



Internal Audit

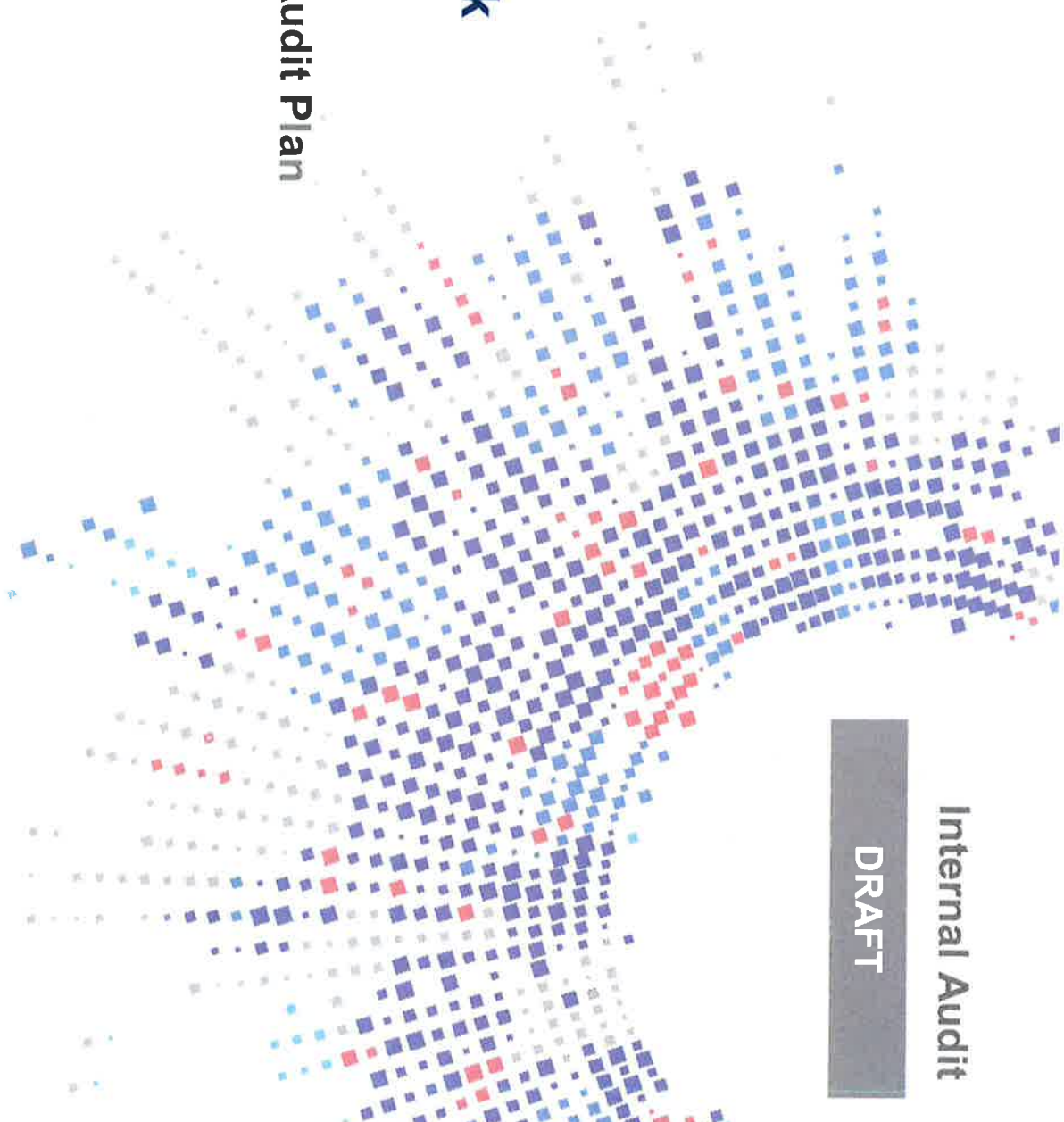
DRAFT

Brecon Beacons National Park Authority

Audit Strategy and Annual Internal Audit Plan

2019/20

April 2019



Overview

Introduction

The Audit Plan for 2019/20 has been informed by an updated audit risk assessment to ensure that planned coverage for the year is focussed on the key audit risks, and that the coverage will enable a summary annual Head of Internal Audit Opinion to be provided.

