REDDITCH BOROUGH COUNCIL

Executive Committee 14th January 2014

PUBLIC SERVICES NETWORK COMPLIANCE AT RBC

Relevant Portfolio Holder	Cllr John Fisher
Portfolio Holder Consulted	Yes
Relevant Head of Service	Deb Poole
Ward(s) Affected	N/A
Ward Councillor(s) Consulted	N/A
Key Decision / Non-Key Decision	Non-Key Decision

1. PURPOSE

1.1 To update the Executive Committee on the requirement to achieve compliance with the Public Services Network (formerly known as the Government Secure eXtranet) and to seek approval for the release of funds for year 2013/14 to start achieving compliance in the current financial year. The Cabinet Office has made it clear that they expect to see the authority moving towards a position of compliance with immediate effect.

1.2 This is the first stage of the work required and further funding will be needed to achieve full compliance in 2014 and 2015. These additional financial implications will be included in the budget setting process for 2014/15.

2. RECOMMENDATIONS

The Executive Committee is requested to RECOMMEND that

1) an increase to the 2013/14 capital programme of £90k, to be funded from borrowing, be approved;

2) the borrowing costs be released from balances in 2013/14 and be included as unavoidable pressures in the 2014/15 medium term financial plan; and

3) the release of £39k from balances in 2013/14 to fund the associated revenue costs be approved.

2 BACKGROUND

3.1 The Council is in the process of migrating its connection from the Government Secure eXtranet (GSX) to a new, secure, UK Government network, the Public Services Network (PSN). The same services it currently accesses through the GSX will be available through the PSN. The Cabinet Office 'own' and manage the PSN.

3.2 The Cabinet Office has issued a new set of conditions which all local authorities must adhere to in order to have continued access to the GSX whilst fully

migrating to the PSN. Unlike previous GSX compliance regimes, the Cabinet Office has taken a zero-tolerance approach to compliance, and is advising local authorities that they will lose their connection to the GSX and any future connection to the PSN should they not fully adhere to all PSN requirements.

3.3 The Council have been receiving electronic files from the Government Connect Secure Network (GCSX) for a number of years without any major problems or security breaches e.g.: DWP data relating to Benefits. During this time the Government became increasingly concerned about security holes and possible network breaches.

3.4 As previously mentioned the Cabinet Office have moved to a 'zero tolerance' position on compliance. This means that unless the Council can demonstrate that it has addressed the Government's concerns, they will cease our connection to the Public Services Network.

3.5 If the Council were to be disconnected this would prevent RBC from managing citizens benefits, transferring secure information with our partners such as the Police and the NHS, managing secure emails and access to secure government web sites. In addition it would prevent future plans to implement Individual Electoral Registration (IER) from June 2014.

3.6 However, the Cabinet Office announced a further shift in its PSN compliance regime on 4th October 2013. PSN compliance has proved challenging for many public sector organisations and the Cabinet Office has struggled to provide feedback on submissions within prescribed time limits. The latest announcement removes the immediate suspension risk for organisations whom the Cabinet Office considers are demonstrating a genuine appetite to achieve compliance.

3.7 It has been made clear that this is not a weakening of the stance taken by the Cabinet Office; all organisations will still need to move towards 100% compliance with PSN requirements, and the Cabinet Office has not removed the option of disconnecting from the PSN those organisations which are not compliant and do not demonstrate a clear willingness to become so. For this reason and following discussion with the Portfolio Holder, a release of funds in this financial year is required to continue to achieve PSN compliance.

3.8 The PSN requires that staff no longer use their own IT equipment to access PSN business systems or data from home. This means the council will now have to provide a PC or similar device for staff to use at home. A 'two factor' authentication device similar to those used by some banks will also be required.

3.9 The Cabinet Office have also confirmed that all staff using PSN applications must meet the Baseline Personnel Security Standard (BPSS) which will be covered by a Basic Disclosure Check (previously a CRB check).

