**AGENDA ITEM NO 9**

**REPORT NO 20/24**

**ANGUS COUNCIL**

**SCRUTINY AND AUDIT COMMITTEE – 23 JANUARY 2024**

**DETAILED RISK REPORTING TO SCRUTINY AND AUDIT COMMITTEE**

**REPORT BY CATHIE WYLLIE – SERVICE LEADER - INTERNAL AUDIT**

## ABSTRACT

This report presents detailed risk information to the Scrutiny and Audit Committee in line with the programme agreed by the Scrutiny and Audit Committee in June 2023 (Report 175/23/ refers).

## 1. RECOMMENDATIONS

It is recommended that the Committee:-

(i) scrutinise and note the information presented about the IT Resilience and Cyber Attack (Business Continuity) risk; and

(ii) Agree to amend the programme to include the Performance Management risk for discussion in March 2024, or propose an alternative risk from those noted at 4.3 below.

## 2. ALIGNMENT TO THE COUNCIL PLAN

The contents of this report, and the related presentation provide the Committee with a deeper understanding of a key corporate risk that may prevent achievement of the Council Plan, and the steps being taken to mitigate the risk.

## 3. BACKGROUND

The following timetable for individual risk presentations, based on the Corporate Risk Register at 9 May 2023, was agreed for 2023/24:

| S&A meeting date | Lead officer | Risk to be presented | Risk Score May 2023 | Risk Score Updated | Risk Target |
|---|---|---|---|---|---|
| 22 Aug. 2023 | Director of Finance | Financial Sustainability | 25 | | 9 |
| 26 Oct. 2023 | Director of Legal & Democratic Services | Legislation | 9 | 6 (October 2023) | 6 |
| 28 Nov. 2023 | Chief Executive | Transforming for the Future | 15 | | 6 |
| **23 Jan. 2024** | **Director of HR, Digital Enablement, IT & Business Support** | **IT resilience & Cyber-attack (Business Continuity)** | **16** | | **8** |
| 7 March 2024 | TBC | National Care Service (if included in CRR by then) | TBC | | TBC |

| | | | | | |
|---|---|---|---|---|---|
| 23 April 2024 | Director of Vibrant Communities and Sustainable Growth | Climate Change | 16 | | 12 |

## 4. CURRENT POSITION

4.1 There will be a short presentation at Committee on the IT resilience & Cyber-attack (Business Continuity) risk. The related information from the Corporate Risk Register is included in Appendix 1.

4.2 There have been no changes to the Corporate Risks since the last Scrutiny and Audit Committee meeting on 28 November 2023.

4.3 The National Care Service was previously flagged as an emerging risk and planned for presentation to the Committee in March 2024. It has not yet been expanded on in the risk register and therefore will not be discussed at Committee. The table below includes the current risks in the register that were not selected for this year's programme and therefore have not been discussed this year so far. Based on the fact that it has not been discussed before and is above target, it is proposed that the Performance Management risk is discussed at the March 2024 meeting.

| **Corporate Risk** | **Risk Score May 2023** | **Risk Score Target** | **Last discussed at Scrutiny and Audit Committee** |
|---|---|---|---|
| Performance Management | 6 | 4 | Not discussed |
| Partnerships | 9 | 6 | October 2022 |
| Information Governance | 8 | 8 | Not discussed |
| Public Protection | 8 | 8 | Not discussed |
| Health & Safety Compliance | 12 | 6 | March 2023 |

## 5. FINANCIAL IMPLICATIONS

There are no direct financial implications.

## 6. EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment is not required, as this report does not impact on people. It does not impact on people because this report provides information about risks and their mitigation. Any people impact would be dealt with at other active stages of risk mitigation if applicable.

**Background Papers**

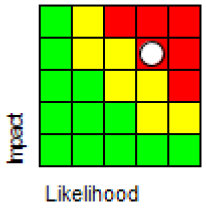
**NOTE:** One background paper as defined by Section 50D of the Local Government (Scotland) Act 1973 (other than any containing confidential or exempt information) was relied on to any material extent in preparing this report.

**Report 218/23 Corporate Risks and Risk Management**

**REPORT AUTHOR** Cathie Wyllie – Service Leader Internal Audit
EMAIL DETAILS ChiefExec@angus.gov.uk

List of Appendices:
Appendix 1- Corporate Risk Register – IT resilience & Cyber-attack (Business Continuity)

Appendix 1



CORRR0019 IT Resilience & Cyber Attack (Business Continuity)

**Risk Description**

Interruption to service or inability to provide IT services due to loss of the data centre and/or other critical infrastructure components caused by factors such as fire, vandalism, cyber-attack, equipment malfunction.

