Item:

Asset Management Sub-committee: 2 September 2025.

Information Technology Strategy – Delivery Plan Update.

Report by Director of Infrastructure and Organisational Development.

1. Overview

1.1. The Information Technology Strategy is a technical plan which underpins and supports delivery of the Digital Strategy and focusses on improving and sustaining the Council's IT systems and infrastructure. The Digital Strategy sets the vision and objectives through which all services across the Council will harness digital developments to provide improved, more efficient services for the public.

1.2. On 28 January 2025, the Asset Management Sub-committee recommended that the Information Technology and Cyber Security Strategy, for the period 2025 to 2029, be approved.

1.3. The Strategy groups actions under the following headings:

- Cyber Security
- Governance
- Customer Focus
- Digital Workforce
- Infrastructure and system
- Internal and external communications

1.4. The Strategy seeks to:

- Continue to improve the Council's underlying infrastructure.
- Provide the foundations for the rapidly moving shift towards digital delivery and support the objectives of the Digital Strategy.
- Provide an IT Strategy Delivery Plan to cover the same period as the Information Technology Strategy to ensure its successful delivery.

1.5. Attached as Appendix 1 to this report is the IT and Cyber Security Delivery Plan update for the period up to September 2025.

2. Recommendations

2.1. It is recommended that members of the Sub-committee:

- Note the updated IT and Cyber Security Delivery Plan, attached as Appendix 1 to this report.

For Further Information please contact:
Thomas Aldred, Service Manager (ICT), extension 2152,
Email: thomas.aldred@orkney.gov.uk.

Implications of Report

1. **Financial –** The report does not attempt to quantify the financial implications arising from the Strategy. Any costs arising from works associated with the delivery plan will require to be funded from within existing revenue or capital budget allocations, with any request for additional funding required to come forward as a separate report for consideration.
2. **Legal -** No implications.
3. **Corporate Governance** – No implications.
4. **Human Resources** – No implications.
5. **Equalities –** An Equality Impact Assessment is not required in respect of performance monitoring.
6. **Island Communities Impact** – An Island Communities Impact Assessment is not required in respect of performance monitoring.
7. **Links to Council Plan:** The proposals in this report support and contribute to improved outcomes for communities as outlined in the following Council Plan strategic priorities:
   ☐Growing our economy.
   ☐Strengthening our communities.
   ☒Developing our Infrastructure.
   ☒Transforming our Council.
8. **Links to Local Outcomes Improvement Plan:** The proposals in this report support and contribute to improved outcomes for communities as outlined in the following Local Outcomes Improvement Plan priorities:
   ☐Cost of Living.
   ☒Sustainable Development.
   ☒Local Equality.
   ☐Improving Population Health.
9. **Environmental and Climate Risk -** Where resources allow, improvement works can include 'greener' solutions.

10. **Risk** - Improvement of existing assets can help reduce risks associated with these assets, particularly in relation to Cybersecurity.
11. **Procurement** – All purchases of infrastructure required will meet all the requirements of the Financial Regulation and Contract Standing Orders and the Council's procurement policy.
12. **Health and Safety** - Well-maintained assets will assist the Council in ensuring Health and Safety for staff and public.
13. **Property and Assets** – Well maintained assets add value and IT security.
14. **Information Technology** - Up to date IT systems work towards a reduced risk to the Council.
15. **Cost of Living** – Not applicable.

List of Background Papers

None.

Appendix

Appendix 1 - IT and Cyber Security Delivery Plan update September 2025

Appendix 1 - IT and Cyber Security Strategy Delivery Plan Update September 2025

1. Purpose

This Delivery Plan update provides information on the progress made in delivering each of the objectives of the IT and Cyber Security Strategy Delivery Plan 2025-2029.

2. Introduction

2.1.

The IT and Cyber Security Strategy Delivery Plan update is a technical plan which underpins and supports the IT and Cyber Security Strategy and aims to improve and maintain the Council's IT infrastructure and systems.

2.2.

The table below sets out the detail of how the IT and Cyber Security Strategy is being delivered. The IT and Cyber Security Strategy has a number of strategic targets, grouped into 6 themes. Objectives have been abstracted from the strategic targets in the strategy, and the table in sub-section of section 3 below, corresponds to a group of actions (one per row) contributing to that objective.

2.3.

