Executive Summary NC2325 Cyber Security

OVERALL ASSESSMENT

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

Cyber Risk is the likelihood of suffering harmful disruptions to sensitive data, finances, or Council operations. Common Cyber Risks are ransomware, phishing, malware, data leak, supply chain and nation-state cyber-attacks.

KEY STRATEGIC FINDINGS

- **There is a need to enhance the Cyber Security training needs analysis process for IT staff.**
- **Consideration be made to using cyber security insurance services.**
- **The Bitlocker laptop disk Encryption standard is 128bit, which we recommend is upgraded to 256bit.**
- **The Council does not hold Independent IT accreditations such as Cyber Essentials/ Cyber Essentials Plus or ISO 27001.**

GOOD PRACTICE IDENTIFIED

- **Incident Management Training procedures and training are in place.**
- **Patch Management arrangements are in place, including third party application updates.**

SCOPE

A risk has been raised in the Corporate Risk Register relating to the impact of a critical cyber security incident. An audit of this area was last carried out in 2020/21 and given a reasonable assurance grading however the threat from this risk continues to increase. A cyber security assurance audit was carried out to establish the Council's current level of control to preventing an attack from being successful.

ACTION POINTS

Urgent	Important	Needs Attention	Operational
0	2	3	0

Executive Summary NN2326 Disaster Recovery

OVERALL ASSESSMENT

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

CID04 (Directorate risk CS08): In the event of a catastrophic outage of the IT service running at city hall - the council will not be able to operate efficiently. In addition, the council will have lost all the information and records that it holds within the council's database and filing systems.

KEY STRATEGIC FINDINGS

- **Disaster Recovery Plans have not been reviewed and approved by the Council.**
- **No feasibility assessment has been carried out to substantiate if disaster Recovery Time Objectives (RTOs) can be met and align to Council needs.**
- **The Business Continuity Steering Group has been formed to review and approve Disaster Recovery Plans. However, the Group has not met since May 2022.**
- **The Council to review system recovery priorities and confirm that they are current.**
- **The Council to establish logs of contractor visits to enable auditing of the Disaster Recovery site access.**

GOOD PRACTICE IDENTIFIED

- **A Backup and Restore Policy has been established and regular data and system backups are taking place.**
- **A matrix for critical skills required for disaster recovery has been established and there is more than one member of staff covering each area of competence.**

SCOPE

A risk has been raised in the Corporate Risk Register relating to the impact of a critical cyber security incident. An audit of Disaster Recovery has provided assurance that in the event of an incident the Council is able to respond quickly in line with expectations. Note that a physical visit to the Lakenham Disaster Recovery was not possible. Hence, findings related to the site are based on verbal testing with adequate supporting evidence provided.

ACTION POINTS

Urgent	Important	Needs Attention	Operational
0	5	1	0