Appendix 3 - Joint FRS **Information Security** & **Assurance** Sub Group **Action Plan**

Version 2 – 5th Oct 2010

Objective 1 - Introduce mandatory requirements 11, 12, 14, 15, 16, 19, 21, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42, 43, 45, 46, 47, 48, and 49 of the HMG Security Policy Framework by January 2012

Objective 2 – Support the work the other Protective Security Sub Groups

Primary Objectives (taken from the 70 mandatory requirements contained within the HMG Security Policy Framework)

1. Introduce a Protective Marking scheme.

2. Provide staff with guidance on the Official Secrets Act, Data Protection Act and Freedom of Information Act.

3. Not required for the FRS

4. Ensure the minimum standards for handling data are followed – HMG 1A No6 Protective Data and Managing Risk Information.

5. Ensure that protectively marked material to be released under the FIO must be declassified first and the originator informed.

6. Ensure access to protectively marked assets is only granted on a need to know basis.

7. Not required for the FRS

8. Not required for the FRS

9. Ensure that baseline controls are applied to all Protectively Marked material.

10. Not required for the FRS

11. Introduce a breach system which details how deliberate or accidental compromise of Protectively Marked material can lead to discipline or criminal proceedings.

31. As part of an overarching Security Policy, develop an Information Security Policy detailing how the organisation and delivery partners comply with the minimum standards of the SPF.

32. Must conduct annual technical risk assessment using HMB 1A standard. Risk management decision must be recorded in the Risk Management and Accreditation Document Set (RMADS) using HMG 1A Standard no 2.

33. In conjunction with a Protective Marking System, use business Impact Levels to assess and identify the impacts to the business.

34. Report how Information risks are being addressed within departmental annual statements of internal control which is signed off by the accounting officer.

35. Determine the need for the following posts within each FRS or within the region : -

a. Senior Information Risk Officer (SIRO) at board level
b. Information Technology Security Officer (ITSO)
c. Communication Security Officer (ComSO)
d. Information Asset Owner

36. Ensure that ICT systems are accredited to HMG 1A Standard No2 – Risk Management and Accreditation of IT systems. Ensure that the status must be renewed annually.

37. Must Audit Information Assets regularly: -
    a. Compliance checks carried by ITSO and document in RMADS
    b. Forensic readiness policy

38. Ensure that all IT systems must have suitable identification and authentication controls.

39. Consider the feasibility of utilising secure codes of connection i.e. gsi

40. Not required for the FRS

41. Not required for the FRS

42. Develop and introduce a Protective Security Policy regarding the implications of remote working

43. Ensure that security requirements are specified in ICT contracts.

44. Not required for the FRS

45. Develop and introduce a policy and procedure to ensure that sensitive information is disposed of or sanitised in accordance with HMG 1A standard No. 5 – Secure sanitisation of protectively marked or sensitive information.

