



Pembrokeshire Coast National Park Authority

Internal Audit Progress Report

Committee Meeting Date: 12 November 2025

INTRODUCTION

This report provides an update of progress towards delivery of the 2025/26 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 report since the last committee meeting:

- IT Continuity & Disaster Recovery (01.25/26)

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>IT Continuity & Disaster Recovery (01.25/26)</i>	<i>FINAL</i>	Substantial	0	0	3
TOTAL:			0	0	3

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. Our Internal Audit Strategy and audit reports are shared with External Audit annually, with the opportunity available for them to liaise with us.

INTERNAL AUDIT PLAN CHANGE CONTROL

Change	Date	Agreed By
November 2025		
No changes to report.		

WORK IN PROGRESS OR YET TO START

Audit	Start Date	Debrief Date	Draft Report Issued	Planned Audit Committee	Comments
Customer & Stakeholder Engagement	8 Sept 2025	18 Sept 2025		February 2026	Quality review stage
Asset Management - Commercial Management	4 Nov 2025			February 2026	
Governance: Strategic Planning	1 Dec 2025			February 2026	
Risk Management	9 Dec 2025			May 2026	
Follow Up	15 Dec 2025			May 2026	
Key Financial Controls	10 Feb 2026			May 2026	

LEGISLATION & PUBLICATION UPDATE

September 2025 – Economic Crime & Transparency Act & Failure to Prevent Fraud Offence

The UK Government has announced a new that become legislation from 1 September 2025. The Economic Crime and Corporate Transparency Act 2023 became 'live' on 1 September 2025 and includes the new 'failure to prevent fraud offence' that we highlighted last November. The offence joins similar 'failure to prevent' offences such as bribery and tax evasion.

The new offence holds large organisations (both private and public) accountable for fraudulent activities committed by their employees. The legislation suggests that an organisation will be able to avoid prosecution if it is able to prove that it had 'reasonable procedures' in place to prevent fraud from occurring.

Further information from the Home Office to help organisations with this legislation, including whether it applies as it only applies to large organisations, can be found here: [Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud \(accessible version\) - GOV.UK](#)

September 2025 – Risk in Focus 2026

The European Confederation of Institutes of Internal Auditing publishes an annual Risk in Focus report which is the output of a thought leadership research project analysing the top risks faced by organisations across Europe.

Key findings include:

1. Digital disruption, new technology and AI continued to be a growing risk, moving from 4th to 3rd place in 2026, with organisations across Europe striving to develop AI strategies despite being unclear on the potential benefits and risks.
2. 83% of respondents indicated that cybersecurity and data security was the top risk yet again in this year's survey, with sophisticated cyber attacks continuing to be a key concern for audit functions.
3. Human capital, diversity, talent management and retention held its 2nd place ranking with 48% of Chief Audit Executives placing it as a top 5 risk.



We have provided a copy of the full Risk in Focus 2026 - Board Briefing Report to include in this Committee's pack as an appendix.

2026

RISK IN FOCUS

Hot topics for
internal auditors
BOARD BRIEFING

[Read more](#)



ECIIA

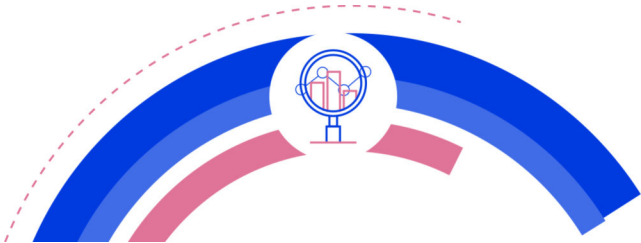
RISK IN FOCUS 2026 EXECUTIVE SUMMARY

- With organisational strategies disrupted by geopolitical uncertainty and fast AI developments, businesses are struggling to get on the front foot.
- Growth is stalling because of persistent uncertainty and the impact of US tariffs on the world economy. Managing cyberthreats, changes to global markets and skills shortages – all while investing in digital innovation – present big challenges.
- Organisations must combine a deep and rapid grasp of the unfolding risk landscape with fast and purposeful decision-making to thrive.
- CAEs are providing a greater level of advisory services in areas such as new product launches and AI implementations, strengthening risk assessment and mitigations processes, but the pace at which the risk landscape is evolving means that board-level support is critical.