Key Emerging Themes

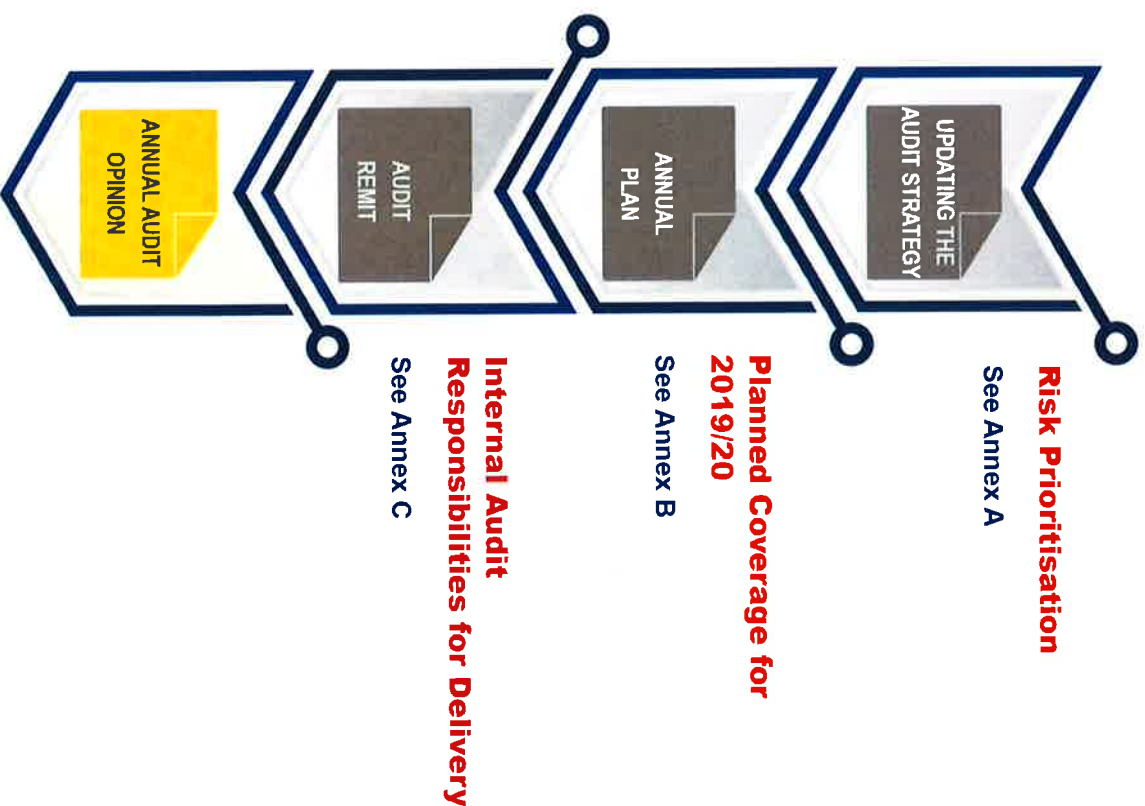
This year will be another challenging year for the Welsh Public Sector in terms of income and also the pressures on service delivery. We have identified a number of key areas which require consideration when planning internal audit coverage.

- **Brexit** – The Business Plan and Risk Register need to be stress-tested against continuing uncertainty, which may have knock-on impacts on recruitment and retention of staff and on procurement and suppliers.
- **Data Protection Act 2018** – this has a significant impact on how data is held and protected and could lead to an increase in access requests.
- **Cybercrime** – all the indications are that there will be continued and more sophisticated attempts to disrupt and deny services often for no clear motive.
- **Financial sustainability** - increased reliance on short term funding and contracts. Additional funding (almost a third of core funding) made available by Welsh Government late in the year requiring quick decision making in line with business plan and capacity to manage expenditure.

Adequacy of the planned audit coverage

The Fundamental reviews identified in the audit plan for 2019/20 support the Head of Audit's annual opinion on the adequacy and effectiveness of the organisation's framework of governance, risk management and control. The Organisational reviews have been identified from your assurance framework, risk registers and key emerging themes.

