CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE
Tuesday 7th May 2024

REPORT AUTHOR:	**County Councillor Cllr David Thomas** **Portfolio Holder for Cabinet Member for Finance and Corporate Transformation**
REPORT TITLE:	**Strategic Risk Register Report Quarter 3 2023/2024**

REPORT FOR: **Decision**

1. Purpose

1.1 The purpose of this report is to set out the Council's latest position on managing its key risks, contained in the Strategic Risk Register (SRR).

2. Background

2.1 Our Strategic Risk Register is key to safeguarding the organisation and building resilience into our services. At a time when the Council has faced and is still facing tough challenges, the effective management of risk is needed more than ever. A risk-managed approach to decision making will help us to achieve the well-being objectives in Stronger, Fairer, Greener: Our Corporate plan, deliver services more efficiently and using innovative and cost-effective means.

3. Advice

3.1 To ensure a risk managed approach to decision making and good governance of the Council, it is proposed that Cabinet.

- Review progress to mitigate strategic risks
- Review SRR proposals

Review of progress to mitigate Strategic Risks

3.2 As at the end of quarter 3 2023-2024, there are 13 risks on the strategic risk register and all strategic risk owners have provided a short summary of progress since last quarter, to give assurance that mitigating actions are being actioned and monitored.

3.3 Please see appendix A for full details of the 13 strategic risks including the mitigating actions identified to control them and progress reviews.

3.4 Please see appendix B to view a heat map which presents the results of the quarter 3 risk assessment process visually. It highlights (for the residual risks) the following:

One has a probability of ‘almost certain’ and an impact of ‘major’, three have a probability of ‘likely’ and an impact of 'major' and three have a probability of ‘likely’ and an impact of 'severe'.

3.5 During Qtr. 3 the following risks have changed their probability or impact:

FIN0001: IF the Council is unable to deliver a financially sustainable budget over the short and medium term, THEN the Council will not be financially resilient.
Impact change: major to severe
Score: gone up to 20

PROC0008: IF global supply chain issues arise such as Political, Economic or Environmental pressures affect the global market THEN this could lead to increased price variations and/or labour & material shortages.
Probability change: possible to unlikely
Score: moved down to 6

HTR0018: IF we do not take action to address the nature emergency declared by Powys County Council THEN the impact of this emergency will affect our ability to deliver future services.
Impact change: major to severe
Score: gone up to 20

And RCPCH0007: Failure to complete process to secure agreement for service continuation has been closed.

<u>Escalation of risk to the Strategic Risk Register</u>

3.6 Digital services would like to escalate the following risk:

ICT0067: If we receive and act upon a phishing email THEN there is a risk that our information and systems will be vulnerable to a cyber-attack. Rating score 16 (risk profile of ‘likely’ and ‘major’).

Phishing emails are the route cause of the majority of Cyber attacks experienced by any organisation. Gloucester City council’s Cyber-attack in December 2021 was caused by a spear phishing email which enticed the recipient to click on a malicious link and download malware, resulting in a large-scale Ransomware attack, costing the Authority in excess of £1.14M.

Everyone everywhere is experiencing a rise in the amount of phishing emails being received. What is now more convincing is the rise of Business Email Compromise which in turn is generating phishing emails

from known contacts. Spear Phishing and Whaling are a type of attack which target high profile staff members such as CEO's and Chief financial Officers.

Phishing emails can be received by any member of staff in any service area, including elected members and improved awareness at a corporate level is needed. Those with public profiles and publicly available email addresses are more likely to receive phishing and targeted phishing (Spear phishing) emails. It affects the entire authority and is not specific to Digital Services staff. The consequences of a phishing email can result in any member of staff being the conduit to a cyber incident and/or information security incident which can impact part of, or the whole of the authority at any time, exposing confidential data belonging to any number of service areas. In a worst-case scenario, a serious cyber security incident caused by a phishing email could result in multiple council systems being unavailable affecting the entire authority and its customers and service users.

Whilst the Digital Services department takes responsibility for trying to reduce and eradicate phishing emails from entering the authorities email system, and also by implementing training and awareness campaigns amongst other technical security controls to reduce the risk of cyber-attacks, the consequence of a successful cyber incident caused in the first part by a phishing email could affect the whole authority.

During 2023 PCC there have been 2 instances (that we are aware of) where our staff have been convinced by a phishing email they received and as such we experienced 2 Cyber incidents as a result. Thankfully no serious consequences this time although costs were incurred in resources to investigate, remediate and report the incidents. We consider ourselves lucky there was no serious impact this time, but the risk is still present and therefore needs escalation to ensure it remains a corporate priority to address it.

4. Resource Implications

4.1 There are no direct resource implications in relation to this report however all risk owners need to consider the resource implications of managing the risk and decide if the best course of action is to tolerate or treat.

4.2 The Strategic Risk Register outlines the key risks to the Council's activities, as well as risk to delivery of objectives contained within the Corporate Improvement Plan. There are no direct financial implications from the report although these may arise as new risks are identified on an on-going basis.

The Head of Finance (Section 151 Officer) notes the comment above, financial implications are identified through the relevant service and are considered through the financial management processes in line with the

authority's financial regulations. All services are considering the financial impact of any risks that are expected to continue into 2023/24 and beyond in their Service Integrated Business Plans.

5. Legal implications

5.1 Legal: Comment sought

5.2 The Head of Legal Services and the Monitoring Officer has commented as follows: Comment sought

6. Climate Change and Nature Implications

There is a strategic risk regarding climate and another on nature. Both topics are considered by all services when assessing and managing risk.

7. Data Protection

7.1 N/A

8. Comment from local member(s)

8.1 N/A

9. Integrated Impact Assessment

9.1 N/A. The Service Risk Register is not setting out any changes or proposals to service delivery.

10. Recommendation

It is recommended that Cabinet notes the current Strategic Risk Register and is satisfied with progress against mitigating actions for quarter 3, approves the escalation of ICT0067 (detailed under point 3.6).

The recommendation above will ensure:

- **Appropriate understanding and management of strategic risks which could prevent us from achieving our objectives**
- **A risk managed approach to decision making and good governance of the Council**

Contact Officer: Jane Thomas, Head of Finance

Tel: 01597 827789

Email: Jane.Thomas@powys.gov.uk

Head of Service: Jane Thomas, Head of Finance Corporate Director: Emma Palmer, Chief Executive officer.

CABINET REPORT NEW TEMPLATE VERSION 3