4. KEY ISSUES

Financial Implications

4.1 The schedule at Appendix 1 details the costs for 2013/14 associated with achieving compliance with the PSN. The analysis shows £90k capital funding required together with revenue costs of £39k. Whilst this report concentrates on the immediate requirement to demonstrate our commitment to achieving compliance it is important to note that the long term solution has further cost implications. These costs are based on **current PSN** requirements as determined by Central Government. However, these requirements change constantly so the financial implications may increase in future as the Cabinet Office continues to change the specification.

4.2 Several business applications and their servers are required to be upgraded to enable compliance. The costs for these are as yet unknown but will be included in the budget setting process for 2014/15. A number of systems will require upgrading or replacing to include; Haven (Leisure), IBS (Revenues and Benefits) and M3 (Environmental Services)

Legal Implications

4.3 There are implications regarding the Data Protection Act should staff not use the PSN to exchange private, confidential or sensitive information with our partners.

Service / Operational Implications

4.4 The longer term solution will require several changes to the way we operate including:

- PSN requires that all servers are updated to the latest security patches which in some cases are not compatible with current versions of business systems. Some of the business systems have not been upgraded for some years as there may not have been a business need to do so. However, the environment has changed as a result of PSN and this will have major cost implications

- All Business Application servers will be required to have Microsoft Patches applied on a regular basis. Initially, this is a considerable piece of work for ICT and for departments while testing the patches. There will also be considerable amounts of ‘down time’ for the services whilst the work is completed. An on-going procedure for regular upgrading, testing and downtime will need to be put in place to ensure continued compliance.

- Two factor authentication for any remote access to our network including Citrix, Secure Global Desktop and Ipads will be required.

- All passwords will need to be a minimum of twelve characters in length.

Customer / Equalities and Diversity Implications

4.5 During the work to patch and upgrade the servers and applications there will be breaks in the availability of the technical systems which may impact on service delivery to the customer. Details of the scheduled works have been discussed with system administrators and Heads of Service. Regular communication briefs have been sent out to staff and placed on the ORB (intranet) and where possible, works are being carried out after hours or during weekends to minimise the impact on services. However, given the quantity of patches to be applied and the tight timescales, some work will have to be done during core hours.

5. RISK MANAGEMENT

5.1 The PSN compliance criteria change on a regular basis, depending on which representative from the Cabinet Office is involved. Consequently there is a risk that even if the Authority commits to the spend and business changes mentioned in this report, that it could still fail future compliance audits and require additional spend and further business changes to ensure PSN access.

5.2 There are significant risks to business if we do not achieve compliance particularly in relation to the Benefits Service and the Elections Service. Loss of our connection would also have a detrimental effect on data sharing between the Council and other public bodies e.g.: the Police, NHS etc.

5.3 The Council has been working with Cabinet Office Representatives for some months on an ‘air-gap’ solution that would have removed the need to apply security patches to all of the corporate servers. Only the servers contained within the ‘air-gap’ would have needed patches applying to them. A discussion on 11th September with a different person at the Cabinet Office made it clear that the only way the new Individual Electoral Registration (IER) information would be sent to Councils was via the PSN, effective from June 2014. This ended the ‘air-gap’ as a solution as Elections rely on data from several other servers which would need to be moved into the ‘air-gap’. This would effectively bring large parts of our existing network in to the ‘air- gap’. The need to patch all corporate servers has now become critical as a result. This work is now underway but will cause disruption to many of our services.

5.4 Assurances have been sought from the Cabinet Office that if we carry out the work as stated that we will achieve compliance, but, at the time of writing this report, no assurances have been received.

5.5 In order to help with the management of these risks the PSN Code of Connection compliance is being added to the Corporate Risk Register.

6. APPENDICES

Appendix 1 – PSN Budget Pressures RBC (this appendix is exempt)

7. BACKGROUND PAPERS

None

AUTHOR OF REPORT

Name: Deb Poole
Email: d.poole@bromsgrovea.nredditch.gov.uk
Tel: 01527 881256

Name: Mark Hanwell
Email: markhanwell@bromsgroveandredditch.gov.uk
Tel.: 01527 881248