SPF Compliance Checklist

SPF Security Compliance

This compliance checklist is designed to assist businesses in assessing their ability to meet the requirements of the UK Government's Security Policy Framework. It is not a substitute for a detailed assessment by a professional and is not suitable for submission to HMG agencies as proof of compliance. This is provided "as is" without any warranty or guarantees. It is essential that current regulations are checked to properly determine compliance.

Security Risk Management

Security Policy Framework Compliance

Audit Checklist

SPF Version 3.0 (October 2009)

Checklist Version 1.0 (January 2010)

Security Policy Framework (v 3.0) Audit Check List

Auditor Name: ..... Audit Date: .....

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
Governance, Risk Management and Compliance					
1.1		Governance			
1.1.1	1		Ensure staff are aware of the requirements and responsibilities placed upon them by the SPF		
1.1.2	1		Identify any statutory security requirements which take precedence.		
1.1.3	2		Identify delivery partners liable to be subject to SPF.		
1.1.4	2		Ensure delivery partners are compliant with SPF requirements.		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
1.2		Roles, accountability and responsibilities			
1.2.1	3		Identify board level representative responsible for security		
1.2.2	3		Identify where security responsibilities lie		
1.2.3	3		Identify relationships between organisations board and the boards of the parent agency or other bodies.		
1.2.4	4		Identify designated DSO		
1.2.5	4		Ensure DSO day to day responsibilities cover all aspects of Protective Security		
1.3		Risk Management			
1.3.1	5		Adopt an organisation-wide risk management approach to protective security		
1.3.2	5		Maintain a Protective Security Risk Register		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
1.4		Assurance, Self Assessment & Reporting			
1.4.1	6		Make departmental security policy widely available internally and reference this in overall business plans		
1.4.2	6		Have a system of assurance of compliance with security policy.		
1.4.3	6		Produce an annual report to HOD / Management Board on the state of all aspects of security.		
1.4.4	7		Submit annual report to COSPD via parent Department / Agency		
1.5		Audit and Review			
1.5.1	8		Comply with oversight arrangements as set out by Cabinet Office		
1.6		Culture, Training and Professionalism			
1.6.1	9		Ensure board members responsible for security undergo appropriate		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			familiarisation upon appointment.		
1.6.2	9		Ensure DSOs are given security briefings from Cabinet Office / CPNI on appointment.		
1.6.3	9		Ensure DSOs have attended relevant training courses before, or at earliest opportunity after appointment.		
1.6.4	9		Ensure all security staff posses competencies & training to the appropriate level for their role.		
1.6.5	9		Ensure Security awareness & education is built into staff induction.		
1.6.6	9		Ensure all staff complete regular security familiarisation.		
1.6.7	9		Ensure there are demonstrable plans to foster a culture of proportionate protective security.		
1.6.8	9		Ensure there is a clearly stated and		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			available policy, and mechanisms in place, to allow for independent and anonymous reporting of security incidents.		
1.7		International security agreements			
1.7.1	10		Ensure organisation adheres to any UK obligations in multilateral or bilateral international agreements.		
Protective Marking and Asset Control					
2.1		Protective Marking System			
2.1.1	11		Organisation must apply the Protective Marking System and the necessary controls & technical measures as outlined in the SPF.		
2.2.		Legal Requirements			
2.2.1	12		Organisation must provide staff with guidance on the OSA, DPA and FOIA.		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.2.2	12		Staff handling PMI must be given guidance on how legislation relates to their role.		
2.3		Official Secrets Act			
2.3.1	13		Organisation must ensure staff who are notifiable under Section 1(1) of OSA 1989 are notified in writing.		
2.3.2	13		Organisation must issue notified employees with renewal notices every 5 years.		
2.3.3	13		Organisation must keep under review the need for continuing notification of individual posts.		
2.3.4	13		Organisation must maintain and keep under review the number of notifiable posts.		
2.4		Data Protection Act			
2.4.1	14		Organisation must follow the minimum standards & procedures for handling and		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			protecting citizen or personal data as outlined in HMG IA Standard 6		
2.5		Freedom of Information Act			
2.5.1	15		Organisation must ensure that any PMM that is to be released under the FOIA is properly de-classified first and is marked as such.		
2.6		The “need to know” (NTK) principle			
2.6.1	16		Organisation must ensure that access to PM assets is only granted on the basis of the “need to know” principle.		
2.6.2	16		All employees much me made fully aware of their personal responsibility in applying this principle.		
2.7		International Security Agreements			
2.7.1	17		Organisation must adhere to any UK obligations in regard to international markings.		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.8		Material Originating Outside HMG			
2.8.1	18		Organisation must ensure that non-HMG material which is marked to indicate sensitivity is handled at the equivalent level with the PM System.		
2.9		Government Protective Marking System			
2.9.1		Universal Controls			
2.9.1.1	19		Organisation must ensure access to PMM is granted only on a genuine NTK basis.		
2.9.1.2	19		Assets must be clearly and conspicuously marked.		
2.9.1.3	19		Protective markings are only changed with permission by the originator or designated owner.		
2.9.1.4	19		Assets sent overseas (including to UK posts) must be protected as indicated by the originators marking.		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.9.1.5	19		Assets sent overseas (including to UK posts) are protected from foreign FOI legislation as required.		
2.9.1.6	19		No official record can be destroyed unless it has been reviewed for historical interest under the Public Records Act		
2.9.1.7	19		A file, or group of protectively marked documents or assets, must carry the PM of the highest marked document or asset contained within.		
2.9.2		Special Handling			
2.9.2.1	20		Organisational procedures must meet special handling arrangements where they apply.		
2.9.2.2	20		Must ensure staff handling information subject to special handling requirements understand the arrangements in place.		
2.9.3		Breaches			

