

Report of Internal Audit: Astari

Subject: Internal Audit Progress Report

INTRODUCTION

This report provides an update of progress towards delivery of the 2023/24 Internal Audit Annual Plan, as well as a summary of the work undertaken to date.

SUMMARY OF PROGRESS

As per the agreed plan, we have finalised the following reports since the last committee meeting:

- Risk Maturity (01.23/24)

Overall, the status of the internal audit programme is as follows:

Assignment <i>Reports considered today are shown in italics</i>	Status	Opinion	Recommendations:		
			High	Medium	Low
<i>Risk Maturity (01.23/24)</i>	<i>FINAL</i>	<i>Advisory</i>	1	2	2
Health & Safety (02.23/24)	Fieldwork				
Value for Money					
Income Generation					
Key Financial Controls					
Estates Management					
Follow Up					
Information & Cyber Security & Data Protection					
TOTAL:			1	2	2

Note: Opinions and recommendations will be included when reports are finalised.

LIAISON WITH MANAGEMENT & EXTERNAL AUDIT

There has been ongoing communication between Internal Audit and Senior Management within the Authority in relation to the completion of the audit plan as well as getting a greater understanding of the Authority and how it operates.

INTERNAL AUDIT PLAN CHANGE CONTROL

The following changes have been made to the Internal Audit Annual Plan since it was agreed:

Change	Date	Agreed By
Facilitating a Risk Maturity Workshop was delivered by Astari in September 2023 in addition to the audit plan.	September 2023	Chief Executive
The Income Generation audit has been postponed from October 2023 to January 2024 as key actions were due to be undertaken in November 2023 and it was agreed that it would be more efficient to capture these within the audit. The change will have no impact on committee reporting timescales.	October 2023	Chief Executive
The audit of Governance: Value for Money was impacted by the Finance Manager leaving the organisation and so this was agreed to be postponed to January 2024 and the Chief Executive will now be the lead officer.	October 2023	Chief Executive

Audit	Start Date	Debrief Date	Draft Report Issued	Planned Committee	Comments
Health & Safety (02.23/24)	25 Oct 23				
Value for Money	8 Jan 24				
Income Generation	10 Jan 24				
Key Financial Controls	26 Feb 24				The timing of these may change slightly depending on whether they are undertaken in a block or as separate reviews.
Estates Management	26 Feb 24				
Follow Up	26 Feb 24				
Information & Cyber Security & Data Protection	25 Mar 24				



ASTARI

Pembrokeshire Coast
National Park Authority

Risk Maturity

Internal Audit Report: PCNPA-2023/24-01

Date: 23 October 2023



1. EXECUTIVE SUMMARY

1.1. Introduction

An audit of Risk Maturity was undertaken as part of the approved internal audit periodic plan for 2023/24 and sought to assess the organisation's risk maturity and to provide advice on how to develop the risk management framework further. This review is advisory and therefore does not result in an assurance opinion; however, it will have an impact on the Head of Internal Audit's annual opinion.

Risk Maturity is defined as: *“the extent to which a robust risk management approach has been adopted and applied as planned by management across the organisation, to identify, assess, decide on responses to, and report on opportunities and threats that affect the achievement of the organisation's objectives.”*¹

The intention of the review was to assess what risk management processes were operating within the organisation, how effective they were and how much value they added to the organisation's operations. Based on our findings we have provided a summary of the key points below, our evaluation of the organisation's Risk Maturity is provided in section 1.3 and more detailed findings can be located in section 2. We have raised recommendations and suggestions to help increase the organisation's risk maturity and therefore make processes more effective and value adding.

