**SHARED RESOURCE SERVICE**

**Summary of Internal Audit Activity**

**2025 – 26 Year to date**

**Introduction**

The purpose of this report is to:

* Advise of the progress to date with the current year’s Audit Plan (2025 – 26)
* Provide details of the audits finalised in the period; and
* Raise any matters relevant to the Finance & Governance Board role.

**Audit Plan 2025 - 26**

Internal audit plan progress overview:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **STAGE** | **NUMBER** | **%AGE** | | NOT ISSUED **(NID)** | 6 | 54.55 | | ISSUED **(ISS)** | 2 | 18.18 | | FIELDWORK **(FLD)** |  |  | | REPORTING **(REP)** |  |  | | COMPLETED **(COM)** | 3 | 27.27 |  |  |  | | --- | --- | | **CODE** | **NARRATIVE** | | **P** | Planned | | **I** | Issued | | **C** | Completed | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Ref** | **Stage** | **Type** | **Title** | **Quarter** | | | |  |  |  |  | **P** | **I** | **C** | | SRS – 25001 | ISS | SYS | Change Management | 1 | 1 |  | | SRS – 25002 | NID | SYS | Cybersecurity | 4 |  |  | | SRS – 25003 | ISS | FUP | Data Centre – GPA | 2 | 2 |  | | SRS – 25004 | NID | SYS | Firewall | 4 |  |  | | SRS – 25005 | COM | SYS | Identity and Access Management | 1 | 2 | 2 | | SRS – 25006 | COM | FUP | Information Security Management System | 1 | 1 | 1 | | SRS – 25007 | NID | FUP | IT Disposals | 3 |  |  | | SRS – 25008 | NID | FUP | IT Service Continuity Management | 3 |  |  | | SRS – 25009 | COM | FUP | Mobile Computing | 2 | 1 | 1 | | SRS – 25010 | NID | SYS | O365 | 4 |  |  | | SRS – 25011 | NID | SYS | Virtualisation | 4 |  |  | |