Each action is owned by a specific member of staff, who is accountable for the correct and thorough completion of the task, and each is led by a specific member of staff who is responsible to the owner for the planning, execution and implementation of each necessary piece of work.

2.4.

For each action, progress will be reported with a BRAG status on progress with an indication given of the next steps planned. Where appropriate, an indication is given about where to find more information about the project or workstream.

3. Actions to Support IT Strategy Objectives

3.1. Cyber Security Objectives

We will maintain a secure physical and virtual environment, with a high degree of resilience and confidence, based on national standards to present a difficult target for all forms of attack and exploitation online. To achieve this will involve detecting, understanding, investigating and disrupting hostile action against us.

Objective 3.1.1: We will implement suitable security controls to present a difficult target for all forms of attack and exploitation online.

Action.	**Owner.**	**Lead.**	**BRAG**	**Current position, September 2025**	**Next Steps.**
3.1.1.1. Public Services Network (PSN) accreditation.	Kenny MacPherson	Tony Whenman	Green	Current accreditation is in place until 30 April 2026. Preparations for the next PSN accreditation due May 2026 have started.	Organise next IT Health Check and penetration tests for September 2025. Once this is completed draw up Remediation Plan and action plan.
3.1.1.2. Build and Maintain IT Network defences following recognised (NCSC) security protocols.	Tony Whenman	Thomas Aldred	Green	Network design is based on National Cyber Security Centre (NCSC) guidelines and security protocols. A review of network design to ensure it meets guidelines has found that some IT systems, while in a secure design do not meet current best practice. A review to move systems into secure network design has been completed with new infrastructure requirements being detailed.	Continue to develop best practice designs 2025-2026 and establish financial cost implications 2025-2026. Migrate to best practice 2026-2029 where resources permit.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.1.1.3. Undertake an annual IT Health Check using an independent specialist	Kenny MacPherson /Tony Whenman	Thomas Aldred	Green	A health check is conducted annually by an external accredited cyber security specialist. Any issues identified are programmed into an Action Plan that is worked through by IT and stakeholder services. Weekly internal checks are performed by the Information Security and Assurance Officer.	Review Health Check Report. Finalise Action Plan. Apply remediation steps as per plan by May 2026. Continuous review of internal checks.
3.1.1.4. Support Systems Security	Tony Whenman	System Owners	Amber	Systems security is supported using multi-factor authentication, where technically possible, and use of password protocols with high entropy. This means reliance on password length rather than complexity as per NCSC guidelines.	Work with System Owners to introduce multi-factor authentication on an ongoing basis.
3.1.1.5. Train and educate users to defend against cyber threats	Tony Whenman	OD/ Communications /IT Support	Green	Regular notification of new threats by bulletin email and SharePoint distribution. iLearn courses.	Continue to develop ways of enhancing user participation.

Objective 3.1.2: We will develop a coordinated and tailored approach to risks and threats that we may encounter and mitigation of potential vulnerabilities.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.1.2.1. Develop and maintain Cyber risk management framework.	Kenny MacPherson	Tony Whenman	Green	Internal controls and governance for the prevention and detection of irregularities and fraud are in place.	Review and adjust controls, due end 2025.
3.1.2.2. Ensure that major cyber security risks are present on the corporate risk register.	Kenny MacPherson	Tony Whenman	Green	Cyber security is currently recorded as a risk on the Corporate Risk Register.	Ensure the cyber security risk register is reviewed and updated regularly. Ongoing
3.1.2.3. Implement processes, procedures and controls to manage changes.	Kenny MacPherson	Tony Whenman /Thomas Aldred /System admins	Green	Change Advisory Board (CAB) is in place.	Generate assurance that changes are presented to the CAB. Review 2025, with implementation 2026 onwards.
3.1.2.4. Review Process for Change management.	Kenny MacPherson	Tony Whenman /Thomas Aldred /System admins	Green	It is important that all significant System changes are documented and agreed. It is known that some system administrators commit unrecorded changes.	Work with system owners to ensure changes are recorded and agreed before changes are made. Ongoing.
3.1.2.5. Manage IT Infrastructure vulnerabilities that may allow an attacker to gain access to critical systems.	Tony Whenman	Thomas Aldred	Green	Internal network is scanned on a weekly basis to capture the threat level and vulnerability position. Remediation is in place to correct vulnerability position.	Continue to enhance remediation actions and reporting. Ongoing