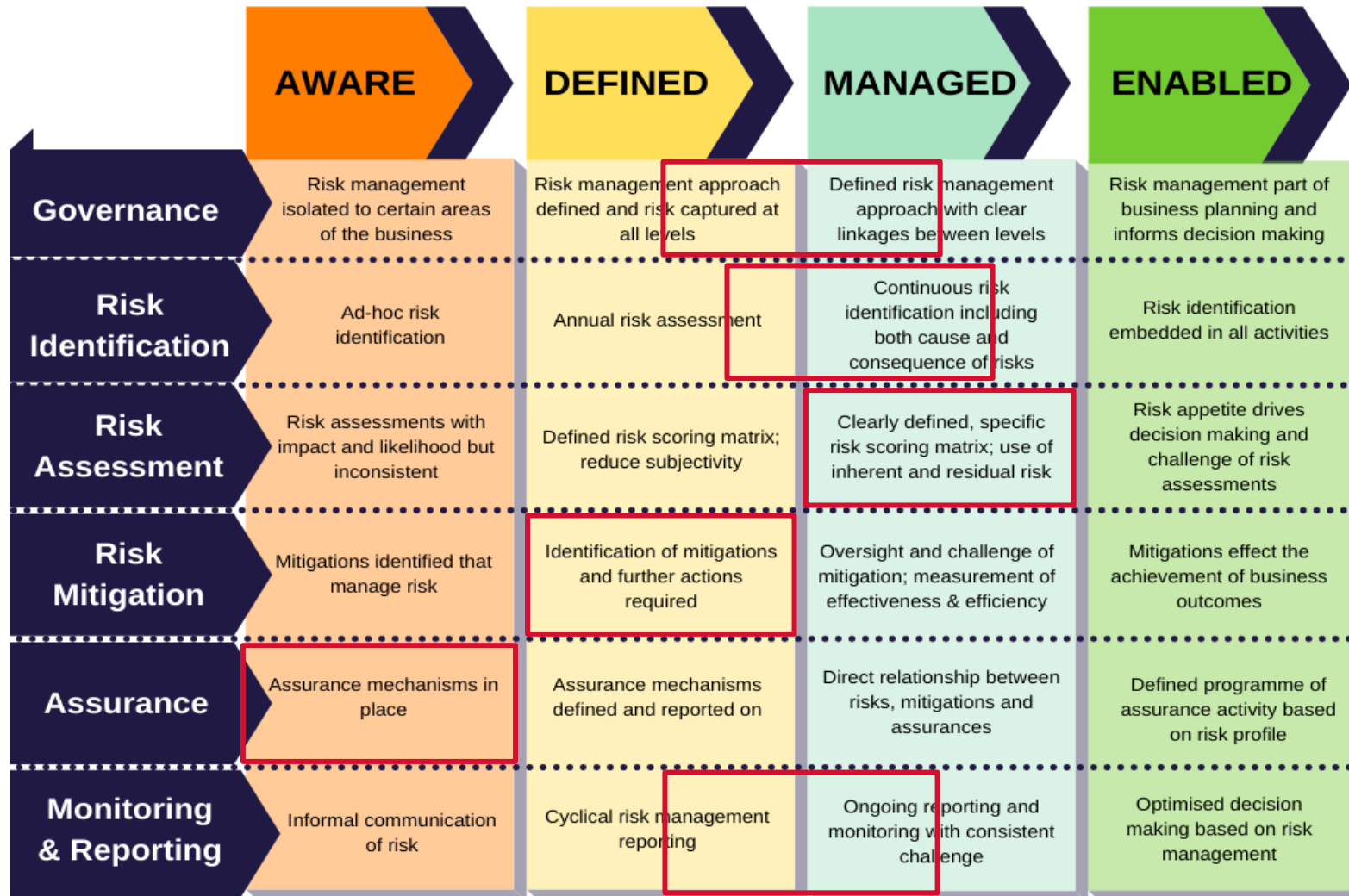
1.2. Key Findings

The Key findings from the review were that:

- The organisation clearly had a positive culture around risk and everyone spoken to clearly had a good understanding of the importance of identifying and appropriately managing risk.
- The organisation's Risk Strategy provided a strong foundation for the organisation's risk management activities; although it lacked guidance around 'how' to undertake risk management effectively, particularly around risk identification, controls and assurance.
- Risk appetite had been defined but also being refined at the time of our review and we facilitated a Risk Appetite workshop as part of this development.
- The Risk Register did not include objectives, resulting the risks being too generic and reducing the effectiveness of the risk register as a useful for tool for the organisation.
- Risk assessment processes had been defined for different categories of risk and to help promote consistent scoring.
- There was an opportunity to improve the documenting of controls to evidence work to manage the organisation's key risks and demonstrate value for money. The format of the Risk Register could also be improved to increase effectiveness and clarity as well as to remove duplication.
- The organisation was not making use of assurance to evidence the work undertaken to manage the Authority's key risks and therefore demonstrate that objectives were going to be achieved.
- Monitoring and reporting processes were operating effectively and there was good engagement with formal risk management processes from the management team up through the Audit and Corporate Services Review Committee to the National Park Authority.