RISK IN FOCUS 2026

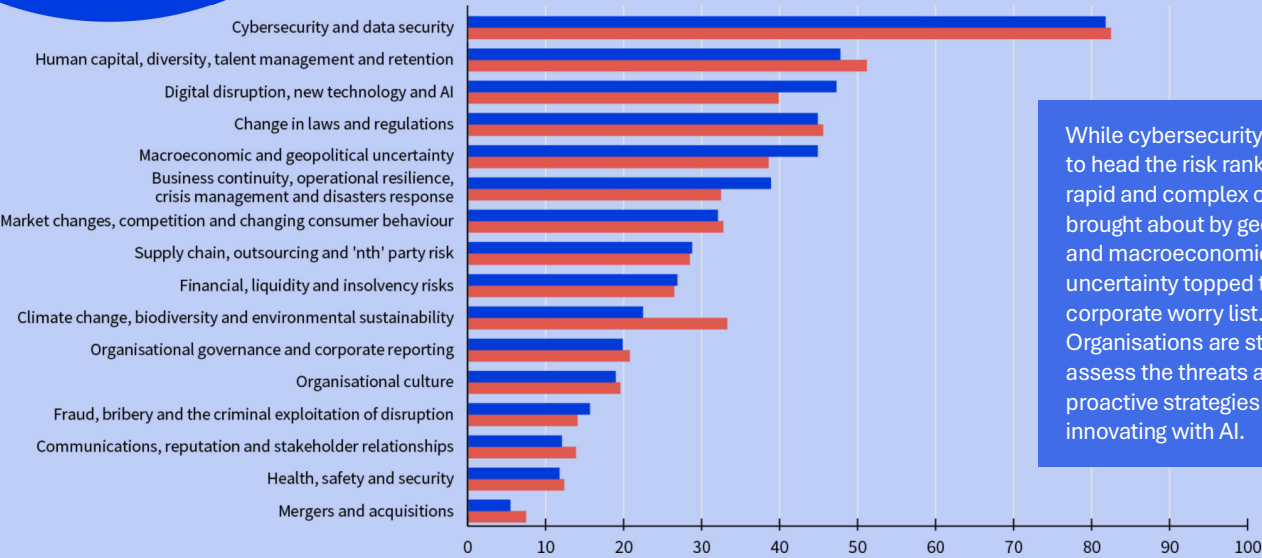
HOT TOPICS

- While **macroeconomic and geopolitical uncertainty** was in joint 4th place for 2026 (with changes to laws and regulations), the threat permeated every other risk category. Global trade wars, tariffs and sanctions impacted changes to laws, cyber threats, market conditions and AI, all of which were high on organisations’ agendas.
- Digital disruption, new technology and AI continued to rise.** It moved from 4th to 3rd place as a risk and 10th to 8th place as an area of internal audit effort: 58% said it would be a top 5 priority in 3 years’ time. CAEs said that they were focusing on governance to ensure strategically sound and safe implementation of AI.
- Cybersecurity and data security** remained the biggest overall risk. CAEs described it as a constantly “emerging risk” with increased sophistication in attacks and a rapidly approaching threat of quantum computing.
- Human capital, diversity, talent management and retention** remained the 2nd largest threat to organisations in 2026. A major focus was to create a skills strategy fit for the era of AI. Fears of deskilling, talent shortages and uncertainty over how careers could be transformed by the technology were core concerns.
- The biggest falling risk was **climate change, biodiversity and environmental sustainability**. It dropped from 8th place to 10th place in the risk rankings. CAEs at the roundtable expressed frustration over the prevailing regulatory uncertainty shaped by changing political attitudes in Europe and globally. Only 24% predicted it would be a top 5 area of audit focus by 2029.



