Report No. 13/21

Audit & Corporate Services Review Committee

REPORT OF BUSINESS IMPROVEMENT AND IT MANAGER

SUBJECT:
CYBER RESILIENCE

Background:

Over the past year the Authority has received two reports relating to Cyber Security. The first is a general report by Audit Wales on "Cyber Resilience in the Public Sector Report" and the second a review of our Cyber Security arrangements by our Internal Auditors TIAA.

Audit Wales has requested that the "Cyber Resilience in the Public Sector Report" is treated as a confidential item when discussed by Audit Committees or other meetings, therefore it is proposed to request that Members take this item in private.

RECOMMENDATION:

To note the findings of the two reports on Cyber Security.

Background documents

(For further information, please contact Debbi Church, extension 4812 or at Debbic@pembrokeshirecoast.org.uk)

ICT Audit

FINAL

Pembrokeshire Coast National Park Authority

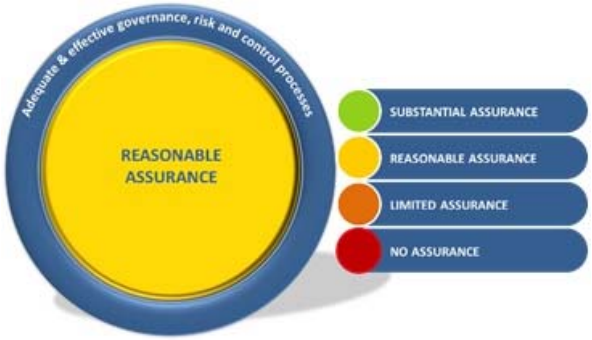
ICT Review of Cyber Security

2020/21

March 2021

Executive Summary

OVERALL ASSESSMENT



ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

20. Risk of major IT failure or virus attack etc.

22. Loss of key documents & inaccurate GIS or other documents.

23. Risk of inaccurate GIS and other data for decision making.

40. Breach of General Data Protection Regulations

KEY STRATEGIC FINDINGS

The Authority has not carried out penetration testing to provide assurance that appropriate measures have been taken to reduce the impact of a Cyber Attack.

Whilst the Authority's Information and Data Security Policy requires all sensitive data to be encrypted when removed from the premises, the Policy does not recognise the impact of sensitive data being held on a user's own device (BYOD).

GOOD PRACTICE IDENTIFIED

The Authority ensures that data backups are taken off site each week.

The ICT User Policy provides clear direction on what is acceptable and unacceptable use of IT resources.

SCOPE

The review considered the security management arrangements for the pro-active identification, prioritising and mitigating against cyber-crime risks. The scope of the review included policies, procedures and risk management activities in place for the key elements of the CESG framework, including: • Information Risk Management Regime• Secure configuration• Network security• Managing user privileges• User education and awareness• Incident management• Malware prevention• Monitoring• Removable media controls• Home and mobile working.

ACTION POINTS

Urgent	Important	Routine	Operational
0	2	2	3

Assurance - Key Findings and Management Action Plan (MAP)

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Directed	The Information and Data Security Policy states that sensitive data must be encrypted when removed from the Authority's premises. The Policy fails to recognise the impact of permitting the use of personal devices for business activity (known as BYOD or Bring Your Own Device). There is a risk that sensitive data may be lost or exposed as a result of the loss of a user's personal device. For example a manager may receive an e-mail on their own device at home with an attachment relating to a staffing matter; the manager opens the document and adds further comments that would be deemed sensitive. Returning to the office, the manager loses their device or has the device taken from them resulting in a potential data loss, leaving the Authority exposed to penalties being imposed by the Information Commissioner.	The Information and Data Security Policy be amended to state that sensitive data is never saved onto an unencrypted laptop or any other portable storage device	2	*Recommendation accepted, the Information and Data Security Policy will be amended.*	*30/04/21*	*Business Improvement and IT Manager*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Directed	Within the "Appropriate Use" section (6.4) of the ICT Users Policy, it was noted that the Authority permits the use of personal webmail outside of normal hours. This is a high risk to the IT infrastructure as a result of not being able to block spam messages or filter hazardous attachments. It is also an unnecessary risk as the Authority provides public Wi-Fi that could be used for sending and receiving personal e-mails. Allowing users to access their personal webmail accounts using corporate devices has been the major factor in a number of successful cyber-attacks and is detailed as one of the case studies in the CESG Common Cyber Attacks: Reducing the Impact guidance. CESG is the information security arm of GCHQ, the Government Communication Headquarters.	ICT need to introduce controls to prevent users from accessing personal webmail through the Authority's network, encouraging users to use their own mobile phone, tablet or other device in order to access their e-mail through the public Wi-Fi.	2	*Recommendation to be reviewed with Authority Leadership team – under consideration will be the following implications – risk of not preventing access to personal email accounts, the practicalities of preventing access and the potential impact on staff members who do not have the financial resources available for personal devices.* *Note: Timetable lengthy as, should the recommendation be accepted:* • *An update to the ICT Policy, approval and subsequent welsh translation will be required prior to publication.* • *Controls will need to be put in place on all Authority devices to prevent access to both webmail and mail applications.*	*30/08/21*	*Business Improvement and IT Manager*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Directed	A review was carried out of the Data Protection Policy for the Authority. The document provides a detailed explanation of the Data Protection Principles without really explaining how the Act relates to Pembrokeshire National Park Authority. Currently the policy is ineffective as it is too wordy and would overwhelm the reader with the level of detail. In order to be an effective policy, the document needs to be relevant and concise, allowing the reader to understand how the Act relates to them and their role within the Authority. The Data Protection Policy is due to be reviewed in 2022. The Policy Document should include a commitment by the Authority to meet the Principles of the Data Protection Act. Links can be provided within the document to the Information Commissioner's Website to provide the reader with further explanation if required.	The Data Protection Policy be re-written to provide a concise and clear explanation of how the Data Protection Act impacts on the Pembrokeshire Coast National Park Authority.	3	*Recommendation accepted.*	*To be determined – post currently vacant.*	*Data Protection Officer*
2	Directed	Undertaking a simulated attack on the networked systems using techniques that are likely to be employed by a potential attacker would enable the Authority to have a greater understanding of its vulnerabilities and allow appropriate measures to be taken to reduce the threat.	The possibility of carrying out a simulated attack on the Authority's systems using the approach that a likely attacker would use be further investigated.	3	*Recommendation accepted. Timescale to implement is dependent on completion of the current infrastructure and associated security controls – penetration testing would be more relevant at this point.*	*30/10/21*	*Business Improvement and IT Manager*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Operational - Effectiveness Matter (OEM) Action Plan

