Powys County Council
Technology Assurance Framework Review

Final Report

Issue Date: 25th April 2023

Executive Summary

Background

To support the future direction of how ICT is provided for the authority by providing a focused and targeted ICT audit plan, SWAP have undertaken an outline ICT risk scope assessment which takes a high-level view of the strategy, infrastructure, estate, and projects. No formal testing has been undertaken however an opinion on any inherent risk has been stated. This can be a useful reporting tool for committees and for ICT audit planning going forward.

A remote workshop session was facilitated by the SWAP Technology and Digital Audit Team on Thursday 25th October over Microsoft Teams. It was attended by the following:

- Senior Manager Digital Operations
- Head of Economy and Digital Services

Opinions and findings in this report are based on the workshop held and where stated, any subsequent follow up meetings with evidence provided by management.

Pages 5 to 19 of this document show a breakdown of the areas covered and audit notes around risk. Where a solution is already in progress or the organisation has already identified the risk, a summary is provided in the findings.

Conclusion

This review has highlighted elements of potential inherent risk to the ICT Service Provision both operationally and strategically. These are detailed in full within the main findings and are summarised below. These also represent the suggested high priority areas for further full risk-based assurance reviews subject to agreement with management. For other areas reported SWAP can also help with specific risk advisories to add value to findings.

1. **Strategic Documentation**
   We recognise that the authority has adopted an agile approach to its strategic documentation including the Digital Strategy. However, there may be an inherent risk that controls relating to the policy and procedure documents that are dependent on these strategies may not align with a strategic requirement being created from the agile approach. Consequently, we would the opportunity to provide further assurance regarding the control framework of the strategic approach with a further detailed review on this theme.

2. **Infrastructure and Enterprise**
   As highlighted under section 1, there has not been previous formal assurance on risk regarding the current strategic approach to provide direction to any developments in this area. Therefore, both any changes or the current approach to the enterprise and infrastructure would be dependent on the objectives outlined in such strategic documentation.

3. **Data Centre and Hosting Arrangements**
   We have recognised the continued imperative nature in terms of data processing/storage of the Councils Data Centre. No assurance has been given by SWAP regarding the operation of these data centres in over five years. Though we do recognise that the Council has received external assurance on the operation of its data centre and has achieved an IASME Gold Status. Given its continued imperative nature in terms of data processing/storage and the potential single point of failure for the delivery of the ICT service, we recommend a further review to provide assurance on the management at this facility including the impact of the assurance provided by IASME.

4. **Network**
   We are encouraged that the current approach to the provision of the WAN presents little risk in terms of network management. However, planning for future network capacity in line with digital ambitions has a dependency on the issues already raised above in Section 1.

5. Applications and Software

We have recognised that there is a strategy to the wider approach of applications, however this is currently out of date. While we recognise that the Digital Strategy does provide high level goals, these goals should be supported within a timely applications strategy. This may highlight risk for the effective management of applications at the authority. As an example, without a clear and current applications strategy, there remains a risk that applications may be in use or be commissioned that add little value to the wider corporate objectives of the authority.

Additionally, while we recognise that a number of applications have been identified as core applications within the application register, we have noted that other critical applications are not highlighted. For example, Active Directory, contact centre and customer relationship applications, and remote access applications e.g. VPNs. This may present risk for the effective management of applications which, in turn could lead to the inability to effectively integrate and manage data across applications and platforms.

6. Ongoing Projects

Whilst the current management of the wider operational project processes within the Digital Delivery group do not present immediate risk, we would highlight our earlier finding in Section 1. Any activity undertaken must be defined within requirements agreed as part of the control framework within the ICT Strategy and Digital Strategy. Consequently, we would welcome the opportunity to provide further assurance regarding the control framework of the strategic approach with a further detailed review on this theme. Once assurance has been given regarding mitigated risks with the associated governance routines supporting these strategies, it will help define the accountability and responsibility of the Digital Delivery Group with the associated involvement of the ICT Service.

