West Northamptonshire Council

WEST NORTHAMPTONSHIRE COUNCIL AUDIT AND GOVERNANCE COMMITTEE

29TH SEPTEMBER 2021

Portfolio Holder for HR and Corporate Services: Councillor Mike Hallam

Report Title	**Corporate Risks Update** - **Critical incidents** - **Information security**
Report Author	**Sarah Reed, Director of Corporate Services,** sarah.reed@westnorthants.gov.uk **Chris Wales, Chief Information Officer** Chris.wales@westnorthants.gov.uk

1. Purpose of Report

1.1. At the last meeting of the Audit and Governance Committee, the risk register was reviewed, and an update requested in relation to two risks: EO8 Critical Incidents and E10 Information Security. The purpose of this report is to provide an update on work being undertaken to mitigate both these risks. These risks are very much linked, and a number of the future mitigations will improve the control measures for both areas.

2. Recommendations

2.1 It is recommended that the committee note the actions that have been taken to mitigate both risks.

3. Report Background

3.1 Risk E08 relates to Emergency Planning – Critical Incident not managed effectively

3.2 Risk E10 relates to Information Security and there being insufficient security or recovery plans for data held and IT Systems used by the Council and resulting in a risk of a data breach, a loss of service, malicious attacks, or inability to deliver services due to loss of systems and data.

3.3 **Risk EO8 (Emergency Planning) has a residual risk score of 12 which is a medium risk.** The latest update as of July was that significant resource was still being utilised in the COVID response but that the Council was moving to the restore, recover and react stage.

3.4 Good Controls had been assessed in relation to:

- Key contact lists updated monthly
- BC Plans for in house and external providers
- Dedicated Emergency Planning Officer in post to review, test and exercise plan and to establish, monitor and ensure all elements are covered
- Dedicated reception centres in place in case of evacuation
- Senior Management attending civil emergency training
- Multi agency emergency exercises conducted to ensure readiness
- Deliver and participate in multi-agency training and exercise programmes to enable a more combined, coordinated, and robust response to incidents
- All officers that are involved in emergency responses are trained for their roles
- Full participation in Local Resilience Forum (LRF) activities
- Maintain and provide a single point of contact for NCC on 24 hours a day, 365 days of the year for major incidents and ICT on call arrangements confirmed

3.5 Reasonable controls had been assessed in relation to:

- Business Continuity plans for in house and external providers
- Business Continuity Strategy, Critical Incident Plan and BC Service Plans in place and up to date
- Services prioritised and recovery plans reflect the criticality of services and finances
- Business Continuity Plans tested
- Added resilience from cover between shared public health team, environmental health team and housing team (Bronze incident liaison officers)
- Information Management training – mandatory and completion reported to IM Board through DP and IGO roles
- Inter Authority Agreements created for shared services between North and West and, where appropriate, DPIAs and data sharing agreements developed where data is shared.
- ICT disaster recovery arrangements in place

3.6 **Risk E10 (Information Security) had a residual risk score of 15 which is a medium risk.**

The update in July advised that the following actions were in progress: -

- ICT capability assessment in train to risk assess gaps, over provision and create a properly functioning ICT resource
- A future road map for change and improvement had commenced and been shared with ELT
- Effective controls and mitigations were in place in relation to Cyber Security Incidents which are inevitable, and these include audit and review.
- Multi-factor authentication was being rolled out
- High priority agreed projects had been mapped by the Transformation team working with ICT.
- Work was being done to look at capability across the whole organisation with regard to Office 365, Teams etc and relevant training and support

3.7 Good controls had been assessed in relation to: -

- File and Data encryption on computer devices
- Managing access permissions and privileged users through AD and individual applications
- Consistent approach to information management and security training and awareness programme for staff
- GDPR Training online
- Password security controls in place
- Robust information and data related incident management procedures in place
- Appropriate robust contractual arrangements in place with all third parties that supply systems or data processing services
- Anti-virus checks up to date and all patches applied in a timely way
- Appropriate plans in place to ensure ongoing PSN compliance
- Adequate preventative measures in place to mitigate insider threat, including physical and system security

