Previous Updates to the Corporate Risk Register Reported to the Committee During 2025/26

- **AUDIT COMMITTEE Meeting - September 2025**

  As included within the Committee's work programme, it was planned on presenting the regular Corporate Risk Update to this meeting of the Committee. However, it is proposed to take a pragmatic approach to accommodate the various existing commitments that form part of the planned wider review of risk as set out within the AGS, including the associated training requested by the Committee. With this in mind, it is proposed to organise a 'working' session with members of the Committee outside of the formal programme of meetings, that will aim to encompass a training session alongside the planned review previously discussed. The outcome from the proposed session can therefore be considered formally if necessary at the subsequent scheduled meeting of the Committee in February 2026. Although this presents a slight delay in formally updating the Committee with regard to the Council's current risk register and associated arrangements, it is important to highlight that various underlying risk management activities remain ongoing within existing governance arrangements, which in turn are also currently being complemented by additional activities such as:

  • The review of Departmental risks as part of the Directorate / Service Planning Process along with Management Team recently reinforcing the importance of risk management at an operational and corporate level.

  • The monthly reporting of associated risks at the Regeneration and Capital Delivery Board.

  • The establishment of the Senior Officer Project Board as highlighted with the AGS, with Management Team identifying a number of key risks / projects for them to review as part of their early work programme.

  • A broader review undertaken during Management Team's regular project and performance meetings.

- **AUDIT COMMITTEE Meeting – March 2026**

Risk Management Review

Associated activities undertaken to date, involving both officers and members, has included:

- *Training provided in terms of the Role of the Audit Committee that was delivered by an external specialist trainer in January 2025.*
- *More targeted training delivered by an external specialist trainer in January 2026 based on challenging and reviewing the Council's current Corporate Risk Framework, register and approach.*
- *Following on from 2) above, a facilitated session was held with Members on 5 March 2026 to review and consider potential changes to the Council's approach.*

In terms of the training provided as highlighted in point 2) above, it covered a number of key areas including:

- *Benefits and characteristics of effective risk management*
- *Audit Committee and other members role in risk management*
- *Risk registers*
- *Appetite and tolerance*
- *Assurance and challenge*
- *Re-framing risk management*

The session also identified the characteristics of effective risk management along with a high- level view of what an assurance risk framework should ideally include, which is summarised below:

Financial Management	*Legislative Compliance*
Workforce Management / HR	*Decision Making*
Information Systems Management	*Health & Safety*
Information Governance and Compliance	*Business Continuity and ER*
Performance Management and Data	*Ethical Standards and Conduct Management*
Procurement and Contract Management	*Equalities and Inclusion*
Project and Programme Management	*Risk Mgt / Gov. Assurance*

Partnership and Collaboration Governance	*Compliance with IA, Ext Audit and Inspections etc.*

All of the above elements were reviewed and considered at the facilitated session on 5 March within the following context:

Key Background / Issue	*Current Position / Comments*
What do we do already?	*We already have in place and actively apply:* *A Code of Corporate Governance* *An Annual Governance Statement and Review* *Performance Management Reporting* *Corporate Risk Register and Framework* *Departmental Risk Registers* *Other risk / governance reviews and activities* *Internal and External Audit Inspection and Reviews. (In terms of External Audit, they concluded that the Council had effective risk management arrangements in place and there were no significant overall governance weaknesses identified within their recent VFM review)*
Our risk appetite	*Treat, tolerate not terminate*
Assurance frameworks v risk frameworks	*They ask different questions and capture different things e.g.* *RISK – Strategic risks are those risks that could materially affect a local council's ability to function effectively, achieve its statutory duties and strategic objectives,*

	or maintain financial sustainability, governance, and public confidence. *ASSURANCE - What arrangements do we rely on to ensure success, delivery, performance and compliance.* *Risks concentrate on things going wrong / failures, where assurance focuses on a positive approach of what needs to be in place etc. to ensure / provide assurance across the issues identified within the earlier table above.* *Using financial sustainability as an example:* *RISK APPROACH - There is a risk that the Council does not have sufficient funding or resources to deliver its priorities, leading to service failure and financial instability.* *ASSURANCE APPROACH - The Council has effective financial management, medium-term financial planning, budget monitoring and governance arrangements in place to ensure it can deliver its priorities and remain financially sustainable within available resources* ***What Management / Members would therefore need to seek assurance on would include:*** • *MTFS exists, is up to date, and is stress-tested* • *Budget monitoring is timely and acted upon* • *Reserves strategy is clear and aligned to risk appetite* • *Statutory officer oversight (s151) is effective*
What do other Local Authorities do and what is promoted by relevant organisations within the	*Evidence suggests that many authorities take a traditional approach adopting the same as the Council in terms of*

risk management and assurance sectors?	*identifying key risks, scoring them and how the Council is responding with inherent and residual risks highlighted. It is also fair to say that this approach aligns with many aspects of advice / guidance from sector experts.* *However, it is noted that a limited number of Council's are adopting a comprehensive Assurance Framework and 'translating' a number of their existing risks alongside other assurance elements into a fully revised assurance focused approach.*