**Audits Completed in the Period**

|  |  |  |  |
| --- | --- | --- | --- |
| **Audit Title:**  SRS – 25005 Identity and Access Management | **Audit Sponsor:**  Matt Lewis / Kathryn Beavan-Seymour | | **Final Report Issued:**  15 August 2025 |
| **Assurance Opinion:**   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | | FULL | SUBSTANTIAL | MODERATE | LIMITED | NONE | |  |  |  |  |  |   34 of the 37 key controls were adequate and operating effectively. | | **Recommendations / Management Action(s)** | |
| **Audit Timeline:** 101 days | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ISS.1 – G.1 | | | Priority: Medium |
| **Control Requirement:**  Identity and Access Management objectives are defined.  **Issue:**  Management stated that individual partner policies and procedures contain the objectives, and a specific strategy or policy does not exist.  The policies/procedures provided for TCBC i.e. Acceptable Use Policy, Password policies etc. IG006, IG006A, IG008, IG008A, Doc 8.1 showed that they do not state IAM objectives.  **Risk:**  Ineffective governance and a lack of accountability. | **Recommendation:**  The SRS SLA/Service Catalogue needs to reference IAM, and its objectives stating its key objectives and linked measurable key results, (see table 1 for examples). | **Management Response:**  Agreed.  The 25/26 SLA has been rewritten to include IAM. The June 25 strategic board was cancelled so this will be formally signed off at the next meeting.  The objectives will be referred to the One Wales Governance Group for discussion with partner SIRO’s.  **Responsible Officer:**  Kathryn Beavan-Seymour  **Target Date:**  December 31 2025 | |
| ISS.2 – G.2 | | | Priority: Medium |
| **Control Requirement:**  Formal policies covering access, authentication, account lifecycle and monitoring have been developed and implemented.  **Issue:**  The policies in place do not align with those expected, as such required elements have not been adequately addressed i.e. Role-based or attribute-based access control (RBAC/ABAC) is not in place, Least privilege enforcement or Segregation of duties is not covered in the SRS Acceptable use policy, No written policy for Biometric or token-based authentication, Periodic access reviews are not in place.  **Risk:**  Ineffective governance and a lack of accountability. | **Recommendation:**  The policies in place should aligned with those expected. | **Management Response:**  Agreed.  **Responsible Officer:**  Kathryn Beavan-Seymour  **Target Date:**  April 30, 2026 | |
| ISS.3 – SAM.5 | | | Priority: Medium |
| **Control Requirement:**  When an individual leaves all access is disabled promptly.  **Issue:**  The Active Directory extract for TCBC was compared to a report of leavers, which identified individuals who still had an enabled AD account as of July 24, 25.  **Risk:**  Increased risk of compromise and inappropriate access. | **Recommendation:**  All individual access should be disabled/removed promptly after cessation of employment. | **Management Response:**  Agreed.  The SLAM process automatically deletes accounts after 1 day except where staff accounts are required for handover purposes. The One Wales Governance Group will discuss this with partner SIRO’s.  **Responsible Officer:**  Kathryn Beavan-Seymour  **Target Date:**  December 31 2025 | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Audit Title:**  SRS – 25006 Information Security Management System (ISMS) | **Audit Sponsor:**  Matt Lewis / Kathryn Beavan-Seymour | | | **Final Report Issued:**  14 May 2025 |
| **Assurance Opinion:**   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | | FULL | SUBSTANTIAL | MODERATE | LIMITED | NONE | |  |  |  |  |  |   All 71 key controls are adequate and operating effectively, the following action(s) to address the identified risk(s) have been taken:   * Business Continuity playbooks for adverse situation have been reviewed considering Information Security requirements. * Business Continuity Log includes the Information Security team (Cyber Team) who are now brought in at the start of any incident * DR Plan includes training needs and the requirement to adhere to all operational policies and procedures, including those for Information Security. | | **Recommendations / Management Action(s)** | | |
| **Audit Timeline:** 56 days | | | | |
| **Audit Title:**  SRS – 25009 Mobile Computing | **Audit Sponsor:**  Matt Lewis / Kathryn Beavan-Seymour | | | **Final Report Issued:**  12 June 2025 |
| **Assurance Opinion:**   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | | FULL | SUBSTANTIAL | MODERATE | LIMITED | NONE | |  |  |  |  |  |   The previous systems audit (ref SRS – 24009) dated January 30, 2025, identified several devices with no encryption, devices that had not been removed from SCCM, and devices that were not reporting Bitlocker Detail.  These were devices with the older version of Bitlocker.  As a result of the follow-up audit, I can report that Management undertook the following action(s) to address the identified risk(s):   * Tasks created to run every Saturday which will delete inactive client data after 90 days; to push Bitlocker out to any existing device on which it is not enabled for all LA’s. * As part of the Windows 11 rollout bitlocker will be reinstalled, reducing dramatically the number of protected devices not reporting back correctly. * Information Security will be moving to Intune reporting (the Microsoft recommended reporting mechanism for bitlocker activity).   Review of the May 2025 Delivery group PSN/Security reports showed devices still exist with no encryption or reporting no data.   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Partner | TCBC | BGCBC | MCC | NCC | GPA | **Totals** | | No Encryption | 19 | 6 | 8 | 32 | 20 | **85** | | No Data | 712 | 48 | 73 | 86 | 23 | **942** | | | | **Recommendations / Management Action(s)**  Management needs to ensure that the scripts are actively monitored to prevent instances of inadvertent removal and ensure BitLocker is reinstalled on all machines requiring it. | |
| **Audit Timeline:** 21 days | | | | |

**Key Points to Note**

*The plan is on course to be completed by the year end.*

**Audit Team**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Telephone** | **Email** |
| **Peter Williams** | Head of Audit | 01495 742278 | [Peter.williams@torfaen.gov.uk](mailto:Peter.williams@torfaen.gov.uk) |
| **Michael Corcoran** | Group Auditor | 01495 742270 | [Mike.corcoran@torfaen.gov.uk](mailto:Mike.corcoran@torfaen.gov.uk) |
| **Arran Rosser** | Senior Auditor | 01495 742275 | [Arran.rosser@torfaen.gov.uk](mailto:Arran.rosser@torfaen.gov.uk) |

**Contact Information**

Torfaen Internal Audit Service

Civic Centre, Pontypool NP4 6YB

Fax 01495 742439

[mike.corcoran@torfaen.gov.uk](mailto:mike.corcoran@torfaen.gov.uk)