¹ Chartered Institute of Internal Auditors

1.3. Risk Maturity Evaluation



1.4. Work Undertaken

The following work was undertaken as part of this review:

Review of risk management documentation, including:

- ◆ Risk Management Strategy
- ◆ Risk Register
- ◆ Audit & Corporate Services Review Committee papers;
- ◆ National Park Authority papers;
- ◆ Annual Governance Statement;
- ◆ Previous audit reports;
- ◆ Corporate and Resources Plan; and
- ◆ Delivery Plans.

Interviews with or information from key individuals, including:

- ◆ Tegryn Jones, Chief Executive
- ◆ Richard Griffiths, (former) Finance Manager
- ◆ Sara Morris, Director of Placemaking, Decarbonisation and Engagement
- ◆ Jessica Morgan, Head of Decarbonisation
- ◆ Caroline Llewellyn, Democratic Services Manager

1.5. Summary of Recommendations

	High	Medium	Low	Suggestion
Governance	-	-	-	1
Risk Identification	1	-	1	-
Risk Assessment	-	-	-	2
Risk Mitigation	-	1	1	-
Assurance	-	1	-	-
Monitoring & Reporting	-	-	-	-
TOTAL:	1	2	2	3

The Action Plan at Section 3 details the specific recommendations made as well as agreed management actions to implement them.

2. DETAILED FINDINGS

	Details Findings:	Finding Ref.
Governance	<ul style="list-style-type: none"> A Risk Management Strategy (“the Strategy”) was in place that detailed the Authority’s approach to risk management along with key responsibilities and accountabilities. The Strategy was clearly written and provided a sound basis for the organisation. The Strategy included that risk management is not about not taking risks, specifically stating that “<i>risk management is not about taking no risks at all. It is about being able to take calculated and controlled risks to improve the services that the Authority provides.</i>” The Strategy detailed the organisation’s strategic objectives and how these were to be delivered, clearly inferring the link between objectives and risks. We noted clear intentions within the Strategy for embedding risk management, such as the statement: “<i>The management of risk will become an integral part of corporate policy decisions and the initiation of major projects, which will include a statement on risk to help inform the decision-making process.</i>” Although we noted the intention, it was evident that this was an ongoing process and wasn’t fully occurring at the time of our review. The Authority’s Risk Appetite was described in the Strategy and a risk appetite workshop was undertaken in September 2023 with Members to increase understanding and to update the Authority’s Risk Appetite. Through the workshop, which we facilitated, and the detail in the Strategy, we believe there is an opportunity to increase the effectiveness of the use of risk appetite by joining up the Authority’s “decision making” risk appetite with its appetite for managing risk. We noted through our interviews and review of reports that the Authority and Audit and Corporate Services Review Committee (ACSRC) were aware of each group’s responsibilities. 	S1
Risk Identification	<ul style="list-style-type: none"> No guidance was in place within the Risk Strategy or other document on risk identification. Through interviews undertaken and review of the Risk Register and other documentation we ascertained that there was a good understanding of risk throughout key areas and that risks and issues would be communicated, including through internal Officer Groups such as the Health and Safety Group and the Asset Management Group; however, there was not a clear process for incorporating risks into the formal risk management process except at senior manager and leadership level – see Recommendation 2. We did not identify any guidance regarding risk identification linked to processes such as business planning or change management. We were informed that risks were considered at project level but there wasn’t a formalised link between project and operational risk and strategic risk. Through review of the latest Risk Register (June 2023) we noted that objectives were not included on register, indicating that risks may be identified in isolation and not in relation to specific objectives. This invariably ends up making risks more generic and make risk assessment processes less consistent, which in turn makes resource allocation for mitigation activities less efficient. 	R1 R2