3.8 Reasonable controls had been assessed in relation to:

- Disaster recovery plan in place
- Key business systems moved to the Cloud to reduce risk of loss and increase resilience
- Regular DR Tests and Back up of data
- DPIs in place for all services where systems and data shared between West and North Northants and agreed with ICO

4. Update on progress with Risk E08

4.1 Dealing with Emergency Situations: In order to improve the controls of dealing with an emergency, it was agreed that prior to vesting day, that both West and North Northants would ensure that they had their own arrangements in place before spring 2022. This would also include working together in collaboration wherever necessary. Work is being undertaken to ensure that West Northants council arrangements will ensure all statutory requirements are fulfilled and that the new team will be an effective element of the overall resilience planning of

the council. This also takes into consideration the role that the Emergency Planning Service has taken in relation to Covid-19.

4.1.1 Emergency Planning (EP) as a function is a statutory role within the Council. The Chief Executive and senior leaders play a crucial role in civil resilience and must ensure their councils are adequately prepared for emergencies. They must stand ready to provide leadership when responding to emergencies and in recovering from them. The Civil Contingencies Act 2004 is the primary legal framework that sets out roles and responsibilities of emergency responders in England and Wales. All principal local authorities are considered category 1 responders under the Act, with a basic framework outlining statutory duty requirements, as follows:

- assessing the risk of emergencies occurring and use this to inform contingency planning.
- developing and implementing emergency plans.
- business continuity management arrangements.
- ensuring information is made available (and updated) to the public regarding civil protection and maintaining arrangements to warn, inform and advise the public in the event of an emergency;
- sharing information with other local responders and partners to enhance co-ordination.
- working closely with other local responders to enhance co-ordination and efficiency; and
- providing advice and assistance to businesses and voluntary organisations about business continuity management.

4.1.2 In meeting these requirements, West Northants Council must have in place appropriate, proportionate, and resilient plans and arrangements to both respond effectively to incidents and emergencies and ensure the continuity (or rapid recovery) of council critical functions.

4.1.3 In addition to the above Act, there are many other legal frameworks and policies where the Council has linked duties and consideration. These include the Flood and Water Management Act 2010, the Pipe-Lines Act 1962, the Health and Social Care Act 2012, control and containment of contagious animal diseases, regulations regarding control of hazardous substances and many more. The majority of these require the Council to have a management plan in place relevant to the subject.

4.1.4 The council is also a critical partner within all Local Resilience Forums (LRFs) which are multi-agency partnerships made up of representatives from local public services to review risk and plan for emergency situations. In addition to the Local Authority, LRFs include the emergency services, NHS, the Environment Agency, and others – all considered to be Category 1 responders. They are also supported by Category 2 responders, such as the Highways Agency and public utilities companies. All LRFs throughout the country are based on police boundaries – Northamptonshire has a whole county forum which collectively review likelihood and impact of local and national emergency risks, with mitigation planning as necessary.

4.1.5 In addition to its planning and preparedness activities, Emergency Planning provides a key operational response role. It provides routine monitoring of alerts and warnings to ensure that appropriate precautionary action is taken and if necessary, more substantial response mobilised. For larger incidents EP provide tactical advice and support to strategic managers and typically coordinates several aspects of the multi-agency response.

4.2 **Business Continuity Arrangement:** In order to improve the controls related to EO8 considerable effort has been put into West Northants business continuity arrangements. Local Government Re-organisation is a highly complex issue with services from April 2021 operating in different locations in different ways until services are all unified and transformed. This includes:

- updating the council's overarching business continuity plan to reflect the range of risks and working arrangements
- refreshing critical service business continuity plans to reflect new working arrangements
- establishing an overarching Business Continuity Officer Steering Group
- recruitment of new business continuity officers to support arrangements

4.3 **Recent Fire:** In August we also dealt with a significant business continuity issue. At approximately 1930hrs on Weds 11/08/2021, a fire in an electrical substation caused a power loss to the former NCC data centre at County Hall. At the same time and unrelated to the fire, engineers had taken the uninterruptible power supply (UPS) and backup generator unit offline for its annual maintenance. As a result, power was abruptly lost for all systems in what is now WNC's primary data centre. Power was restored by the power company at 0530hrs the following morning, but systems were not fully restored to staff until 1127hrs on Fri 13/08/2021. This meant disruption for the bulk of our services, as most business applications are still hosted on-premises at the data centre. This tested both our emergency planning and business continuity arrangements and the council is currently pulling together lessons learned, and additional controls will be added to be actioned for both risk areas. This includes consideration for:

