INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Database Security
TO:	Deputy Chief Executive (AJ)	**DATE:**	1 November 2018
C.C.	Chief Executive Head of Finance ICT Services Manager Portfolio Holder – Cllr. Mobbs		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2018/10 an audit review of the Council's database security controls was completed in October 2018. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 This audit was undertaken to ensure that database system administration processes are sound and that adequate logical security settings have been implemented on the Council's live database server environment.

3 Scope and Objectives of the Audit

3.1 The objective of the report was to perform a review of the controls in place to ensure the confidentiality, integrity and availability of data stored in Council databases.

3.2 Testing was performed to confirm that controls identified operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on discussions with relevant staff.

3.3 The audit was designed to assess and provide assurance on the risks pertaining to the following key areas:

- Access rights for database administrators
- Super-user privileges
- Password controls
- Security patching
- Vulnerability scanning
- Database auditing
- Capacity / performance management.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not applicable as this the first audit of this subject area.

4.2 Policies & Procedures

4.2.1 The ICT policies and procedures relevant to the management of database security were obtained and reviewed during the audit. These were used in the process of reviewing the suitability of the controls in operation at the Council.

4.2.2 The 'Microsoft SQL Server Database Security Policy' was identified as being of particular relevance to this audit, as it details the requirements and controls in place to ensure that all Council databases are secured to a minimum security standard.

4.2.4 Policies reviewed were found to be subject to regular review and revision on at least an annual basis, and included sections for version control, a revision history and details of the relevant ICT staff who own and are accountable for the policy.

4.3 Access rights for Database Administrators/ Superuser Privileges

4.3.1 A sample of key Council systems w selected for testing. Database security settings and supporting evidence were obtained and reviewed with ICT management. Audit testing verified that database superuser access rights were restricted to valid and authorised ICT personnel.

4.3.2 On a SQL Server database, superuser privileges are automatically assigned to the System Administrator (SA) account. It is good practice to ensure that admin activities are performed via named individual accounts rather than using the SA accounts. It was noted during testing that administration activities are required to be performed using individual administrator accounts, but that "SA" accounts were retained and secured for use in case of emergency.

4.3.3 Audit testing confirmed that ICT actively sought to secure superuser accounts by both renaming the SA account and securing it via the use of a complex password. Review of a sample of SQL Server databases identified that the majority of these accounts had been renamed. The review, however, did identify one instance where the SA account had not been renamed.

Risk

As a known account with administrator privileges there is a risk of an SA account being exploited in an external attack.

Recommendation

ICT management should ensure that all SA accounts are renamed.

4.4 Password Security

4.4.1 The ICT 'Microsoft SQL Server Security Policy' recommends "*a strong password policy, including an expiration and complexity policy*" and that new logins be changed upon issue. Database password parameters were obtained and reviewed during the audit and found to meet these requirements.

4.4.2 It was noted that high privilege SA account passwords are currently stored on a SharePoint server. This currently poses a risk as passwords could potentially be unavailable in the event of a Disaster Recovery (DR) situation.

4.4.3 We were advised by management that a number of cloud based password solutions were being investigated at the time of audit.

Risk

There may be system and service unavailability and/or the inability to recover database systems in the event it is not possible to retrieve superuser passwords in a DR when required.

Recommendation

ICT management should identify and obtain a password management solution for the secure storage of key passwords.

4.4.4 The Cyber Essentials Scheme guidelines on Secure Configuration recommend that unnecessary user accounts (such as guest accounts and administrative accounts that won't be used) should be removed and disabled.

4.4.5 Testing of a sample of SQL Server platforms identified six instances where 'Guest' accounts were enabled on Council databases. The 'Guest' account is a default account designed to enable users without an account to log on as a guest. It is recognised good practice that these accounts are disabled and/or renamed to improve the security of the domain.

Risk

There is a risk of failure to comply with CES security guidelines and an increased risk of unauthorised access to the live database environment.

Recommendation

ICT management should ensure all SQL Server database 'Guest' accounts are reviewed and disabled.