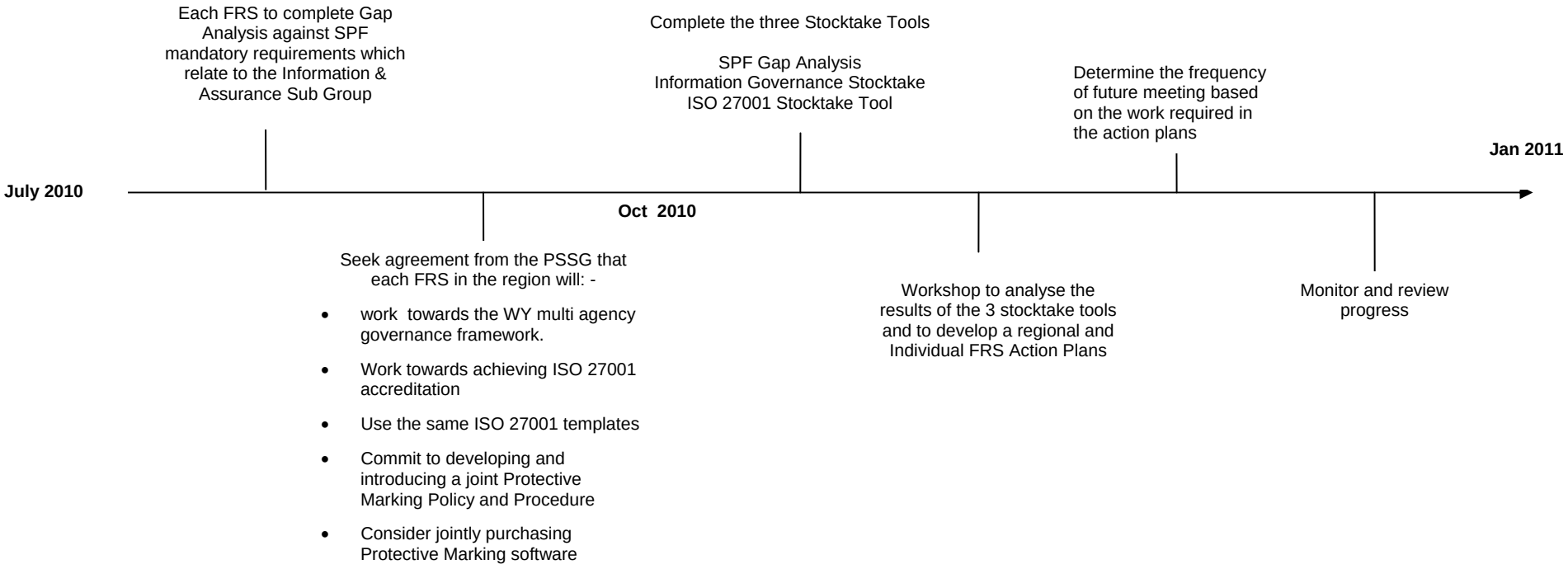
46. Ensure that ICT users with high levels of privilege are subject to evaluation for National Security clearance.

47. Ensure that locations where IT systems are kept must be subject to an appropriate level of physical security.

48. Ensure that users of IT systems are familiar with security operating procedures.

49. Must have appropriate Business Continuity and Disaster Recovery plans.

Project Milestones for 2010



Governance Arrangements	
1	???????? is be Executive Level Lead
2	Each FRS should will be represented by the Head of IT and another IT/Information Management professional
3	Meetings will take place every quarter at the ???? and will be arranged to take place a couple of weeks prior to the PSSG
4	Teleconference meetings may be called if appropriate in between the quarterly meetings
5	The Joint FRS PS Co-ordinator will Co-ordinate activity and manage correspondence across the group
6	To ensure maximum efficiency any work required to develop PS policy will be shared equally between the four services in the group and will be presented as a joint FRS piece of work.
7	The Executive Lead/Chair will report progress to the PSSG. The Joint FRS Co-ordinator will report to the Regional CFOA Group and YHRORG.

Members		
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

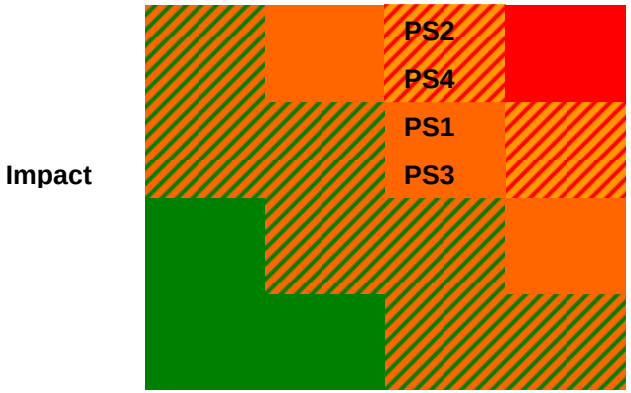
Information Security and Assurance Project Risk Register (To be discussed and developed further by the Information Security & Assurance Sub Group)

	Risk Description	Initial Risk (High, Medium, Low)	Control Measure	Potential Risk (Post control Measure)	% Progress against Control Measure	Current Risk	Risk Owners
IS1	Information accessed and utilised for criminal activity		Implementation of SPF Mandatory Requirements 22, 23, 24, 25, 27 and 30		**0%**		
IS2	Information Accessed and utilised for Terrorist Activity.		Implementation of SPF Mandatory Requirements 22, 23, 24, 25 and 30.		**0%**		
IS3	Reputation and Financial Risk from non compliance with FOI, Data Protection and Official Secrets Act		Implementation of SPF Mandatory Requirements 22, 23, 24, 25 and 30.		**0%**		
IS4	Life risk associated with mobilising and Risk Critical information system failures due to terrorist of malicious attack		Implementation of SPF Mandatory Requirements 22, 23, 24, 25, 27 and 30.		**0%**		