1. ICT Governance and Links to the Executive Board

Findings

1.1 Governance & Service Delivery

Powys ICT Service is delivered largely in house, with some supplier services consumed for cloud arrangements. The service also provides support to the local health board, Powys Teaching Health Board. The Councils ICT services are led by the Head of Economy and Digital, who is supported by the Digital Operations Manager. The Head of Economy and Digital forms part of the Senior Leadership Team and directly reports the Director for Corporate Services who forms part of the Executive Leadership Team. Under the Digital Operations Manager there are approximately 80 staff and six key managers within the ICT Service:

- ICT Operations Manager – Applications Team
- ICT Operations – Infrastructure Team
- ICT Operations Manager – End User Services Team
- ICT Technical Architect
- ICT Technical Architect – Applications
- Cyber Security Manager – Security Team

Further to this, there is also a separate Digital Programme Team that falls under the Head of Economy and Digital, with the Manager for Digital Services sitting adjacent to the Digital Operations Manager. It should be noted that the Digital Operations Manager specifically manages the ICT Service, not the Digital Service, and has no direct connection to the Digital Service besides the adjacency to the Manager for Digital Services.

We established that there is not a technical design authority in place. However, the Change Authorisation Board (CAB) features Technical Architects, Security Reps, and Infrastructure Reps. This is then supported by the ICT Governance Board which has oversight of all activities within the ICT Service. The CAB meets at least once a month to discuss changes and allow the technical members of the team to provide technical assessment of any changes.

We were informed that staff professional development is supported through a skills and training matrix that was created by Powys to assess staff training needs. There is also a program ensuring that once training required for roles is completed that potential future training opportunities are explored. These form part of the annual appraisal process that services across the authority use to identify their staff training needs.

We established that the ICT Service have built and operate their own ICT Service Management System called LogIT. Within this there is also maintained a catalogue of the services provided by the ICT Service. Within this, work is also underway to construct a configuration management tool within LogIT.

1.2 Strategy and Policy Framework

We were informed that the Digital Strategy contains reference to technology and how this fits with the Councils digital ambitions. We were provided with a copy of the Digital Strategy which spans from 2019 to 2025 and is due to be refreshed in 2023. Whilst there is no formal ICT stand-alone strategy, we were informed that there is a view to approach the ICT Strategy in an agile way. Powys has purposely not invested in the creation of certain strategic documentation, as success has been found with this approach, such as the move to large scale remote working in 2020.

We were informed that there is an Information Security Policy, however this has a last review date of May 2018 and a next review date of June 2020. As such this document is out of date and may not accurately reflect the current approach to information security at the authority. We were informed that this is supported by additional security policies e.g acceptable use, and we were provided with evidence of these supporting policies. Review of these policies is undertaken by the security manager, and each policy has its own date scheduled for review. We were informed that these are currently due for review.

These documents are made available to all staff via the corporate intranet, and the Digital Strategy is also publicly available on the Councils website.

Audit Note on Risk
We have noted that the current approach to the strategic framework covering technology at the authority. Whilst appreciating the Agile approach to the ICT strategy, later findings in this report indicate a clear dependency to an effective control framework starting from the Digital Strategy. At present, as part of this review, we are unable to offer specific assurance around this control framework. Therefore, we would recommend a further risk-based review thematic to this strategy approach, to provide management with assurance over the mitigation of risk. *We noted the Information Security Policy is out of date and may not accurately reflect the Councils current approach to information security. Additionally, the supporting framework of policies are due for review. We would welcome the opportunity to undertake an assurance review with regards to addressing risks surrounding the operational management of the policy as whole.*

Management Response	Timescale	30th June 2023
ICT have previously recognised that many of its policies are over due a review and have committed to reviewing every policy annually. There is also a council wide workstream currently ongoing to manage the review and update of policies which ICT are feeding into.	Responsible Officer	Cyber Security Manager

2. Infrastructure, Enterprise and Platform

Findings

2.1 Infrastructure and Enterprise

We were informed that the authority supports approximately 3000 corporate staff as well as users within schools e.g. teachers. Additionally, support is also provided to approximately 3000 health board users as part of an agreement with Powys Teaching Health Board.

Desktops and Laptops

We established that the authority makes use of a mix of desktop and laptops, with 154 desktop devices, and 2,537 laptop devices. These are a mix of Dell and Lenovo devices. However, a very small number of laptops in use are Apple products used by graphic designers, and there are also a small number of Microsoft Surface devices. All desktop and laptops operating on Windows OS are operating on Windows 10, with a small number of laptops also trialling Windows 11 within the ICT Service. These devices are all operating on a thick client basis (see glossary).