	Details Findings:	Finding Ref.
Risk Assessment	<ul style="list-style-type: none"> ◆ Risk assessment matrices were included in the Risk Strategy and include a guide to risk impact by 'category' / type of risk and also to likelihood. ◆ Five 'categories' of risk had been defined, in line with good practice, in the Risk Strategy including: financial, service, reputation, legal and environment. Through the Risk Appetite Workshop it was noted that these could be reviewed to check that they are still the correct categories and others may need to be considered, such as health and safety. ◆ A 4 x 4 matrix of impact v likelihood was defined in the Strategy with red, amber, dark green and light green sections indicated by the numbers to show the level of risk faced by the organisation. This colour distribution was not linked explicitly to the organisation's Risk Appetite. ◆ Good practice was noted in that the organisation used both inherent and residual risk, which enables an understanding of the 'strength' of the controls in place and the potential risk level should all control measures fail. ◆ After the 'residual risk' column, a "Target Risk (Risk Appetite)" column was included where the organisation was planning on indicating the risk appetite related to the specific risk. This was in development at the time of our review and the Risk Appetite workshop discussed some potential opportunities for how this could be set and used. ◆ A "Trend this qtr" column was included on the Risk Register, which usefully showed the direction of change from the previous quarter and therefore enabled consideration of whether risks were greater or lesser than previously. 	<p>S2</p> <p>S3</p>
Risk Mitigation	<ul style="list-style-type: none"> ◆ Our discussions undertaken throughout this review noted that there was a good understanding of actions to reduce risks and that many actions were being taken; however, this was not translated into the detail recorded on the Risk Register. ◆ We did not identify any guidance available in relation to risk mitigation / control – see recommendation 1. ◆ Through review of the latest Risk Register we noted that the organisation had two columns on the Risk Register relating to mitigation: a "Mitigation" column, which was a mixture of controls and comments / descriptions, and a "Control / monitoring" column, which included mainly high-level, generic items. It was not evident that the organisation was maximising the value of these two columns. ◆ Our review of the controls recorded noted that they were very high level / generic in many cases and did not enable easy assessment of how they reduced the risk. We concluded that this was likely due to the generic nature of the risks (see Risk Identification above), which was in turn due to not linking the risks to objectives. There was significant opportunity to add more value in this area and make the Risk Register into a value-adding tool for both management, the ACSRC and the National Park Authority (NPA). ◆ There was no "gaps in control" or equivalent column on the Risk Register, although there was a "Progress Update" column where additional comments were made and we noted that some of these were information on what additional work was being undertaken to further reduce the risk; therefore, essentially they were gaps in control. 	<p>R3</p> <p>R4</p>

Assurance	Details Findings:	Finding Ref.
	<ul style="list-style-type: none"> ◆ We did not identify any guidance available in relation to assurance – see recommendation 1. ◆ There was no “assurance” column or equivalent on the Risk Register and, although terms like “monitoring” (which is a form of control) were used in the Risk Register, there was no actual assurance documented, such as the output from that monitoring that would potentially provide assurance that the actions were having the intended effect. Recording assurance would make the Risk Register more meaningful as a document and increase the reliance that could be placed on it. It would also enable more efficient reporting by incorporating performance information into the Register so it could be removed from other reporting, reducing the need for separate reports. ◆ As assurance was not included in the Risk Register, gaps in assurance were also not recorded 	R5
Monitoring & Reporting	<ul style="list-style-type: none"> ◆ The organisation’s Risk Strategy detailed monitoring and review requirements, which included the monitoring required of individual risks by risk owners and that the Risk Register would be reported to the Leadership Team at each meeting, quarterly by the Corporate Management Team and also to the Audit and Corporate Services Review Committee. ◆ We confirmed that the reporting requirements in relation to risk were being met; although the effectiveness of that reporting was limited by the points raised in this report, particularly regarding: linking risks to objectives (R2); a lack of clarity regarding the actual controls in place and their impact on the risk (R3); and the lack of ‘actual’ assurance documented (R4). 	

3. BACKGROUND AND SCOPE

3.1. Objectives and risks

Client’s objective:	Key risks to the achievement of the Authority’s objectives are identified, assessed and appropriate action taken to mitigate the risk’s impact and/or likelihood.
Engagement objective:	To assess the Authority’s risk maturity and to provide advice on how to develop the risk management framework further.

3.2. Background to the Engagement

An audit of Risk Maturity was undertaken as part of the approved internal audit periodic plan for 2023/24. Risk Maturity is defined as: *“the extent to which a robust risk management approach has been adopted and applied as planned by management across the organisation, to identify, assess, decide on responses to, and report on opportunities and threats that affect the achievement of the organisation’s objectives.”*²

To effectively assess an organisation’s risk maturity, there are six main elements of the Risk Management Framework that need to be assessed. This review will provide a high level assessment against all of these six elements as per the ‘areas within scope’ below, to identify the level of maturity of each. This review is advisory and will not result in an assurance opinion; however it will have an impact on the Head of Internal Audit’s annual opinion.

Areas within scope:	The governance arrangements in place relating to risk. The approach to risk identification. The approach to risk assessment. The identification, documenting and assessing of mitigations. The identification, evidencing and review of assurances. The organisation’s approach to the monitoring and reporting of risk.
----------------------------	---

3.3. Limitations to the scope of the review

- Due to the time limitations of the review, we will carry out a high level assessment of all areas within scope.
- This review will not comment on whether individual risks are appropriately managed or whether the Authority has identified all of the risks and opportunities facing it.

