CEREDIGION COUNTY COUNCIL

Report to: **Governance and Audit Committee**

Date of meeting: **3 June 2021**

Title: **Internal Audit Report – Risk Management**

Purpose of the report: **To inform Members of the findings and assurance provided following the recent internal audit of the Risk Management Framework within the Council**

Cabinet Portfolio and Cabinet Member: **Cllr Ray Quant MBE, Deputy Leader of the Council and Cabinet Member for Legal and Governance, People and Organisation, and Democratic Services**

The Internal Audit Section recently reviewed the Council's Risk Management Framework and the supporting corporate procedures in place during the 2020/21 financial year.

Only minor actions were identified, one of which was actioned immediately, resulting in the Internal Audit Section providing high assurance that there is a sound system of controls, governance and risk processes in place.

Recommendation: **To note the contents of the report**

Reasons for decision: **That the Members are informed of the outcome of the audit**

Appendices: Internal Audit Report – Risk Management

Head of Service: Elin Prysor
CLO-Legal and Governance / Monitoring Officer

Reporting Officer: Amanda Roberts
Corporate Manager – Internal Audit

Date: 16 March 2021

GWASANAETHAU CYFREITHIOL A LLYWODRAETHU

LEGAL & GOVERNANCE SERVICES

GWASANAETH ARCHWILIO MEWNOL

INTERNAL AUDIT SERVICE

Cyngor Sir
CEREDIGION
County Council

ADRODDIAD ARCHWILIO – AUDIT REPORT

Corporate Risk Management and Framework Procedures

Report Prepared by: Neal Wellens, Auditor

Report Approved by: Amanda Roberts, CMIA

Date of Issue: 15 March 2021

INTERNAL AUDIT REPORT

Corporate Risk Management and Framework Procedures

EXECUTIVE SUMMARY

A review has recently been undertaken to evaluate the Council's risk management procedures, including the risk management framework and the corporate risk register. Testing was undertaken for the financial year 2020/21 from which a few issues are brought to your attention.

On the whole, most of the areas checked were found to be satisfactory, for example good formal management and reporting structures are in place, and a nominated CLO has overall responsibility for the process.

Only minor issues have been noted in the Action Plan below, which enables the Internal Audit Section to continue to provide high assurance that there is a sound system of control, risk and governance in the corporate risk management and framework procedures.

Due to the current circumstances, audit reviews and testing have been limited to areas requiring least staff input.

OBJECTIVE

The main objective of the assessment was to inform the Corporate Lead Officer – Policy, Performance & Public Protection, of Internal Audit's evaluation of the Council's corporate risk management and framework arrangements.

AUDIT APPROACH

The assessment was designed to evaluate the attainment of specific standards. These are the standards set out by the Chartered Institute of Public Finance and Accountancy, and other policies issued. In doing so, Internal Audit has:

- Examined key documents and policies relating to the risk management procedure, and
- Reviewed the procedures employed by the Council with regard to its approach to risk management.

SUMMARY OF FINDINGS

The main findings in relation to the areas audited are set out below:

KEY	✓ = Findings Satisfactory	• = Action Recommended

Audit Area	Findings
Corporate policies and procedures that have an impact on risk management	✓ Core policies, codes and procedures are in place, regularly updated and communicated well. ✓ The links to some documents don't always work on Cerinet – this has been reported to officers to update. • The risk management framework is currently unavailable via Cerinet, and access on the Council website is via Committee agendas only. **(See Action Plan – point 1 below)**
Formal management and reporting structure	✓ Management and reporting structures are clear, well-defined and well communicated via Cerinet and the Council website. An explanation of the structures in place forms part of the induction for new employees.
Human Resources and information security policies and procedures	✓ The Council has a comprehensive set of HR and information security policies & procedures to support risk management to include a DBS/Safe recruitment Policy, and an appraisal scheme for all employees.
Strategic objective setting	✓ The Council has a clearly defined vision supported by four corporate priorities as documented in the Corporate Strategy, which has been approved by Council. ✓ Risk management is embedded within the Council's objective setting process and implementation.
Recording of objectives	✓ The Wellbeing of Future Generations Act 2015 ensures that all objectives and strategies are fully risk assessed, cascaded down and comply with the associated requirements.
Actioning strategies and risk responses	✓ Management reviews of both service and staff performance ensure that strategies and risk responses are actioned appropriately.
Effectiveness of risk management	✓ The Council has established a formal risk management reporting process. ✓ Risk management is considered as part of the annual corporate governance review. ✓ Newly identified risks are referenced and proposed eg RO16 re Brexit and RO18 re pandemic. ✓ The framework clearly demonstrates the Council's commitment to risk management with a thorough and definitive procedural overview.