Desktop devices have been rationalised where possible, and the remaining number represent those where a fixed workstation is required, such as in libraries for public use, as well as some depot locations. The long-term approach to laptops is to continue refreshing these devices in a cycle every five years, however consideration for extending this to 6-7 years is ongoing. Laptops have a general standard build that is provided to most users. There is also a higher specification build that can be requested by managers for a user. However, distribution of these is ad hoc and undertaken at the end of a refresh cycle, subject to budget approval for the device.

Mobile Phones and Tablets

We were informed that approximately 100-150 iPads are in use. Tablet devices are primarily assigned to field-based roles, such as members of the outsourced property team. Tablets can be requested for users by managers via the same process as requesting high spec laptops devices.

There are 1807 Android mobiles and a further 298 talk and text exclusive phones in use. These are Samsung Galaxy A9's for the android mobiles, and Nokia devices for the talk and text devices. All android devices are operating on Android 10 and above.

The approval of purchasing and assignment of mobile phones for users is undertaken by individual heads of service. Android mobiles are primarily issued to field-based roles that may need access to emails or other online items when not able to make use of a laptop. The Nokia devices are also primarily for field-based roles where there is a need for the user to call and check in, or for emergencies. The Nokia devices are exclusively call and text only and have no mobile data capabilities. The current approach is to reduce the mobile estate and move to adopt a Bring Your Own Device (BYOD) for Office 365 functions to address the number of corporate mobiles.

Server Infrastructure
We established that there are currently 16 physical servers in use, which are running approximately 200 virtual machines (VMs). All of these physical servers are Dell devices, and the virtual machines are MS Hyper V and VMWare supported VMs. We were provided a list of the physical servers and confirmed that these are all Dell devices. These servers provide storage, Active Directory, Business Application Servers, and Virtual VPN functions for the authority. There is some clustering of the virtual servers, specifically the VPN and Active Directory Servers are each clustered, and there is a VMWare Hypervisor cluster that provides load balancing functions.

Hardware Inventory
We established that there are multiple tools used to maintain the hardware inventory:

- Servers and network devices are inventoried using the network monitoring and management tool Solarwinds.
- CISCO Devices are monitored and inventoried through the CISCO Identity Services Engine and Prime system.
- Laptop and Desktop devices are inventoried by the Microsoft Configuration Manager (SCCM) and MS Intune.

We were informed that there is not one central repository for this information where a complete hardware inventory can be viewed. However, an approach is being established to move to store all hardware items within a central repository within LogIt. Currently these inventories are maintained separately and primarily manually, however there is some automation conducted by applications such as SolarWinds and Intune.

ICT Service Management
We established that the authority currently supports a total of 10 corporate sites, and approximately 90 school sites. We were informed that the LogIt system, as outlined in section 1, is the ICT Service management system. It also provides the authorities Service Desk functions. Powys maintains an in-house service desk and provide first, second, and third-line support.

Users are able to contact the service desk via phone, web portal and email, although email contact is discouraged, between 8:30am and 4:00pm Monday to Friday. Consideration is also being given to establishing a web chat function as another contact route. There is no out of hours support for general users and any contact outside of the supported hours is picked up the following working day. However high priority users e.g. councillors can contact ICT Managers for issues. We were informed that through the Digital Hub web portal there are guides and support articles available to users, but little provision for user self-service, such as automatic password resets. All support tickets at first, second and third line are processed and monitored within the LogIt system. We were informed that second line support is provided by the Infrastructure and Applications Teams, these teams will contact external supplier support as well as needed. Third line support can be provided by Software Developers and Solutions Architects if necessary.

We were informed that the authority has based its approach to security and vulnerability management around the penetration testing conducted as part of the PSN compliance and annual ITHC. Additionally, the authority maintains Cyber Essentials Plus accreditation. There is also work underway towards ISO27001 accreditation due to the support provided to the Powys Teaching Health Board.

2.2 Platform

We established that the Digital Strategy contains some reference to adopting a cloud first/cloud on replacement approach, although currently that majority of platform used is in house. The in-house platform hosting supports the on-site backups, application servers and storage, while the cloud platforms consumed are Azure primarily for back-up storage and a few select application purposes, and Amazon Web Services (AWS). There is also a project underway to review moving a greater amount of the service to a cloud platform.

Audit Note on Risk
As highlighted under section 1, there has not been previous formal assurance on risk regarding the current strategic approach to provide direction to any developments in this area. Therefore, both any changes or the current approach to the enterprise and infrastructure would be dependent on the objectives outlined in such strategic documentation.

