EAST AYRSHIRE COUNCIL

CABINET – 5 FEBRUARY 2014

PUBLIC SERVICES NETWORK COMPLIANCE

Report by Executive Director of Finance and Corporate Support

PURPOSE OF REPORT

1. The Report advises the Cabinet on the Council's progression in terms of complying with the Cabinet Office's 2013 requirements for connection to the Public Services Network (PSN), and on the options which are currently being considered to ensure compliance for 2014.

BACKGROUND

2. The Public Services Network (PSN) provides an assured "network of networks" over which government can safely share services, to collaborate more effectively and efficiently than ever before.

3. The PSN is managed within the Cabinet Office, and a PSN Programme has been designed to oversee and implement elements of the UK Government ICT Strategy and any consequential changes that are required.

4. All Local Authorities must comply with the new PSN "connection controls" or face disconnection from the government network; PSN compliance recently introduced new measures that extended beyond technical operations and now include information and risk governance. These control measures are included in Appendix 1 of this report.

5. The Cabinet Office has issued various communications stating that incomplete or weak compliance will not be tolerated; effectively, PSN compliance will be more rigorously managed than its predecessor, the Government Code of Connection (CoCo) for GSi and GSX. The background papers provided with this report contain additional detail on this approach.

6. Under the Government Code of Connection (CoCo) scheme, all Local Authorities were subject to an annual audit that specified a minimum set of security standards that had to be adhered to in order to meet CoCo compliance.

7. Since Cabinet Office took over compliance from the Communications-Electronics Security Group (CESG), Local Authority accreditation is more difficult to achieve as the Cabinet Office have, for example:

- Increased the scope of the ICT "Health Check"
- Introduced several new controls concerning information and risk management
- Changed the regulations surrounding mobile and remote working
- Increased the scope of disclosure checks on Council staff

8. The Council was advised by the Cabinet Office on 22nd November 2013 that it had achieved PSN accreditation for 2013. Accreditation was achieved on completion of the Council's third PSN submission, having initially been rejected against fifteen 'control measures' and subsequently against six 'control measures'.The administration of the PSN

submission and accreditation process, as experienced by this Council during 2013, has been broadly in-line with that experienced by all other UK Councils.

9. The process of PSN accreditation is now required on an annual basis and consequently the Cabinet Office has advised the Council that its 2014 PSN submission will require to be fully accredited by 23rdSeptember 2014. Cabinet Office guidelines stipulate that the Council should submit one month prior to the accreditation date, hence the Council's next PSN submission date is now set as 23rdAugust 2014.

10. An 'ICT Health Check' which is a key element of the PSN Submission will require to be completed approximately 1 month prior to the submission date, i.e. end-July 2014. The 'ICT Health Check' requires to be outsourced to a recognised ICT Security Consultant who will undertake several security vulnerability tests on the Council's ICT infrastructure, the object of which will be to identify ICT security weaknesses which will require to be addressed prior to the PSN submission date.

11. Current guidelines stipulate that should the Council fail to comply with the PSN Code of Connection on its accreditation date, it will be disconnected from the PSN.The consequence of disconnection from the PSN will mean that the Council would not have electronic access to the following PSN networked services :

- Level of Service / Case Management Inventory (Criminal Justice)
- Patient Discharge System (Social Work)
- Department for Work and Pensions (Revenues & Benefits and Payroll)
- Local Authority data searching tool (Revenues & Benefits)
- Scottish Police Authority's Criminal History System (Social Work)
- Northgate Blue Badge System (Social Work)
- Department for Work and Pensions "Tell Us Once" System(Registrars)
- The General Register Office for Scotland's Forward Electronic Register (Registrars)
- Secure E-mail (170 users across the Council)

2014 SUBMISSION: MAJOR WORK-STREAMS

12. The Cabinet Office has yet to provide a definitive list of areas which will be audited as part of the 2014 PSN submission and accreditation process. The Council's experience during the 2013 process would indicate that the list of areas to be audited will continue to evolve over time as the Cabinet Office reflect upon the results of the 2013 process, and further consider the advice of their Communications Electronics Security Group (CESG) Listed Advisors Scheme (CLAS) consultants.