Key survey findings

The top 5 risks organisations face today



While cybersecurity continued to head the risk rankings, the rapid and complex changes brought about by geopolitical and macroeconomic uncertainty topped the corporate worry list. Organisations are struggling to assess the threats and develop proactive strategies while innovating with AI.

Looking ahead

The top 5 risks organisations will face by 2029



MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY: KEY FINDINGS

"Organisations need to be specific about how expected changes to the macro and micro political environments are likely to impact them"

- Macroeconomic and geopolitical uncertainty was in joint 4th place in 2026 together with changes in laws and regulations. Continuing conflicts and the threat of a global tariff war meant that 32% of CAEs who chose this category said it was their number one risk.
- While there was a real risk of an economic downturn in key global markets, organisations were also considering potential upside risks. CAEs were providing advisory services to support innovation and new product launches.
- The wide-ranging potential impact of such a fluid situation saw many organisations refreshing business resilience and continuity planning processes.
- Organisations expected regulatory uncertainty to increase over the next few years given potential policy swings created by changes to domestic and global administrations.

MACROECONOMIC AND GEOPOLITICAL UNCERTAINTY: KEY BOARD CONSIDERATIONS

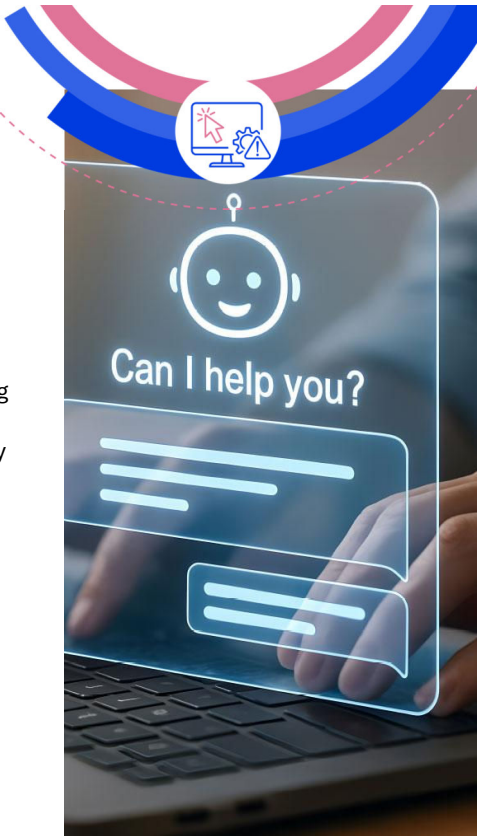
“I want to know whether the business is sufficiently in control of achieving its operational and strategic objectives”

- Are issues related to geopolitical and macroeconomic uncertainty properly reflected in the organisation’s risk framework and are proactive responses developed and tested?
- How resilient is the organisation’s supply chain strategy and third-party risk management and are they able to respond quickly to upside risks?
- How far do regulatory compliance efforts avoid costly fragmentation and prioritise long-term resilience?

DIGITAL DISRUPTION, NEW TECHNOLOGY AND ARTIFICIAL INTELLIGENCE: KEY FINDINGS

“We decided to make a lot of these tools available with safeguards around the data and then let people get on with it”