Management Response	Timescale	31st October 2023
Significant work has been done over the last 5 years to reduce the risk relating to the County Hall Datacentre; specifically due to system migrations to the cloud or supplier hosted datacentres. Although single points of failure do still exist in the on-premise infrastructure many of the key systems are cloud based and require no or limited on premise infrastructure including but not limited to O365, HR & Payroll, Finance, WCCIS, Telephony, Revs and Bens, Paygate, Teacher Centre, Website, CRM.	Responsible Officer	Senior Manager Digital Operations

3. Data Centre and Cloud Provision

Findings

3.1 Data Centre, Hosting and Cloud Provision

We established that there is a single data centre in use located at County Hall with the premises and equipment for this site managed by Powys. There are some comms cabinets in other locations e.g. depots that retain server devices. Additionally, Powys Teaching Health Board maintains its own data centre, however the equipment e.g. server devices for this is managed by Powys. The Powys data centre hosts all the on-premises applications and 12 of the physical server devices. This site is managed by the ICT and Facilities functions, with ICT providing the equipment and specifications, and facilities providing the environment e.g. air conditioning and fire detection/suppression. This set up is mirrored in the management of the Powys Teaching Health Board data centre, but with Powys Teaching Health Board facilities providing the environment instead. External assessment of the current data centre arrangements has also been undertaken as part of the Cyber Essentials plus project. This was provided by Gaia Technologies and following changes made on the recommendations of this assessment, the authority has now achieved IASME Gold Status in its data centre.

We established that the Council operates in a hybrid environment, including hosting in MS Azure and applications hosted by the providers. The applications hosted by the providers are iTrent provided by MHR Global, E-Financials provided by Advanced Business Solutions, and the Welsh Community Care Information System (WCCIS) provided by the NHS. Consideration is being made to moving other resources from the data centre to cloud hosting where appropriate.

We were informed that backups of the on-premises items take place overnight, and this back-up is then mirrored to the Azure Cloud. Additionally, the SQL servers in use take incremental back-ups during the day to provide a complete daily back-up. To support this, we were provided with examples logs of the completed back-up schedule in Azure. Further review is under consideration with regards to air gapping of backups to prevent the back-up of an infected source data.

We were informed that there has been difficulty previously in establishing a Corporate Business Continuity Plan (BCP) and there is currently no Corporate BCP document established. Each service area maintains its own BCP, and there is no central indication of the priority of recovery in the event of a whole council business continuity disruption. We were informed that there has been difficulty in making clear to service areas that during a BCP event they need plans to operate without ICT. There is a BCP specific to the ICT Service that we have been provided with. This also functions as the ICT disaster recovery plan.

We established that there is a Disaster Recovery Plan (DRP) in place, however we have not received evidence of this document. As above with the BCP, the priority for recovery does not link to recovery objectives, as the priority of recovery has not been decided centrally. We have not received evidence of the last test of the disaster recovery plan.

Audit Note on Risk		
We have recognised the continued imperative nature in terms of data processing/storage of the Councils Data Centre. No assurance has been given by SWAP regarding the operation of these data centres in over five years. Though we do recognise that the Council has received external assurance on the operation of its data centre and has achieved an IASME Gold Status. Given its continued imperative nature in terms of data processing/storage and the potential single point of failure for the delivery of the IT service, we recommend a further review to provide assurance on the management at this facility including the impact of the assurance provided by IASME. *We were unable to obtain details of any corporate business continuity plan. Additionally, the ICT disaster recovery plan is included as part of the business continuity plan. There is a risk that without separating these plans, the different points for invocation of the disaster recovery plan and business continuity plan may be unclear, leading to inefficient or incorrect response in a disaster event. Given the imperative nature in these plans in providing a managed and effective approach in dealing with the loss of business-critical functions/processes, it is imperative that a corporate business continuity plan and a separate ICT disaster recovery plan be implemented.*		
Management Response	Timescale	30th September 2023
ICT have committed to developing a final DR and BC plan by the end of 2023/24. Although there are plans in place to deal with DR and BC it has already been identified as an area for improvement in terms of the organisation understanding its priority systems. A report was submitted to EMT and a working group has been established headed up by the councils Head of Legal and Democratic Services to agree a definitive list of key systems and priorities. *ICT are key to this process and will be completing its tasks by the end of Q2.*	Responsible Officer	Senior Manager Digital Operations

4. Network and Comms including Contact Centres

Findings

4.1 Network

We were informed that there is no network strategy in place, although feedback is being sought from technical architects regarding an approach in establishing this strategy.