13. Notwithstanding that clear and unambiguous advice is not yet available on the additional measures which will be required for 2014, nevertheless it is recognised that there are elements of the Council's ICT infrastructure which will require upgrade and/or re-configuration in order to meet with current 'Code of Connection' requirements.

14. Consequently, and in order to progress matters, the following 'major work-streams' have been identified; in recognition of the extremely tight project timescales the necessary works are required to be progressed with immediate effect, where possible :

- UNIX (operating system) server upgrades
- Operating system upgrade from Microsoft Windows XP to Microsoft Windows 7
- Application upgrade from Microsoft Office 2003 to Microsoft Office 2010 (or later)
- Software updating (patching) of physical servers

- Software updating (patching) of all voice and data network hardware such as hubs, routers and switches
- Software updating (patching) and upgrading of applications systems such as CIVICA, SWIFT and Orchard
- Software updating (patching) of desktop software such as Microsoft Office, Java and Adobe products

15. It had been assumed that the Cabinet Office would issue specific guidance on their requirement for "network separation" that would require significant investment to:

- Re-configure the ICT network between the Corporate network and schools, libraries and Learning Centres
- Re-configure the ICT network between the Corporate network and East Ayrshire Leisure Trust

On 22 January 2014 however, the Cabinet Office confirmed to The Council (via e-mail) that the level of network separation required to meet 2014 PSN compliance was at a greatly reduced level than had been anticipated.

16. For 2014 PSN compliance, the Cabinet Office confirmed that "VLAN" separation is acceptable. VLANs (Virtual Local Area Networks) are used to group a range of IT network devices together within a specific site, which have a common function or user base. These VLANs facilitate the separation and securing of corporate, curricular and public access computers from each other, and in turn between corporate and non-corporate network traffic – therefore ensuring PSN compliance.

17. Cabinet Office gave no indication of future year network separation requirements to meet PSN compliance.

18. Whilst these measures are required to comply with Cabinet Office guidance to ensure continued connection to key government systems, they represent best practice in terms of IT security and will enhance the Council's data protection arrangements.

19. SOCITM leaders have been actively involved in a dialogue with the PSN Programme through a Local Government Seniors forum that includes SOLACE, and the LGA to agree a new compliance regime; they will also participate in The Local Government PSN Secure Solutions Group (SAG) to help broker future changes to PSN compliance as risks change and technical solutions mature.

20. Concerns have been raised over the level of information security compliance requirements and the pace of their implementation; whilst we await the outcome of discussions between Cabinet Office and the representative bodies, the Cabinet Office's latest correspondence has stated there will be an "ongoing review of pragmatic risk mitigation" around PSN compliance and that this will "require ongoing learning from all parties to deliver a level of security proportionate to the business risk and pragmatic in its implementation".

21. SOCITM have stated they are "cautiously confident that the 2014 / 15 experience will be considerably less frustrating than the 2013 / 14 has been". The most recent Cabinet Office letter (PSN Cabinet Office Jan 14) is included in background papers for information.

22. COSLA has been updated on PSN by the Scottish Local Government ICT Strategy Project Board.

SYSTEMS and APPLICATIONS UPGRADING and PATCHING

23. Until now, systems and applications software upgrading and patching has either been delayed until a suitable period of systems downtime could be scheduled or alternatively postponed indefinitely as individual upgrades or patches were deemed as non-essential. This strategy, which is generally in line with practice in other organisations had the benefit of minimising disruption to Servicesand guarded against degraded systems performance resulting from the installation of untested patches and upgrades.

24. The 'Code of Connection' now requires the implementation of a strict regime of patching and upgrading of systems and applications software than had been in place previously within the Council, the consequence of which is that systems and applications software upgrades and patches must be installed whenever available or shortly thereafter, to ensure that the latest ICT security levels are being maintained at all times.