2019/20 Audit planning process



Internal Audit Plan

Audit Strategy Methodology

We adopt a proprietary risk based approach (GUARD) to determining your audit needs each year which includes reviewing your risk register and risk management framework, previous internal audit work for the organisation, the Regulatory Framework and assessment of Brecon Beacons National Park Authority, external audit recommendations together with key corporate documentation such as your business and corporate plan, standing orders, and financial regulations. For 2019/20 we have conducted an assurance survey of the chair of the Audit and Scrutiny Committee and Finance Manager at our clients using Strategic Risk Insight Tool (SRIT) to inform our annual planning. The Audit Strategy is based predominantly on our understanding of the inherent risks facing Brecon Beacons National Park Authority and those within the sector and has been developed with senior management and Committee.

Risk Prioritisation

Each year an updated risk assessment is carried out to ensure the Audit Strategy remains fully aligned with the key risks facing Brecon Beacons National Park Authority. The resultant changes for 2019/20 which underpin your Audit Plan is set out at Annex A.

Audit Strategy and Annual Plan

Following the risk prioritisation review, the Audit Strategy has been updated (Annex B) and the Annual Plan (Annex C) sets out the reviews that will be carried out, the planned times and the scopes for each of these reviews.

The Annual Plan will be subject to ongoing review and could change as the risks change for the organisation and will be formally reviewed with senior management and the Audit and Scrutiny Committee mid-way through the financial year or should a significant issue arise.

The overall agreed time for the delivery of the Annual Plan includes: research, preparation and issue of terms of reference, production and review of working papers and reports and site work. The Annual Plan has been prepared on the assumption that the expected controls will be in place.

The total number of days required to deliver the Audit Plan is as agreed in the contract between TIAA and Brecon Beacons National Park Authority. This number of days is fixed and it is TIAA's responsibility to deliver the Audit Plan for this number of days. Where Brecon Beacons National Park Authority agrees additional work the required number of days and the aggregate day rate will be agreed in advance with the Finance Manager and will be clearly set out in the terms of reference for the additional review(s).

Audit Remit

The Audit Remit (Annex D) formally defines internal audit's purpose, authority and responsibility. It establishes internal audit's position within Brecon Beacons National Park Authority and defines the scope of internal audit activities.

Reporting

Assignment Reports: A separate report will be prepared for each review carried out. Each report will be prepared in accordance with the arrangements contained in the Terms of Reference agreed with TIAA and which accord with the requirements of TIAA's audit charter and the Public Sector Internal Audit Standards (PSIAS).

Progress Reports: Progress reports will be prepared for each Audit and Scrutiny Committee meeting. Each report will detail progress achieved to date against the agreed annual plan.

Annual Report: An Annual Report will be prepared for each year in accordance with the requirements set out in TIAA's audit charter and the PSIAS. The Annual Report will include our opinion of the adequacy and effectiveness of Brecon Beacons National Park Authority's governance, risk management and operational control processes.

Other Briefings: During the year Client Briefing Notes, Benchmarking and lessons learned digests will be provided. These are designed to keep the organisation abreast of in-year developments which may impact on the governance, risk and control assurance framework.

Assurance Mapping

For each assurance review an assessment of the combined effectiveness of the controls in mitigating the key control risks will be provided. The assurance mapping process is set out in Annex E.

Liaison with the External Auditor

We will liaise with Brecon Beacons National Park Authority's External Auditor. Any matters in the areas included in the Annual Plan that are identified by the external auditor in their audit management letters will be included in the scope of the appropriate review.

Performance

The following Performance Targets will be used to measure the performance of internal audit in delivering the Annual Plan:

Area	Performance Measure	Target
Achievement of the plan	Completion of planned audits. Audits completed in time allocation.	100% 100%
Reports issued	Draft report issued within 10 working days of exit meeting. Final report issued within 10 working days of receipt of responses.	95% 95%
Professional Standards	Compliance with TIAA's audit charter and the PSIAS.	100%

Conflict of Interest

We are not aware of any conflicts of interest and should any arise we will manage them in line with TIAA's audit charter and the PSIAS, the Brecon Beacons National Park Authority's requirements and TIAA's internal policies.

Limitations and Responsibility

Substantive testing will only be carried out where a review assesses the internal controls to be providing 'limited' or 'no' assurance with the prior approval of Brecon Beacons National Park Authority and additional time will be required to carry out such testing. Brecon Beacons National Park Authority is responsible for taking appropriate action to establish whether any loss or improperly has arisen as a result of the control weaknesses.