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
2.9.3.1	21		There must be a breach system in place.		
2.9.3.2	21		Staff must be given clear guidance that deliberate or accidental compromise of PMM may lead to disciplinary or criminal proceedings.		
Personnel Security					
3.1		Risk Management			
3.1.1	22		Must, as part of the risk management approach, assess the need to apply personnel security controls against specific posts & the access to sensitive assets.		
3.2		Baseline Personnel Security Standard (BPSS)			
3.2.1	23		Must apply the requirements of BPSS to all staff, contractors and temporary staff.		
3.3		National Security Vetting (NSV)			
3.3.1	24		Organisation must ensure that NSV is only		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			applied where it is necessary, proportionate & adds real value.		
3.3.2	25		Organisation must follow the procedures for NSV as contained in the relevant supplementary material with the SPF.		
3.3.3	26		Vetting decisions can only be made by Government Departments & Agencies and Police Forces.		
3.3.4	27		There must be in place personnel security aftercare arrangements.		
3.3.5	27		Managers must be reminded of their responsibility to inform the vetting authorities of any change in circumstances that may impact on the suitability to hold a security clearance.		
3.3.6	28		Organisations must have in place an internal departmental vetting appeals process for existing employees.		
3.3.7	29		The Cabinet Office Security Policy Division		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			must be informed when an individual initiates a legal challenge in respect of an NSV decision.		
3.3.8	30		Records must be maintained as to how many, and what type of security vetting clearances have been undertaken on an annual basis. This should be included in the annual security report.		
3.3.9	30		Records must be maintained as to the number, and outcome of, internal and independent appeals. This should be included in the annual security report.		
Information Security and Assurance					
4.1		Information Security Policy			
4.1.1	31		Organisation must have, as a component of their overarching security policy, an information security policy explaining compliance with the minimum requirements of this policy and the wider		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			framework.		
4.2		Managing Information Risk			
4.2.1	32		Must conduct an annual technical risk assessment (using HMG IA Standard 1) for all ICT projects and programmes.		
4.2.2	32		Must conduct a technical risk assessment when there is a significant change to existing HMG ICT systems in operation.		
4.2.3	32		Assessment and risk management decisions must be recorded in the RMADS using HMG IA Standard 2.		
4.3		Business Impact			
4.3.1	33		Organisation must, in conjunction with the PM system, use Business Impact Levels (ILs) to assess and identify the impact to the business through the loss of CIA.		
4.4		Roles and Responsibilities			

