

ANGUS COUNCIL

SCRUTINY AND AUDIT COMMITTEE – 31 JANUARY 2023

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 2022 (Report 163/22 refers) and confirmed in August 2022 (Report 207/22 refers).

1. RECOMMENDATIONS

It is recommended that Committee:

- (i) Scrutinise and note the information presented about the IT resilience & Cyber-attack (Business Continuity) risk, and
- (ii) Confirm any changes to the program of risk reporting in Section 3 in light of the changes noted at 4.2.

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 17 May 2022, was agreed for 2022/23.

S&A meeting date	Lead officer	Risk to be presented	Risk Score May 2022	Risk Target	Revision
23 August 2022	Director of Finance	Financial Sustainability	20	9	December 2022 Score 25
27 October 2022	Director of Strategic Policy, Transformation & Public Sector Reform	Partnerships	12	9	August 2022 Score 9 Target 6
29 November 2022	Chief Executive	Transforming for the Future	9	6	October Score 15
31 January 2023	Director of HR, Digital Enablement, IT & Business Support	IT resilience & Cyber-attack (Business Continuity)	16	8	
9 March 2023	Depute Chief Executive	Health & Safety Compliance	12	6	December 2022 Score 9
25 April 2023	Director of Vibrant Communities and Sustainable Growth	Climate Change	16	12	

4. CURRENT POSITION

- 4.1 There will be a short presentation 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 the following changes to the Corporate Risks since this was last reported to the November 2022 Scrutiny & Audit committee in Report number 399/22.:
- Financial Sustainability risk score has increased to 25
 - Health & Safety risk score has reduced to 9

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

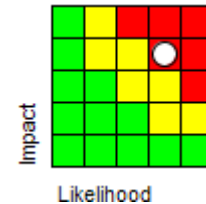
NOTE: No background papers as defined by Section 50D of the Local Government (Scotland) Act 1973 (other than any containing confidential or exempt information) were relied on to any material extent in preparing this report.

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

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.

Potential Impact

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. 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-2023	 In progress	Improved security and resilience	Service Leader – Digital Enablement & IT	Action is ongoing. Regular review of cyber threats by the Network & Security team and consideration/implementation of additional measures where appropriate.	12-Dec-2022
AC-COR-00075 Address outstanding actions from automated failover testing	31-Mar-2023	 In progress	Increased automated resilience	Service Leader – Digital Enablement & IT	As we transition our services to the cloud, the reliance on our on-premise infrastructure is reduced. For our current on-premise infrastructure, failover testing for all services is successful but there are a few manual steps to perform, mainly relating to DNS and Active Directory.	12-Dec-2022
AC-COR-00076 Implement Security Operations Centres (24/7)	31-Mar-2023	 In progress	24/7 alert response reducing risk of effective cyber-attack against the organisation.	Service Leader – Digital Enablement & IT	Extensive work to determine requirements and understand suitable suppliers. Budget requested for 23/24 and embarking on a free proof of concept with our existing datacentre provider to deliver a fully managed Security Operations Centre (SOC) and Security Information and Event Management (SIEM) service.	12-Dec-2022

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-2023	 In progress	Improved security and resilience	Service Leader – Digital Enablement & IT; Manager - Risk, Resilience & Safety	Action is ongoing. There are regular reviews of the actions from the SEPA gap analysis. This work is managed by the Strategic Digital Board.	12-Dec-2022
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-2023	 In progress	Cyber incident response training for senior leaders and all other relevant resources. Improved security and resilience.	Service Leader – Digital Enablement & IT	4 x Cyber Security Courses in Always Learning but not mandatory for staff and no reporting. For January 2023, will be adding the National Cyber Security Centre (NCSC's) e-Learning package to Always Learning, making the package mandatory and reporting on compliance.	12-Dec-2022
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-2023	 In progress	Different approaches taken in the provision of IT services	Service Leader – Digital Enablement & IT	Action is ongoing. Ongoing programme to migrate applications, data and services to the 'cloud'. The AC/DC project is progressing at pace and several services have been migrated including our web filtering service. Approval to move more core applications to fully managed, cloud hosted versions as per the applications strategy.	12-Dec-2022
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-2023	 In progress	List of agreed prioritised actions	Service Leader – Digital Enablement & IT	Action is ongoing. Recovery Time Objective (RTO) and priorities communicated with services and updated in the Service Catalogue. Move to the cloud and fully managed services sees this shift from technical recovery to supplier and contract management.	12-Dec-2022

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.	Andrew Howe	12 Dec 2022