² Chartered Institute of Internal Auditors





- Risk management remains the responsibility of the Authority and senior management to agree and manage information needs and to determine what works most effectively for the organisation.
- Due to the nature of the work required to complete the review, it will be undertaken remotely.
- Our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.


3.4. Key dates & personnel involved:



Debrief Meeting / Last Information Received:	21 September 2023
Draft Report Issued:	20 October 2023
Responses Received:	23 October 2023

Auditor:	Nigel Ireland, Chief Audit Executive
Client Sponsor:	Tegryn Jones, Chief Executive
Distribution:	-



4. ACTION PLAN

Priority:	 = Low	 = Medium	 = High	 = Suggestion
------------------	---	--	---	--

Ref.	Summary of Finding	Risk	Recommendation	Priority	Agreed Action	Responsible Person & Date for Implementation
R1	We noted some key areas of guidance that were missing and would likely mean that there was either a lack of understanding regarding those areas or a lack of consistency in the application of those areas.	Risk management may not be undertaken as efficiently as it could be or, in the worst case, key risks may be missed due to a lack of understanding, leading to a range of impacts including injuries, loss of finance or damage to reputation.	Guidance on the following areas should be made available and this could be achieved through the existing Risk Strategy or a separate guidance document: <ul style="list-style-type: none"> ◆ Risk identification; ◆ Controls, including the different types of control (preventative, directive, corrective and detective); and ◆ Assurance, including the different types of assurance and the difference between potential assurance and actual assurance – see Appendix 2. 		Risk Management Policy to be updated.	Responsible Person: Tegryn Jones, Chief Executive Date: 31 March 2024

Ref.	Summary of Finding	Risk	Recommendation	Priority	Agreed Action	Responsible Person & Date for Implementation
R2	Through review of the latest Risk Register (June 2023) we noted that objectives were not included on the register, indicating that risks may be identified in isolation and not in relation to specific objectives.	Risks become more generic and risk assessment processes become less consistent, which in turn makes resource allocation for mitigation activities less efficient.	A column for objectives should be added to the start of the Risk Register and all risks should be clearly linked to one or more objectives. A review of the risks should then be undertaken to identify any risks to the objectives that haven't yet been considered and also to ensure that current risks are re-worded to make it clear what the cause of the risk is and what the effect is on the objective to which the risk is linked ³ .		Risk Management Policy to be updated and Management Team to agree objectives.	Responsible Person: Tegryn Jones, Chief Executive Date: 31 March 2024
R3	Through review of the latest Risk Register we noted that the organisation had two columns on the Risk Register relating to mitigation: a "Mitigation" column, which was a mixture of controls and comments / descriptions, and a "Control / monitoring" column, which included mainly high-level, generic items. It was not evident that the organisation was maximising the value of these two columns.	A lack of clarity regarding what should be recorded in which column; duplication of information; creating a document that is significantly larger than it needs to be for the amount of information included; reduced ability to consider the 'strength' of controlling activities.	We recommend that the organisation removes the second "Control / monitoring" column and has just one either "Mitigation" or "Controls" column where the current Mitigation column is. Within this column should be recorded the tangible, key controls that are in place to reduce either the impact or the likelihood of risk occurring.		Recommendation to be considered as part of a review of the Risk Management Policy.	Responsible Person: Tegryn Jones, Chief Executive Date: 31 March 2024

³ The risk 'cause' enables you to identify what action you could take to reduce the risk. The risk 'effect' indicates how much resources you should apply to addressing the cause.

Ref.	Summary of Finding	Risk	Recommendation	Priority	Agreed Action	Responsible Person & Date for Implementation
R4	There was no “gaps in control or assurance” or equivalent column on the Risk Register, although there was a “Progress Update” column where additional comments were made and we noted that some of these were information on what additional work was being undertaken to further reduce the risk; therefore, essentially they were gaps in control.	The Risk Register is not useful as an action plan to clearly communicate either (1) what further action is planned to reduce the risk to within the organisation’s risk appetite; or (2) what further assurance is required to evidence that controls are operating effectively.	Either in addition to or instead of the “Progress Update” column, a “Gaps in control or Assurance” column should be added and this should be used to record planned further action to reduce the risk (controls) or planned assurance to be gained that controls are operating effectively (assurance). For ease of understanding, consideration should be given to recording this with either an “(c)” for gaps in control or “(a)” for gaps in assurance.		Recommendation to be considered as part of a review of the Risk Management Policy.	Responsible Person: Tegryn Jones, Chief Executive Date: 31 March 2024
R5	There was no “assurance” column or equivalent on the Risk Register and, although terms like “monitoring” (which is a form of control) were used in the Risk Register, there was no actual assurance documented, such as the output from that monitoring that would potentially provide assurance that the actions were having the intended effect.	The Risk Register does not include specific, meaningful information and is not a useful ‘tool’ for the organisation. It therefore becomes a tick-box exercise that does not add value and wastes resources, rather than helping the organisation achieve its objectives.	An assurance column should be added to the Risk Register and this should be used to record specific, actual assurance that risk management activities are having the intended effect. Consideration should be given to having two assurance columns: one for internal (2 nd Line) assurance and one for independent (3 rd Line) assurance – see Appendix 2.		Recommendation to be considered as part of a review of the Risk Management Policy.	Responsible Person: Tegryn Jones, Chief Executive Date: 31 March 2024

