



Committee and Date

Item

Public

## **IT SERVICES, IMPROVEMENTS TO THE CONTROL ENVIRONMENT 2022/23**

### **Responsible Officer**

e-mail: David.baker@shropshire.gov.uk      Tel: 01743 254118

### **1. Synopsis**

**This report provides an update on the actions taken or planned to address the recommendations arising from the following audit reports:**

- Legacy Infrastructure and Systems
- IT Business Administration Follow-up
- Microsoft Azure and M365 Management Arrangements
- Telecommunications
- Third Party Access Controls

This report outlines the Council's current position and response to the Audits of: -

- *The management of legacy systems within the Authority. Legacy systems are those systems not in full support by the supplier or have no direct upgrade path available.*
- *The management of third-party contractor access. Third-party contractors are those external software or system suppliers that provide ongoing support and maintenance to the internal network-based systems of the council.*
- *The management of the ICT business administration. ICT Management have responsibility for the running of the internal ICT service including normal office administration of technical equipment, invoices etc.*
- *The management of Microsoft Azure and M365 services. The current arrangements the ICT department has in place to*

*manage the Microsoft based Azure and M365 services it utilises, including plans to strengthen arrangements for this area.*

- *The management of telecommunications contracts within the Authority. The council has two areas covered by telecommunications contracts, mobile phones, and unified Communications.*

## **2. Executive Summary**

- 2.1. This report outlines the Councils current position and response to several audit areas which themselves form part of an extensive programme of audit assurance undertaken each year around the Councils provision of ICT services and systems.
- 2.2. A renewed focus has been placed on contract and procurement management following the recent appointment of the Assistant Director and the Head of Service posts supervising this area.
- 2.3. The Council has a limited number of Legacy systems none of which are key corporate systems. Current Information Governance and process controls help to manage the risk posed by legacy systems.
- 2.4. The current arrangements to manage third-party contractor access have been in place for many years and have proved highly successful in safeguarding internal systems from unauthorised access to applications and data.
- 2.5. The past two and half years have seen an unprecedented fluctuation in the availability of ICT equipment which has required differing approaches to ensure that supplies are available to the Council as required. The weaknesses identified have either been addressed or are in the process of being addressed.
- 2.6. Shropshire Council has subscribed to Microsoft 365 services since 2015, in that time the functionality available to and services utilised by the Council has increased substantially. The Microsoft contract is the largest contract held by ICT, correct resourcing and investment in this area will likely yield benefits and cost savings in the wider Council.
- 2.7. A strong base of control arrangements is in place within the department however there is currently no clear direction on the scale, pace, and cost of future adoption. The new Digital Strategy 2022-2025 addresses the direction of travel and is aligned tightly to the Shropshire Plan. The scale, pace and cost will be dependent upon organisational priorities.
- 2.8. The Councils telephony contracts underpin critical Council business functions and stability in the delivery of these services is crucial to their successful operation. Regular monitoring of these contracts takes place via quarterly supplier review meetings and monthly internal contact review meetings.

### **3. Recommendations**

- 3.1. Members of the committee are asked to consider the contents of the report and the progress made to address the audit recommendations.
- 3.2. That Members of the committee consider further measures that may be appropriate, or areas for further measures that they may wish officers to investigate.

## **REPORT**

### **4. Risk Assessment and Opportunities Appraisal**

- 4.1. Legacy systems run at an increased risk of cyber-attack, service disruption and data loss due to the systems not continuing to receive security patches or are operating using outdated vulnerable components.
- 4.2. Improperly controlled external access to Council systems poses a significant risk to system and data security.
- 4.3. Improperly managed contracts pose a financial and service delivery risk to the Authority.
- 4.4. Improper control of administration rights to the Councils Microsoft estate could lead to critical loss of services and/or data.
- 4.5. Failure to control changes to the Councils Microsoft estate could lead to critical loss of services and/or data.
- 4.6. Telephony contracts (in particular fixed line) are evolving due to changing technology. PSTN connections will be removed from national use by 2025.
- 4.7. Correct investment and management of the Councils Microsoft estate will present opportunities for the Council to realise goals detailed in the Shropshire Plan.

- 4.8. A new Equipment Replacement Programme will allow for staff to receive refreshed and more modern equipment.