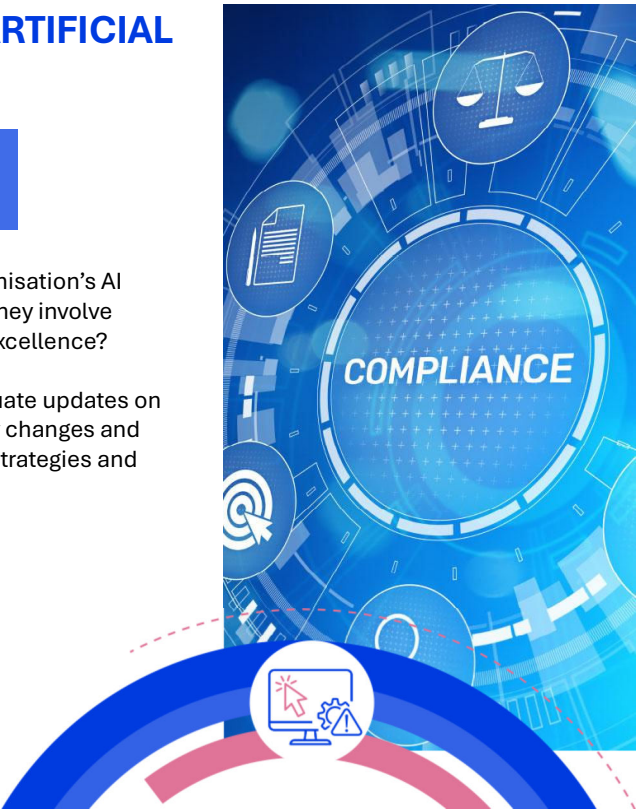
- Digital disruption, new technology and AI continued to rise, moving from 4th to 3rd in the risk rankings. CAEs were expecting to increase the time spent on the issue with 58% saying it would be a top 5 priority for them in 3 years’ time.
- Given the high speed of AI developments, organisations were concerned about vendor lock-in. Organisations were adopting a multi-provider approaches and benchmarking key services and technologies regularly. But overdependence on US providers exposed them to higher risk from geopolitical threats.
- Innovation strategies aimed to balance fast implementation with secure controls. Cutting down on the uncontrolled adoption of the generative AI was of particular concern. A key challenge is to understand how AI decision-making and results support organisational strategy.
- Geopolitical tensions spilled out into the legislative sphere with the US and Europe drawing back on regulatory frameworks. That has made the balance between innovation with AI and compliance more complex.



DIGITAL DISRUPTION, NEW TECHNOLOGY AND ARTIFICIAL INTELLIGENCE: **KEY BOARD CONSIDERATIONS**

“It’s hard to develop a strategy more than two or three quarters out, so agility and being adaptive is key at this point”

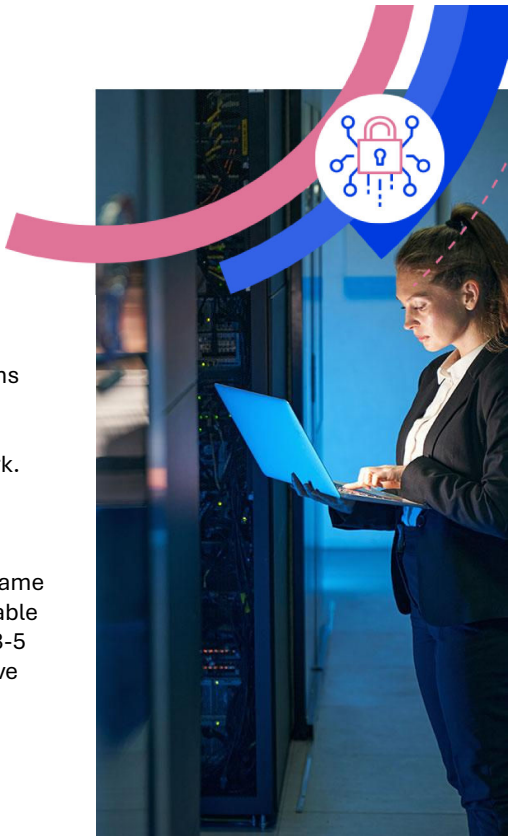
- Is the organisation’s AI strategy flexible enough to take advantage of emerging technical developments while avoiding the risk of vendor lock-in and the uncontrolled use of applications across the business?
- Does the organisation have processes that enable it to assess the quality of AI investments and assess how its results specifically contribute to the business’ strategic objectives and align with corporate values?
- How widespread are the organisation’s AI literacy programmes and do they involve multidisciplinary centres of excellence?
- Does the board receive adequate updates on global and regional regulatory changes and how those may impact its AI strategies and operations?