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
4.4.1	34		Information risk must be specifically addressed in the departmental annual Statement on Internal Control and signed off by the Accounting Officer.		
4.4.2	35		Departments must have a designated Senior Information Risk Owner (SIRO).		
4.4.3	35		Departments must have a designated Information Technology Security Officer (ITSO).		
4.4.4	35		Departments must have a designated Communications Security Officer (ComSO) if cryptographic material is handled.		
4.4.5	35		Departments must have a designated Information Asset Owners for each identified information asset.		
4.5		Accreditation and Audit			
4.5.1.1	36		ICT systems that process PM Government data must be accredited using HMG IA		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			Standard 2.		
4.5.1.2	36		Accredited systems must be reviewed at least annually to judge whether material changes have occurred which could alter the accreditation status.		
4.5.2.1	37		Organisation must have the ability to regularly audit information assets and ICT systems.		
4.5.2.2	37		Must conduct regular compliance checks by the Accreditor.		
4.5.2.3	37		Must implement and maintain a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system.		
4.5.3.1	38		All ICT systems must have suitable identification and authentication controls to manage the risk of unauthorised access,		
4.5.3.2	38		All ICT systems must have suitable identification and authentication controls		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			to enable auditing.		
4.5.3.3	38		All ICT systems must have suitable identification and authentication controls correctly manage user accounts.		
4.6		Codes of connection and technical controls			
4.6.1	39		Organisation must follow the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which they are signatories.		
4.7		Cryptography			
4.7.1	40		Must comply with HMG IA Standard 4 (parts 1-3) for the protection of PMM.		
4.8		Eavesdropping and ECM			
4.8.1	41		Organisation must follow specific Government procedure to manage the risk posed by eavesdropping and electro-magnetic emanations.		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
4.9		Remote working / mobile media			
4.9.1	42		Must have a policy on remote working which complies with the requirements of the SPF.		
4.10		Procurement			
4.10.1	43		Must ensure that security requirements are specified in ICT contracts and all new ICT contracts handling personal data must adhere to the OGC model terms and conditions.		
4.11		Reporting Incidents			
4.11.1	44		There must be in place clear policies and processes for reporting, managing and resolving ICT security incidents.		
4.11.2	44		All security incidents must be reported to appropriate security authorities and HMG incident management bodies / ICO / CSIA as required,		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
4.12		Secure disposal			
4.12.1	45		Organisation must ensure all media used for storing or processing PM or otherwise sensitive information is disposed of in accordance with HMG IA Standard 5.		
4.12		Personnel and Physical Security			
4.12.1	46		Must ensure that ICT used with higher levels of privilege and / or potentially wide access, or those with responsibility for ICT security are subject to evaluation for NSV clearances appropriate to the protective marking of the information processed.		
4.12.2	47		Must ensure all locations where information and system assets (inc cryptographic items) are kept have an appropriate level of physical security as set out in this framework.		
4.13		Education, Training and Awareness			

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
4.13.1.1	48		Organisation must ensure all users of ICT systems are familiar with SyOPs		
4.13.1.2	48		Organisation must ensure all users of ICT systems receive appropriate security training and are aware of local processes for reporting issues of security concern.		
4.13.2.1	48		Staff who manage and maintain the secure configuration of ICT systems must be appropriately trained, aware of incident reporting and the minimum standards relating to the handling of PMM.		
4.14		Business Continuity and Disaster Recovery Planning			
4.14.1	49		Must ensure that all location s where information and system assets (including cryptographic items) are kept have appropriate BC and DR plans.		
Physical Security					
5.1		Defence in Depth			

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
5.1.1	50		The organisation must adopt a "layered" approach to physical security, ensuring their physical security policy incorporates identifiable elements of prevention, detection and response.		
5.2		Storage of Sensitive Assets			
5.2.1	51		Must use the Physical Security Assessment Questionnaire and Physical Security Baseline Controls Matrix to identify appropriate physical security measures.		
5.2.2	52		Must ensure that PM or valuable material is secured in appropriate security containers or secure rooms.		
5.2.3	53		Must ensure that windows, doors, locks and entry controls meet appropriate security standards in rooms holding PM or sensitive assets.		
5.3		Office Areas			

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
5.3.1	54		In office areas there must be put in place, procedures to avoid access to PMM by individuals who do not have a NTK.		
5.4		Building Security			
5.4.1	55		Organisation must assess the security risks to their estate ensuring that security is fully integrated early in the process of planning, selecting, designing and modifying their facilities.		
5.5		Physical Access Control			
5.5.1	56		Organisation must control access to their estate using safeguards that will prevent unauthorised access.		
5.5.2.1	57		There must be plans and procedures in place for dealing with & intercepting unauthorised visitors or intruders.		
5.5.2.2	57		There must be plans and procedures in place for a systematic search of premises		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			where necessary.		
5.5.3	58		Must ensure access control policies are available to all staff and that staff are briefed on their personal responsibilities.		
5.6		Incoming Mail and Deliveries			
5.6.1	59		There must be appropriate procedures in place for screening incoming mail / deliveries for suspicious items.		
5.7		Manned Guarding			
5.7.1	60		Must consider the use of guard forces to protect assets held.		
5.7.2	60		Where guards are deployed the GSZ Manned Guarding Services Manual is considered best practice.		
5.8		Perimeter Security			
5.8.1	61		There must be a secure perimeter with appropriate security barriers and entry		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			controls.		
5.8.2	61		Perimeter should offer physical protection from unauthorised access, damage and interference & allow for quick ID of suspicious individuals / items.		
5.9		Procurement			
5.9.1	62		Must produce a detailed Operational requirement before deciding to deploy a security measure.		
5.10		CCTV			
5.10.1	63		Deployment of CCTV must be in accordance with DPA 1998.		
Counter Terrorism					
6.1		Categorisation of Estate			
6.1.1	64		Establishment must be categorised according to likelihood of being, or in close		