25. Whilst a comprehensive patching schedule has now been developed and as far as possible automated, nevertheless it has yet to be implemented across the ICT infrastructure for physical servers, network devices, the Microsoft Office suite, UNIX, Apple Macintosh, and non-Microsoft software including Adobe, Java and QuickTime.

26. It is anticipated that the implementation of these patches is likely to cause performance issues with some business applications. For example a new version of Java, a programming language used by several Council business applications, could potentially render individual applications temporarily unstable, or unusable, until a work-around has been identified and applied.

UPGRADING of UNIX BASED APPLICATIONS

27. It is expected that infrastructure upgrades to the UNIX environment which support critical applications will be required within both 2014 and 2015; these systems include:

- CIVICA (Finance system)
- SWIFT (Social Work system)
- ORCHARD (Housing system)
- SERVITOR (Building & Works system)
- UNIFORM (Planning system)
- TRANMAN (Transport system)
- UNICORN (Libraries System)

Potentially this could include new hardware coupled with systems software upgrades. The Council's UNIX hardware will fall into the 'end of life' category over 2014 and 2015, and work is scheduled in early 2014 to address the overall UNIX compliance issue.

SEPARATION of CORPORATE and SCHOOLS, LIBRARIES, LEARNING CENTRES and LEISURE TRUST – DATA and VOICE NETWORKS

28. In May 2006, the Council's corporate and schools data networks were merged. This increased the bandwidth for schools and reduced annual costs. This merged network configuration, similar to that which is operational across many other council's, has operated satisfactorily since that decision was taken.

29. This merged network configuration is now in breach of the PSN Code of Connection however, and consequentlythe Council will be required to address the issue by

reconfiguring the ICT interface between the corporate network and schools, libraries, Learning Centres and Leisure Trust.

30. The separation of the corporate and school networks will help to facilitate the greater use of tablet devices and other services within our school estate, with work already underway to pilot iPad devices; the network separation will ultimately allow the Head of Schools to determine how the most up-to-date IT hardware is deployed, implemented and managed across the school estate, and to decide the appropriatelevel of risk management control that will need to be adopted to ensure such hardware is used in line with Council policies.

ICT INTERFACE TO PARTNER ORGANISATIONS

31. It is envisaged that the existing arrangement in terms of data transfer and usage between the Council and NHS Ayrshire & Arran will not be affected by PSN restrictions. However, as ICT requirements for the new Integrated Health and Social Care Partnership are defined in the coming months, there may be further implications for the council's PSN compliance with respect to connecting networks and sharing systems more extensively.

32. The Ayrshire Roads Alliance will be unaffected by the requirements of PSN as it will be a logical and physical extension of the Council's main corporate network.

MIGRATION FROM WINDOWS XP AND MS OFFICE 2003

33. Both Microsoft Windows XP and Microsoft Office 2003 are widely used throughout the Council and both products are deemed by Microsoft to be at 'end of life' in April 2014. In terms of the Code of Connection, the Council will require to migrate to equivalent supported systems by that date. This means that, in respect of the corporate network, replacing all PC's running Windows XP, and fully migrating Office 2003 to Office 2010 (or later), by April 2014 if possible, and certainly by the PSN submission date of 23rd August 2014.

34. It is already recognised that a migration away from Windows XP will cause applications access problems similar to those expected from unilateral application of patching and upgrading For example Windows 7 cannot access archived data retained on the old CYBORG Payroll/HR system.

35. It remains unknown if there will be a requirement to replace/upgrade Microsoft Windows XP and Microsoft Office 2003 across the schools estate for the sole purpose of PSN accreditation, nevertheless it is recognised that these products should both be replaced to ensure that the Council is not exposed to a security breach or loss of data which could lead to financial penalties.

36. The installed distribution of Windows XP and Office 2003 across the Council is detailed within Appendix C of this Report. It should be noted that as the employee numbers within the Council decrease, there may be opportunities to re-use existing compliant pc hardware thereby reducing the number of new pc's to be purchased.

37. The replacement programme will be carefully and systematically managed to ensure that only hardware that needs to be replaced is replaced. PCs which are on the asset register but which are identified as not in active use will not be replaced for example.