CYBERSECURITY AND DATA SECURITY: **KEY FINDINGS**

“Segmentation is designed to cut down the severity of an attack and improve our resilience”

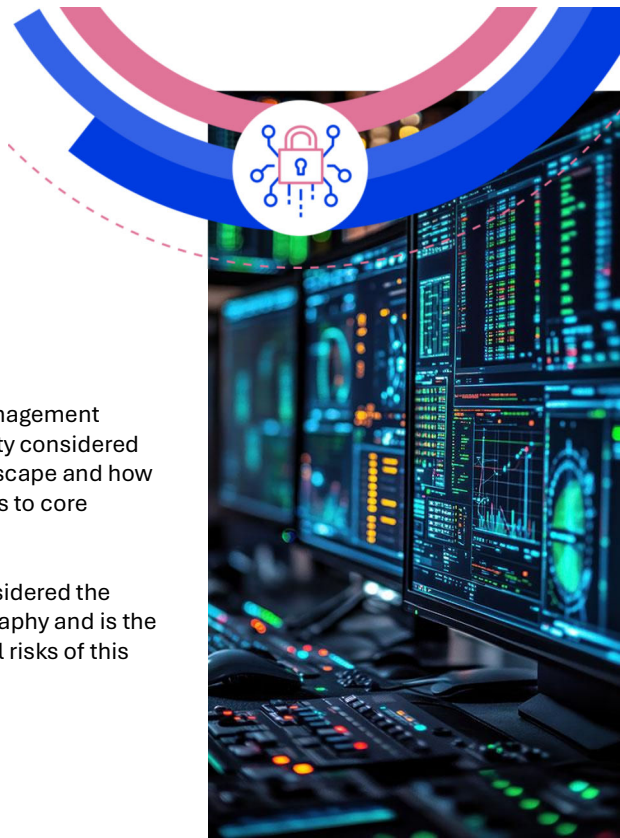
- With 82% of CAEs scoring it as a top 5 threat, cybersecurity and data security remained the biggest overall risk. CAEs described it as a constantly “emerging risk” with greater sophistication in attacks and the approaching advent of post-quantum encryption.
- Increasingly authentic phishing emails generated by AI and deepfake attacks on key personnel are rising. Recent successful breaches of systems relying on multi-factor authentication (MFA) were of particular concern.
- To reduce vulnerability, some organisations had begun to restructure their digital infrastructures by segmenting business functions to isolate them from the network. Others had strengthened security over backups.
- Post-quantum encryption algorithms became available in 2024 and commercially available quantum machines could appear within 3-5 years. As a result, some organisations have begun reviewing cryptography and key management strategies.



CYBERSECURITY AND DATA SECURITY: KEY BOARD CONSIDERATIONS

“There may no longer be sufficient time for an orderly migration to quantum-resistant algorithms, posing a significant operational and security risk to organisations”

- How dependent are key security processes on multi-factor authentication (MFA) and is the business confident that security processes around MFA are up to date and effective?
- Has the organisation’s cyber defence strategy considered the possible segmentation of physical sites or IT programs to reduce the risk of corporate takeover by hackers?
- Has the organisation’s risk management processes around cybersecurity considered the changing geopolitical landscape and how events may block future access to core systems and processes?
- How far has management considered the transition to quantum cryptography and is the board informed of the potential risks of this transition to the organisation?



HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION: KEY FINDINGS

“We are struggling to understand how senior people in future will get critical skill sets and how we can restructure those careers with AI”

- Human capital, diversity, talent management and retention retained its place as the 2nd largest threat to organisations in 2026. Turnover is high and tenure is low. AI is transforming roles, raising deskilling fears and disrupting career planning. Structural talent shortages created by population decline in Europe and an aging demographic suggests the impact of such threats could worsen.
- AI adoption has created stress and uncertainty in the workplace, CAEs said, especially in organisations where HR and AI strategies are unaligned. Businesses are responding by being transparent about the impact of AI and communicating change.
- Some businesses were struggling to strengthen career development and well-being programmes, as well as psychological safety processes – the latter being key to improving diversity of thought within the business.
- Organisations were preparing for the EU’s Pay Transparency Directive, which commences in some regions during 2026. Extended reporting on pay differences within and between roles could require more robust data systems in many businesses.



HUMAN CAPITAL, DIVERSITY, TALENT MANAGEMENT AND RETENTION: **KEY BOARD CONSIDERATIONS**

“Some organisations lacked top-level ownership of, involvement in, and strategic oversight of human capital risks”

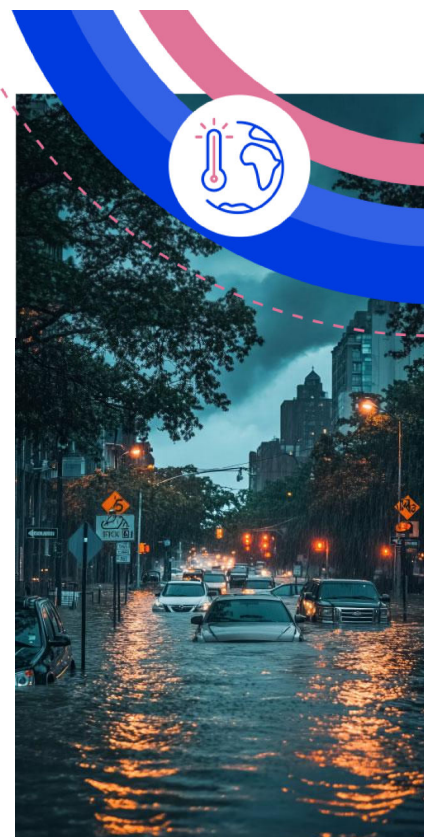
- How far is the board involved in and responsible for strategic HR planning and does responsibility sit at the right level in the organisation?
- Do emerging AI strategies and HR strategies align and are processes in place to keep them synchronised as a better understanding of the impact of technology on the workforce becomes clearer?
- How far have career planning and progression routes taken account of the impacts of digital disruption and has the organisation’s strategy – including opportunities – been clearly communicated to staff?
- How prepared are the organisation’s data and governance processes for the introduction of the EU’s Pay Transparency Directive?



CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY: **KEY FINDINGS**

“This uncertainty in policy direction in Europe and the fact that climate-related risks have too long a timescale mean that it has fallen down the agenda in many boardrooms”

- The biggest falling risk was climate change, biodiversity and environmental sustainability, dropping from 8th to place to 10th place in the risk rankings. CAEs at the roundtable expressed frustration over regulatory uncertainty shaped by changing political attitudes.
- While the European Union’s Omnibus simplification package has signalled significant deregulation, organisations were in limbo until clear details emerge.
- Double materiality assessments that seek to understand how the business and its environment impact one another were helping organisations focus on the right threats.
- Despite an overall decline in a focus on this risk, companies have increasingly found a business case for circularity in their supply chains – both to address the availability of core materials and to increase supply chain resilience.



CLIMATE CHANGE, BIODIVERSITY AND ENVIRONMENTAL SUSTAINABILITY: KEY BOARD CONSIDERATIONS

“Double materiality assessments are really important for internal auditors because they help us understand which topics to focus on”

- How well does the organisation understand the changing regulatory landscape and the potential impact of those changes on its business strategy and model?
- How well has the organisation considered the balance between potential cost savings through reduced compliance efforts and its impact on other risks, such as operations and reputation?
- How robust are the organisation’s data and governance systems for avoiding greenwashing in ESG and sustainability reporting, as well as for creating reliable double materiality assessments?
- What opportunities does the organisation have to increase circularity in its supply chain and realise the potential competitive advantages that may bring?