## **5. Financial Implications**

- 5.1. Capital investment identified to support equipment replacement business case.
- 5.2. Potential for spend to be reprofiled, allowing more equipment replacement to fall in year and all aged equipment to be replaced.
- 5.3. Consideration of centralising of IT Equipment budgets from service areas to part fund the ongoing replacement scheme.
- 5.4. Failure to effectively manage services and resources based in Azure could lead to excessive and unplanned revenue costs.
- 5.5. Safe, planned expansion of use in Azure and M365 has the potential to reduce required capital investment in future years, in particular relating to networking and infrastructure services.
- 5.6. Savings identified in mid-term financial strategy relating to telecommunications were delivered.
- 5.7. Potential future investment required to support the mandatory migration away from PSTN services by 2025.

## **6. Climate Change Appraisal**

- 6.1. Environmental impact and power utilisation of replacement equipment will be considered as part of the equipment tender.
- 6.2. Expanded use on M365 services in the future has the potential to reduce the Councils carbon footprint, for example energy costs relating to data centre services, reduction in travel and paperless services.

## **7. Background**

- 7.1. Management of legacy systems within the Authority.
  - A. Shropshire Council utilises many systems to provide services internally and externally to our citizens and partners.
  - B. The majority of systems are in full support by the relevant vendors using up to date versions.
  - C. For business area operational reasons some systems are no longer in full support by their vendors or have a limited / no direct upgrade path. These systems are classed as 'Legacy' systems and require additional controls and mitigations to be in place.

- D. All main Council supporting systems managed by ICT services are not considered to be legacy systems and are in full support with the software or system vendor.
- E. Legacy systems are recognised as posing an increased threat to data and system security and so are subject to greater scrutiny under our commitments to the Public Services Network (PSN) certification.
- F. Legacy systems are recognised as posing an increased threat to data integrity and therefore potential breaches of Data Protection legislation (Data Protection Act and GDPR).
- G. The current Information Governance process is supporting the activity to address the recommended actions identified in the audit report.

## 7.2. Management of third-party contractor access.

- A. Shropshire Council has many systems that are directly supported or maintained by external software suppliers.
- B. The breadth and complexity of systems in use in the Authority makes the exclusive internal ICT based support and maintenance of the systems an unrealistic goal.
- C. Software providers are expected and assumed to be best placed to support their product set and therefore should support best value and reliability for in use Council systems.
- D. Shropshire ICT manage and maintain the technical infrastructure supporting third party contractor access.
- E. Larger software suppliers such as Civica or Capita often have different teams supporting different products and indeed may have different technical requirements to be able to deliver their specific support.
- F. The responsibility of authorising and managing the supplier access is the responsibility of the specific system administrators.
- G. Third-party contractor access has been a feature of systems support for many decades and has evolved over time to adopt modern technologies and practice.
- H. The length of time this process has been in place has meant changes in responsibility and management within the Council has in some cases reduced business area focus on reviewing and refreshing contractor access rights.

## 7.3. Management of ICT Business Administration.

- A. The Council has a dedicated team in ICT responsible for business administration activities, with major procurement activities being co-ordinated by a member of the ICT management team.
- B. Workload and demand on this team over the past 2 years has been exceptionally high, with issues being compounded by difficulty in recruitment of appropriate staff.
- C. Process documentation is ongoing as processes will evolve, however all major processes in this team are now documented and stored centrally for staff to access.

- D. A full list of department contracts has been developed and shared with Procurement, this is now reviewed on a monthly basis with ICT and Procurement staff.
- E. Since the expiration of the previous framework contract for equipment the department has utilised multiple quotes for purchases under £50K.
- F. A competitive tender using CCS frameworks is being developed with the intention to be published this year, this will include the supply of laptops, PC's, tablets and general peripherals.
- G. Since the beginning of the pandemic equipment markets have been in a near constant state of flux, making it extremely difficult to maintain a standard equipment offering without incurring significant delays in equipment delivery.
- H. Recent world events and instability in the global financial market is contributing to ongoing disruption in the supply of ICT equipment.
- I. With support from Finance a full business case for capital investment to fund an ongoing end user equipment replacement programme is being developed prior to the issuing of the equipment tender.
- J. Engagement with major suppliers (Lenovo and Microsoft) is ongoing to determine the most suitable devices to provide to staff in the future.
- K. Initial equipment purchases have been made in support of the equipment replacement programme to allow for new equipment to begin being issued to staff.
- L. Completion of the business case and procurement are an area of particular focus for the Assistant Director of Finance and Technology and Head of Automation and Technology.

#### 7.4. Management of Microsoft Azure and M365 services

- A. The Councils adoption of M365 is at a level where its stable use and management is critical to the stable day to day operation of the authority.
- B. Management of the M365 and Azure estate is coordinated by several managers in the ICT department.