We established that the WAN (see glossary) is provided by the Public Service Broadband Aggregation (PSBA, see glossary) which is managed by BT. This provides the WAN and internet for all authorities in Wales. Reliance on the resilience of the WAN is placed upon the PSBA as this is provided for the authority, and as such effectively outsourced. However, we did establish that the internet feed that runs out from the single data centre to provide this connection does represent a single point of failure in the network. Security of the network is facilitated using three main firewalls to segment the network, such as between the internet access and the main network, or between the PSN connection and the main network.

We were provided with a copy of the Powys County Council infrastructure overview, which included a high-level network topology. We established that this is a fixed document, with updates being undertaken manually with changes to the network. The network is set up in an MPLS format, and remote access to the network is facilitated using Microsoft Always On VPN (See glossary).

The network monitoring and management tool SolarWinds is used and supplied by Kedron UK. This is used to monitor the network performance and identify any bottlenecks in the network, as well as providing an inventory of network devices as outlined in section 2.

We were informed that the Powys County Council Corporate Wi-Fi is segregated from the Guest Wi-Fi, with the Guest Wi-Fi being controlled by a separate CISCO Wi-Fi controller and segmented from the corporate network by a firewall. Connection to the corporate Wi-Fi is controlled through device certificates, with only trusted devices being able to connect to the network, this is provided using CISCO Wireless Access points and these are all centrally managed through a CISCO Wireless LAN controller.

4.2 Telephony

For telephony, we established that unified comms system in use was Microsoft Teams supported by an 8x8 cloud solution provided by Softcat. All telephony is directly routed through this, including the contact centres. Calls are initially routed to the 8x8 cloud, and then directed to MS Teams. To support this, we were provided with a flowchart of the call progression through 8x8 and teams. 8x8 also provides an integrated Customer Relationship Management (CRM) system. We were informed that there is no strategy regarding any solutions nearing end of life/support or any future plans or changes to the telephony arrangements.

Audit Note on Risk
We are encouraged that the current approach to the provision of the WAN presents little risk in terms of network management. However, planning for future network capacity in line with digital ambitions has a dependency on the issues already raised above in Section 1. *Management may wish to consider further internal audit involvement as an extended risk advisory for network management in relation to the wider strategy and policy framework.*

Management Response	Timescale	31st March 2024
ICT are currently in the process of developing a business case to decide the future of the infrastructure and in particular cloud. It is therefore anticipated that the direction will change and further assurance may be sought at this stage.	Responsible Officer	Senior Manager Digital Operations

5. Applications and Software

Findings

5.1 Applications and Software

The Council makes use of the Microsoft Productivity suite (M365) with primarily E3 licenses across the estate, with 150 E1 licenses for those users that don't need the functionality of an E3 license. We established that licenses are reviewed every 12 months and there is an ongoing review of licensing, but generally the license numbers are remaining stable. We also established that some users are running on 32-bit systems, which Microsoft is ending Windows 10 support for in October 2025. The M365 and Azure tenancies are managed by the Applications Team within the ICT Service through SCCM, Intune and manual processes. These methods were established following the decommissioning of the SNOW software licensing system, as it was determined that this was more effective than the previous method. There is an approach to eventually build a full software asset management process into the LogIt platform that will be managed by the End User Service Team.

We established that there is an applications strategy, in the form of the Automation Strategic Framework. However, the timeline within this ran until March 2022. Decisions regarding software as a service (SaaS) are made based on the "Embrace Cloud First Technology" mentioned in the Digital Strategy. SaaS products are inventoried on a case-by-case basis and this requires ICT to know about it in order to add it to the inventory of SaaS products. Any service that procures SaaS becomes the contract holder and are ultimately responsible for the management of it, however they do consult with ICT prior to the procurement of any SaaS as long as a full procurement process is undertaken. Additionally, SaaS providers will not be signed off by procurement unless security checks have been completed by ICT. There is a view to move to using a cloud-based web proxy and web filtering to identify any SaaS that ICT are not aware of, as the current process requires there to have been a full procurement process for ICT to have been informed. The current approach when any unauthorised SaaS is identified would be to either retrospectively authorise the software, or deny it and remove the software, this would be addressed by ICT Governance.