Security Policy Framework (v 3.0) Audit Check List

Reference		Audit area, objective and questions		Results	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			proximity to, a potential terrorist target.		
6.2		Counter Terrorism Response Level Systems			
6.2.1	65		DSO must ensure that the organisation has baseline CT physical security measures and CT incremental measures in pl ace at each Response Level.		
6.2.2	65		DSO must ensure that there is a system to apply the correct identified CT incremental security measure at each response level.		
6.3		Counter Terrorist Protective Security Policy and Plans			
6.3.1	66		As part of the overall security policy, there must be a Counter Terrorist protective security policy in place.		
6.3.1.1	66		This policy must include application of central advice and guidance.		
6.3.1.2	66		This policy must include departmental roles and responsibilities, including 3rd parties and contractors.		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
6.3.1.3	66		This policy must include management controls and assurance that appropriate measures and plans are in place.		
6.3.1.4	66		This policy must include communication arrangements including briefing of staff.		
6.3.1.5	66		This policy must include arrangements for testing CT plans.		
6.3.1.6	66		This policy must include liaison with emergency services and multi-agency contingency pans		
6.3.2	67		There must be a Counter Terrorist protective security plan in place.		
6.3.2.1	67		This plan must include details of all protective security measures to be implemented following an increase or decrease in the Response Level.		
6.3.2.2	67		This plan must include instructions on how to respond to a specific threat, event or		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			item.		
6.3.2.3	67		This plan must include a search plan.		
6.3.2.4	67		This plan must include evacuation plans including details on securing the premises in the event of a full evacuation.		
6.3.2.5	67		This plan must include business continuity plans.		
6.3.2.6	67		This plan must include a communications with the media strategy, including handling enquiries from concerned family & friends.		
6.3.2.7	67		This plan must include liaison with emergency services and any multi-agency contingency plans.		
6.4		Assurance			
6.4.1	68		The annual security report made by the DSO to the Head of Department must explicitly provide a statement of assurance on CT protective security including		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
			compliance with additional measures implemented after any increase in the Response Level.		
6.4.2	69		As part of BC and emergency response plans the CT protective security plans must be tested regularly in line with the establishment threat level.		
Business Continuity					
7.1		Business Continuity Management			
7.1.1	70		Organisation must have robust, up to date, fit for purpose and flexible business continuity management arrangements.		
7.1.2	70		Business Continuity arrangements must be tested on a regular basis.		
7.1.3	70		Business Continuity plans must be regularly reviewed and supported by competent staff.		

Security Policy Framework (v 3.0) Audit Check List					
Reference		**Audit area, objective and questions**		**Results**	
Checklist	**SPF MR**	**Section**	**Audit Requirement**	**Findings**	**Compliance**
7.1.4			Business Continuity arrangements must be appropriately communicated to staff.		

Halkyn Security Consulting Ltd

Halkyn Security is an independent security consultancy offering a specialised security compliance service to assist enterprises of all sizes become compliant with HMG regulations, and remain compliant for the lifetime of contracts. As an independent consultancy all our security advice is vendor neutral and we are committed to ensuring our clients get the best possible value for money.

We utilise experienced staff with a minimum of SC clearance to conduct detailed assessments against current regulations to allow you, or your key stakeholders, to determine what your current security posture is and what (if anything) would be required to meet the standards laid down by the relevant Government Department or Agency.

For companies currently working on Government contracts we offer a review service to ensure that you are still current with the regulations and that you have employed the most cost effective solutions. While this is not in place of the reviews carried out by the sponsoring Agency, it will place you in the best possible position to ensure a clean bill of health.

To find out more, or get a free, no-obligation quote visit www.halkynconsulting.co.uk or email info@halkynconsulting.co.uk with your requirements.