- C. Adoption and use of this area has been expanding over the last several years and this is expected to continue.
- D. All administrative access to M365 had recently been reviewed and any anomalies investigated and remediated.
- E. Strict controls of administrative access to the M365 estate have been introduced and are managed on the basis of “minimum permission required”.
- F. A project managing the adoption of security best practise has been established and work prioritised based on risk/level of exposure.
- G. Due to the wide range of services available via M365 and Azure maintaining a full awareness of all services available for use is not possible given the departments other workload and available resources.
- H. This is mitigated in part by monthly contract management meetings which are held with Microsoft where use and adoption of Microsoft services are discussed, along with technology updates given to ICT staff.
- I. An automated process to notify relevant ICT staff of changes and developments to adopted Microsoft technologies has been implemented and has been successful in ensuring Microsoft communications are monitored for relevant communications.
- J. The current management of the M365 and Azure estate is currently dispersed to staff in several different ICT teams. The planned restructure will consider if this should be maintained, or parts should be centralised to a single team.
- K. Automation capabilities in M365 and Azure have the potential to greatly support the Council in achieving the goals listed in the Shropshire Plan.
- L. There are numerous examples of use of M365 and/or Azure services throughout the Council which have been implemented with the support of ICT, which are supporting service areas to cope with increased workload and reduced resources.
- M. Future adoption of M365 and Azure services will require the expansion of skillsets for this area. Training in critical areas will be needed to avoid key staff becoming single points of failure.

#### 7.5. The management of telecommunications contracts.

- A. The Council's primary contracts for mobile telephony and fixed line communication were each left in a position where they were "rolling" beyond the specified contract end dates.
- B. This was in part caused by fluctuations in management responsibilities within the ICT department, workload prioritisation and disruption caused by the onset of the Pandemic.
- C. A full competitive tender process was completed to replace the mobile telephony contract, this was awarded to EE for a period of three years. This was signed in Autumn 2021 and fully implemented over the following six months.
- D. The previous incumbent supplier (Gamma Telecoms) contract has been fully closed decommissioned.
- E. Regular contract monitoring is now in place with EE (quarterly).
- F. Initial market engagement relating to re-procurement of this contract is programmed into ICT's work schedule to commence in Autumn 2023, with the intention to tender and fully implement a replacement contract to coincide with the expiration of the current contract.
- G. The Councils fixed line telephony contract has been reprocured for a period of two years, with the award being placed with the incumbent supplier (Maintel).
- H. Due to changes in technology (shut down of PSTN) it was not possible to migrate our current calls and lines services to a different supplier as new PSTN connections already cannot be installed due to the technologies planned decommissioning.
- I. Contract monitoring arrangements are in place with Maintel and a formal project is currently being scoped to allow all services dependent on this contract to be migrated to new solutions prior to its expiry.

## **8. Additional Information**

- 8.1. Under PSN certification unsupported systems must not be used without proper suitable mitigations that help protect from cyber-attack or general system failure. Where legacy systems exist ICT services work with business areas to attempt to mitigate the potential risks posed by such systems or to support projects to close down or upgrade legacy systems.



- 8.2. Computer system and services owners are expected to maintain their systems to PSN certification standards and where known any failure to do so is reported via the Information Governance process to the relevant senior management level.
- 8.3. The current posture of the authority and process is reducing the number of active legacy systems within the Authority.
- 8.4. The central control to managing third party access is that access is turned off by default until a proper authorisation from a business owner or system administrator is received by ICT.
- 8.5. When access is granted a time limit period is required as no open-ended access is allowed. Setting a time limit ensures that an external access is not left open after the required actions have been carried out.
- 8.6. The need for external contractors to be granted access also ensures systems administrators are fully aware of the actions of their contractors. Managing access ensures that business impacting changes cannot be carried out without proper planning and this does prevent unexpected disruption to services.
- 8.7. The recommendations in the audit report highlights that an element of renewal and review is required with the current process to ensure it continues to successfully manage third party contractor access.
- 8.8. Monthly meetings are now held with Procurement and ICT Services to better enable effective management of technology procurement activities
- 8.9. Development of an online portal where staff can order equipment is underway, once complete this will hopefully reduce workload and manual processes which ICT staff currently must follow
- 8.10. The decision on what equipment to offer to staff in future will be based on a total cost of ownership model rather than initial purchase price, which has been the driving factor in the past
- 8.11. Electricity usage and carbon emissions will also be a major part of the equipment tender, supporting the Council in its move to Net Zero and supporting with reduced electrical costs
- 8.12. Ongoing focus on procurement and contract management activities will allow for timely procurement activities to be undertaken
- 8.13. Revised Executive Management structure will allow for potential slippage or issues to be effectively managed and prioritised