Suggestions in line with good practice or processes seen in other organisations			
Ref.	Finding	Suggestion	Management Response
S1	The Authority's Risk Appetite was described in its Risk Strategy and a risk appetite workshop was undertaken in September 2023 with Members to increase understanding and to update the Authority's Risk Appetite. Through the workshop, which we facilitated, and the detail in the Strategy, we believe there is an opportunity to increase the effectiveness of the use of risk appetite by joining up the Authority's "decision making" risk appetite with its appetite for managing risk.	The Authority should consider more clearly defining its appetite for managing particular risks and could do this by defining an appetite for each of the 'categories' in its Risk Strategy that it has established for risk scoring (noting Suggestions 2 and 3 below). Defining a guide to the maximum 'score' for each category would provide a framework to set each risks 'target risk' score so that it aligns to the other elements of the organisation's risk appetite. Please also note the additional guidance provided in Appendix 1.	A revised policy for Risk Appetite is being developed and will be incorporated in a revised Risk Management Policy.
S2	Five 'categories' of risk had been defined, in line with good practice, in the Risk Strategy, including: financial, service, reputation, legal and environment. Through the Risk Appetite Workshop it was noted that these could be reviewed to check that they are still the correct categories and others may need to be considered, such as health and safety.	In light of the points raised in this report, the organisation should re-review these categories and check that they remain correct and this should also include whether they could be used for risk appetite (see Suggestion 1 above). Another category that should be considered for inclusion is Health and Safety.	The current Risk Register includes different categories of risk. It is considered that an issue such as Health and Safety underpins a number of the identified categories and therefore should not have its own category. However, the matter will be considered as part of the review of the Risk Management Policy.
S3	A 4 x 4 matrix of impact v likelihood was defined in the Strategy with red, amber, dark green and light green sections indicated by the numbers to show the level of risk faced by the organisation. This colour distribution was not linked explicitly to the organisation's Risk Appetite.	Consideration should be given to moving to a 5 x 5 matrix, which is considered good practice. In addition, consideration should be given to creating individual matrices for each of the organisation's risk categories (linked to Suggestions 1 and 2 above) and the colour distribution could be used to show the alignment of risk management activity to the organisation's risk appetite; i.e. red = above risk appetite; amber = within risk appetite but further controls are required if possible; and green = within risk appetite and no further controls are required.	Consideration will be given to revising the matrix as part of a review of the Risk Management Policy. The current revised matrix for risk appetite includes a matrix identifying whether the risk is currently outside the risk appetite parameters.

APPENDIX 1 – GUIDANCE ON RISK APPETITE

An organisation's Risk Appetite is the level of risk (taking into account both impact and likelihood) that the organisation is willing to tolerate; i.e. it is a choice. It is distinguishable from Risk Tolerance, which is the level of risk the organisation is able to tolerate, but it is unlikely an organisation would *choose* to go to that level of risk. When defining an organisation's risk appetite the following elements should be considered:

- Risk appetite needs to be measurable. Otherwise there is a risk that any statements become empty and vacuous⁴; and
- Risk appetite is not a single, fixed concept. There will be a range of appetites for different risks which need to align and these appetites may well vary over time; the temporal aspect of risk appetite is a key attribute to this whole development⁴.

There are many ways to define risk appetite and which one is most appropriate for an organisation depends on a number of factors including:

- The risk maturity of the organisation;
- The knowledge and skills of the organisation's management;
- The knowledge and skills of the organisation's Board (or equivalent);
- The objectives of the organisation; and
- The environment / market that the organisation operates in.