Audit Area	Findings
Risk assessment process	✓ Each risk has an 'owner' who is responsible for managing it. ✓ The corporate risk register is updated quarterly and is reported regularly to Leadership Group and Audit Committee for information / monitoring. • The risk register details each risk, its score (current and over the past year), scoring matrix, associated hazards & any evidence of them occurring, mitigating actions and their status; however, it doesn't clearly distinguish between inherent and residual risk. **(See Action Plan – point 2 below)**
Communications that support risk management	✓ Communication is frequent between different services, management, the Leadership Group and Members. ✓ Audit Committee usually meets 6 times a year, where the corporate risk register is a standing agenda item, as well as internal audit matters. ✓ Gold Command was set up to enable swift decisions regarding the COVID-19 pandemic, which are communicated in a 'roadmap' on the website.
Identification of Hazards	✓ The Framework gives a detailed overview of the 'Risk Identification' stage of the risk assessment process. ✓ Council's Collaboration List (November 2019) notes the identified risks for each partnership. • Hazards are not strictly classified or categorised into relevant PESTLE categories in the risk register, although the potential consequences are often described as being financial, legal, social etc. **(See Action Plan – point 3 below)**
Impact and Likelihood of Hazards Occurring	✓ The Framework gives both a brief overview of the risk matrix, as well as a more detailed breakdown as to what constitutes each level of impact. • Risk management procedure requires threats to be recorded & assessed; however, positive effects are not always noted in the risk register. **(See Action Plan – point 4 below)**
Responsibility and commitment to risk management	✓ Risks that are scored 5 or above (medium) are required to be entered into the corporate risk register. ✓ The CLO for Policy, Performance and Public Protection is responsible for risk management as a whole, while individual risks are assigned to the appropriate CLOs. • Risk management training has been rolled out to Management and Members; an e-learning package is available, but is not compulsory for employees. **(See Action Plan – point 5 below)**

Audit Area	Findings
Information Gathering	✓ Information to support the risk management process is frequently and effectively gathered, shared and acted upon through a number of means.
Monitoring and Evaluating Risk Management	✓ Risk framework and register are regularly presented to Leadership Group and Audit Committee. ✓ Managers may be called to Audit Committee if planned mitigating actions are not put in place, and/or a failure has occurred in a system.
Information Controls	✓ The Council has an extensive, clearly defined and well communicated set of information and data protection procedures (all but one have been reviewed/created within the last 2 years). ✓ All policies are available via Cerinet

Where improvement opportunities have been identified, the required actions have been reported in the Action Plan below.

I wish to thank the Corporate Lead Officer – Policy, Performance & Public Protection and the Corporate Manager – Partnerships & Performance for their input to the action plan in order to finalise the audit.
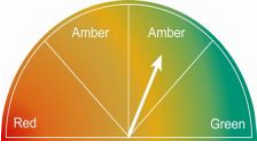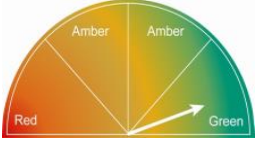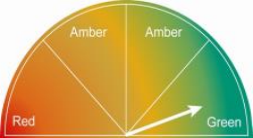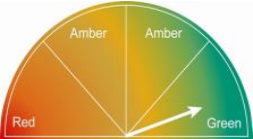
MAR/NW/Risk
15 March 2021

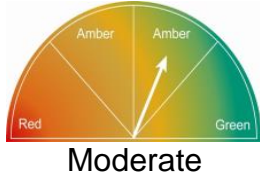_____
Corporate Manager - Internal Audit

<u>Report Distribution</u>
Alun Williams, Corporate Lead Officer – Policy, Performance & Public Protection
Diana Davies, Corporate Manager – Partnerships & Performance
LG/AC/AW