- 8.14. Investigation is being carried out on training additional staff in ICT to support the procurement function, which will remove bottlenecks in capacity which currently exist
- 8.15. Monthly meetings are held with Microsoft and ICT Services to better enable effective management of Microsoft activities and services
- 8.16. Several engagements have been held with Microsoft reviewing the security and control aspects of their services which are available to the Council
- 8.17. Several engagements are being held/planned with Microsoft to explore further adoption of their services and identify their potential to realise efficiencies and savings in other areas of the Council
- 8.18. Safe management of the Microsoft estate will require maintaining and developing new skillsets to ensure the Council remains current in its control of this area
- 8.19. Given the frequent number of updates Microsoft releases there will be a requirement for the controls in place to be reviewed regularly to ensure they are meeting the Councils requirements
- 8.20. The replacement mobile phone contract has allowed staff to make use of new technologies (such as 5G) which started to become available in Shropshire during the tender process
- 8.21. Fixed line telephony is dependent on PSTN (Public Services Telephony Network) connections. This technology is being decommissioned nation-wide with a formal shutdown date announced for 2025
- 8.22. All services reliant on PSTN must be migrated to new solutions before 2025, and in parts of Shropshire it is already not possible to install new PSTN connections
- 8.23. Ongoing focus on procurement and contract management activities will allow for timely procurement activities to be undertaken
- 8.24. Revised Executive Management structure will allow for potential slippage or issues to be effectively managed and prioritised, and there is a renewed focus on ensuring the appropriate controls are in place
- 8.25. Investigation is being carried out on training additional staff in ICT to support the procurement function, which will remove bottlenecks in capacity which currently exist.

## 9. Conclusions

- 9.1. For its size and breadth of service delivery the Council has a limited number of Legacy systems which continues to diminish over time.
- 9.2. The councils overarching security measures help to protect the legacy systems from malicious attack.
- 9.3. Third-party contractor access poses a risk to system and data integrity, but the risk is effectively managed with the current process.
- 9.4. The technical landscape for remote access is constantly evolving and the technical capabilities supporting the process should continue to be reviewed to ensure they are still suitable for the task.
- 9.5. Effective management and completion of procurement activities is vital to ensuring stable delivery of service
- 9.6. The supply of ICT equipment has been heavily impacted by global and nationally events which will need to be monitored to ensure that this does not present difficulties to the Council in the future
- 9.7. Effective controls are in place for the ICT Business Support function
- 9.8. Appropriate plans are in place to allow for the completion of the outstanding equipment business case and framework procurement contract
- 9.9. The technology landscape relating to communications is evolving rapidly and appropriate focus will be needed on this area to ensure that this does not present difficulties to the Council in the future
- 9.10. Effective controls are in place for the management of our telecommunication contracts
- 9.11. The revised management arrangements for ICT will allow for better control of these areas in the future

**List of Background Papers (This MUST be completed for all reports, but does not include items containing exempt or confidential information)**

**Cabinet Member (Portfolio Holder)**

**Local Member**

**Appendices**

[Please list the titles of Appendices]

## Appendix A

### KEY

<b>BLUE</b>	COMPLETE / IMPLEMENTED
<b>GREEN</b>	PROGRESSING ON TARGET / RISK EFFECTIVELY MANAGED
<b>AMBER</b>	DELAYED / POTENTIAL FOR RISK ESCALATION
<b>RED</b>	SIGNIFICANT DELAY / RISK NOT EFFECTIVELY MANAGED

### LEAD OFFICER

DB	DAVID BAKER
IC	IAN CHURMS
DP	DEAN PRESSLEY
CH	CLAIRE HALL

Recommendation	Status	Rec. Rating	Management Response	Lead Officer	Date To Be Actioned	New Target Date	Updated Position	Rag Status
----------------	--------	-------------	---------------------	--------------	---------------------	-----------------	------------------	------------

The legacy it hardware and software security policy lists thirteen mitigations. As some of these are not related solely to legacy systems or are no longer applicable the policy should be reviewed and updated.	Open	Requires attention	The policy will be reviewed by ict and a proposed revision will be submitted to ig.	IC	31/05/2022	Dec-22	Policies have been taken to ISIG and are being reviewed as part of the ISIG programme.	Green
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
Either as part of the information gathering process for the system register replacement or as a separate exercise, legacy systems, i.e. Those being close to or out of support, should be identified together with mitigations in place. This is a complex and time consuming exercise which will require drawing together various pieces of information gathered from various existing record and device discovery exercises. As such it should be treated as project to ensure it is properly co-ordinated. The council needs to understand any exposures in its attack surface and as legacy systems present a risk to the overall ict security posture of	Open	Significant	This will be discussed with the Exec Director of Resources to determine if it is appropriate to be included in DTP phase 2 as it is an outstanding action from DTP phase 1. Any activity in this area would require significant investment in time and resources from staff across the Council so any activity to fulfil this would require significant senior management support.	DB	31/05/2022	Apr-23	David Baker has discussed with Ben Jay and keen to press ahead. Will need significant time allocated, potential issue around timescales. Data gathering exercise will take place to determine how we best use info to identify legacy systems. Needs to be run as a project.	Green