PROJECT MANAGEMENT AND GOVERNANCE

38. A PSN Project Board, chaired by the Head of Corporate Infrastructure has been established to manage the 2014 PSN Accreditation project and, where appropriate, Prince2 and the Council's ASTA Project Management system will be used to manage the project.

39. The Information Governance Officer will be a member of the Project Board and The Head of Schools and the Chief Executive of the Leisure Trust will similarly be invited to be represented on the Project Board.

40. The Head of Corporate Infrastructure will provide regular progress updates to The Corporate Management Team.

CODE OF CONNECTION 'CONTROL MEASURES'

41. The current list of "'Control Measures" defined within the PSN Code of Connection and against which the Cabinet Office currently measure PSN compliance, are outlined within Appendix D of this Report. The '2014 Current RAG Status' within Appendix D, provides an indication ofthe Council's current compliance status going into the 2014 submission, and is based upon the Council's current interpretation of whether each Control Measure :

- will be compliant (Green),
- will require additional work to remain compliant (Amber), or,
- be non-compliant until identified works have been completed (Red)

FINANCIAL IMPLICATIONS

42. It is currently estimated that the total costs associated with major workstreams required for the Council's 2014 PSN submission, as outlined within Sections 12 to 37 of this Report will be approximately £2.300m (a detailed breakdown of these costs is attached at Appendix A). It should be noted that these estimates are based upon an assumption that Council systems should be as secure as possible and thus compliant with the Cabinet Office 'Code of Connection' requirements for 2014.

43. It is therefore proposed that the capital costs (detailed in Appendix 1) required to comply with PSN be funded through acceleration and reallocation of existing balances for ICT projects within the Council's 10 Year Capital Investment Programme. These balances include allocations for the Schools ICT and GLOW Programmes which were intended to fund improvement works to the education network and refresh of hardware / software which now require to be accelerated. As a result of accelerated works, all Council schools will be provided with a modernised ICT infrastructure at a much earlier date and will have the freedom to roll out technological developments, such as iPAD's, at their own pace. The following table sets out the revised position taking account of proposed transfers between years.

	Original			**Revised**		
Scheme	**2013/14 to 2017/18**	**2018/19 to 2022/23**	**Total**	**2013/14 to 2017/18**	**2018/19 to 2022/23**	**Total**
ICT Programme	£2.450m	£2.500m	£4.950m	£2.250m	£2.300m	£4.550m
Schools ICT Programme	£2.400m	-	£2.400m	£1.400m	-	£1.400m
GLOW	£1.000m	£1.000m	£2.000m	£0.200m	£0.900m	£1.100m
PSN Programme	-	-	-	£2.300m		£2.300m
TOTAL	**£5.850m**	**£3.500m**	**£9.350m**	**£6.150m**	**£3.200m**	**£9.350m**

44. It should be noted that whilst it is proposed to fully fund the capital costs associated with the Council's PSN 2014 submission from General Services, there will be some changes required to the IT systems used by Housing Asset Services (e.g. Orchard and Servitor). These are likely to be in the region of £0.100m and can be met from current resources.

45. In addition to the capital costs associated with the Council's 2014 PSN submission noted above, there will be further costs of £0.520m to comply with PSN from 2015 onwards (a detailed breakdown of these costs is attached at Appendix B). It is therefore proposed that these costs initially be funded from the remainder of the general ICT Capital Programme allocation to 2018. However, given the priority of these works and the on-going pressure on the ICT Capital budget, other opportunities to fund the costs will be examined and recommended to Members for consideration if appropriate.

46. Whilst it is recognised that the work-streams detailed in Appendix B of this report may require funding from the ICT capital programme, it is anticipated that the delivery of new ICT programmes will need to be aligned to future budgetary constraints.

47. There will also be revenue consequences resulting from PSN compliance which have been estimated at £0.130. These costs are currently not provided for within existing revenue budget allocations and provision will require to be made within Revenue budgets from 2015 / 16 onwards.