Ref	Risk Area	Finding	Suggested Action	Management Comments
1	Directed	The Data Protection Policy refers to both the EU General Data Protection Requirements (GDPR) and the Data Protection Act 2018.	There is no longer a requirement to refer to GDPR within the Data Protection Policy as the Data Protection Act 2018 is the UK law that has been designed to meet GDPR requirements following departure from the European Union.	*Authority will ask new external DPO to review Policy once appointed, Data Protection Policy will be updated to reflect the required changes.*
2	Directed	A copy of the Authority's Risk Register was obtained as at January 2021. The Authority has identified four risks, in relation to • IT failure/Virus Attack, • failure of phone systems, • loss of key documents & inaccurate GIS or other documents. The first risk that has been identified is really two separate risks, (i) the loss of ICT and the damage and disruption caused by a Malware attack. The loss of ICT may simply be caused by a major power failure resulting in the loss of the network services. A Malware Attack could result in the loss of ICT, however it may also result in the loss of data, unauthorised changes to data, fraud/ransomware and lead to the costly recovery of the Authority's systems.	The Authority should consider separating risk no 20 in relation to IT Failure and Virus Attack into two separate risks, the risk of the loss of ICT systems and the risks arising from a Malware attack as although both are equally relevant they constitute different threats with different mitigating controls and actions.	*We will consider updating the risk registered to reflect the suggested changes.*

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Ref	Risk Area	Finding	Suggested Action	Management Comments
3	Directed	The Authority's Risk Register includes a risk, Risk 40, in relation to a “breach of GDPR” (the European Union General Data Protection Regulation). The UK Data Protection Act 2018 is the UK legislation that advises how the General Data Protection Regulation will be applied within the UK and this should be reflected in the wording of the risk which should refer to "breach of the Data Protection Act 2018" rather than "breach of GDPR".	The wording of the Risk 40 be amended to “breach of the Data Protection Act 2018” replacing the current reference to the General Data Protection Regulation when the Risk Register is next reviewed.	*Risk Register will be updated to reflect the suggested changes.*

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Findings

Directed Risk:

Failure to properly direct the service to ensure compliance with the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
GF	**Governance Framework**	There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation.	In place	1, & 2	1
RM	**Risk Mitigation**	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	In place	-	2, & 3
C	**Compliance**	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Partially in place	3, & 4	-

Other Findings
The Authority has documented an Information and Data Security Policy and an ICT User Policy. Both Policies are comprehensive and detail what is acceptable use and what isn't acceptable.
Copies of the previous audit reports that relate to Cyber Security were obtained. All of the agreed actions from the previous audit reports have now been implemented.
The Authority has not obtained independent assurance on security controls in place by carrying out penetration testing. The previous two audit reports included a recommendation to carry out penetration testing. The recommendation was rejected in both cases on the basis of cost. Whilst it is recognised that the likelihood of an attack on the Authority's IT infrastructure is low, there will always be a threat of malicious attacks by disgruntled individuals or random malware attacks initiated via e-mail. One of the other Welsh National Park Authorities has recently suffered a ransomware attack, the lessons learned from this incident, puts into context the impact and cost of recovery.