Internal controls can only provide reasonable and not absolute assurance against misstatement or loss. The limitations on assurance include the possibility of one or

more of the following situations, control activities being circumvented by the collusion of two or more persons, human error, or the overriding of controls by management. Additionally, no assurance can be provided that the internal controls will continue to operate effectively in future periods or that the controls will be adequate to mitigate all significant risks that may arise in future.

The responsibility for a sound system of internal controls rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses that may exist. Neither should internal audit work be relied upon to identify all circumstances of fraud or irregularity, should there be any, although the audit procedures have been designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of internal control may not be proof against collusive fraud.

Reliance will be placed on management to provide internal audit with full access to staff and to accounting records and transactions and to ensure the authenticity of these documents.

The matters raised in the audit reports will be only those that come to the attention of the auditor during the course of the internal audit reviews and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. The audit reports are prepared solely for management's use and are not prepared for any other purpose.

Audit and Scrutiny Committee Responsibility

It is the responsibility of the Audit and Scrutiny Committee to determine that the number of audit days to be provided and the planned audit coverage are sufficient to meet the Committee's requirements and the areas selected for review are appropriate to provide assurance against the key risks within the organisation.

Release of Report

The table below sets out the history of this plan.

Date plan issued:	18 th April 2019
Date final plan issued:	1 st July 2019

Changes for 2019/20

In addition to the core audit work required to underpin the Head of Audit Annual Opinion (governance, risk management, core financial systems, network controls, follow up etc.) a GUARD assessment of key risks has been completed, to identify those that are most relevant to the organisation and where internal audit assurance would be best focussed. These are summarised below.

LINKED TO RISKS ON PAGE 1	GUARD Risk Analysis			Cross Ref to Annual & Strategic Plan (Annex B, C)
Risk Areas	BBNPA Specific	TIAA National Intelligence Assessment	Updated Guard Assessment	
<p>Brexit – There is likely to be significant uncertainty and potential fast-emerging risks developing as a result of the UK leaving the EU in March 2019, which will not be fully understood until after the departure date.</p> <p>How we intend to review this risk: We will assess the extent that the Business Plan and Risk Register have been stress-tested against the continued. We will consider the actions taken by the organisation to prepare for Brexit and to mitigate the impact of known Brexit issues such as the availability of labour, procurement, and the increased cost of materials and the supply of materials and the availability of future grant funding.</p>				2019/20
<p>Data Protection Act 2018 – This will be an ongoing issue and source of risk for all organisations given the regulatory and public expectation about how data is held and protected, together with a likely increase in access requests.</p> <p>How we intend to review this risk: We will assess the organisation's arrangements for storing hardcopy and electronic information that is covered under the Act and how it is managed to ensure its accuracy and completeness. We will consider responsibilities for managing data including awareness among the wider staff base on processing and providing data. Our approach also includes the arrangements in place for effectively dealing with access requests within the prescribed timeframe.</p>				2018/19
<p>Cybersecurity – All the indications are that there will continue to be more sophisticated hacking attempts designed to disrupt or deny services, often for no clear motive.</p> <p>How we intend to review this risk: We will consider the practical and technical security measures that the organisation has deployed to minimise the risk of succumbing to a cyber-incident. We will also consider the extent to which staff awareness has been addressed to minimise the risk of behaviours giving rise to a cyber-incident.</p>				2019/20
<p>Income pressure</p> <p>How we intend to review this risk: Cyclical review of budgetary control. Audit work will also be undertaken on expenditure including procurement where testing will consider arrangements for value for money.</p>				2019/20

Client Specific Risks

Areas of review with limited or no assurance in previous year – none.

How we intend to review this risk: A follow up audit is undertaken of all prior year recommendations to ensure action has been taken within appropriate timescales.

