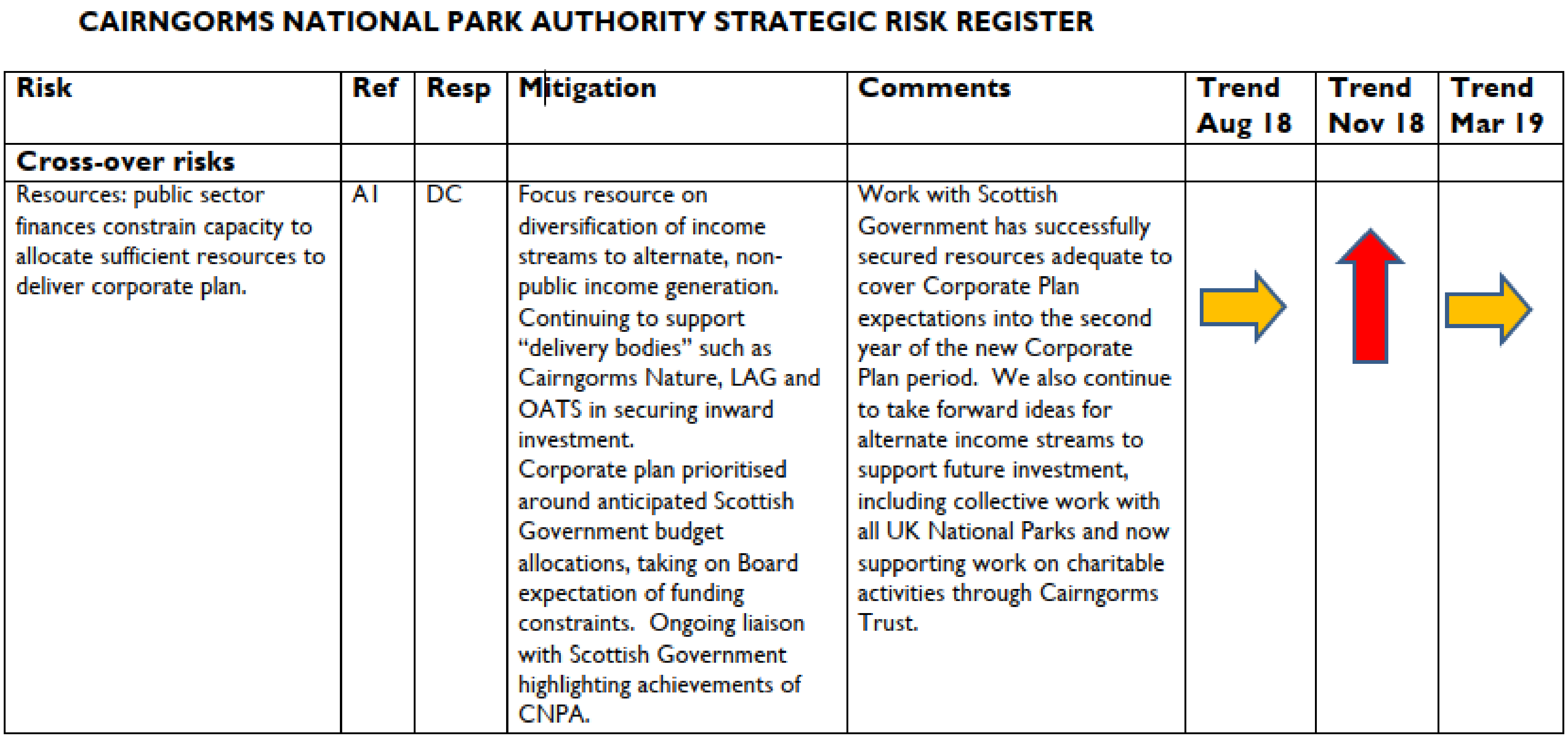
- Cairngorms NPA may not have set out clearly its strategic direction and objectives in relation to risk management (including policy, roles and responsibilities, objectives and communication).
- Cairngorms NPA may not have adopted a systematic process in identifying, evaluating and measuring its key strategic and operational risks.
- Cairngorms NPA may not have adequate reporting to its committees and the Board in relation to risk management activities.
- Cairngorms NPA may not be providing appropriate risk management training.

SCOPE

The following areas will be covered as part of this review:

- To assess whether a suitable risk strategy and policy is in place.
- To assess whether the structure, roles, and responsibilities for risk management are clear, including the respective roles and responsibilities of the Board, Audit Committee and Management.
- To assess whether Cairngorms NPA has robust systems for identifying and evaluating all significant strategic and operational risks.
- To assess whether mitigating controls, net risk and target risk are sufficiently identified and agreed.
- To assess whether the reporting arrangements in place for risk management are appropriate.
- To assess whether appropriate risk management training is being provided.

