Report to:	**AUDIT AND GOVERNANCE COMMITTEE**
Date:	**23rd November 2022**
Title:	**IT and Communications Risks**
Report of:	**Chief Internal Auditor**
Ward(s):	**All**
Purpose of report:	**To provide answers to questions raised by the committee around IT and communication risks.**
Officer recommendation(s):	**That the information provided be noted and members identify any further information requirements.**
Reasons for recommendations:	**The remit of the Audit and Governance Committee includes the duty to keep under review the probity and effectiveness of internal controls, both financial and operational, including the council's arrangements for identifying and managing risk.**
Contact Officer(s):	**Name: Jackie Humphrey**
	Post title: Chief Internal Auditor
	E-mail: jackie.humphrey@lewes-eastbourne.gov.uk
	Telephone number: 01323 415925

1 Introduction

1.1 The remit of the Audit and Governance Committee includes the duty to keep under review the probity and effectiveness of internal controls, both financial and operational, including the council's arrangements for identifying and managing risk.

1.2 At the meeting of this committee held on 28th September 2022, the members requested a report relating to the robustness and reliability of the council's IT and communications systems and that proportionate mitigation of those risks is mitigated.

2 IT and Communications Risks

2.1 In order to answer the questions raised, the following officers were requested to provide the information which has been collated into this report.

- Communications Lead
- Transformation Programme Manager
- Insurance Officer
- Head of Customer First
- Head of ICT

2.2 The issues raised were around certain risks within the Strategic Risk Register and therefore this report is laid out using these risks as headers.

2.3 It is felt that the responses regarding IT security should be exempt from publication on the grounds of prevention of crime. The responses can therefore be found at **Exempt** Appendix A. **Should members wish to discuss this**

appendix they will need to resolve to move to exclude the press and public first.

2.4 SR_007 – Impact of an event under the Civil Contingencies Act

Q. Bad weather can affect power and water supply. There is also the current energy crisis which could see black outs in the winter. What plans does the council have for mitigating the risk of a power outage, with particular reference to staff working from home?

A. If there was a power outage at the Town Hall only, then staff would be decanted to other buildings where power is not affected. These include the Point and other buildings in the Devonshire Quarter at Eastbourne, Southover House in Lewes and the Port office in Newhaven. Also, staff could be asked to work from home.

Unless it was unsafe to do so, a member of staff would be retained on reception to manually record enquiries for logging when the power returns.

If the outage covers Lewes and Eastbourne, or is county-wide, the it would have a far greater impact as staff could not be decanted and would not be able to work from home, unless they live in another part of the country. The scenario for a county-wide outage sits with the Sussex Resilience Forum and they are waiting for central governance guidance. They are also planning to hold an exercise in the next few weeks.

One solution would be to purchase and maintain a generator but there is no current capacity for all staff to attend one office.

In terms of getting information out to the public the council's social media platforms and website would be used to push messages. It is also possible to enable short term messages on our telephone system to advise that the council is experiencing issues. These are only effective if the public are able to receive the messages on their own devices. Eastbourne's telephone system has a fail over to Lewes. The council would also be regurgitating information pushed out by the electricity companies and there are schemes where the council encourage residents to sign up to updates directly from them in the case of them being vulnerable.

For sheltered housing the Neighbourhood Caseworkers would ensure customers are informed and looked after.

In an absolute worse-case scenario, decisions would have to be made about which services the council could continue to provide in such circumstances.

2.5 SR_010 – Data Protection

Q. As well as maintaining the data risk on the council's systems, there are risks through the use of subcontractors.

i. How is the council insured against the risk?

ii. How would the council manage the reputation risk arising?

A. i. Data protection breaches are covered, under the council's Officials' Indemnity policy (current period of cover 1 April 2022 – 31 March 2023)

The council's cover is as follows (*excerpt from policy wording follows*):

A. Data Protection

The insurer will indemnify the insured for legal costs and expenses incurred with the insurer's prior consent, and all sums the insured is required to pay as damages to an individual arising from proceedings brought against the insured under:

a) Sections 168 and 169 of the Data Protection Act 2018
b) Article 82 of Regulations (EU) 2016/679 (General Data Protection Regulation)

Provided always that:

i) The insurer shall not be liable under this extension for:
   1) fines, penalties, liquidated, punitive or exemplary damages
   2) The costs of notifying any person regarding loss of personal data
   3) The cost of replacing, reinstating, rectifying or erasing any personal data
   4) Any deliberate or intentional criminal act or omission giving rise to any claim under this extension committed by the insured

ii) The liability of the insurer under this extension shall not exceed £1,000,000 in any one period of insurance. (*excerpt ends*)

In addition to the Council's own insurance, our data sharing agreements with third parties such as subcontractors processing personal data on our behalf include indemnity provisions. These ensure that where the data breach has occurred due to an integrity or confidentiality failure on their part, they indemnify the Council against the legal costs arising from any civil claims pursued by injured parties.

A ii. In the event of such a breach, the Council would follow the notification requirements under articles 33 and 34 of the UK GDPR. In parallel, ICO (Information Commissioner's Office) guidance would be followed; key items on their checklist would ensure that –

- We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk. (We would typically do this via direct communication with those affected.)
- We would inform affected individuals without undue delay.
- We would notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- We would provide advice to these customers help them protect themselves from its effects.
- We may also consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

Furthermore, we would be open and transparent in our response to any media, customer or other relevant enquiries about the breach, how it occurred, the steps we have taken including notifying the ICO and other relevant bodies and the further steps we will take to reduce the risk of future breaches.

2.6 Further information provided by IT

IT holds a risk register but this does not include sub-contractors. The Head of ICT stated that "we only used trusted partners that have been fully vetted".

An exercise has also been undertaken to ensure that none of the sub-contractors have any services or ties with Russia.

All redundant IT equipment goes for disposal and is not recycled. The equipment is destroyed to military grade so that no data can be recovered. Once destruction is complete, a certificate to confirm destruction is provided to the council.

3 Financial appraisal

3.1 There are no financial implications relating to expenditure arising from this report.

4 Legal implications

4.1 In relation to paragraph 2.5 Ai above, Article 82 of the UK GDPR confers on persons the right to receive compensation from any organisation whose infringement of this Regulation has caused them material or non-material damage. Section 168 of the Data Protection Act 2018 provides that "non-material damage" includes distress.

Section 169 of the 2018 Act provides an equivalent means of redress for persons affected by any organisation's failure to comply with the Act.

Responses given in Appendix A comply with the confidentiality and integrity principle specified in UK GDPR Article 5(1)(f), namely:

'Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

Legal advice provided 27.10.22 *Legal ref: 011515-EBC-OD*

5 Risk management implications

5.1 If the council does not have an effective governance framework that is subject to proper oversight by councillors it will not be able to demonstrate that it has in place adequate means to safeguard council assets and services, and it could be subject to criticism from the council's external auditor or the public.

6 Equality analysis

6.1 An equalities impact assessment is not considered necessary because the report is for information only and involves no key decisions.

7 Environmental sustainability implications

Not applicable

8 Appendices

Appendix A – IT responses (EXEMPT)