- Having a more joined up approach between emergency planning and business continuity and clear flow charts
- Ensuring we have a 6-monthly test/trial run every six months of our arrangements
- A welfare protocol is produced to ensure sustainability in the workforce whilst responding to an incident.
- We tailor our incident response communications to the specific organisation in future so that messaging is appropriate to the Children's Trust and North Northants. IT provide people who are acting on behalf of West Northants in an emergency have access to both a West and North account.
- We review our partnership response process and ensure that representatives from MK and Cambridge are present at Incident meetings when needed.
- Reviewing our approach to cyber security (this links to E10)
- Reviewing our approach to putting more of our IT systems into the cloud environment (this links to E10)
- We begin to mandate colleagues' use of Teams/MS365 to ensure that it is part of our ways of working. It is recommended that Teams training forms part of our induction process. (this links to E10)

4.4 **Climate change awareness**: As part of the council's goal to be carbon-neutral by 2030, it will be necessary to review the systems we use for managing emergency incidents, along with our general IT hardware, as servers and data centres are a contributor to the council's carbon footprint.

5. Update on progress with Risk E10

5.1 Information security and cyber security continue to be a risk for all businesses and feature on many risk registers. WNC understands that cyber security is an important requirement to keep both staff and citizen data confidential yet accessible based on job function and need. The council is also required to maintain policies and practices that meet high security standards. Without these, it would be unable to function and connect to key entities to provide services required by law.

5.1.1 **Estimation of threat.** Recent examples have shown that cyber-attacks on public sector bodies, including local authorities, can be devastating. Last year, Redcar and Cleveland Borough Council were left without services for weeks, resulting in 135,000 people losing access to online services and council staff resorting to pens and paper at a cost of £8.7m to the council[1]. A hack on Hackney Council took over a year to repair[2], likely costing lives and losing the council £500,000 a month in missed payments[3], and costing near £10m to rectify[4]. These examples show the seriousness of the cybersecurity threat.

5.2 With the advent of West Northants Council, considerable work has been undertaken by the Chief Information Officer to understand the key capabilities, functions, and risks for information management. This has already led to agreement for additional funding to address key missing staff capabilities around system management and cyber security.

5.3 The service has also undertaken an assessment of cyber security risks to assess compliance readiness and areas for improvement. It assesses WNC's existing technologies against common attack methods and increasingly complex attack vectors, to ascertain changes and improvements that are necessary. This has given greater insight into the detail of requirements.

5.3.1 **Security requirements and best practices**

WNC has several legal requirements and adheres to compliance requirements for key connectivity, such as to the NHS for social care and PSN for pensions and benefits data. To fulfil these, WNC must achieve minimum standards and show evidence of this.

5.3.2 **The basics**

- WNC needs to be able to block most counterproductive and obscene content. This is true for both the staff network and the "people network" that provides access within libraries.
- WNC must maintain records of contracts and suppliers for the IT environment. The records should include contact details, start, and end dates of contracts and security accreditations

[1] https://www.bbc.co.uk/news/uk-england-tees-57433800

[2] https://www.wsj.com/articles/london-borough-of-hackney-struggles-with-recovery-months-after-ransomware-attack-11626427801

[3] https://www.bbc.co.uk/news/uk-england-london-58009789

[4] https://www.lgcplus.com/finance/hackney-still-reeling-from-cyber-attack-six-months-on-13-04-2021/

requested and achieved. Security accreditations can be CyberEssentials registered, ISO-27001 IT security or similar.

- WNC must monitor inbound and outbound communications to and from the internet. It must be able to provide details, if required, by bodies such as the ICO (Information Commissioner's Office) to confirm or rebut allegations of data misuse.
- WNC must stop unwanted communication by means of a network firewall to the corporate network.
- WNC must provide cyber security training to key personnel. This training should include phishing attack prevention, data confidentiality and physical security.