5.2 Primary Applications

We were provided an extract of the applications register. We were informed that there is no priority given to these applications in terms of recovery and as highlighted under section 3 regarding business continuity and disaster recovery. As such we have based the following list based on those applications listed as 'core' within the applications register.

1. **Civica Document Management –** This is on premises hosted and provides document management for all financial services, planning and building control service, and Social Care service. Ownership of this is split between each module, i.e. the finance module is owned the finance service, the social care module by the social care service etc. This is on a 'site wide' license with a cap of 2000 users. The contract term ends this year and is currently undergoing renewal. Primary support for this is provided by the Applications team.

2. **Advanced Business Solutions (ABS) eFinancials –** eFinancials is hosted by the supplier, ABS, and used by all service areas and some schools for financial management and the processing of payments. This application is owned by the finance service. This currently supports 652 users and the current contract term ends in 2023. Support for this is provided by the applications team and the supplier

3. **ABS E-Procurement –** eProcurement is hosted the supplier, ABS, and used by all service areas and some schools for procurements and purchase orders. This application is owned by the finance service. This currently supports 549 users and the current contract term ends in 2023. Support for this is provided by the applications team and the supplier.

4. **MHR iTrent –** iTrent is hosted by its supplier, MHR, and provides the HR & Payroll functions for the Council. This application is owned by the employment services service. This is on a site wide license to allow access for all users, and the current contract term ends in 2025. Support for this is provided by the supplier.

5. **Northgate iWorld –** iWorld is hosted by Northgate and provides all the revenues and benefits functions for the Council, including billing and collection. This application is owned by the income and awards service. The current license supports 500 users and the current contract term ends in 2024. Support for this is provided the applications team.

6. **Smoothwall –** Smoothwall provides the schools web filtering functions and without it schools are unable to access the internet and applications and compromise child internet safety. The application is owned by the schools' services and is hosted on premises. The current license supports 20,000 users and there is no contract end date provided. Support for this is provided by the applications team.

7. **Teacher Centre –** Teacher Centre is provided and developed by Ceredigion County Council. Teacher Centre is the Primary School Management Information System and provides pupil records, admissions and transfers and SEN assessment records. This application Is owned by the Schools Service and is hosted by the provider. This is currently licensed for 2000 users on a rolling contract with Ceredigion County Council. Support for this is provided by the applications team.

5.3 User Developed Applications

User Developed Applications (UDA - see glossary) are solutions that are developed using proprietary office productivity applications apps within M365. They are then used to deliver business critical data and outcomes such as the Applications List created as part of the work by the Corporate Projects Team.

We established that the ICT service's current approach to UDAs is to encourage users to make use of Power Apps and other developmental resources available within M365. There are inherent risks surrounding UDAs as these are unlikely to be supported by appropriate development or testing controls. Some UDAs also do not support formal audit trails to record data changes and there is the potential loss of the accidental deletion.

Audit Note on Risk
We have recognised that there is a strategy to the wider approach of applications, however this is currently out of date. While we recognise that the Digital Strategy does provide high level goals, these goals should be supported within a timely applications strategy. This may highlight risk for the effective management of applications at the authority. As an example, without a clear and current applications strategy, there remains a risk that applications may be in use or be commissioned that add little value to the wider corporate objectives of the authority. *Additionally, while we recognise that a number of applications have been identified as core applications within the application register, we have noted that other critical applications are not highlighted. For example, Active Directory, contact centre and customer relationship applications, and remote access applications e.g. VPNs. This may present risk for the effective management of applications which, in turn could lead to the inability to effectively integrate and manage data across applications and platforms.*

Management Response	Timescale	30th September 2023
Please see response to Item 3 regarding priority systems. This will be completed by Q2 but continually updated. The strategy mentioned above has since been updated.	Responsible Officer	Senior Manager Digital Operations

6. Supporting Project and Digital Ambitions

Findings

6.1 Projects

We established that the project register is managed by the Digital Programme Manager, who leads the Digital Delivery Group. The Digital Delivery Group then make decisions on projects to proceed with.

We were provided with a copy of the current project register which is maintained using MS Planner to track the progression and identify those projects that are in progress. Each project has a project manager, each project manager may be managing multiple projects. They provide updates each month to the Digital Programme Manager.