--	--	--

Follow Up

Key to Risk Assessment Grades:



<p>RP Specific</p>	<p>The control framework relating to the specific area has been identified as 'High' risk as per Assurance Framework, senior management, internal and external audit. 'Medium' priority determines that the control framework has been identified as 'reasonably' vulnerable to control weaknesses based on discussions with management, internal and external audit. 'Low' priority means that review of the control framework has not revealed any significant issue.</p>
<p>TIAA portfolio</p>	<p>Across our client portfolio of similar types of housing providers, our intelligence has tracked a large or growing ('High' priority); mid-range or flat line ('Medium' priority); or relatively low or decreasing ('Low' priority) number of control issues in this specific area for this type of organisation.</p>
<p>National Policy/Issue</p>	<p>National bodies (including the Regulator of Social Housing, Homes England, HIAF, National Federation for Housing amongst others) have identified a growing or high level of control weaknesses ('High' priority); mid-range or flat line ('Medium' priority); or relatively low or decreasing ('Low' priority) in this specific area. There may also be a national policy emphasis on a specific area which will be reflected in this priority rating.</p>

Fundamental Review Areas To support the Head of Internal Audit opinion	BAF / Risk Ref.	Type	2019/20 Yr 1	2020/21 Yr 2	2021/22 Yr 3
---	-----------------	------	-----------------	-----------------	-----------------

Governance

Key governance areas will be reviewed on a rotational basis each year such as strategic planning, strategic control, regulatory compliance, performance management, board assurance framework, partnership working, management of conflicts, health and safety, subsidiary governance and third party assurances.

13

Year 1 – Health and Safety Management

Assurance

✓

✓

✓

Year 2 – Strategic Planning

Year 3 – Performance Management

Risk

A robust risk management framework is critical to all organisations to ensure risks are effectively management and emerging risks identified our cyclical annual reviews will cover embedding risk, risk identification, risk mitigation and risk workshops.

Appraisal

✓

✓

✓

Year 1 – Business Continuity Arrangements

Financial systems - Cost Control and Income Maximisation

Cost control, income maximisation and robust financial systems are essential to financial well-being of any organisation. Our reviews of key financial systems are designed to ensure compliance with IIA standards and help protect against potential frauds. We will carry out a high level review of key financial systems each year supported by a rolling programme of financial system reviews such as payments health check, income, payroll, budgetary control/management reporting, cost improvement planning and nominal ledger.

18

Assurance

✓

✓

✓

Year 1 – General Ledger, Creditors and Procurement

Year 2 - Income and Debtors, Cash and Bank and Treasury Management

Year 3 – Budgetary Control, Payroll and Expenses and Fixed Assets

ICT

We will use our GUARD risk assessment to continue to review ICT risks and controls in place within the organisation. The rolling programme of reviews will include data protection, ICT governance, ICT management and business support, application reviews, network security, data quality and cyber-security.

03.3

Assurance

✓

✓

✓

Year 1 – Cyber Security

Follow Up

We will carry out a continuous follow up of internal audit recommendations utilising TIAA's client portal and recommendation tracker. Updates will be provided to each Committee.

Follow Up

✓

✓

✓

Organisational Review Areas	BAF / Risk Ref.	Type	Yr1	Yr2	Yr3
Human Resources		Assurance	✓	-	-
Health and Safety Management	06, 09	Assurance	✓	-	-
Planning	01, 03, 07, 08	Assurance	-	✓	-
Staff Attendance and Wellbeing Strategy	19	Assurance	-	✓	-
Project Management		Assurance	-	-	✓
Buildings Management and Maintenance	17	Assurance			✓
Management and Planning					
Briefings		-	✓	✓	✓
Planning		-	✓	✓	✓
Annual Report		-	✓	✓	✓
Management		-	✓	✓	✓