4.5 Security Patching

4.5.1 The ICT 'Microsoft SQL Server Security Policy' states that the aim of database patching is to stay as current as possible and that "*ICT Services will attempt to maintain all operational software at a level that is no more than two major releases from the currently shipping product*".

4.5.2 Reporting detailing the patching status/ software version of the Council's databases and supporting operating systems was obtained and reviewed. This identified that there was one exception where the database software version was not within ICT's targets.

4.5.3 We were advised that this is due to the software on the 'Horizon' virtual desktop deployment system not supporting the latest SQL Server service pack. It is understood that ICT are in the process of upgrading the Horizon software to a newer version which will enable them to upgrade the database service pack.

Risk

There may be an impact to systems and services in the event of issues caused by known bugs or vulnerabilities being exploited.

Recommendation

ICT management should upgrade to the latest SQL Server service pack following the upgrade of the Horizon software.

4.6 Vulnerability Scanning

4.6.1 Annual vulnerability scanning and external penetration testing is undertaken as part of the annual IT Health Check (ITHC) exercise required for the Public Services Network (PSN) accreditation process. This includes testing of a selection of key databases for known vulnerabilities. Actions resulting from this ITHC report are logged and tracked through to completion using an actions log.

4.6.2 There is not currently any regularly scheduled vulnerability scanning performed on a more frequent basis. However we were advised by ICT management that the need for any internal vulnerability scanning is reviewed on a regular basis.

4.7 Database Auditing

4.7.1 In addition to ad-hoc and day-to-day checks, ICT perform a regular six monthly exercise of reviewing and sanity checking Council databases to help ensure compliance with requirements of the 'MS SQL Security Policy'. This includes review of patching and version status, the current operating system, and review of admin accounts and service accounts.

4.7.2 A sample of databases was selected and reviewed to confirm that database logging was enabled and that failed login attempts were recorded, and no exceptions were identified. Database logs were also reviewed to ensure data was retained for a suitable timescale.

4.7 Capacity Management

4.7.1 During the audit it was observed that ICT make use the System Centre Operations Manager (SCOM) application to monitor and provide active database alerting to ensure database and server availability is maintained.

4.7.2 Audit testing verified that the SCOM platform was configured to generate real time alerts for any issues on database performance, disc space, capacity, CPU, user connections and disc memory.

5 Conclusions

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did identify, however, four Medium-rated issues which, if addressed, would improve the overall control environment. As a result the findings are considered to give SUBSTANTIAL assurance around the management of database security risks.

5.1 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Database Security – November 2018

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.3	ICT management should ensure that all SA accounts are renamed.	As a known account with administrator privileges there is a risk of an SA account being exploited in an external attack.	Medium	Infrastructure Manager	Accepted: Four sql installs have 'sa' enabled. Tegan4 – this box is being decommissioned. Energy2 – 'sa' account has now been disabled Datapulse2 – the supplier will look into this, however this is a low risk box. Pncserver – the supplier has quoted £450 to make changes. However, a complex password is being used which we believe has mitigated the risk.	No Further Action

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.2	ICT management should identify and obtain a password management solution for the storage of key passwords.	There may be a system and service unavailability and/or the inability to recover systems and services in the event it is not possible to retrieve key passwords when required.	Medium	Head of ICT	Accepted. A new password vault will be investigated.	May 2019
4.4.5	ICT management should ensure all SQL Server database 'Guest' accounts are reviewed and disabled.	There is a risk of failure to comply with CES security guidelines and increased risk of unauthorised access to the live database environment.	Medium	Infrastructure Manager	Accepted. All identified 'guest' accounts have been disable apart from Metacompliance where the 'guest' user only has connection rights to view the database table diagram.	No Further Action
4.5.3	ICT management should upgrade to the latest SQL Server service pack following the upgrade of the Horizon software.	There may be an impact to systems/ services in the event of issues caused by known bugs or vulnerabilities being exploited.	Medium	Infrastructure Manager	Accepted. Horizon upgrade is in the final planning stage. Once complete the latest service pack will be applied.	May 2019

* Risk Ratings are defined as follows:

High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.