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.1.2.6. Manage third party system vulnerabilities that may allow an attacker to gain access to critical systems.	Tony Whenman	System Owners	Green	Internal systems are scanned on a weekly basis to capture the threat level and vulnerability position. Remediation is only partly in place to correct vulnerability position as is reliance on suppling vendor to provide security updates.	Continue to work with System Owners, System Administrators and supplying vendors to enhance patching regime and to ensure only fully supported systems are procured. Ongoing
3.1.2.7. Operate a Council network penetration testing programme.	Tony Whenman	Thomas Aldred	Amber	Penetration testing is completed yearly on all systems. However, due to ever increasing criminal cyber incidents, penetration testing should be increased to match the threat.	Develop a more robust testing regime. Continuous review and improvement.
3.1.2.8. Upgrade all end user devices to latest operating system.	Thomas Aldred	Ray Groundwater	Amber	IT are working through an upgrade cycle of moving End-Of-Life (EOL) Windows operating systems. School devices numbering 1809 are now upgraded to Windows 11. Of the 810 Windows devices used by corporate staff 728 have been upgraded to Windows 11.	Continue to upgrade with deadline of 14 October 2025 for EOL of Windows 10.

Objective 3.1.3: We will increase defences to mitigate cyber risks as far as possible.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.1.3.1. Develop a new web proxy system to ensure devices are always secured.	Tony Whenman	Thomas Aldred	Green	Current Web proxy is due for replacement in September 2025. Remote working has brought a new threat where devices not on the Council network are not protected by a Web Proxy. A new Web Proxy system has been procured and is in the process of being installed. This new system offers improved protection and covers the use of devices used at home and in Schools. As an added protection this will also be used on Council mobile devices when used for web browsing.	Continue to roll system out to all corporate and school devices numbering in the region of 2900 devices.
3.1.3.2. Purchase, set up and run a security information and event management (SIEM) solution.	Tony Whenman	Thomas Aldred	Amber	No SIEM in place – relying on SolarWinds reporting. SIEM is a standard component in cybersecurity which reviews logs across multiple systems automatically generating a clear overview for IT security management purposes.	Investigate most suitable SIEM solution and implement by end 2025.

Objective 3.1.4: We will develop a culture of security by raising awareness of personnel to vulnerabilities, risks and threats from cyberspace and the need to protect information systems.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.1.4.1. Identify and implement measures to develop a culture of security.	Kenny MacPherson	Tony Whenman.	Green	Information Governance Group owns and maintains standards. Use of regular all staff bulletins and email alerts to educate and inform. Information Security Officer developed content for mandatory online training courses for all staff, now delivered through iLearn. Close co-operation between Information Security Officer and Information Governance Officer, within Information Governance Group and operationally.	Ongoing work to ensure high levels of security awareness remains.

3.2. Governance Objectives

We will report on progress and make sure that decision makers have the information they need to make sound decisions.

Objective 3.2.1: Regular reporting to Council Asset Management Sub-committee on the delivery of Digital & ICT Strategy, ICT Asset Management Plan and ICT Capital Programme.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.2.1.1. Establish regular Asset Management Sub-committee reporting.	Kenny MacPherson	Thomas Aldred	Green	Reports to Asset Management Sub-committee are being submitted at least twice a year, either as stand-alone reports or included in broader financial reports.	Continue to submit reports.

Objective 3.2.2: The Corporate Leadership Team reviews ICT Performance, considers significant change requests, agrees the ICT Capital Programme and ensure strategic fit working with the Council's Asset Management Strategy.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.2.2.1. Significant changes are reported to Corporate Leadership Team (CLT).	Kenny MacPherson	Thomas Aldred	Green	Reports to CLT are submitted in the form of briefings.	Continue to ensure significant changes are reported to CLT on an ongoing basis.
3.2.2.2. Ensure IT Capital Programme is strategically aligned to the Council's Asset Management Strategy.	Kenny MacPherson	Thomas Aldred/ Tony Whenman	Green	IT Capital Replacement Programme is approved by Asset Management Sub-committee, following oversight by CLT.	Ensure reports are completed.

Objective 3.2.3: Establish and operate effective ICT infrastructure and systems to support delivery of the outcomes in the Digital Strategy.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.2.3.1. Ensure full cooperation between IT and the Improvement and Performance team.	Kenny MacPherson	Thomas Aldred/ Tony Whenman	Green	IT and the Improvement and Performance team meet on a monthly basis to review status and cooperation between the Council's ICT Strategy and Digital Strategy.	Continue to enhance cooperation and systems to the benefit of the Council to ensure the ICT and Cyber Security Strategy aligns with the Digital Strategy.