Quarter	Fundamental Audits	Type	Days	Rationale and Scope
Block 1	Risk Management – Business Continuity Planning	Appraisal	3	<p><u>Rationale</u> Key business risk.</p> <p><u>Scope</u> The review considers the arrangements for business continuity planning including policy/strategy and procedures, organisational responsibility, plan details for various scenarios and testing. The audit will consider the planning in place in the context of Brexit and the continuity and resilience of the response by the Authority. The scope of the review does not include providing assurance that the business continuity planning covers all the risks faced, or that the arrangements proposed operate continuously and effectively.</p> <p><u>Rationale</u> A review of ICT is included in each year of the Strategic Plan.</p> <p><u>Scope</u> The high level review will consider the practical and technical security measures that the organisation has deployed to minimise the risk of succumbing to a cyber-incident. It will also consider the extent to which staff awareness has been addressed to minimise the risk of behaviours giving rise to a cyber-incident. The audit will be undertaken by a specialist IT auditor.</p> <p><u>Rationale</u> Operational risk area.</p> <p><u>Scope</u> The review will consider whether Human Resources (HR) processes and records are appropriate to the needs of the organisation and identify if any improvements can be made in the way information on staff absence, recruitment, expenses, timesheets, performance and other records are managed and processed. The audit will consider whether appropriate staff and other resources are available for robust HR management.</p> <p><u>Rationale</u> Key Financial controls. Annual review looking at core areas on a cyclical basis.</p> <p><u>Scope</u> The review considers the effectiveness of the key financial controls which provide assurance that the following systems are operating in accordance with the organisation's requirements:</p> <ul style="list-style-type: none"> • General Ledger; • Creditors; • Procurement.
Block 1	ICT Security – Cyber Security	Assurance	3	<p><u>Rationale</u> A review of ICT is included in each year of the Strategic Plan.</p> <p><u>Scope</u> The high level review will consider the practical and technical security measures that the organisation has deployed to minimise the risk of succumbing to a cyber-incident. It will also consider the extent to which staff awareness has been addressed to minimise the risk of behaviours giving rise to a cyber-incident. The audit will be undertaken by a specialist IT auditor.</p> <p><u>Rationale</u> Operational risk area.</p> <p><u>Scope</u> The review will consider whether Human Resources (HR) processes and records are appropriate to the needs of the organisation and identify if any improvements can be made in the way information on staff absence, recruitment, expenses, timesheets, performance and other records are managed and processed. The audit will consider whether appropriate staff and other resources are available for robust HR management.</p> <p><u>Rationale</u> Key Financial controls. Annual review looking at core areas on a cyclical basis.</p> <p><u>Scope</u> The review considers the effectiveness of the key financial controls which provide assurance that the following systems are operating in accordance with the organisation's requirements:</p> <ul style="list-style-type: none"> • General Ledger; • Creditors; • Procurement.
Block 1	Human Resources	Assurance	3	<p><u>Rationale</u> Operational risk area.</p> <p><u>Scope</u> The review will consider whether Human Resources (HR) processes and records are appropriate to the needs of the organisation and identify if any improvements can be made in the way information on staff absence, recruitment, expenses, timesheets, performance and other records are managed and processed. The audit will consider whether appropriate staff and other resources are available for robust HR management.</p> <p><u>Rationale</u> Key Financial controls. Annual review looking at core areas on a cyclical basis.</p> <p><u>Scope</u> The review considers the effectiveness of the key financial controls which provide assurance that the following systems are operating in accordance with the organisation's requirements:</p> <ul style="list-style-type: none"> • General Ledger; • Creditors; • Procurement.
Block 2	Key Financial Controls (General Ledger, Creditors, Procurement)	Compliance	3	<p><u>Rationale</u> Key Financial controls. Annual review looking at core areas on a cyclical basis.</p> <p><u>Scope</u> The review considers the effectiveness of the key financial controls which provide assurance that the following systems are operating in accordance with the organisation's requirements:</p> <ul style="list-style-type: none"> • General Ledger; • Creditors; • Procurement.

Quarter	Fundamental Audits	Type	Days	Rationale and Scope
Block 2	Health and Safety Management	Assurance	3	<p><u>Rationale</u> Brought forward from 2020/2021 at Management's Request.</p> <p><u>Score</u> The review will consider the management and reporting of health and safety and the underlying health and safety risk assessment processes.</p>
Block 2	Follow-up	Follow up	1	Follow-up of implementation actions from audit reports, ensuring the Organisation is implementing recommendations, and providing reports to the Audit and Scrutiny Committee.
1	Annual Planning	Management	1	Assessing the Organisation's annual audit needs – requirement of Internal Audit Standards.
4	Annual Report	Management	1	Reporting on the overall conclusions and opinion based on the year's audits and other information and providing input to the Annual Governance Statement.
1-4	Client Portal			The client portal provides a one stop shop of internal audit reports, progress and recommendation tracker as well as briefings, fraud alerts, fraud updates and committee briefings.
1-4	Management, Planning & Audit and Scrutiny Committee Reporting/Support	Management	3	This time includes: meeting client management, overseeing the audit plan, reporting and supporting the Audit and Scrutiny Committee, liaising with External Audit and Client briefings (including fraud alerts, fraud digests and committee briefings).
	Total Days		21	

Role

The main objective of the internal audit activity carried out by TIAA is to provide, in an economical, efficient and timely manner, an objective evaluation of, and opinion on, the overall adequacy and effectiveness of the Brecon Beacons National Park Authority framework of governance, risk management and control. TIAA is responsible for giving assurance to Brecon Beacons National Park Authority "Governing Body" (being the body with overall responsibility for the organisation) on the adequacy and effectiveness of Brecon Beacons National Park Authority risk management, control and governance processes.