LEGAL IMPLICATIONS

48. Failure to comply with the requirements of 'Code of Connection' would result in the Council being disconnected from the PSN, and hence unable to electronically access the services outlined in Section 11 of this Report, some of which are statutory in nature.

49. SOCTIM has recommended that individual Councils similarly devise business continuity/contingency plans for this eventuality. Through discussions with external suppliers and other Scottish local authorities we have concluded that some PSN service providers (such as GROS) are willing to consider the possibility of supplying a contingency solution, however it should be noted that other PSN service providers (such as the Department for Work and Pensions and the Scottish Police Authority) cannot offer any alternative solution other than the PSN at this time.

RECOMMENDATIONS

50. It is recommended that Cabinet;

a) notes the achievement of securing the Council's PSN Accreditation for 2013;
b) endorses the approach being adopted to deliver PSN Accreditation for 2014;
c) notes the current estimate of costs associated with achieving PSN Accreditation for 2014;
d) notes that clarity has been provided by the Cabinet Office on fundamental issues surrounding the design of network interfaces;
e) approves the re-profiling of ICT capital budgets from 2013/14 to 2022/23 to meet the costs associated with complying with the Council's 2014 PSN submission, and

f) otherwise notes the contents of the Report

Alex McPhee
Executive Director of Finance and Corporate Support
5 February 2014

LIST OF BACKGROUND PAPERS

- PSN Compliance – Zero Tolerance Approach (February 2013)
- SOCITM Scotland – Potential PSN disconnection in Scottish Councils (August 2013)
- PSN Cabinet Office (Jan 14)

Any person wishing further information should contact Malcolm Roulston, Head of Corporate Infrastructure email: malcolm.roulston@east-ayrshire.gov.uk

IMPLEMENTATION OFFICER: Malcolm Roulston, Head of Corporate Infrastructure

PUBLIC SERVICES NETWORK REQUIREMENT

(GLOSSARY OF TERMS)

PSN:	Public Services Network – a secure government network designed for the purpose of information sharing
PSN Connection Controls:	a set of control measures designed to ensure compliance with Government information security
PSN ICT Health Check:	a system designed to identify and resolve vulnerabilities in IT systems and networks which may compromise the confidentiality and / or integrity of information held on IT systems
PSN SUBMISSION:	A Government “check list” template of IT and information and security measures that must be met to retain PSN connectivity
ICT SECURITY CONSULTANT:	A “pool” of information assurance consultants with the remit to advise Government and Public Sector bodies (referred to as CLAS consultants)
IT PENETRATION TEST:	A set of tests carried out by an approved security specialist whose function it is to gain elevated access to a server, desktop machine, or network device by exploiting known software vulnerabilities
SOCITM:	Society of Information Technology Management
SOLACE:	Society of Local Authority Chief Executive and Senior Managers
LGA:	Local Government Association

APPENDIX A

Workstream	Requirement	Maximum Capital Costs £m	Maximum Annual Revenue Costs £m
Replace Windows XP and Office 2003	Up to 4,350 PCs will require to be replaced from April 2014 onwards	2.120	0.080
VLAN separation of networks		0.100	0.000
Replace UNIX operating system	Migration to supported platform or upgrades for all major systems	0.080	0.050
Total		**2.300**	**0.130**

APPENDIX B

Workstream	Requirement	Capital Costs £m	Additional Revenue Costs £m	Resource Implications
Replace Corporate ISDX Telephone Network	Replace telephone network switch by March 2017	0.350	0.000	Significant; Mix of in-house and external support
Core Network Switches	Replace two main network switches by March 2018	0.160	0.000	Installation by hardware supplier
Windows Servers	Replace 120 Windows servers by April 2015	0.005	0.000	Significant; Mix of in-house and external support
SQL Server	Replace SQL server by April 2015	0.005	0.060	Significant; Mix of in-house and external support
Total		**0.520**	**0.060**	