5.3.3 Confronting modern day attacks

- WNC needs to maintain an interest in current and prevailing attack patterns. Resources and budgets are finite. Therefore, the return on capital invested requires that any protection is relevant and fit for purpose. To achieve this the council should be proactive in **learning new threats** and attack vectors to better prevent a cyber-attack becoming successful.
- The systems should have an element of **dynamic content updates**. This is to automate prevention based on known current attack patterns being detected. Further, these attacks should be stopped at the earliest entry point whenever possible.
- There are three elements that should be maintained. The gateway (links between the council assets and others), the corporate network (data centre or cloud), the endpoint (PC, smartphone or device used to access services and content).
- By using encryption methods like those employed when accessing bank websites, attackers try to hide their actions at gateway points. These can equally be machines already compromised talking back out to the hacker. Having an ability to **scan for compromised machines** is a benefit.
- Attacks use temporary space in memory. Consequently, powering off is counterproductive as it destroys evidence of the attack and crucially any ability to obtain data such as encryption keys. Consequently, **a remediation process** known within the key IT teams and actively practiced avoids wrong decisions in the heat of the moment.
- **Offsite backups and business continuity** are also a vital strategy against cyber-attack. A viable ability to restore business systems quickly and efficiently, can thwart the business impact and allow law enforcement companies to track and trap the offenders. The council has legal time limits before fines are imposed for not providing key services. Therefore, an asset register and prioritisation against these is a key security requirement.
- For connections to NHS resources the council must have, as a minimum, a signed (physical or electronic) **register of administrators**. The agreement must include that they understand their role requires stricter codes of conduct and that they are open to more explicit monitoring than normal user behaviour.
- For compliance with Cyber Essentials Plus the council must maintain **records of all software and systems used**. To keep these within supported versions and be open to an annual audit by a trusted third party on an annual basis. For compliance to Cyber Essentials (without the plus) the same is true but is self-certified.
- For Public Sector Network (PSN) certification, the council must **maintain all systems against known vulnerabilities** and to have a realistic action plan to remediate any problem systems. This includes interconnected networks between sovereign councils if they have exposure to

public sector network data. This protection level must be verified by a trusted third party on an annual basis.

- The council systems involved in payment card transactions must be **compliant with security and confidentiality standards for payment card transactions**. This includes not recording full credit card information in an accessible format. To protect payment websites with modern security encryption standards. The network sections relevant should be security tested by third party access and any remediation actions completed.
- Although PSN, as a connection, is being dismantled, the **security testing** and remediation action plans are still relevant in terms of cyber-security protection. The services are moving onto the general internet cloud hosted services. Therefore, the attack surface is moving closer to possible malicious actors.
- You can only control what you can measure. A security policy that doesn't have monitoring or measuring capabilities cannot be effective. Councils and companies often deploy money and resources on attack prevention, without measuring the risk. Therefore, a risk assessment before and monitoring afterwards achieves more reward per pound spent.
- The council must have adequate logging within systems and services to be able to understand an attack methodology. These same tools can also provide an early warning that something is wrong. Often showing attacks that have been unsuccessful and a precursor of someone's intent.
- In addition, there should be a known response to any suspicious activity: who to call, what they'd use and how that action would prevent or protect.

5.4 **Next Steps for Information Security:** Improvement recommendations arising from the Cyber Security assessment will help shape the future resource ascertained to support cyber security as well as being discussed through future spending priorities to ensure IT resilient systems (aligned to the lessons learned from the recent loss of service due to the fire).

To support the internal piece of work on cyber security and information management, there is also an external cyber security testing process in train with Microsoft to provide an external assessment. This will also consider the learning points for IT from the recent fire, including the resilience of our data centre back up processes and further mitigations.

6. Implications (including financial implications)

a. Resources and Financial

The financial implications relating to IT pressures have already been flagged as part of revenue reporting and proposals are being developed for the medium-term financial plan.

b. Legal

Legal issues have been picked up in the report where they arise.

c. Risk

The Council's strategic risks include the two risks covered within this report

7. Background Papers

a) Corporate Risk Register
b) Business Continuity Group ToR
c) West Northamptonshire Service BC Plan Template
d) West Northamptonshire Business Continuity Risks and Planning Assumptions
e) West Northamptonshire Draft Business Continuity Policy