Scope

All Brecon Beacons National Park Authority activities fall within the remit of TIAA. TIAA may consider the adequacy of controls necessary to secure propriety, economy, efficiency and effectiveness in all areas. It will seek to confirm that Brecon Beacons National Park Authority management has taken the necessary steps to achieve these objectives and manage the associated risks. It is not within the remit of TIAA to question the appropriateness of policy decisions. However, TIAA is required to examine the arrangements by which such decisions are made, monitored and reviewed.

TIAA may also conduct any special reviews requested by the board, Audit and Scrutiny committee or the nominated officer (being the post responsible for the day to day liaison with the TIAA), provided such reviews do not compromise the audit service's objectivity or independence, or the achievement of the approved audit plan.

Access

TIAA has unrestricted access to all documents, records, assets, personnel and premises of Brecon Beacons National Park Authority and is authorised to obtain such information and explanations as they consider necessary to form their opinion. The collection of data for this purpose will be carried out in a manner prescribed by TIAA's professional standards, Information Security and Information Governance policies.

Annex D: Audit Remit

Standards and Approach

TIAA's work will be performed with due professional care, in accordance with the requirements of the PSIAS.

Independence

TIAA has no executive role, nor does it have any responsibility for the development, implementation or operation of systems. However, it may provide independent and objective advice on risk management, control, governance processes and related matters, subject to resource constraints. For day to day administrative purposes only, TIAA reports to a nominated officer within Brecon Beacons National Park Authority and the reporting arrangements must take account of the nature of audit work undertaken. TIAA has a right of direct access to the chair of the board, the chair of the Audit and Scrutiny committee and the responsible accounting officer (being the post charged with financial responsibility).

To preserve the objectivity and impartiality of TIAA's professional judgement, responsibility for implementing audit recommendations rests with Brecon Beacons National Park Authority management.

Consultancy activities are only undertaken with distinct regard for potential conflict of interest. In this role we will act in an advisory capacity and the nature and scope of the work will be agreed in advance and strictly adhered to.

Irregularities, Including Fraud and Corruption

TIAA will without delay report to the appropriate regulator, serious weaknesses, significant fraud, major accounting and other breakdowns subject to the requirements of the Proceeds of Crime Act 2002.

TIAA will be informed when evidence of potential irregularity, including fraud, corruption or any impropriety, is discovered so that TIAA can consider the adequacy of the relevant controls, evaluate the implication of the fraud on the risk management, control and governance processes and consider making recommendations as appropriate. The role of TIAA is not to investigate the irregularity unless commissioned to do so.

Corporate Assurance Risks

We consider four corporate assurance risks; directed; compliance; operational and reputational, and tailor the type of audit accordingly. For all types of audit we also taken into account value for money considerations and any linkages to the organisational Assurance Framework. The outcomes of our work on these corporate assurance risks informs both the individual assignment assurance assessment; and also the annual assurance opinion statement. Detailed explanations of these assurance assessments are set out in full in each audit report.

Assurance Assessment Gradings

We use four levels of assurance assessment: substantial; reasonable, limited and no. Detailed explanations of these assurance assessments are set out in full in each audit report.



Benchmarking

Where a similar review is carried out at a number of our clients we will subsequent to the completion of the review at each of the clients we will where relevant provide a benchmarking and lessons learned digest. This digest will include Operational Effectiveness Matters for the Brecon Beacons National Park Authority to consider.

Types of Audit Review

The Annual Plan includes a range of types of audit review. The different types of review focus on one or more of the corporate assurance risks. This approach enables more in-depth work to be carried out in the individual assignments than would be possible if all four assurance risks were considered in every review. The suite of audit reviews and how they individually and collectively enable us to inform our overall opinion on the adequacy and effectiveness of the governance, risk and control arrangements is set out in the assurance mapping diagram.