We established that the project methodologies in use are PRINCE2 and Agile, and which method used is decided on a case-by-case basis as some projects are not suited to an Agile approach. Additionally, all Project Managers receive training in PRINCE2 and Agile, and in house Agile training has been rolled out across the whole authority. To support this, we were provided examples of project Kanban's and the project register is set up to support an agile approach.

We were informed that the primary applications used to record and manage projects are MS Planner, MS Project, and a small amount of Azure DevOps.

6.2 Digital Ambitions

Digital ambitions at the Council are the responsibility of the Director for Corporate Services, who is supported by the Head of Economy and Digital. There is also a Digital Transformation board, which includes service leads which sets IT project demands and focus. As highlighted under section 1, there is a Digital Strategy that covers 2019-2025 and outlines the digital transformation strategy.

Additionally, there is a Change Management Board (CMB). This approves all changes that occur that may cause 'significant' impact. Smaller changes are not escalated to the CMB for approval. The CMB also performs the technical design authority functions, as there is representation from Technical Architects and the security and infrastructure teams. This allows the CMB to provide technical assurance for significant changes.

We understand that in terms of business analysis resources there is a separate Business Intelligence function from the ICT service which support the Transformation Analysts within the Digital Team.

Audit Note on Risk		
Whilst the current management of the wider operational project processes within the Digital Delivery group do not present immediate risk, we would highlight our earlier finding in Section 1. Any activity undertaken must be defined within requirements agreed as part of the control framework within the ICT Strategy and Digital Strategy. Consequently, we would welcome the opportunity to provide further assurance regarding the control framework of the strategic approach with a further detailed review on this theme. Once assurance has been given regarding mitigated risks with the associated governance routines supporting these strategies, it will help define the accountability and responsibility of the Digital Delivery Group with the associated involvement of the ICT Service.		
Management Response	Timescale	30th September 2023
We will support any further work required to provide further assurance.	Responsible Officer	Senior Manager Digital Operations

7. Previous Assurance

Findings

7.1 Previous Assurance

We were informed that the most recent PSN ITHC was completed in February 2022, with the certificate for the PSN connection compliance expiring in June 2023. We were provided with copies of the ITHC Penetration Test report and the supporting action plan. Powys County Council has also undertaken the Cyber Essentials Plus assessment which reported in August 2022. Reassessment for Cyber Essentials Plus is due in February 2023. We were also provided with the Cyber Essentials Plus report and the certificate of assurance.

Glossary

Acronym/Term	Definition
AD	Active Directory
Azure	Microsoft's public cloud computing platform.
MPLS	Multi-Protocol Label Switching is a routing technique in telecoms networks that directs data from one node to the next based on labels rather than network addresses.
PSBA	Public Service Broadband Aggregation – The PSBA connects Welsh public sector organisations to a secure wide area network.
PSN ITHC	Public Services Network IT Health Check, The PSN (Public Services Network) is the government's high-performance network, the IT Health Check is used to confirm that an organisations systems meet a specified baseline standard to make use of this network.
SaaS	Software as a service (or SaaS) is a way of delivering applications over the Internet—as a service
SCCM	Microsoft System Centre Configuration Manager (SCCM) is a Windows product that enables administrators to manage the deployment and security of devices and applications across an enterprise.
TDA	Technical Design Authority – The Technical Design Authority provides assurance that business and technical decisions are right, and the solution will be fit for purpose.
Thick Client	Also referred to as desktop, fat, or heavy client, thick clients are systems that connect to servers even without a network. A thick client does not rely on server applications.
User Developed Applications	Activities or tools that involve no coding and that users can create to perform tasks such as data management, workflows, reporting etc. An example of this is an excel spreadsheet created by users to perform a workaround process outside of a primary application.
VOIP	Voice Over Internet Protocol, technology that allows for making voice calls using a broadband internet connection instead of a standard telephone line.
Virtual Machines	A computing resource that uses software instead of a physical computer to run programs and deploy applications.
VPN	Virtual Private Network, provides privacy and security by creating a private network across a public network connection.
WAN	Wide Area Network, A wide area network (WAN) is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking.

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Terms of Engagement. The report has been prepared for the sole use of. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Darren Roberts	Assistant Director, ICT
Tom Weston	Principal ICT Auditor
Adam Tankard	ICT Auditor

Distribution List

This report has been distributed to the following individuals:

Jon Evans	Senior Manager Digital Operations
Diane Reynolds	Head of Economy and Digital Services