Appendix 1

RISK TEMPLATE

Step 2 – Risk Identification

Risk Title: 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 (provide narrative)	Potential Impact (provide narrative)
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.	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 (bullet points):

- For email and other core components there is a project being implemented to provide an automatic switch over to the use of the secondary site in Arbroath.
- The implementation of Office365 will improve resilience for all services.
- Regular and tested data back-up and recovery.
- Business Continuity plans in place for all critical services.
- There is regular maintenance of physical environment and equipment.
- The security standards are regularly reviewed.
- We have PSN accreditation.

Step 3 – Risk Analysis

Risk Likelihood Score:	4 High
Risk Impact Score:	4 Major
Overall Risk Score:	🟥 **16 Red**

Step 4 – Risk Evaluation

Additional controls / actions needed to mitigate risk further?	[✓ Yes] / No	**If Yes go to action plan (section B)**

Step 5 – Risk Treatment

Additional controls / actions to reduce likelihood and/or potential impact scores

Action	**Owned By**	**Target Date**	**Success Criteria**
Where appropriate avoid the risk by provisioning the services differently.	Caroline Cooper	31 March 2020	Different approaches taken in the provision of IT services
IT, with the service units, will review the RTO's against estimates of recovery time and agree priorities for actions.	Caroline Cooper	31 March 2020	List of agreed priorities.
Resilience projects identified from the Technology Roadmap are implemented.	Caroline Cooper	31 March 2020	Increased resilience.

Target Likelihood Score:	2 Low
Target Impact Score:	4 Major
Overall Target Score:	**8 Amber**

Risk Owner: Sharon Faulkner

Step 6 – Risk Monitor & Review

- Risks should be monitored every quarter, or more frequently if required