APPENDIX IV – RISK REGISTER FORMAT



CAIRNGORMS NATIONAL PARK AUTHORITY STRATEGIC RISK REGISTER

Risk	Ref	Resp	Mitigation	Comments	Trend Aug 18	Trend Nov 18	Trend Mar 19
Cross-over risks							
Resources: public sector finances constrain capacity to allocate sufficient resources to deliver corporate plan.	A1	DC	Focus resource on diversification of income streams to alternate, non-public income generation. Continuing to support "delivery bodies" such as Cairngorms Nature, LAG and OATS in securing inward investment. Corporate plan prioritised around anticipated Scottish Government budget allocations, taking on Board expectation of funding constraints. Ongoing liaison with Scottish Government highlighting achievements of CNPA.	Work with Scottish Government has successfully secured resources adequate to cover Corporate Plan expectations into the second year of the new Corporate Plan period. We also continue to take forward ideas for alternate income streams to support future investment, including collective work with all UK National Parks and now supporting work on charitable activities through Cairngorms Trust.	→	↑	→

APPENDIX V – BDO RISK MATURITY ASSESSMENT MODEL

	Risk Governance	Risk Identification and Assessment	Risk Mitigation and Treatment	Risk Reporting and Review	Continuous Improvement
Enabled	Risk management and internal control is fully embedded into operations. All parties play their part and have a share of accountability for managing risk in line with their responsibility for the achievement of objectives.	There are processes for identifying and assessing risks and opportunities on a continuous basis. Risks are assessed to ensure consensus about the appropriate level of control, monitoring and reporting to carry out. Risk information is documented in a risk register.	Responses to the risks have been selected and implemented. There are processes for evaluating risks and responses implemented. The level of residual risk after applying mitigation techniques is accepted by the organisation, or further mitigations have been planned.	High quality, accurate and timely information is available to operational management and directors. The board reviews the risk management strategy, policy and approach on a regular basis, e.g. annually, and reviews key risks, emergent and new risks, and action plans on a regular basis, e.g. quarterly.	The organisational performance management framework and reward structure drives improvements in risk management. Risk management is a management competency. Management assurance is provided on the effectiveness of their risk management on a regular basis.
Managed	Risk management objectives are defined and management are trained in risk management techniques. Risk management is written into the performance expectations of managers. Management and executive level responsibilities for key risks have been allocated.	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk appetite is used in the scoring system for assessing risks. All significant projects are routinely assessed for risk.	There is clarity over the risk level that is accepted within the organisation's risk appetite. Risk responses appropriate to satisfy the risk appetite of the organisation have been selected and implemented.	The board reviews key risks, emergent and new risks, and action plans on a regular basis, e.g. quarterly. It reviews the risk management strategy, policy and approach on a regular basis, e.g. annually. Directors require interim updates from delegated managers on individual risks which they have personal responsibility.	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported. Management assurance is provided on the effectiveness of their risk management on an ad hoc basis. The resources used in risk management become quantifiably cost effective. KPIs are set to improve certain aspects of the risk management activity, e.g. timeliness of implementation of risk responses, number of risks materialising or surpassing impact-likelihood expectations.
Defined	A risk strategy and policies are in place and communicated. The level of risk-taking that the organisation will accept is defined and understood in some parts of the organisation, and it is used to consider the most appropriate responses to the management of identified risks. Management and executive level responsibilities for key risks have been allocated.	There are processes for identifying and assessing risks and opportunities in some parts of the organisation but not consistently applied in all. All risks identified have been assessed with a defined scoring system. Risk information is brought together for some parts of the organisation. Most projects are assessed for risk.	Management in some parts of the organisation are familiar with, and able to distinguish between, the different options available in responding to risks to select the best response in the interest of the organisation.	Management have set up methods to monitor the proper operation of key processes, responses, and action plans. Management report risks to directors where responses have not managed the risks to a level acceptable to the board.	The Board gets minimal assurance on the effectiveness of risk management.
Aware	There is a scattered, silo-based approach to risk management. The vision, commitment and ownership of risk management have been documented. However, the organisation is reliant on a few key people for the knowledge, skills and the practice of risk management activities on a day-to-day basis.	A limited number of managers are trained in risk management techniques. There are processes for identifying and assessing risks and opportunities, but these are not fully comprehensive or implemented. There is no consistent scoring system for assessing risks. Risk information is not fully documented.	Some responses to the risks have been selected and implemented by management according to their own perception of risk appetite in the absence of a board-approved appetite for risk.	There are some monitoring processes and ad hoc reviews by some managers on risk management activities.	Management does not assure the Board on the effectiveness of risk management.
Naïve	No formal approach developed for risk management. No formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	Processes for identifying and evaluating risks and responses are not defined. Risks have not been identified nor collated. There is no consistent scoring system for assessing risks.	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular reviews of risk management.	Management does not assure the Board on the effectiveness of risk management.

www.bdo.co.uk