| **Likelihood** | **Potential Impact** |
|---|---|
| There are resilience and protections in place however there are a number of circumstances where significant damage to the data centre or other critical infrastructure (cloud, hosted or connectivity) components is possible. Cyber-attacks are becoming increasingly common with government and public sector organisations targeted regularly. | Work is being done around the Recovery Time Objectives (RTO's) in our business continuity plans to ensure that they are realistic in relation to available IT resources and time. A number of business critical systems on which the council is wholly dependent to provide services could take several days to recover.<br>As more and more critical systems traditionally delivered by on the premises client / server model move to internet-based delivery and the number of devices and locations being used to access council data assets from outside the corporate network increases, so does the exposure to malware and malicious threat actors and the risk of a successful attack is more likely. The impact of a successful ransomware attack is significant data loss, inability of organisation to function at all in the short term and significant disruption to services over many months. The costs incurred are likely to be in the range £10Ms. |

**Existing Controls**

| | |
|---|---|
| Project being implemented to provide automatic switch over | For email and other core components to switch to the use of the secondary site in Arbroath |
| Implementation of Office365 has improved resilience for all services | |
| Regular and tested data back-up and recovery | |
| Business Continuity plans for all critical services | |
| Regular maintenance of physical environment and equipment | |
| Regular review of security standards | |

| |
|---|
| PSN accreditation |
| Council wide Application Strategy in place. |
| Council wide Application Strategy approved and in place. |

| | |
|---|---|
| **Risk Likelihood Score:** | 4 |
| **Risk Impact Score:** | 4 |
| **Overall Risk Score:** | 16 |

**Additional Controls/Actions to Reduce Likelihood and/or Impact Scores**

| Controls/Actions | | Due Date | Status | Desired Outcome | Owner | Latest Update | Date |
|---|---|---|---|---|---|---|---|
| AC-COR-00035 Ongoing review of new threats and counter measures | | 31-Mar-2024 | ▶ In progress | Improved security and resilience | Service Leader – Digital Enablement & IT | Ongoing Action. Cyber threats are reviewed regularly by the network and security team with additional mitigations put in place as cyber threats evolve. | 07-Dec-2023 |
| AC-COR-00075 Address outstanding actions from automated failover testing | including automation of active directory fail over and review of Hybrid Exchange | 31-Mar-2024 | ▶ In progress | Increased automated resilience | Service Leader – Digital Enablement & IT | Many services have migrated to a Amazon Web Services (AWS), a public cloud environment. This cloud environment provides a high level of redundancy and resilience. For the remaining on-premise services, failover is successful, albeit with some manual steps. | 07-Dec-2023 |
| AC-COR-00076 Implement Security Operations Centres (24/7) | as per business case and options appraisal provided to CLT. | 31-Mar-2023 | ✓ Completed | 24/7 alert response reducing risk of effective cyber attack against the organisation. | Service Leader – Digital Enablement & IT | We have partnered with Brightsolid to implement a Managed detection and response (MDR) service that provides a 24/7 SOC. This is now up and running and we are evaluating the effectiveness. | 19-Jul-2023 |
| AC-COR-00077 Regularly review implementation of actions from SEPA gap analysis programme | Proposed technical, process, and people change actions. Managed by Digital Strategy Board. | 31-Mar-2024 | ▶ In progress | Improved security and resilience | Service Leader – Digital Enablement & IT; Manager - Risk, Resilience & Safety | Actions and improvements are constantly being implemented In line with the National Cyber Security Centre (NCSC) best practice. This includes the imminent launch of Multi- | 07-Dec-2023 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | Factor Authentication (MFA) following successful testing. | |
| AC-COR-00078 Implement and monitor cyber training and awareness across the organisation | includes phishing, cyber incident response. Cyber incident playbooks for technical staff. | 31-Mar-2024 | ▶<br>In progress | Cyber incident response training for senior leaders and all other relevant resources. Improved security and resilience. | Service Leader – Digital Enablement & IT | Additional courses to be added to the new LMS system recently implemented. | 19-Jul-2023 |
| CORRR_0019.2 Where appropriate avoid the risk by provisioning the services differently. | This is an ongoing action as applications are moved to the cloud. | 31-Mar-2024 | ▶<br>In progress | Different approaches taken in the provision of IT services | Service Leader – Digital Enablement & IT | The ACDC project is progressing with services now live in public cloud (AWS) environment. This provides additional security benefits. We have also migrated software applications to the vendors fully managed service (SaaS) which also enables improved security mitigations. The aim is to have the majority of services hosted in AWS or with vendors SaaS offering with a view to closing our datacentres. | 19-Jul-2023 |
| CORRR_0019.3 IT will review, with the service units, the RTO's against estimates of recovery time and agree priorities for actions. | This is an ongoing action as applications are moved to the cloud. | 31-Mar-2024 | ▶<br>In progress | List of agreed prioritised actions | Service Leader – Digital Enablement & IT | | |

| | |
|---|---|
| **Target Likelihood:** | 2 |
| **Target Impact:** | 4 |
| **Overall Target Score:** | 8 |

| | |
|---|---|
| **Risk Owner:** | Sharon Faulkner, Director of Human Resources, Digital Enablement and Business Support |

| **Latest Update** | **By** | **Date** |
|---|---|---|
| Risk reviewed and updated. No change to score. | Alison Frew | 19 Jul 2023 |