the organisation, the recording of legacy systems can be used as the basis for resource allocation to prioritise their replacement.								
Where the Legacy IT Hardware and Software Security Policy mitigations cannot be fully enforced the exceptions should be approved by Information Governance.	Open	Requires Attention	Agreed, this will be included as a clause in the revised policy.	ICT/IG	30/06/2022	Dec-22	Review of legacy IT security and hardware policy to be carried out for ISIG meeting.	Amber
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
The ict risk register should contain details of the legacy system risk level in relation to vulnerability exposure. This should be based on the level of mitigations in place captured as part of the record of legacy systems	Open	Requires attention	This can only be implemented fully if the project recommended in rec 2 is executed. Where known this will be completed.	DB/IC	30/06/2022	Dec-23	This will need to be done in conjunction with rec 2. A full register will need to be developed to allow this to be addressed.	Amber
As part of the project as proposed in recommendation 2, arrangements should be made to investigate and mitigate the risks or seek exceptions for the legacy systems detailed in this audit.	Open	Requires Attention	This can only be implemented fully if the project recommended in rec 2 is executed.	DB	30/06/2022	Mar-23	To be included in the recommend project, considerations around recharging will be discussed with Finance.	Amber

To investigate the use of legacy protocols and where possible to remove this form of authentication.	Complete	Significant	This will be investigated but any decision to remove legacy protocols will require business approval. This will be managed via the IG process. Use of legacy protocols is reviewed during our annual PSN health check and risk rated for business impact if removed.	IC	31/10/2022	N/A	Review of legacy protocols was completed. Procurement activity is underway in print unit to upgrade systems requiring legacy protocols. Print system was upgraded and we are monitoring MS notifications of end of life protocols.	Blue
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
The introduction of some form of standard charge for legacy systems maintained on the network should be considered in order that there is a cost differential established for services retaining unsupported systems.	Open	Requires Attention	Where direct costs are incurred these would be recharged to the specific business area. We will investigate with the Council management whether they wish to introduce more specific charging.	DB	30/04/2022	Mar-23	Will be considered as part of the recommended project. Will be dependant on us knowing legacy system however we need to determine how much extra cost legacy systems are incurring to protect and support.	Amber
Ideally there should be a specific third-party access policy, however as a minimum the various policies and procedures which have some reference to third party external access should be updated to reflect both current and best practices in relation to "external access" arrangements. This should for	Open	Requires Attention	A specific third-party access policy will be discussed in Information Governance (IG) for a decision on whether to document a specific policy, once this has been decided and documented a review of external access arrangements will be carried out to identify where current arrangements	IC DPO Information Governance (policy documentation)	June 2022  September 2022	Dec-22	Policies have been taken to ISIG and are being reviewed as part of the ISIG programme.	Green



example reflect the Council's use of cloud services (e.g., B2B), a requirement for periodic confirmation of third-party access agreements and the removal of outdated information from the guides to "Access to information or systems by a third party".			are not in line with the new policy.					
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
The Identification and Authentication Policy and Network Security policies in relation to third party access should be brought into line with each other in relation to the requirement for multi factor authentication.	Open	Requires Attention	These policies will be reviewed in line with the proposed review of the Third-Party Access policy.	IC DPO Information Governance (policy documentation)	June 2022  September 2022	DEC-22	Policies have been taken to ISIG and are being reviewed as part of the ISIG programme.	Green
Although it appears that Active Directory Organisational Units are used to classify external users, control could be improved if there was a requirement in the process for a comprehensive record of users' external access and authentication mechanisms to be maintained and that all the	Open	Requires Attention	This will be discussed with Information Governance to agree areas of responsibility if we do maintain a central register. Also, roles and responsibilities and processes will need to be agreed and communicated to the business. Once completed a review of external accounts will be carried out to	DP	OCT-22	DEC-22	Being discussed with ICT and IG to determine who is most appropriate to own this process	Green

external AD accounts were now brought into line with the current naming convention of having a "EXT "prefix. The record currently being maintained by the service desk could form the basis of such a comprehensive record.			determine any accounts which need modification to their naming convention.					
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
In addition to the requirement for periodic confirmation of user access compliance through a requirement to renew the access-to-information-or-systems-by-third-parties declaration, periodic reviews of external Active Directory accounts should be completed, and any dormant accounts removed. In addition, Guest user access should be reviewed periodically, Microsoft in their documentation suggest this be conducted every four months.	Open	Significant	This will be considered as part of the general process review recommended elsewhere in this audit. If it is decided to proceed an automated way of monitoring activity and removing unnecessary guest access will be investigated for implementation.	DP/IC	Oct-22	DEC-22	A number of have been disabled that have been inactive for a period of time. We need to review and look at the tools available as well as allocate staff to complete this work	Amber

