High level ICT audit recommendations progress

The Shared Service Improvement Plan made the following high and medium level recommendations. The progress made against each items is shown in the table below:

Shared Service Improvement Plan High-level recommendations:

IT Governance Structure – There are no defined IT policies and procedures in place for the Shared IT Service	• Acceptable Usage Policy – Written and gone to HR for final approval • Data Protection & sharing Policy – Completed and on intranet • Mobile Device Policy – In draft approval awaiting changes in security systems, which will change security environment. • Remote Working Policy – part of flexible working plans. ICT working with HR as impact relates to working practices. • Social Media Policy – Completed and on intranet Protocols: • Security Breach response Protocol – In draft • Change Control Protocol – In draft with change control procedure going live January 2020. Meta- compliance software has been deployed which allows deployment to staff.
IT Governance Structure – Neither the Shared IT Service nor the Councils have defined IT strategies in place, including defined metrics against which to measure the performance of the Service.	ICT strategy has been completed and accepted by Stevenage Borough Council. East Herts senior leadership team has agreed strategy but it has final approach scheduled for December 2019.

Medium Level Recommendations

IT Governance Structure – Job descriptions for staff members within the Shared IT Service are out of date and are not reviewed on a regular basis.	All ICT Job descriptions have been reviewed over the past year with the exception staff related to Print restructure. Information System Analysts JD is under review by HR.
IT Rationalisation – There is not a coordinated approach for identifying and assessing new technologies that would meet the needs of both Councils, including the identification of duplicated services.	ICT audit has been completed which identifies duplicate system. As part of the ongoing Project Management Office (PMO), we will be identifying all update/replacement schedules for systems and aligning when systems can be amalgamated. The ICT strategy also outlines the need to reduce the overall number of systems the council runs and where possible those functions taken over by Office 365. The ICT Steering Group and ICT Partnership board will be used as the sounding board by the PMO for any future ICT projects to evaluate and exploit new technologies identified by ICT or the wider businesses.
IT Budget Management – There are no arrangements to monitor individual project budgets on an ongoing basis nor are there defined budget setting procedures.	The Project Management Office (PMO) now evaluates all projects included the financial aspect of all projects. All projects are identified during the budget setting cycle with finance departments as part of the ICT strategy. Monthly meetings take place between ICT and finance staff from both councils to discuss progress and budgets changes. Members of finance also sit on the partnership and steering group boards.

Cyber Security - follow up 2018/19 recommendations

Management should establish a network access control to block unknown or unauthorised devices from connecting to the Council's IT network. This should include restricting the ability to physically connect to the IT network. Where there is a demonstrable need for a device to connect to the IT network, the Service should require: The purpose for the connection has been recorded Appropriate security controls have been enabled on the device connecting to the IT network The period of time that the device will require the connection All connections are approved before being allowed to proceed. Devices connected to the IT network should be reviewed on a routine basis.	80k has been budgeted to procure a network-monitoring tool, which will provide these functions and others. This procurement exercise will commence in January 2020. The majority of devices, which connect to our wired network, are ZERO thin client boxes with a smaller number of static PCs and Laptops. The majority of laptops use our wireless network and from a security requirement are treated as remote access devices, which reduces their security risk. This structure reduces our security risk but we still need to defend against 'unknown' devices attempting to connect to our network.
There should be a record of the configuration of the Council's firewalls, which includes but is not limited to: The purpose of all of the rules The expected configuration and activity for each rule The member of staff that requested and approved the rule The configuration of the firewall should be reviewed on a routine basis. The Service should develop a Firewall rule policy to provide the list of controls that are required to secure firewall implementations to an approved level of security.	Configuration of firewall rules has been created and is being updated as the requirement changes. This under the control of the security & network team for consistency and auditing purposes. A firewall policy is being created as suggested alongside our redesign of the network. All firewalls and switches are being replaced in Q1/2 of 2020 and this part of that design work.
Management should update the Council's IT disaster recovery plan to include the procedure for establishing all IT services at a single data centre. A complete IT Disaster Recovery scenario test on all applications and systems should take place to provide assurance that recovery could happen within the expected time frame. The Service should document the results of the test to determine the further actions required to improve the efficacy of the plan.	We have secured funds from a Local authority grant to have an outside agency review and amend our DR plans. This will be commissioned post implementation of the replacement of Storage and VDI hosted desktops planed for completion Q1. The new capabilities these systems will give will substantially change and improve our DR capabilities and plans. A secondary link using Microwave technology to remove the single point of failure of the network link between both data centres is scheduled for

	completion in January 2020. Remedial work on electrical systems at both data centres to remove single points of failure has been completed. Tests will be planned post that implementation when resources and business demands allow.

Note: As part of improved governance structure, the ICT strategic Partnership manager will be reporting on a quarterly basis to the Members ICT committee. If required similar reporting to the audit committee on agreed time frame can also be implemented.