3.3. Infrastructure

We will invest in and maintain the Council's ICT assets, both physical and data, to ensure they remain fit for purpose, and we will ensure they are resilient, secure and available, as well as improving services, while supporting innovation and change.

Objective 3.3.1: We will ensure that the ICT asset base is available, resilient and effective.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.1.1. Embed processes for annual review of the ICT asset base.	Kenny MacPherson	Thomas Aldred	Green	The annual ICT Capital Replacement Programme supports this objective by ensuring timely replacement of priority core infrastructure. The ICT Capital Replacement Programme for 2025/26 was approved by Asset Management Sub-committee in March 2025. The delivery programme is on target.	Deliver 2025/26 ICT Capital Programme by 31 March 2026.
3.3.1.2. Upgrade of infrastructure.	Thomas Aldred	Ross Sutherland	Green	There was little resilience in the Council webserver infrastructure and the network design did not align with the NCSC's recommendations. Therefore, a design was updated, and new Infrastructure has been procured and is in the process of being implemented.	Implementation of new webserver infrastructure expected to be completed by October 2025.
3.3.1.3. Replace Analogue Phone systems and lines.	Thomas Aldred	Ray Groundwater	Amber	The analogue switch-off has been delayed from December 2025 until January 2027, Of the 61 phone systems the Council owns, 69% have been migrated. This migration includes the majority of the Council's larger sites. It should be noted that the delay in the analogue switch off is helpful as 6 sites cannot be moved yet as there is no digital connection available from BT to move them over	Continue to migrate phone systems/lines as they become available through BT.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
				to. This includes some of the isles Schools.	

Objective 3.3.2: We will ensure resilience is considered as part of project definition.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.2.1. When new systems are put in place resilience is considered.	Kenny MacPherson	Thomas Aldred	Green	When new systems are being considered resilience of the system is taken as a key priority.	Consider resilience for main Internet feeds, which is dependent on the full implementation of SWAN2 and webserver infrastructure.

Objective 3.3.3. We will seek to provide protection via good Disaster Recovery capability to support business continuity.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.3.1. Disaster recovery project.	Thomas Aldred	Pamela Money	Green	A new data centre has been implemented at the Harbour Master's building at Scapa and is operational. This synchronises IT systems between Kirkwall and Scapa.	Continue to increase resilience via disaster recovery including investigation of additional Internet feed.
3.3.3.2. Immutable backups	Thomas Aldred	Ross Sutherland	Green	Installation of an enhanced backup solution designed with measures to protect against ransomware cyber attacks is underway at both the main Council datacentre and the disaster recovery data centre at the Harbour Master's building at Scapa. This adds an additional layer of	Continue to ensure system is updated and appropriate for needs.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
				protection to systems and data if an attack was orchestrated against the Council.	
3.3.3.3. Backup of MS Teams and OneDrive Storage	Thomas Aldred	Ray Groundwater	Blue	Due to the increased file storage in the cloud now reaching 5TB it has become apparent a system is required to restore lost files above that of the standard MS recovery systems and improve resilience. A system has been purchased and installed.	Complete. Continue to regularly confirm backup is working by regular test restores.

3.3.4.

Objective 3.3.4: We will support the innovation opportunities provided by developing a foundation for Business Intelligence and Data Warehousing to be explored and leveraged.

Work towards this objective will be done under Customer Focus Objective 3.3.

3.3.5.

Objective 3.3.5: We will continue to harden our local core infrastructure to provide an accessible, secure and stable ICT platform for existing and future system requirements.

Work towards this objective will be done under Cyber Security Objectives 3.1 and Infrastructure and Systems Objective 3.5.

3.3.6.