As part of a review of contractor accounts and possible renaming to conform to the EXT naming convention the end date and password expiry settings applied to these accounts should also be reviewed.	Open	Requires Attention	The accounts identified in this finding will be reviewed as they appear to be system accounts rather than supplier or EXT accounts. The password and expiry settings will be considered as part of the policy review recommended elsewhere in this audit.	DP	OCT-22	Q1 2023	Review complete and external accounts have been consolidated, a review of system accounts is in progress.	Green
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
Guest access should be reviewed, and Multi Factor authentication should be enforced, this could be implemented on a risk basis, if necessary based on the nature of the information being accessed. As part of this review the access requirements for the ADASS employees should be reviewed to determine whether the current methods provide an appropriate and secure mechanism of access, particularly given that they have both Active Directory and one or more Azure (B2B) Guest accounts.	Open	Significant	ADASS currently operate within the Shropshire Council (SC) network and conform to the MFA requirement (password and device certificate). Their user accounts and devices are configured to communicate with their separate M365 tenant (which the SC IT department manages) to allow them to have their own email suffix and SharePoint infrastructure. Their guest accounts in the SC M365 tenant will likely be a result of SC SharePoint or Teams sites being shared with WM-ADASS as technically this would be required as they will be accessing SC	DP/IC	SEPT-22	Q2 2023	MFA data is not currently required for guest account logins. This will be tied into zero trust security.	Green

			Teams/SharePoint from a different M365 tenancy. A general review and redesign of how WM-ADASS and other organisations are configured has been planned for some time however due to over overriding work priorities and limited staff resources this has not been possible to date. Once recruitment of the AD for Finance and Technology and Head of Service for Automation and Technology has been completed this will be discussed to determine if it is a corporate priority for delivery, if appropriate we will then resource the required work.					
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
As recommended in 2020/21, The business case for the annual equipment replacement programme as set out in the Council's Workforce Digital Strategy 2020/21 should be completed at the earliest opportunity and submitted for approval. Following this a budget should be agreed, formally approved and subject to regular monitoring to ensure that spend is appropriate.	Open	Significant	A proposed budget for equipment replacement has been included in the 2022/2023 capital budget proposal that will be discussed at the February Council meeting. ICT is beginning preparatory work to implement an ongoing PCR scheme in the new financial year on the assumption that the budget will be approved. Ongoing monitoring of this will form part of the monthly budget monitoring and capital budget monitoring training has been attended by several ICT staff.	DP	February 2022 - Budget April 2022 - PCR Scheme	Oct-22	Budget has been approved by finance. We are setting up a 2 phase implementation for a replace scheme and a business case outlining this is with AD. We haven't yet agreed on ongoing monitoring. This will be discussed with finance business partner. DP is working through. Requested template for appendices DP has been asked to complete. Aiming to feedback to finance by end of the week minus appendices unless they share before then.	Green

As recommended in 2020/21, at the earliest opportunity ICT Business Administration procedure notes should be brought up to date, formalised and disseminated to key officers to ensure that, in the event of new staff or unscheduled absences, clear instructions are available which enable ICT Business Administration tasks to be undertaken.	Complete	Significant	Work has commenced on this however due to 2 staff members leaving this team in the second half of 2021 and delays with recruiting replacements this has not progressed as hoped. A new staff member will be joining this team in mid February and this work will be prioritised following the financial year end.	CH	31/07/2022	N/A	We have procedures saved in SharePoint. Support Services/Admin/New Procedures. It is something that we will keep adding to as processes are reviewed	Blue
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
As recommended in 2020/21, action should be taken to ensure that contract information is up to date in Business World at the earliest opportunity.	Complete	Significant	Significant work has been completed by the ICT Business Support and Corporate Procurement teams on this subject. A single complete view of our contracts has been documented and is available to all relevant staff members for review. Contract updates are provided in the fortnightly ICT Board meetings to ensure any required actions are identified and allocated to the relevant responsible officer	N/A	Implemented	N/A	Implemented	Blue