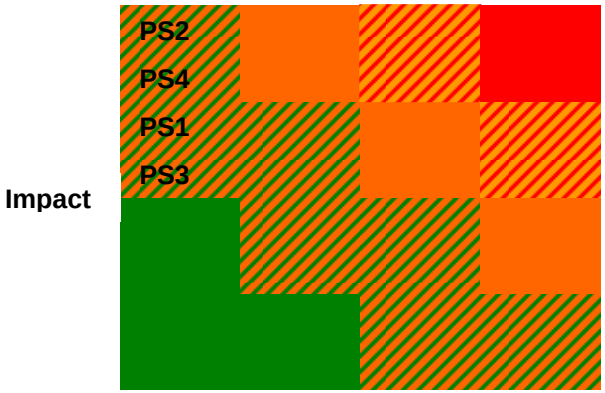
Information Security & Assurance Security Risk Profile

(To be discussed and developed further by the Information Security & Assurance Sub Group

Initial (May 2010)



Objective (Jan 2012)



Impact						
	Major	**4**	4	8	12	16
	Serious	**3**	3	6	9	12
	Significant	**2**	2	4	6	8
	Minor	**1**	1	2	3	4
			1	**2**	**3**	**4**
			Very unlikely	Unlikely	Likely	Very likely
			Likelihood			

Impact rating	Score	Description (threats)
Major	4	• Major potential impact on safety / critical control systems • Major potential impact on operational performance • Prosecution by Enforcing Authorities • Statutory/legislative mandate • National media coverage • Major financial / budgetary implications
Serious	3	• Serious potential impact on safety / control systems • Serious potential impact on operational performance • Attract scrutiny by Regulatory Bodies • Code of practice expectation • Local media coverage • Serious financial / budgetary implications
Significant	2	• Significant potential impact on safety / control systems • Significant potential impact on operational performance • Increased public expectation • Significant financial/budgetary implications
Minor	1	• Minor impact on safety / control systems • Minor impact on operational performance • Minimal disruptions not affecting service • Minor financial loss
Likelihood	**Score**	**Description (threats)**
Very likely	4	• More than 75% chance of occurrence
Likely	3	• 40%-75% chance of occurrence
Unlikely	2	• 10%- 40% chance of occurrence
Very unlikely	1	Less than 10% chance of occurrence

1st Information Security and Assurance Sub Group Meeting –September 10
Attendees
Apologies :

	Decisions/Actions	Action By:	When		Done
1	Having considered the cost along with negative feedback from other organisations it was agreed not to consider regional procurement of the ???? software at this time.	NA		Raised at PSSG who agreed with the Sub Group decision not to progress ????	Done
2	Agreed to utilise the same ISO 27001 templates to enable work to be shared throughout the region without infringing copyright.	All	Immediately	??? FRS have confirmed that they are able to utilise the same templates as WYFR	
3	Agreed to complete three Protective Security related Stocktake tools and return to ??? ?? by 15th October so that a detailed picture of Protective Security within the region could be developed: SPF Gap Analysis, ISO 27001 Stocktake and Information Governance Stocktake.	All	15th October	The Information Governance Stocktake Tool has been developed so that is simple and user friendly. All three Tools have been circulated to all members of the group	
4	Agreed to meet up for a full day at the ??? WC 25 Oct to consider the results of the 3 Check List exercise, identify gaps, determine risks and draw up a joint FRS Action Plan.	All	WC 25 Oct	Date yet to be arranged	
5	Agreed that the frequency of future meetings would be determined by the outcome of the workshop at the end of October.	All		To be	
6	Agreed that ?????? would make arrangements for the workshop at the ???? at the end of October.	?????	ASAP		
7	Agreed that the roll out of the Protective Marking policy and procedure was not an IT issue now that the purchase of ????? software had been shelved. Pass up to the PSSG for decision.	NA	NA	Discussed at PSSG on 22nd Sep who agreed that the Protective Marking Policy would be moved to the Personnel Security Sub Group	
8	Considered the presentation provided by ????of UKGovConsult and requested that he draw up a more detailed Business Case along with an overview of the options available to the FRS for connecting to a secure network.	NA	NA	????? presented to the PSSG on 22nd Sep and is developing a business case and considering options to achieve access to a secure network.	