Objective 3.3.6: We will ensure that our network fully enables access to electronic resources such as the Scottish Educational Digital Network (GLOW), which supports employees working in more flexible and mobile ways.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.6.1. Upgrade network capacity for access to cloud systems.	Thomas Aldred	Pamela Money	Green	Network capacity has been upgraded to meet increased demands for access to cloud-based systems.	Implement SWAN2 which will increase bandwidth and improve network capacity.
3.3.6.2. Upgrade core networking infrastructure to ensure bandwidth capacity across network.	Thomas Aldred	Pamela Money	Green	Core network infrastructure is currently within bandwidth requirements for Council services. However, a number of core infrastructure devices are nearing End-Of-Life (EOL) within the next 12 months. Quotes for replacement infrastructure are being sought.	Procure new infrastructure and install before EOL.
3.3.6.3. Make use of R100 infrastructure to enhance rural Wide Area Network (WAN) connections.	Kenny MacPherson	Thomas Aldred	Green	Make use of the Scottish Government R100 infrastructure as and when it becomes available to enhance rural Wide Area Network (WAN) connections where suitable. Investigations are underway to improve bandwidth using R100 infrastructure in Stromness.	Continue to review and make use of connections as required.

Objective 3.3.7: We will develop co-operative connectivity with public sector and third sector bodies.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.7.1. Implement SWAN2 services.	Thomas Aldred	Vince Buchan	Amber	The Scottish Wide Area Network (SWAN) used by many councils and public sector organisations delivers connectivity to the Council headquarters and other Council sites (mainly outside Kirkwall and Stromness). The national contract for SWAN has ended and the procurement process for a successor (SWAN2) has now completed, with transitions to new BT circuits to be completed by March 2026. Successfully transitioned OIC sites are Burray Primary School, Evie Community School, St Andrews Primary School, Westray Junior High School, Westray Care Home. Rousay Community School, Eday Community School, Sanday Junior High School are in the process of having new BT fibre installed	Due to the delays in the R100 programme BT are experiencing issues in delivering fibre to North Ronaldsay Community School, Papa Westray Primary School, Flotta Primary School, and Stronsay Junior High School. OIC IT and BT are discussing options available, with the present migration plan being to have all OIC sites transitioned by end of October 2025. BT infrastructure and resourcing are the limiting factor.
3.3.7.2. Implement joint systems with NHS Orkney.	Vince Buchan	Ray Groundwater	Green	The Scottish Government Digital Office Microsoft 365 collaboration project has been set up to create a Digital Partnership between Orkney Islands Council and NHS Orkney to recognise the transformational potential of using M365 as a collaboration platform between the	Waiting for Scottish Government Digital Office Phase 2 collaboration project.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
				two organisations to provide concrete deliverables.	

Objective 3.3.8: We will introduce and promote the use of cloud technologies to enhance our ICT offerings to customers and staff on an enhanced expanded local to cloud-based network infrastructure.

Future work towards this objective will be done as part of Governance Objective 3.2 and Objective 3.3.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.8.1. Develop appropriate cloud technologies.	Thomas Aldred	Ray Groundwater	Green	Microsoft Azure Virtual Desktop in place as is MS Teams.	Continue to develop new technology as it becomes available and work with OIC Services to assist in moving appropriate systems to the cloud for better efficiencies.

Objective 3.3.9: We will work with staff and partners in meeting their expectations and needs through identifying what systems and equipment are required, and we will improve efficiencies by identifying and removing redundant systems on our infrastructure.

Work towards this objective will be done as part of Governance Objectives (technology standards) and Customer Focus Objectives (account management), as well as within projects under the Digital Strategy Delivery Plan.

Objective 3.3.10: We will ensure our ICT infrastructure represents value for money and supports the Council's business objectives, including the objectives in the Digital Strategy.

Work towards this objective will be done as part of Governance Objective 3.2 above.

Objective 3.3.11: We will improve our publicising of our forward schedule of change to keep staff and customers informed.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.3.11.1. Establish a process for keeping colleagues informed.	Thomas Aldred	Ray Groundwater	Green	Alerts via email and SharePoint portal are in place.	Develop a robust process. This is a continuous process when new systems become available.
3.3.11.2. Implement a change management system for core corporate, and other sensitive and major systems.	Tony Whenman	System Owners	Green	IT are working closely with stakeholders to ensure major/ sensitive systems are upgraded in a controlled manner using recognised change and project management methodologies. At present systems are upgraded without change management in place.	Cement robust processes with stakeholders. Review during 2025 and implement changes from 2026 onwards.

Objective 3.3.12: We will ensure that our data holdings are secure, accurate and available to services to derive maximum value from the data we hold.

Work towards this objective will be done as part of Customer Focus Objective 3.6 and above.