As recommended in 2020/21 a contract for the provision of ICT hardware i.e. PC's, laptops and mobile devices should be secured in line with the Council's Contract Procedure Rules at the earliest opportunity.	Open	Fundamental	Activity is underway to procure a contract for this provision, it has been delayed due to limited staff time and other procurement activities requiring attention. Given current lead times on these activities we are forecasting April for this to be complete – it is also a pre-requisite of a formal PCR programme. In the interim when equipment is purchased multiple quotes are sought and individual purchases are below the procurement threshold, however it is recognised that this is not a sustainable position.	DP	30/04/2022	Dec-22	Doing 2 procurements to cover this. Using the KCS framework to allow for direct award based on price. 2nd is a 3 year contract through ccs. KCS implemented this month. Had call with suppliers on different technologies and call with Microsoft next week to discuss hardware options.	Green
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
As recommended in 2020/21, in addition to action being taken to ensure that an appropriate contract is in place for the provision of ICT Hardware, officers should be reminded to ensure compliance with the Council's Contact Procedure Rules. This includes adherence to the formal tender process for major contracts, which includes the contract for the provision of ICT Hardware which has been identified at pre award as a major contract. The management of contracts should be prioritised, this includes their	Complete	Significant	ICT staff have attended recent procurement training and contracts/procurements are a standing agenda item on ICT Board meeting agendas.	N/A	Implemented	N/A	Implemented	Blue

renewal which should be considered well in advance of contracts expiring to ensure that appropriate, approved and ongoing arrangements are in place.								
As recommended in 2020/21 a list of consumable products from approved suppliers should be established and kept up to date.	Open	Requires attention	This is not currently possible due to ongoing market fluctuations relating to global supply issues for electronic products. Once the market situation stabilises this will be put in place, however we cannot currently "standardise" our consumable product list without risking significant delays fulfilling staff orders.	CH	June 2022 - market review	Mar-23	We are still struggling with stock at the moment – so we need to give the market longer to settle down – we are finding we get a quote for something one day and come to order it the next its gone at the moment so not able to do this one at the moment.	Green
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
As recommended in 2020/21, action should be taken at the earliest opportunity to undertake monthly stock checks to ensure that ICT equipment can be accounted for and is fit for purpose. Any discrepancies and/or concerns should be reported to senior management and where applicable the supplier without delay. Assurance should be sought that the processes and procedures in place for the delivery and receipt of ICT purchases are appropriate and steps are being taken to ensure that the risk of stock being misappropriated, lost or received as damaged or	Complete	Significant	Monthly stock checks are now in place, due to staff turnover and limitations placed on Shirehall access this did take longer to implement that originally planned. Investigations are proceeding on implementing an electronic stock management system however it is not known if this can be achieved within our existing system portfolio. If this is not possible given the current financial situation it is unlikely this will be pursued.	CH	April 2022- investigatory work	Q3 2022	We are doing the monthly stock checks and we are looking into using Ivanti as a stock system	Blue

incorrect is mitigated or reduced. Furthermore, investigations should be progressed on the use of a barcoding system to track stock more efficiently.								
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
There should be a fundamental review of the services delivered by ICT and of the delivery and support methodology and staffing. The council should establish where it is in relation to the cloud adoption framework and use it for azure to build the right adoption strategy, to ensure that the council takes full advantage of azure to meet its digital transformation goals.	Open	Fundamental	A proposed restructure of ICT as a service is being proposed as part of the Corporate Digital Strategy. Through normal operation and audit review the gaps in responsibility and ownership have been identified and these findings should feature as part of an overall ICT services review that can feed into the proposed service restructure. Alignment to corporate and business aims should be to the fore and of any tool or service. Currently the alignment has been ICT lead rather than business lead and this has been identified in other audits outside of ICT. The new Corporate and Digital strategy should address this.	DB	Following the formal adoption of the digital strategy and after direction and approval by the head of resources on the approach. Q4 2022	Q2 2023	N/A	Green