Other Findings

A copy of the network overview diagram was provided. The very basic IT infrastructure covers a number of small outlying sites and the main HQ in Llanion Park. The systems are supported in-house by two IT officers. In discussions with the Business Improvement & IT Manager and one of the IT Officers, they emphasised that as a small organisation that does not hold a significant amount of sensitive personal records other than employee data and planning data, the controls have to be proportionate and delivered within a limited budget. This was recognised when reviewing the control processes.

The Authority's IT officer provided details of the perimeter security controls, the configuration of devices and the access controls. The controls were considered appropriate for an organisation of this size. There is recognition of the requirement to replace the firewall as the existing Cisco system will no longer receive updates in 2022.

Details of the security monitoring carried out by the Authority were also provided. Currently monitoring is limited to the Anti-Virus software reports which are received via e-mail. The replacement of the Firewall should provide improved monitoring of potential security attacks. There is recognition that the network infrastructure has limited resilience in the event of power failure with the UPS (Uninterruptable Power Supply) limited to 1 hour and no backup generator, allowing sufficient time for devices to be powered down in a controlled manner.

Delivery Risk:

Failure to deliver the service in an effective manner which meets the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
PM	**Performance Monitoring**	There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner.	Out of scope	-	-
FC	**Financial Constraint**	The process operates within the agreed financial budget for the year.	Out of scope	-	-
R	**Resilience**	Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.	In place	-	-

Other Findings

The Authority's systems are backed up using Veeam. Monthly and weekly full backups to tape are taken off site and these tape backups are augmented by daily Veeam incremental backups which are stored on the server. In the event of the major loss of the Authority's IT systems, the maximum amount of data that would be lost would be one week's processing if the systems were lost at the end of the week prior to the weekly backup to tape being completed. The Authority's Planning and HR systems are outsourced to external providers and these systems would not be impacted directly by the loss of the Authority's systems and the potential limited data loss for in-house hosted systems has been risk assessed and deemed to be acceptable.

EXPLANATORY INFORMATION

Appendix A

Scope and Limitations of the Review

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. As set out in the Audit Charter, substantive testing is only carried out where this has been agreed with management and unless explicitly shown in the scope no such work has been performed.

Disclaimer

2. The matters raised in this report are only those that came to the attention of the auditor during the course of the review, and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Effectiveness of arrangements

3. The definitions of the effectiveness of arrangements are set out below. These are based solely upon the audit work performed, assume business as usual, and do not necessarily cover management override or exceptional circumstances.

In place	The control arrangements in place mitigate the risk from arising.
Partially in place	The control arrangements in place only partially mitigate the risk from arising.
Not in place	The control arrangements in place do not effectively mitigate the risk from arising.

Assurance Assessment

4. The definitions of the assurance assessments are:

Substantial Assurance	There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved.
Reasonable Assurance	The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved.
Limited Assurance	The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved.
No Assurance	There is a fundamental breakdown or absence of core internal controls requiring immediate action.

Acknowledgement

5. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

6. The table below sets out the history of this report.

Stage	Issued	Response Received
Audit Planning Memorandum:	8th December 2020	8th December 2020
Draft Report:	22nd February 2021	26th February 2021
Final Report:	4th March 2021	

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Pembrokeshire Coast National Park Authority		
Review:	Cyber Security		
Type of Review:	Assurance	**Audit Lead:**	Principal Auditor - ICT

Outline scope (per Annual Plan):	The review considers the security management arrangements for the pro-active identification, prioritising and mitigating against cyber-crime risks. The scope of the review includes policies, procedures and risk management activities in place for the key elements of the CESG framework, including:• Information Risk Management Regime• Secure configuration• Network security• Managing user privileges• User education and awareness• Incident management• Malware prevention• Monitoring• Removable media controls• Home and mobile working	
Detailed scope will consider:	Directed Governance Framework: There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation. Risk Mitigation: The documented process aligns with the mitigating arrangements set out in the corporate risk register. Compliance: Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Delivery Performance monitoring: There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner. Financial constraint: The process operates with the agreed financial budget for the year. Resilience: Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.
Requested additions to scope:	None	
Exclusions from scope:	See above	

Planned Start Date:	25/01/2021	**Exit Meeting Date:**	26/01/2021	**Exit Meeting to be held with:**	Business Improvement & IT Manager

SELF ASSESSMENT RESPONSE

Matters over the previous 12 months relating to activity to be reviewed	**Y/N (if Y then please provide brief details separately)**
Has there been any reduction in the effectiveness of the internal controls due to staff absences through sickness and/or vacancies etc?	N
Have there been any breakdowns in the internal controls resulting in disciplinary action or similar?	N
Have there been any significant changes to the process?	N
Are there any particular matters/periods of time you would like the review to consider?	N