3.4. Internal and External Customer Communication

We will communicate effectively with our customers, partners and staff, and where appropriate with citizens of Orkney and visitors; we will find way continuously to improve our services, especially when resources are limited to the benefit of the Orkney Community.

Objective 3.4.1: We will continuously improve the Council's digital communications infrastructure and encourage its use, through providing facilities to support Council employees and customers to work and interact in a more flexible and mobile way, supporting sustainable communities.

Work towards this objective will be done as part of other objectives above, especially Governance Objective 3.2 and Customer Focus Objectives 3.6.

Objective 3.4.2: We will actively participate in national initiatives for sharing intelligence.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.4.2.1. Identify and implement measures to participate in national intelligence sharing initiatives.	Kenny MacPherson	Tony Whenman.	Blue	The Information Security Officer is a member of the UK-wide CiSP (Cyber-security Information Sharing Partnership), ensuring that the Council shares and receives intelligence on current cyber threats. SciNET (Scottish Cyber Information Network) is a sub-group for Scotland of CiSp. The Scottish Local Authority Information Security Group is a sub-group of SciNET. The Council also participates in Cyber Resilience Partnerships including Cyber intelligence matters.	While action complete IT will continue to work with our partners and develop more as we develop our Cyber robustness.

Objective 3.4.3: We will introduce and promote digital document and record management to support secure document creation and storage.

Work towards this objective will be done as part of Digital Objective 3.5.

Objective 3.4.4: We will ensure easy access for staff and customers to information and meet our legislative data management requirements.

Work towards this objective will be done as part of Cyber Security Objectives and Customer Focus Objectives.

Objective 3.4.5: We will roll out enhanced desktop communications tools in keeping with our Microsoft 365 digital and governance strategies, as and when available, e.g., video, email, instant messaging, telecommunications, document and records management.

Work towards this objective will be done as part of Customer Focus Objective 3.6.

Objective 3.4.6: We will review our use of technology and work towards using systems that are used by others, where possible

Work towards this objective will be done as part of Governance Objective 3.2 above.

Objective 3.4.7: We will work proactively with partner organisations and other councils to achieve the best fit technologies for our customers, and so that we do not re-invent the wheel; this will include support for the ‘Empowering Communities’ programme.

Work towards this objective will be done as part of other objectives above, especially Governance Objective 3.2.

Objective 3.4.8: We will improve fault reporting, ICT status information and staff communications through the ICT Helpdesk, Customer Services announcements, and creation of staff self-help. Work towards this objective will be done as part of Customer Focus Objective 3.6.

3.5. Digital Objectives

We will embrace emerging technology and deliver a service that meets our customer expectations, also supporting our workforce to develop their own digital skills and implementing hardware that supports a more digital approach.

Objective 3.5.1: We will support the introduction of new streamlined electronic processes and collaborative communications through the use of available interactive technologies.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.5.1.1. Provide IT support to the Electronic Document and Records Management (EDRMS) project.	Vince Buchan	Ray Groundwater	Green	Technical input to the EDRMS project continues to be provided. It should be noted that the EDRMS project itself is not led by IT.	Work to be completed as required in the EDRMS Project Plan.
3.5.1.2. Upgrade of systems.	Thomas Aldred	Ross Sutherland	Amber	Some systems procured and used by Services have been identified in the latest IT Health Check as requiring immediate upgrade. Two systems need upgrade. Iken, which is used by Legal Services, is in the process of being moved to an OIC SharePoint space. A new system to replace the StaffPlan system, which is used by OHAC home carers, is in the process of being evaluated.	IT will work with System Owners to identify new replacement systems that meet NCSC security guidelines. Once replacement systems have been identified by System Owners on an ongoing basis.

Objective 3.5.2: We will demonstrate leadership behaviour that supports and fuels a digital culture among staff and customers.

Work towards this objective is being done as part of the Digital Strategy Delivery Plan objectives, under the theme of Digital.

Objective 3.5.3: We will listen to and support staff on how to get the best from digital systems.

Work towards this objective is being done as part of Customer Focus Objectives, at Objective 3.6, and within implementation projects described elsewhere in this plan, and in the Digital Strategy Delivery Plan.

Objective 3.5.4: We will improve and develop our staff's digital competency.

Work towards this objective is being done as part of the Digital Strategy Delivery Plan objectives, under the theme of Digital.

