Veritau
Assurance Services for the Public Sector

Server Room Security

City of York Council

Internal Audit Report 2016/17

Business Unit: Customer & Corporate Services
Responsible Officer: Assistant Director Customer Services & Digital
Service Manager: Head Of ICT
Date Issued: 15 May 2017
Status: Final
Reference: 10245/009

	P1	P2	P3
Actions	**0**	**0**	**0**
Overall Audit Opinion	High Assurance		

CITY OF YORK COUNCIL

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. To ensure the ongoing provision of council services, it is vital that access to network services and data is maintained.

The key hardware supporting the services provided by City of York Council is located in a dedicated server room at West Offices, with a secondary facility at the Hazel Court Eco Depot.

Servers and other network infrastructure housed in these rooms need to be protected from fire, flood, power outages and other environmental hazards, and also damage, theft or sabotage. Weak physical security arrangements could also lead to unauthorised access to sensitive information.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls over the physical and environmental security of the server room will ensure that:

- interruptions to services are minimised;
- unauthorised access to sensitive information is prevented;
- loss and / or disclosure of data are prevented; and
- disruption or loss of operational services and activities are minimised.

Key Findings

It was found that the IT server facilities at West Offices and Hazel Court were effective in mitigating against the risk of interruptions to services, unauthorised access, loss of data and loss of operational services.

The Council's main server rooms are at the West Offices and were built for purpose. As such, consideration has been given to important factors such as access, security, fire suppression, environmental controls and maintenance of equipment.

In the event that a service interruption occurs, back-up servers are held ay Hazel Court in a much smaller facility. Overall, no major issues were identified. However, there was a fair amount of combustible packaging left on the floor which would prove hazardous in the event of a fire. The area surrounding the IT equipment should be kept free of all flammable materials; therefore care should be taken to keep this area clear and accessible.

Overall Conclusions

It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided High Assurance.

Annex 1

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.