ACTION PLAN

Ref	Finding and Associated Risk	Action Required and Priority	Service's Comments, Target Date & Responsibility
1	**Corporate Policies and Procedures** There is no link within Cerinet to the risk management framework, which can only be accessed via Committee agendas on the Council's website. **Risk**: Risk management framework not easily accessible; staff have less awareness which could result in non-compliance.	The risk management framework should be available to view bilingually on Cerinet, along with a link on the Council website (or vice versa) to ease accessibility. Moderate	**Comments**: Already actioned. The risk management documents are now easily available on the Council website.
2	**Monitoring Risk Responses** The framework and risk register do not distinguish between inherent and residual risk. However, the risk register does contain a chart for each risk which details the past scores of the risk over a set time period. **Risk:** Over/underestimating the threat a risk poses; no measure as to how effective mitigation strategies have been.	Ideally, inherent and residual risks should be noted to estimate the outcome of planned mitigating actions; and to provide a fuller understanding of the impact of any change, by evaluating the effectiveness of any mitigation strategies implemented. Merits Attention	**Comments**: Accept as good practice.

Ref	Finding and Associated Risk	Action Required and Priority	Service's Comments, Target Date & Responsibility
3	**Identification of Hazards** Hazards are not strictly classified or categorised into relevant PESTLE (Political, Economic, Social etc) categories in the risk register, although the potential consequences are often described as being financial, legal, social, etc. **Risk:** The hazard may not be evaluated from the six unique standpoints, resulting in some risks being missed.	Ideally, all issues should be evaluated using the PESTLE categories and noted in the risk register to confirm potential hazards have been considered / identified from all six standpoints. Merits Attention	**Comments**: Accept as good practice.
4	**Impact and Likelihood of Hazards Occurring** Positive impacts of risks are not always noted in the way negative impacts are recorded. **Risk:** Opportunities not recorded.	Potential positive impacts could be included in the corporate risk register, to ensure that any opportunities are acted upon in order to gain maximum benefit for the Council, and its residents. Merits Attention	**Comments**: Accept. Could be useful as we do tend to concentrate on the negative, rather than the positive issues.

Ref	Finding and Associated Risk	Action Required and Priority	Service's Comments, Target Date & Responsibility
5	**Responsibility and Commitment to Risk Management** Training in risk management is only compulsory for Management and Members. Other members of staff have the option of an e-Learning module. **Risk:** May result in a lack of understanding leading to the possibility of key risks being missed and not dealt with appropriately.	Consideration could be given to making the risk management e-learning training module mandatory for all employees, to ensure all staff are aware of what to do when encountering a hazard that may may become a threat to the Council. Moderate	**Comments**: Risk management is a tool for managers and whilst interesting for other staff it is not a training priority over operational matters.

Guide to the assurance criteria used:

Level:	High	Substantial	Moderate	Limited
Adequacy of Controls:	Controls in place to ensure achievement of service objectives and to protect Council against significant foreseeable risks. No fundamental weaknesses found.	Controls in place to ensure achievement of service objectives and to mitigate significant foreseeable risks. Some areas of improvement identified.	Controls in place to varying degrees. Gaps identified which leaves service exposed to certain risks. Improvement required.	Controls considered insufficient. Need to strengthen procedures significantly and ensure compliance.
Risks:	Minor risks only.	Opportunity exists to improve on risk exposure.	Need to introduce additional controls and/or improve compliance.	Failure to improve controls leaves Council exposed to significant risk (major financial loss, reputation, failure to achieve service's key objectives).
Guide:	No fundamental or significant actions required.	No fundamental actions required. Limited significant actions.	Number of significant actions.	Number of fundamental / significant actions.
Follow-up required:	Initial audit only.	Follow-up of any significant actions only / self-assessment with samples to evidence compliance.	IA follow-up with sample tests undertaken to ensure all actions implemented, and to re-assess assurance.	IA follow-up with full testing undertaken to ensure all actions implemented, and to re-assess assurance.

Guide to the classification of actions used:

Classification of Actions

Fundamental	Significant	Moderate	Merit Attention
Weakness that is crucial to the management of risk within the service. Needs to be notified and requires the attention of the CLO.	Important findings that identify non-compliance with established procedures that could lead to a risk of financial / reputational loss to Service.	Findings that identify non-compliance with established procedures but do not represent any major risk of financial / reputational loss to Service.	Items requiring little or no action. Included as may be of interest to service or best practice advice.