In terms of taking the review forward and in light of the challenge proposed via the training session in January 2026, the following sets out the key issues being considered along with the context behind developing the Council's future approach:

- *The Council already has a number of key elements in place but there are opportunities to bring them together in a more coherent and accessible way.*
- *There are timely opportunities to embrace a stronger assurance based approach, albeit in a potentially hybrid way. This could also be considered as a framework that may be especially helpful in terms of promoting such an approach as part of the establishment of a new Unitary Council. It is recognised that key governance matters such as assurance and risk management practices play an important part in influencing the underlying culture of organisations which would equally apply to the successor organisation.*
- *Challenging ourselves in terms of what are strategic risks and what should be captured at a corporate level versus departmental level. With this in mind it is worth revisiting the very high-level definition of a strategic risk as follows:*

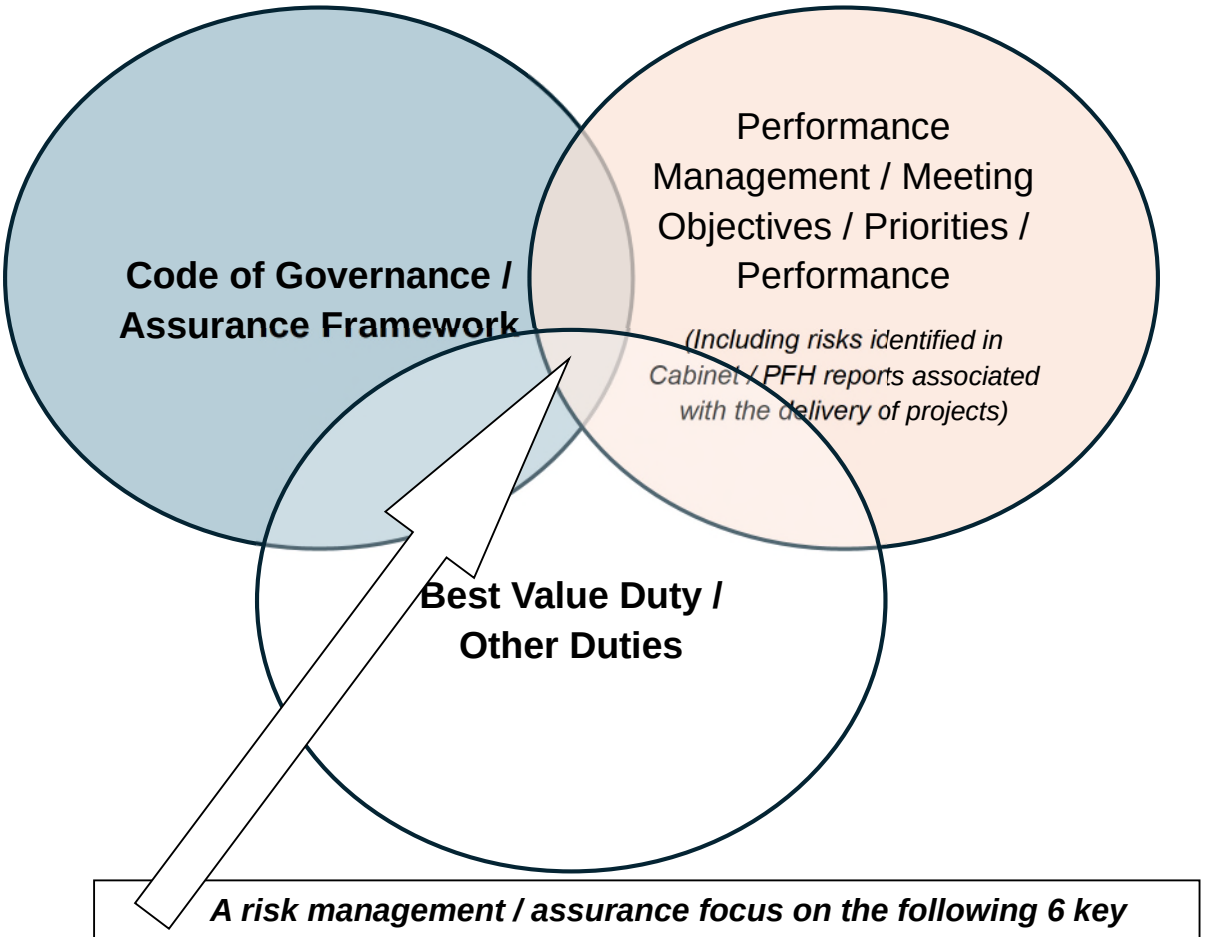
Where failure would materially impair the organisation's ability to function or deliver its purpose