Governance and operational procedures for allocating, managing and reviewing active roles should be documented and implemented. A fundamental review of the current allocation of azure roles and azure active directory roles should be undertaken and best practices in relation to both should be adopted.	Complete	Significant	This has been captured in other audits and some previous proposed actions have been superseded by the proposed ICT restructure. Temporary allocation of roles and responsibilities has been implemented pending the restructure and further work is being undertaken based on actions identified by other audits. One such activity is a full review of roles and responsibilities for elevated privileges that has been prioritised as part of our cyber security readiness work	DB	As above q4 2022 other actions supporting the immediate need as identified in other audits elevated rights review and related actions March 2022	N/A	Review of admin roles of IT staff has been undertaken and anomalies identified and rectified. PIM has been implemented for m365 based roles.	Blue
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
The council should adopt best practice in relation to the concept of least privilege for the allocation of both azure and azure active directory roles.	Complete	Significant	Agreed and work is being undertaken as part of our cyber readiness work	DB	31/03/2022	N/A	Reviewed access and implemented PIM and removed access for those who those who it was believed it was no longer required.	Blue
Azure and O365 administrative and security procedures should be documented including the rational for any security settings within the portals	Open	Requires Attention	Agreed. Urgent reviews of current settings are being carried out as part of our cyber readiness work. We will explore ways of efficiently recording the rational for each setting.	IC	Documentation of our key security settings June 2022	March 2023	A project reviewing our security position in M365 is underway, this will be included in that work	Green

<p>A detailed review of the existing procedures, configurations and policies and evaluation against the NCSA/Microsoft O365 security assessment guide and the blueprint for secure configuration in the public sector should be completed to ensure that they meet the "better" level of security advised by Microsoft.</p>	<p>Open</p>	<p>Requires Attention</p>	<p>We have an ongoing relationship with Microsoft around best / better practice and have made changes as part of that engagement over many years. We are currently working with Microsoft around the adoption the e5 security features to ensure we apply correctly and appropriately to meet business need. As part of the this process a review of security stances and postures is included.</p>	<p>IC</p>	<p>The second of these assessments is being undertaken now. Final report will be completed March 2022</p>	<p>Q4 2022</p>	<p>Microsoft assessments have been completed and recommended actions have been factored into a work plan developed by ICT which is being reported on a fortnightly basis to the safety and resilience group.</p>	<p>Green</p>
<p><b>Recommendation</b></p>	<p><b>Status</b></p>	<p><b>Rec. Rating</b></p>	<p><b>Management Response</b></p>	<p><b>Lead Officer</b></p>	<p><b>Date To Be Actioned</b></p>	<p><b>New Target Date</b></p>	<p><b>Updated Position</b></p>	<p><b>Rag Status</b></p>
<p>As part of the recommended general review of azure and o365 responsibilities, cost monitoring and billing responsibilities and azure role allocations should be clearly defined.</p>	<p>Open</p>	<p>Requires Attention</p>	<p>ICT management/global administrators currently have budgetary responsibility for azure costs. Temporary allocation of roles and responsibilities has been implemented pending the restructure and further work is being undertaken based on actions identified by other audits. A proposed restructure of ICT as a service is being proposed as part of the</p>	<p>DB</p>	<p>Completed Completed ICT restructure Q4 2022</p>	<p>MAR-23</p>	<p>Linked to restructure of ICT</p>	<p>Green</p>

			corporate digital strategy. Through normal operation and audit review the gaps in responsibility and ownership have been identified and these findings should feature as part of an overall ICT services review that can feed into the proposed service restructure.					
The monitoring and response to m365 updates should be included as part of the overall review of procedures and management review.	Open	Significant	A proposed restructure of ICT as a service is being proposed as part of the corporate digital strategy. Through normal operation and audit review the gaps in responsibility and ownership have been identified and these findings should feature as part of an overall ICT services review that can feed into the proposed service restructure	DB	Q4 2022	N/A	Linked to restructure of ICT Taken actions to make sure we are monitoring MS updates and are now allocated out to relevant teams when they get issued to us.	Green
<b>Recommendation</b>	<b>Status</b>	<b>Rec. Rating</b>	<b>Management Response</b>	<b>Lead Officer</b>	<b>Date To Be Actioned</b>	<b>New Target Date</b>	<b>Updated Position</b>	<b>Rag Status</b>
The fixed line and mobile contracts should be prepared and issued for tender as soon as reasonably possible. A full business case should be prepared for the fixed lines contract. In future the process to retender contracts should be started prior to the expiration of the current contract.	Complete	Fundamental	Procurement activities for these contracts are underway. As communicated during this audit there are technical reasons why some of the procurement activity has been delayed, these reasons still exist (the main one being the proposed closure of Shirehall in three years). Staffing resources in the ICT department and the Telecoms area in particular have been severely stretched, we are	DP	Business Care RE Additional Staff – Sept 2020  RFI for Fixed Lines – Sept 2020  Business Case for Procurement– November 2020	Q3 2022	Mobile phone and fixed line contracts have both been awarded.	Blue

			currently attempting to obtain funding for an additional position to alleviate the work burden which should allow more attention to be given to this area in future. A procurement timeline for these contracts has been developed.		Procurement – Jan 2021			
--	--	--	---	--	------------------------	--	--	--