APPENDIX C

DISTRIBUTION OF WINDOWS XP PC's and OFFICE 2003 INSTALLATIONS

Department	Product		
	Windows XP PC's	Office 2003 Installations	Total
Educational & Social Services	2,870	290	**3160**
Finance & Corporate Support	220	60	**280**
Neighbourhood Services	491	145	**636**
EA Leisure Trust	209	65	**274**
Totals	**3,790**	**560**	**4,350**

***** No cost under the terms of the Microsoft / Schools Enterprise Agreement

APPENDIX D

CODE OF CONNECTION - CONTROL MEASURES

REFERENCE	SUBJECT	CONTROL	2014 / CURRENT STATUS
NETWORK DIAGRAM & SCOPE			
DIA1	Network Diagrams & Scope	The Council must provide an up-to-date network diagram with each Code of Connection (CoCo) submission.	**G** the current network diagram will be updated before the submission date.
DIA2	Network Diagrams & Scope	This control is not applicable to EAC as we do not expose any services to the PSN.	**G** Not applicable.
INFORMATION RISK MANAGEMENT			
RIS1	Information Risk Management	The Council must produce a risk assessment for each external organisation wishing to connect to the network.	**A** A risk assessment template exists but the Information Governance Manager (IGM) will be required to update as and when appropriate.
RIS2	Information Risk Management	The Council must identify an individual officer responsible for information governance.	**G** Head of Democratic Services.
PHYSICAL SECURITY			
PHY1	Physical Security	The Council must ensure that physical access to hosts, servers, network equipment and data centres is secure.	**A** The IGM must keep the existing 'PSN Locations' spreadsheet up to date whenever a new site is added to the Corporate network.
PHY2	Physical Security	The Council must ensure that physical access to the building that hosts the PSN routers is secure.	**G** The PSN routers are based in the Civic Centre South BUDC. The building is secured by three locked doors before access can be gained to the racked equipment.
PERSONNEL SECURITY			
PER.1	Personnel Security	The Council must ensure that all employees are BPSS / Disclosure Scotland checked before commencing employment with East Ayrshire Council.	**R** All Council employees to be BPSS / Disclosure Scotland checked.
USER EDUCATION			
EDU1	User Education	The Council must ensure that all employees are fully aware of information governance, all policies and procedures that are associated and must receive appropriate training (dependant on job function).	**R** The IGM, via the CIGG, must ensure that all Council officers are fully aware of the importance of Information Governance. Several employees are finalising online training courses for all employees, the IGM / CIGG will have overall responsibility and ensure compliance.
EDU2	User Education	The Council must have an Acceptable Use Policy. All employees must confirm acceptance of this policy.	**A** The ICT Security Manager (ISM) must ensure that the Acceptable Use Policy is up to date and that all employees confirm their acceptance of it.
INCIDENT RESPONSE			
RES1	Incident Response	The Council must have an incident reporting policy.	**G** The IGM must ensure that the incident reporting policy is up to date, that all employees are aware of it and that reporting procedures are contained within.
RES2	Incident Response	The Council must have a written procedure for escalating security incidents contained within the incident reporting policy.	**G** The IGM must ensure that the incident reporting policy is up to date, that all employees are aware of it and that reporting procedures are contained within.