- *There is still a place for maintaining a 'scoring' type approach', albeit it is recognised that this may be based on a 'traffic light' approach rather than a numerical style approach.*

- *There is a need to balance capacity, resources and effectiveness that includes 'buy-in' from Officer and Members and be complementary rather than potentially introducing a disproportionate and new 'layer' of work / bureaucracy.*

Taking all of the above into account, initial outcomes from the facilitated session held with members on the 5 March 2026 has highlighted some key elements to take forward that aim to reasonably balance the various elements of good governance and its effectiveness.

The following chart helpfully sets out the underlying structure / approach being proposed for further development:



A risk management / assurance focus on the following 6 key strategic risks:

1. Financial Sustainability
2. Workforce Capacity & Resilience
3. Cyber, Data and Information Security
4. Business Continuity and Organisational Resilience
5. Management of Assets
6. Governance and Decision Making

Ensuring a coherent two-way 'relationship' / 'cascade' to Service Plans / Departmental Risks and Key Business Continuity Activities

As reflected in the recommendations [above], officers plan to develop the approach further with the aim of presenting the proposed revised assurance and risk management framework to the next meeting of the Committee in June. This may include further facilitated sessions with Officers and Members during the interim period to ensure a timely implementation and embedding of the revised approach as early as possible in 2026/27.

Notwithstanding the above, it is acknowledged that the Committee have not been presented with a full risk register report since January 2025, albeit updates were provided in September 2025 as necessary. It is therefore important to provide the Committee with the assurance that various underlying risk management activities remain ongoing within existing governance arrangements, which in turn are also currently being complemented by additional activities such as:

- *The review of Departmental risks as part of the Directorate / Service Planning Process along with Management Team reinforcing the importance of risk management at an operational and corporate level.*
- *The monthly reporting of associated risks at the Regeneration and Capital Delivery Board.*
- *The establishment of the Senior Officer Project Board last year as highlighted with the AGS.*

Within the context of the above there are no major issues to bring to Audit Committee's attention at the present time. It is however important to highlight the current four 'red' rated residual risk items, as follows:

Risk	***Status / Comments / Update***
RISK 1d - Ineffective Cyber Security Physical and Application (software) Based Protection Management	*The network infrastructure hardware was replaced during 2025 and has a realistic end-of-life longevity of 5-7 years (2030 – 2032). The Cloud Infrastructure provides significantly enhanced resilience / recovery capabilities in terms of hardware failure. Remote working capabilities provides key business continuity and service delivery options if / when key office locations are unavailable. Cyber-security arrangements include 24/7 network visibility, monitoring, reporting and alarms together with a 24/7 Security Operations Centre (SOC) provided by a 3rd party – all facilitating both reactive and pro-active response. The greatest cyber-security protection is afforded by*

	the Council's adoption of managed-device only access to services with zero-trust real-time monitoring of devices for vulnerabilities. Cyber-security is robust but it is recognised that any breach could be significant in terms of service loss and / or data theft.
RISK 2a - Coastal Defence	*Associated risks continue to be mitigated via conducting annual inspections of coast protection structures and responding swiftly to public reporting of minor faults. An annual maintenance programme for the coastal frontage is set each year, supported by associated surveys as necessary, with an appropriate budget to cover the works (one-off funding of £2m was set aside to support such works). Each year sections of the sea defences are also improved as part of a rolling programme of special maintenance schemes funded from an ongoing revenue budget.*
RISK 5A - Financial Strategy	*A robust and sustainable two -year financial plan was agreed by Full Council in February 2026. This included 'cash-backed' investment and responses to a number of financial challenges along with setting out an in-principle / notional approach to meeting obligations to a new Unitary Council from as early as 1 April 2028.*
RISK 6a - Loss of sensitive and/or personal data through malicious actions loss theft and/or hacking.	*As Data Controller, the Council has a legislative duty to evidence and ensure that information is managed / protected in compliance with legislation and protected against unauthorised or unlawful processing and against accidental loss / destruction / damage through using appropriate security. The Council achieves this and mitigates risk of data-breach by: mandatory Data Protection and Cyber Security training, working*

	collaboratively with other local authorities sharing best practices and aligning policies and procedures and ensure consistent governance, improving information governance systems, maintaining a Records of Processing Activities [ROPA], improvements to Security Incident Reporting systems, improving information governance guidance for staff through improved intranet pages, having robust data sharing agreements where partner organisations are managing data on behalf of the Council. *All of the above, together with robust cyber-security, mitigate this risk, as far as reasonably possible, to the organisation.*