Objective 3.5.5: We will continue to identify Account Managers for digital technologies, to encourage our stakeholders to work with these Account Managers to discuss their issues and any planned ICT developments; we will ensure that account managers are visible, knowledgeable, proactive in communicating with stakeholders, and effective in receiving and acting on feedback.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.5.5.1. Identify IT technology specialism teams.	Thomas Aldred	Ray Groundwater	Green	IT specialism team leader roles are clearly visible within IT however work to defined specialisms within other departments is ongoing to enable proactive communication with stakeholders enabling effective action being taken on feedback received.	Create a stronger working relationship with System Owner specialists. On an ongoing basis. Instil a process of change management.

Objective 3.5.6: We will use technology (where available and appropriate) and user workshops to train and inform staff on our service technologies.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.5.6.1. Creation of video files within MS Teams for training purposes	Thomas Aldred	Ray Groundwater	Green	Work is underway to trial the recording of Teams sessions as a resource to be used in specific application areas.	Will continue to develop further training videos as required.

Objective 3.5.7: We will concentrate on developing and updating user guidance with the aim to make our staff more technically skilled and independent with the systems they use.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.5.7.1. Develop and update user guidance.	Thomas Aldred	Ray Groundwater	Green	Guidance is issued to staff as and when needed, generally when a project moves into the delivery phase.	SharePoint site to house all guidance in a user-friendly way. This is a moving and ongoing project.

3.6. Customer Focus Objectives

We will use our experience to work with all Council services to introduce ICT systems with a stronger citizen/customer focus: any new system will meet the needs of users within the Council, and also those outside the Council who use it in any way; system design will take the needs of all these users into account at as early a stage as possible.

Objective 3.6.1: We will continue to implement collaborative technologies

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.6.1.1. Enhance the use of Microsoft technologies.	Thomas Aldred	Ray Groundwater	Green	IT has continued to develop further the adoption and use of Microsoft 365. However, a roadmap should be defined to ensure the Council is making best use of its investment in Microsoft technologies. This along with Artificial Intelligence (AI) should include licensing options, partnership access, Schools, and field workers.	Create a Microsoft roadmap and include new Microsoft releases as they become available. Continue to work with Performance and Business Support Service in AI policy and Co-Pilot trials.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.6.1.2. Enhance technology use between corporate and School staff	Tony Whenman /Paul Kesterton	Schools	Green	Many school staff now have access to corporate email and Microsoft teams. There is however a need to increase its use to ensure sensitive data is not held in GLOW systems.	Continue to develop, support and promote use of M365 in schools.

Objective 3.6.2: We will review our Service Charter and introduce new targets as appropriate to support our changing business needs.

Action.	Owner.	Lead.	Brag	Current position, September 2025	Next Steps.
3.6.2.1. Review IT Service Charter.	Kenny MacPherson	Thomas Aldred	Green	The ICT Service Charter was last reviewed in June 2019. Individual Service Charter highlighting Service Level Agreement for the Orkney and Shetland Valuation Joint Board has been developed and shared.	Review IT Service Charter during 2025.

Objective 3.6.3: We will work to improve internal fault reporting and service delivery through the use of various software tools to ensure that important information is communicated effectively and clearly.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.6.3.1. Power BI for clear reporting.	Thomas Aldred	Ray Groundwater	Green	Microsoft Power BI software enables reporting business intelligence (BI) data to be visualised. Reporting utilisation needs enhancement by greater rollout of tools across the Council.	Enhance processes on an ongoing basis and continue to support BI use by services.
3.6.3.2. We will encourage our stakeholders to work with us to discuss their issues	Kenny MacPherson	Thomas Aldred	Green	IT meet with key stakeholders to find ways for recording portfolio.	Enhance meeting schedules on an ongoing basis.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
and any planned ICT development.					

Objective 3.6.4: We will use opportunities within the ICT team to train staff to cover across more than one system, thus moving away from the risk inherent in specialised, singleton posts.

Action.	Owner.	Lead.	BRAG	Current position, September 2025	Next Steps.
3.6.4.1. Ensure more than one member of IT staff is trained and allocated to provide support for each supported system.	Thomas Aldred	Ray Groundwater	Green	Work is underway to ensure that sufficient staff have the skills and experience to cover the support of all main systems and infrastructure. Many training courses, including by external providers, have been delivered to IT staff. Focus has now moved from general training to specific system training.	Continue to review training needs for IT staff. Also include system owners.