REPORT

SUBJECT:	**ICT Risk Arrangements**
MEETING:	AUDIT COMMITTEE
DATE:	**25th July 2019**
DIVISION/WARDS AFFECTED:	**none**

1. PURPOSE:

The purpose of this report is to outline the arrangements for addressing ICT, Cyber and digital security risks.

2. KEY ISSUES:

2.1 At Audit committee on a question was raised about the arrangements for monitoring ICT risks, This report details the key areas for recording, reporting and mitigating risks.

3. RISK ARRANGEMENTS:

3.1 MCC operates a comprehensive set of arrangements to mitigate any risks surrounding ICT. The risks are recorded in separate progressive registers feeding up into the strategic corporate risk register.

3.2 The key ICT, digital, cyber and information risks are assessed, recorded and mitigated in the following ways:

3.2.1 The independent Security Advice service – MCC, Torfaen and Blaenau Gwent have commissioned an independent security advice and audit service that mitigates our security risks by:

- Assessing the operational ICT security risks inside Monmouthshire and maintains an operational risk register
- Assesses network risks at the SRS
- Assists us with the completion of PCI, PSN and cyber security plus accreditation

3.2.2 Internal Monmouthshire risk assessment registers – MCC maintains 3 risk registers as follows:

- Independent security service risk register – Detailed operational risks are identified through normal operations and recorded in a risk register that is assessed by the Head of Digital and the independent security service advisor on a monthly basis. The operational risks identified can be from within MCC itself or within the SRS. This risk register isn't publicly available for security reasons. The independent security service liaises direct with the SRS in order to ensure they mitigate any risks falling under their responsibility.

- Digital Business Plan risk register pages 13-16

- Corporate risk register item 10a

3.2,3 External accreditation – MCC is required to comply with several external accreditation procedures in order to ensure continued connection to network services and mitigate the risks associated with cybercrime as well as unauthorised access to information.

- IT Health check – This is an annual health check undertaken within the SRS by an independent security service procured and commissioned by the SRS.

- The Public Services Network (PSN) is a network that provides a trusted, reliable, cost-effective solution to departments, agencies, local authorities and other bodies that work in the public sector and need to share information between themselves.

  MCC needs to complete an application showing how it complies with stringent security conditions in order to use PSN connectivity services. We must receive a PSN compliance certificate before we provide PSN services. MCC's application has been refused for the last 3 years as it has fallen short in a small number of elements. All outstanding issues have now been addressed and our PSN submission is currently being prepared by the independent security service.

- Public Sector Broadband Aggregation (PSBA) – The PSBA provides network connectivity for all 22 local authorities in Wales. Teams from different councils can work efficiently across Wales thanks to secure, fast and convenient network access at any council building. It is a managed service that provides ssecure roaming services, resilient web filtering services to determine if content should be blocked and robust firewalls. It mitigates the risk of network penetration by unauthorised personnel.

- Cyber Security Plus – This is an accreditation service undertaken by Welsh Government. It assesses our security arrangements within MCC as well as the SRS.

- Payment card Industry Data Security standard. (PCI)- The PCI Security Standards Council is constantly working to monitor threats and improve the industry's means of dealing with them, through enhancements to PCI Security Standards and by the training of security professionals. MCC has to prove compliance with PCI standards for both network security as well as internal processes relating to record keeping and the knowledge and skills of our staff.

3.2.4 Information security legislation compliance – MCC is required to appoint a SIRO and a DPA officer with responsibilities relating to legislation.

  - Senior Information Risk Owner (SIRO) – This is a mandatory role that each authority has to put in place. The nominated person is responsible and accountable for ensuring that we comply with the legislative requirements of

the General Data Protection Regulation (GDPR), Data Protection Act (DPA), Freedom of Information (FOI) and Subject Access Requests (SAR'S). Though some of our information storage is in a manual format the majority of our information is digital and it must be protected from unauthorised access. This links in with the mitigation of any risks associated with our networks and data storage systems.

3.2.5 Cyber awareness training and monitoring – MCC provides training and monitoring to mitigate the risks surrounding data security and cyber fraud.

- Mandatory GDPR/ DPA and cyber security training – MCC provides mandatory training for both legislation compliance purposes and to mitigate against the risks of cyber fraud and error arising from staff behaviour and knowledge.

- Induction training and ICT checklists – All new employees are provided with information governance and cyber fraud training on their mandatory induction sessions. Managers have ICT induction checklists to complete for new employees as well as ensuring they have ICT training by the ICT trainer.

- System penetration tests – All of our ICT systems are independently tested to ensure there is no risk of unauthorised access.

- Testing of physical and digital security arrangements – The independent security service undertakes security tests, e.g. phishing exercises, to identify the risks associated with employees' lack of cyber awareness.

3.2.6 SRS security services – The SRS has its own security arrangements to mitigate against security risks -

- ISO accreditation
- SRS security advisor

5.1 **CONSULTEES:**

Digital Programme Office
Chief Officer Resources

5. BACKGROUND PAPERS:
Digital Business Plan
Corporate Plan

AUTHOR: Sian Hayward – Head of Digital

CONTACT DETAILS:

Tel: 01633 344309 / 07825 450791
Email: **sianhayward@monmouthshire.gov.uk**