

**SCRUTINY AND AUDIT COMMITTEE – 23 SEPTEMBER 2021**

**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 proposals agreed by the Scrutiny and Audit Committee in August 2021 (Report 256/21 refers).

**1. RECOMMENDATION**

It is recommended that the Committee:-

- (i) Scrutinise and note the information presented about the IT resilience & Cyber-attack (Business Continuity) risk.

**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**

3.1 It was agreed that individual risk presentations would be made to Scrutiny and Audit Committee meetings in line with an agreed programme.

3.2 The following timetable for 2021/22 is based on the Corporate Risk Register at August 2021. This covers one risk that was new at January 2021, and the three highest scoring risks which are all red.

<b>S&amp;A meeting date</b>	<b>Risk to be presented</b>	<b>Risk score</b>	<b>Risk Target</b>
24 August 2021	Financial Sustainability	16	9
<b>23 September 2021</b>	<b>IT resilience &amp; Cyber-attack (Business Continuity)</b>	<b>16</b>	<b>8</b>
30 November 2021	Pandemic - Covid-19	20	15
25 January 2022	Health & Safety	12	6
1 March 2022	Climate change (New)	9	6

3.3 There are no significant changes in risk score ranking, or any new risks added to the risk register and therefore there is currently no need to review the programme.

**4. CURRENT POSITION**

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.

**5. FINANCIAL IMPLICATIONS**

There are no financial implications.

## **6. EQUALITY IMPACT ASSESSMENT**

An Equality Impact Assessment is not required, as this report does not impact on people.

### **Background Papers**

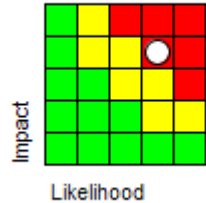
**NOTE:** No background papers as defined by Section 50D of the Local Government (Scotland) Act 1973 (other than any containing confidential or exempt information) were relied on to any material extent in preparing this report.

### **Author Reference**

Cathie Wyllie – Service Leader Internal Audit  
[ChiefExec@angus.gov.uk](mailto:ChiefExec@angus.gov.uk)

Appendix 1- Corporate Risk Register - IT resilience & Cyber-attack (Business Continuity)

## Appendix 1



### Risk Title

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 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. The restoration of Business As Usual (BAU) services could take several weeks.

### 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.	

**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-00034 Start development of council wide application strategy	31-Mar-2021		Increased profile of application planning and improved end to end resilience, security and data availability	Service Manager Digital Enablement and IT	COMPLETED Application Strategy reviewed with all senior managers and approved by Digital Strategy Board June 2021	19-Jul-2021	
AC-COR-00035 Ongoing review of new threats and counter measures	31-Mar-2022		Improved security and resilience	Service Manager Digital Enablement and IT	Ongoing and regular review by Network and Security Team Leader with periodic reports to CLT on threats and counter measure.  Fulfilled in 2020/21 and ongoing for 2021/22.	19-Jul-2021	
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-2022		Different approaches taken in the provision of IT services	Service Manager Digital Enablement and IT	In the last 6 months changes made to AHSC Eclipse, O365 and Backup to provision services such that they are less reliant on on-site physical infrastructure.  Ongoing for 2021/22.	19-Jul-2021
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-2022		List of agreed priorities	Service Manager Digital Enablement and IT	Updated as part of BC plans and ongoing review between BRMs and service areas wrt system uptime and recovery time requirements.  Ongoing for 2021/22.	19-Jul-2021
CORRR_0019.4 Resilience projects identified from the Technology Roadmap are implemented	This action is ongoing but has been severely delayed due to Covid-19.	31-Mar-2022		Increased resilience	Service Manager Digital Enablement and IT	Potential downtime required to undertake complete end to end testing still being hampered by COVID-19 and need for vast majority of staff to be working remotely.	19-Jul-2021

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

<b>Risk Owner:</b>	Caroline Cooper, Service Manager Digital Enablement and IT; Sharon Faulkner, Director of HR, Digital Enablement, IT & Business Support.
--------------------	--

Latest Update	By	Date
Potential downtime required to undertake complete end to end testing of disaster scenarios still being hampered by COVID-19 and need for vast majority of staff to be working remotely, hence very difficult to negotiate downtime required for actual testing and making resilience changes.	Caroline Cooper, Service Manager Digital Enablement and IT	19 Jul 2021