A common way of communicating an organisation's risk appetite is through the organisation's risk register by stating a Target Risk where a risk's residual risk score is above that which the organisation is willing to accept. The organisation's Risk Strategy may then include, in relation to risk appetite, something similar to the following:

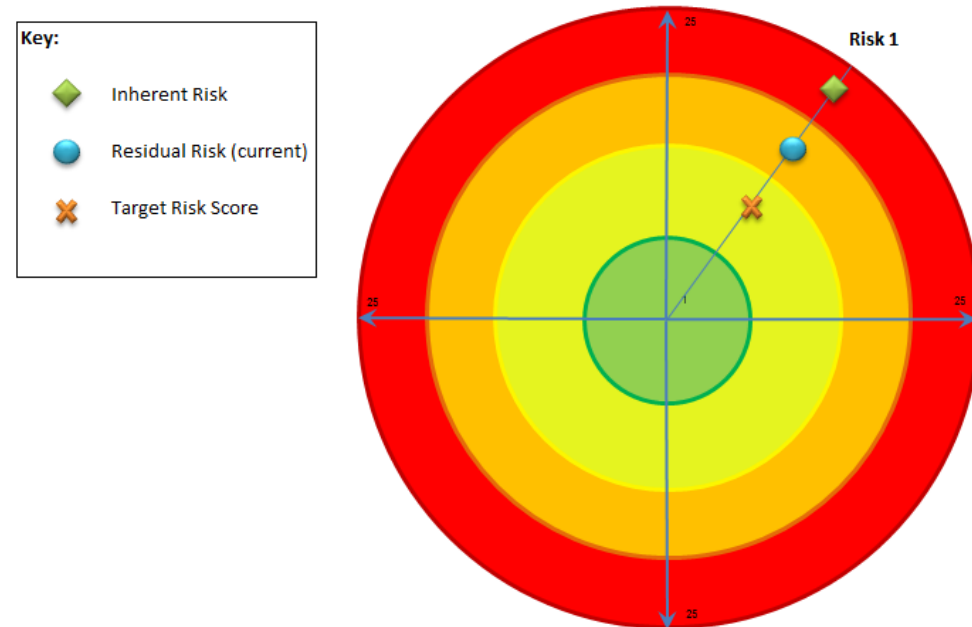
"Our risk appetite is agreed, through the documenting of a 'Target Risk' score, for each individual strategic risk by the [Audit Committee / Board] and is reviewed via our [Strategic Risk Register] at each meeting of the [Board / Committee]. Where a strategic risk is reviewed and is found to not be within our risk appetite, as agreed by the [Board / Audit Committee], action will be taken to put in place further controls, or to seek further assurance that the identified controls are operating effectively."

It is widely recognised that it is almost impossible to encapsulate an organisation's risk appetite in a single phrase such as 'risk averse'. Such a phrase generally fails to recognise the complexity of organisations and that different areas of the business require different risk appetites. The above method of communicating risk appetite recognises this complexity and addresses this by dealing with risk appetite at the individual risk level. Given the information in this report, the organisation should consider defining risk appetites for areas of the business to aid the NPA in considering whether the Target Risk score against individual risks is appropriate.

⁴ Institute of Risk Management Risk Appetite & Tolerance Guidance Paper, 2010

It is often easier to communicate risk appetite pictorially, rather than trying to write about it. The following is an example of how organisations can evidence their risk appetite through the use of inherent, residual and ‘target’ risk scores:

Figure 1: Based on DVLA ‘Dartboard’ approach



The diagram above reflects work undertaken to define the level of risk the organisation is willing to take at either an individual risk level or for an area of the business, such as health and safety or finance. This latter element is often the most difficult task in defining risk appetite and can be done relatively simply through defining a maximum risk score (or tolerance), using impact and likelihood, for each area of the organisation. In the case of PCNPA that may be based on its Risk Categories. The target score for each risk on the risk register can then be compared to the tolerance level defined for the relevant category and a decision made on whether the target score is appropriate.

Whatever method is used for defining risk appetite(s) there should be a fundamental recognition that the organisation is constantly changing, as is the external environment, and that the definition of risk appetite is not a one off task. The organisation’s risk appetite should be reviewed regularly, and challenged even more often, to ensure that it consistently reflects the needs of the organisation, its objectives, the environment in which the organisation operates and the overall risk universe.

APPENDIX 2 – GUIDANCE ON ASSURANCE FRAMEWORKS

'Assurance Frameworks' present an opportunity to elevate a 'standard' risk register into a tool that is used to evidence the likelihood of achieving the organisation's objectives and should be a core element of the Authority's processes around seeking assurance that key requirements, including compliance with regulations and legislation, are being achieved.