RES3	Incident Response	The Council must inform the Cabinet Office PSN Security Manager should any incident occur that involves PSN data.	**G** The IGM must confirm that they will notify the PSN Security Manager should an incident occur that involves the loss of PSN data.
CONFIGURATION			
CON1	Configuration	The Council must lock down each host, server and network device to ensure that any vulnerabilities cannot be exploited.	**R** The ICT Security Manager (ISM) must ensure that networked devices are locked down and as secured as far as possible (without affecting business) before connecting to the network.
CON2	Configuration	The Council must ensure that unauthorised software cannot be installed or executed on host machines.	**G** The ISM must lock down all domain hosts to ensure that software cannot be installed or executed.
CON3	Configuration	The Council must lock down hosts, servers and network devices to ensure that hardware configuration cannot be altered.	**G** The ISM must lock down networked devices and ensure that hardware cannot be modified in any way.
CON4	Configuration	The Council must ensure that users log in with 'least privilege' (ie/ users cannot log in as host, server or domain administrators).	**G** Corporate Infrastructure must continue to ensure that user accounts do not have administrator privileges.
CON5	Configuration	The Council must produce risk assessments before allowing access to active content on the internet (content such as Active-X, Java and Shockwave Flash).	**A** The ISM must produce active content risk assessments as and when required.
CON6	Configuration	The Council must ensure that users cannot execute software without receiving a prompt for consent.	**A** Corporate Infrastructure must ensure that users are prompted before running an application on a host computer / server.
COMPLIANCE CHECKING			
CHE1	Compliance Checking	The Council must undergo an IT Health Check as part of each CoCo submission. The health check must include domain hosts, servers, wi-fi and an external penetration test on the public facing servers. All vulnerabilities found must be remediated before accreditation is granted.	**R** Corporate Infrastructure must extend the current patching policy to include physical servers, all desktop hosts and all network devices. A patching schedule has now been implemented but has yet to be rolled out to physical servers, network devices, the Microsoft Office suite, UNIX, Apple Macintosh and non-Microsoft software (such as Adobe, Java and QuickTime). All host machines running Windows XP must be upgraded before the next submission. All host machines with Microsoft Office 2003 installed must be upgraded before the next submission.
PATCH MANAGEMENT			
PAT1	Patch Management	The Council must have an active patch management policy which covers all domain hosts, servers, network devices and firmware.	**R** Corporate Infrastructure need to extend the current patch policy to include physical servers, all desktop hosts and all network devices. A patching schedule has now been implemented but has yet to be rolled out to physical servers, network devices, the Microsoft Office suite, UNIX, Apple Macintosh and non-Microsoft software (such as Adobe, Java and QuickTime). All host machines running Windows XP must be upgraded before the next submission. All host machines with Microsoft Office 2003 installed must be upgraded before the next submission.
PAT2	Patch Management	The Council's patch management policy must detail a patch installation schedule prioritised by the severity of each missing patch.	**G** Corporate Infrastructure must ensure that the patch policy is updated regularly.
ACCESS CONTROL			

