Information Governance

Peak District National Park Authority

Internal Audit Report 2017/18

Business Unit: Corporate Services
Responsible Officer: Director of Corporate Strategy and Development
Service Manager: Head of Information Management.
Date Issued: 06 March 2018
Status: Final
Reference: 69140/003

	P1	P2	P3
Actions	**0**	**1**	**0**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. The authority should have adequate processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.

The introduction of GDPR in May 2018 has increased the importance of effective controls surrounding information governance. GDPR will introduce additional mandated requirements to the Data Protection Act that it is superseding. Failure to meet these standards could result in a large fine up to the value of 4% of annual global turnover or €20 Million (whichever is greater).

An Information Governance audit carried out in 2014/15 identified seven findings and provided Moderate Assurance. Appropriate actions were agreed to address the issues identified. This was followed up in the 2015/16 Information Governance audit, which identified that suitable progress had taken place and provided a high assurance rating.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system ensure that:

- The agreed actions within the 2014/15 information governance audit have been maintained
- The authority has made sufficient preparations for the introduction of GDPR.

Key Findings

The agreed actions in the 2014/15 information governance audit report have been maintained or superseded with the introduction of GDPR. The authority has introduced secure bins for disposing of confidential data. The authorities head office, Aldern House uses lock mechanisms that restricts access within the building to authorised personal.

We have found that the authority have acknowledged the importance of sufficient information governance processes in preparation for the implementation of GDPR in May 2018. The authority have carried out a gap analysis of current procedures and processes relating to information governance and compared them to GDPR requirements. This exercise identified where they need to implement actions and an action plan was created based on this. The authority has presented this action plan to senior management. We have reviewed the action plan and found that it contains all main requirements of GDPR. The authority have an assigned a Data protection officer (DPO) which is a mandated requirement of GDPR. The DPO has been overseeing the action plan to ensure it is completed.

To educate staff about data protection and GDPR the authority have implemented a training programme. The authority has processes in place to monitor the individuals who have completed the course. There is currently no escalation process in place if an individual does not carry out the training course. In June 2017 the authority assessed what data they hold and created a retention policy based on what data they have stored. However the policy did not explicitly mention the retention of CCTV recordings. The authority is in the process of setting up a data management system that will be used to notify data holders of when data has reached its retention date. When data (hard copy and electronic) is ready for disposal the authority have procedure in place to dispose of it securely.

The authority has defined a data breech within the current version of the Information Management policy. The policy also defines the actions that should be taken when a data breech has been identified and the actions that should be taken in the event that a FOI is received. However the current version of the policy does not define what counts as a FOI. This may be appropriate to include as FOI can be requested in multiple ways.

Before GDPR has come in to effect the authority needs to update their Information Management policy and Privacy notices as well as update their asset register and review new contracts to ensure they comply with GDPR. Once these policies and procedures have been implemented the authority should put in place a monitoring programme to ensure that the policies are being complied with.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 GDPR Readiness

Issue/Control Weakness	Risk
The authorities have not taken out all necessary actions to prepare for GDPR.	The authority does not make necessary changes to information governance processes before GDPR legislation comes in to effect. This would have the potential impact of reputational damage and large fine.

Findings

When GDPR comes in to effect in May 2017 there are a number of actions that the authority would need to carry out in order to become compliant with the regulations. The authority has recognised these actions in an action plan. The action plan covers all the main requirements of GDPR. The authority has fourteen actions on the action plan. At the time of testing (January 2018) the authority was overdue in completing two of the actions that was due to be implemented in December (2017).

There are additional actions that are not scheduled for completion until later in the year, where the authority needs to be able to ensure these are completed as required. It is important that progress is monitored to identify potential delays, and that action is taken to ensure completion. In particular actions that require action by staff or 3rd parties need to include an escalation procedure in case of delays.

Agreed Action 1

The action plan is being actively monitored by the Head of Information Management as a part of the SIRO role with regular update and progress checks taking place. Any delays in completion of actions to be reported to RMM in April as part of the GDPR preparation follow up that was scheduled when the Authority (through RMM) accepted and agreed to these actions as the mechanism for preparing for the GDPR.

Priority	2
Responsible Officer	Head of Information Management
Timescale	30 April 2018

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.

PEAK DISTRICT NATIONAL PARK