Staff within Astari Limited have worked with Assurance Frameworks since they were first introduced into the NHS in 2004 and supported their development at that time and therefore have an increased understanding of the benefits they can bring. We do not see an Assurance Framework as a separate entity to the organisation's risk processes and believe they add most value when they are together as assurance is, in the vast majority of cases, required to evidence that a relevant risk (such as non-compliance) is being appropriately managed.



There is not just one source of assurance and the different sources have different attributes, strengths and weaknesses. The diagram opposite shows two of the key elements that indicate the value of different sources of assurance – independence and knowledge of the organisation.

An effective assurance framework does not seek to maximise the 'amount' of one type of assurance, but to maximise efficiency by seeking the most appropriate source of assurance for the risk and controls that assurance is required over. It is by combining the various sources that the Authority will maximise its evidence that a control is operating effectively, a risk is being effectively managed or that an objective is most likely to be achieved.

The main element that organisation's need to decide on is how to communicate risk and assurance in the most effective way, whilst not duplicating effort. Astari believes that an organisation's risk register (or risk and assurance register) provides a fantastic opportunity to bring a massive amount of information together in one place. The example on the next page has been built on the Three Lines Model referenced in our Risk Appetite training session: [New Three Lines Model – What does it mean for organisations' risk and assurance frameworks? \(astari.org.uk\)](https://www.astari.org.uk/resources/new-three-lines-model-what-does-it-mean-for-organisations-risk-and-assurance-frameworks/).

Figure 3: Example Risk & Assurance Register:

OBJECTIVE	Risks & Controls							ASSURANCE THAT WE ARE ACHIEVING				Risk Appetite	
	Risk Description	Inherent Risk			Key Controls in Place	Residual Risk			OBJECTIVE				
		Risk Impact	Prob.	Inherent Risk Score		Risk Impact	Prob.	Residual Risk Score	Assurance level required	Internal Assurance (Second Line)	Independent Assurance (Third Line)		Assurance level achieved
1. Provide high-quality, appropriately resourced services to meet the needs of our current and future clients.	1.5 - (Covid-19) As our clients return to a mix of office-based and remote working, any misalignment with expectations of our presence may lead to reduced effectiveness of the service, in particular: value added and cultural / partnership integration. This could therefore reduce the impact of our USP in the market place.	4	4	16	1. Keeping in touch with clients, including senior teams, to understand their expectations. 2. Communication with clients about our intended hybrid approach and how this fits with their expectations. 3. Completely set-up for a hybrid approach technologically. 4. Risk assessment completed and communicated to all staff about on-site presence, including effective use of PPE. 5. Wipes, masks and hand gel being provided to all staff prior to return to site. 6. Driving training course mandatory (annual) before driving to site to ensure staff can return to site if required / expected.	3	2	6	Medium	3. IT equipment is working well; only very minor downtime (timesheets). 4, 5 & 6 - RA001 Risk Assessment email to staff 12Apr21 and risk assessment on shared drive. 6 - Certificates of completion on staff files.	1 & 2 - Satisfaction surveys still consistent at 97%. No negative comments regarding on-site v remote operation. 1 & 2 - Specific survey issued to clients regarding remote / hybrid working - all came back in line with expectations that all organisations want a hybrid approach - some on-site; some remote.	Medium	6

This is purely an example and the full version includes additional information / columns as well as formulae to drive various elements. However, what you can see from this example is how risk and assurance have been combined and it provides:

- Risks linked clearly and explicitly to the organisation’s objectives;
- Key controls;
- Inherent and residual risk scoring;
- An assessment, linked to the difference between the inherent and residual risk scores, of the assurance level required and subsequently of the assurance level achieved;
- 2nd and 3rd Line assurances, linked clearly to the specific controls over which they are providing assurance; and
- A Risk Appetite (or target) score.

Not only does this model bring together risk and assurance but also brings in key elements of performance reporting through the assurance columns where key performance indicators (KPIs) linked to the organisation’s key risks should be included. This can remove the need for additional performance reporting.

This engagement was conducted in conformance with Global Internal Audit Standards. The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the strengths and weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regard to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

This report is prepared solely for the use of the Board and senior management of Pembrokeshire Coast National Park Authority. Details may be made available to specified external agencies, including external auditors, but otherwise the report should not be recited or referred to in whole or in part to other third parties without prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended for any other purpose.