ACC1	Access Control	The Council must ensure that all PSN users are authenticated by an individual network logon (generic accounts cannot be used).	G	Corporate Infrastructure must ensure that host users continue to log in with individual (named) accounts.
ACC2	Access Control	The Council must have a Home Working Policy and an Access Control Policy.	G	The IGM must ensure that the Home Working Policy and the Access Control Policy are updated regularly.
BOUNDARY CONTROLS / GATEWAYS				
BOU1	Boundary Controls/Gateways	The Council must have a firewall installed between networks that have a different impact level to their own.	R	Corporate Infrastructure must update the corporate firewall to ensure network segregation.
BOU2	Boundary Controls/Gateways	The Council must have a firewall installed between their Corporate network and the PSN network.	G	If the entire Corporate network is in scope then the Council may need to firewall off schools and public access points. VLANs may be acceptable, we await confirmation from the Cabinet Office.
BOU3	Boundary Controls/Gateways	The Council must have a firewall installed between their Corporate network and the PSN network. This firewall should be configurable to allow / deny specific traffic.	G	If the entire Corporate network is in scope then the Council may need to firewall off schools and public access points. VLANs may be acceptable, we await confirmation from the Cabinet Office.
BOU4	Boundary Controls/Gateways	The Council must configure each firewall to only allow the required protocols and ports to carry out the required tasks.	G	Corporate Infrastructure must update the corporate firewall to ensure network segregation.
BOU5	Boundary Controls/Gateways	The Council must ensure that the data going to / from a non-PSN network to / from the PSN network is scanned and filtered for viruses, malware and other dangerous content.	G	Corporate Infrastucture must actively scan all traffic going to / coming from the PSN network.
BOU6	Boundary Controls/Gateways	The Council must ensure that the email gateway and internet gateway has been configured to deny access to known dangerous file types.	G	Corporate Infrastucture must scan email and internet traffic for dangerous file types.
REMOVABLE MEDIA				
MED1	Removable Media	The Council must ensure that access to USB devices is controlled and managed.	G	Corporate Infrastucture must apply and update the USB control policy via Sophos.
MALWARE PROTECTION				
MAL1	Malware Protection	The Council must ensure that viruses and malware (and other dangerous content) is being detected by the firewall, email gateway and internet gateway.	G	Corporate Infrastucture must scan all incoming and outgoing email and internet traffic.
MAL2	Malware Protection	The Council must ensure that viruses and malware (and other dangerous content) is being detected by the firewall, email gateway and internet gateway.	G	Corporate Infrastucture must scan all incoming and outgoing email and internet traffic.
MAL3	Malware Protection	The Council must ensure that access to USB devices is controlled and managed and that USB devices are scanned for viruses / malware when connected to a host device.	G	Corporate Infrastucture must apply and update the USB control policy via Sophos.
MOBILE / HOME WORKING				
MOB1	Mobile / Home Working	The Council must ensure that remote access to PSN services is managed and operated as defined in the Home Working Policy.	A	The IGM must ensure that the Home Working Policy is updated and contains information on how to access PSN services securely.
MOB2	Mobile / Home Working	The Council must ensure that remote access to PSN services is from fully managed devices and is controlled as defined in the Home Working Policy.	A	The IGM must ensure that the Home Working Policy is updated and contains information on how to access PSN services securely.
MOB3	Mobile / Home Working	The Council must ensure that remote access to PSN services is from fully managed devices and is controlled as defined in the Home Working Policy.	A	The IGM must ensure that the Home Working Policy is updated and contains information on how to access PSN services securely.
MOB4	Mobile / Home Working	The Council must ensure that remote access to PSN services is from fully managed devices and is controlled as defined in the Home Working Policy.	A	The IGM must ensure that the Home Working Policy is updated and contains information on how to access PSN services securely.
MOB5	Mobile / Home Working	The Council must ensure that any device that has remote access to any PSN service is encrypted and fully managed.	A	The IGM must ensure that the Home Working Policy is updated and contains information on how to access PSN services securely.
WIRELESS NETWORKS				
WIR1	Wireless Network	The Council must ensure that any wireless access from the Corporate network to the PSN network is configured as recommended by public sector guidance.	A	Corporate Infrastructure must lock down wireless access to PSN services as and when required. Should the entire network be in scope we may need to reconfigure some wireless access points.
NETWORK OBFUSCATION				
OBF1	Network Obfuscation	The Council must ensure that all details of internal IP addresses, server or host names are hidden before being passed to a less secure network (i.e the public internet).	G	Corporate Infrastucture must hide all internal network information before passing traffic outside the Corporate network.
PROTECTIVE MONITORING				
PRO1	Protective Monitoring	The Council must collate all system logfiles and audit devices that have access to the PSN network as recommended in Good Practice Guide 13.	G	Corporate Infrastructure must keep the GFI EventsManager server updated with hosts that have access to PSN services.
PRO2	Protective Monitoring	The Council must be prepared to supply the PSNA with logfiles and audit information to assist with any investigation that the PSNA may be involved in.	G	The IGM must agree to supply logifles to the PSNA whenever required.
PRO3	Protective Monitoring	The Council must retain the logfiles from all PSN connected devices for a minimum of 6 months.	G	Corporate Infrastructure must keep all logfiles for a minimum of 6 months.
PRO4	Protective Monitoring	The Council must ensure that all devices on the Corporate network synchronise time with the PSN time service.	G	Corporate Infrastructure must keep all hosts synchronising with the PSN time source.
PRO5	Protective Monitoring	All servers on the Council network must be configured with a static IP address.	G	Corporate Infrastructure must assign static IP address to internal severs.
e.MAIL				
EMA1	e.Mail	The Council must adopt an e.Mail classification scheme. The scheme should be in line with the Government Protective Marking Scheme.	A	The IGM must keep the protective marking scheme updated and in line with the GPMS.