Appendix III

Strategic Risk Register

Business area	Information
Responsible officer	DCC as Senior Information Risk Owner (SIRO)
Period	Quarter 3, 2014/15

Identifier	Category	Risk description	Owner	Proximity	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 033	Operational efficiency & effectiveness	DIEU, Op Vanguard & several other IT assets are not connected to the Force network & supported by IS, increasing the probability that equipment failure accidentally compromises the availability of multiple information assets which impacts on the delivery of objectives across the Force	DCC (SIRO)	2015	Med (3)	High (4)	High (12)	⇔	Reduce the probability (DIEU only, temporary): • 6 workstations updated by DIEU; Reduce the probability (all): • IS to review all standalone IT assets across the Force & provide technical support	Reasonable
INF 016	Judicial process	Audio / video recordings passed to CPS are lost within their offices, accidentally compromising availability of evidential information, causing delays which reduce the efficiency of the judicial process & creating unnecessary work for the DIEU	DCC (SIRO)	Every month	Very high (5)	Low (2)	Med (10)	⇔	Reduce the probability: • Issues have been reported to the ICO; • Exploration with CPS of options to tighten the process	Substantial

Identifier	Category	Risk description	Owner	Proximity	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INS 007	Operational efficiency & effectiveness	Force policy to allow remote access to the network via SSL VPN using employees' own devices (BYOD) results in the national accreditor denying accreditation to MFSS, which prevents delivery of the project & realisation of project benefits	DCC (SIRO)	March 2015	Low (2)	Very high (5)	Med (10)	NEW	Avoid the risk: • Change remote working policy to only allow remote access using Force-owned devices; • Provide new laptops to top 200 remote access users	Substantial
INF 008	Operational efficiency & effectiveness	System security vulnerabilities within Windows XP following expiry of MS support enable an external hacker to breach the Force network, deliberately compromising the availability of multiple information assets which impacts on the delivery of objectives across the Force	DCC (SIRO)	2014/15	Low (2)	High (4)	Med (8)	⇔	Reduce the probability: • Existing network security; • Extra 12 months XP support from Microsoft; • Windows 7 project to upgrade operating system	Limited

Identifier	Category	Risk description	Owner	Proximity	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INS 003	Operational efficiency & effectiveness	Force policy to allow remote access to the network via SSL VPN using employees' own devices (BYOD) and continued use of Windows XP results in the national accreditor denying the Force permission to connect to the national Public Services Network (PSN), which reduces operational efficiency and effectiveness	DCC (SIRO)	Summer 2015	Low (2)	High (4)	Med (8)	⇔	Avoid the risk: • Change remote working policy to only allow remote access using Force-owned devices; • Provide new laptops to top 200 remote access users; • Windows 7 project	Reasonable
INF 019	Judicial proceedings	With limited back-up capability at Holmes House, equipment failure accidentally compromises the availability of information assets accessed through DIU IT systems, which impacts on the provision of evidence and reduces the efficiency of the judicial process	DCC (SIRO)	2015	Low (2)	High (4)	Med (8)	↓	Reduce the probability: • Project to relocate DIU to FHQ & utilise back-up capability	Reasonable

Closed risks

Identifier	Risk description	Reason for closure	Date closed	Closed by
INF 030	Breach of FHQ security through unattended main gate resulting in harm to individuals or damage to property	Risk reduced to acceptable level; to be monitored through security incident reporting procedure	August 2014	FIAB
INF 020	Loss of access to information if Mansfield servers overheat following air-con failure	Risk reduced to acceptable level through installation of replacement air-con units	August 2014	FIAB
INF 017	Unauthorised access to Force information by an officer, member of staff or volunteer (probability unknown)	Risk to be assessed by individual information asset	November 2014	FIAB
INF 010	Unauthorised third party access to Force information (probability unknown)	Risk to be assessed by individual information asset	November 2014	FIAB

Appendix – explanatory note

The risk category should be drawn from the following list:

- Crime & community safety
- Operational efficiency & effectiveness
- Judicial process
- Finances
- Reputation
- Life & safety
- Compliance
- Environment

The following definitions and criteria have been used to describe and assess the risks recorded in this risk register:

Probability	Score	Definition
Very high	5	Extremely likely to occur (>90% chance)
High	4	More likely to occur than not (66-90% chance)
Medium	3	As likely to occur as not (36-65% chance); or unknown
Low	2	Unlikely to occur (11-35% chance)
Very low	1	Extremely unlikely to occur (1-10% chance)

Impact	Score	Definition
Very high	5	Significant, lasting or permanent impact on objectives
High	4	Significant, temporary or noticeable, lasting impact on objectives
Medium	3	Noticeable, temporary or minor, lasting impact on objectives; or unknown
Low	2	Minor, temporary or minimal, lasting impact on objectives
Very low	1	Minimal, temporary impact on objectives

When assessing financial impact the following criteria have been used:

Impact	Score	Definition
Very high	5	£x,000,000s (millions)
High	4	£x00,000s (hundreds of thousands)
Medium	3	£x0,000s (tens of thousands)
Low	2	£x,000s (thousands)
Very low	1	£x00s (hundreds)

Probability is multiplied by Impact to give the overall Rating, which is colour coded, dependent upon whether the risk represents a threat (negative impact) or opportunity (positive impact) using the matrices below:

Impact						
	V high (5)	5	10	15	20	25
	High (4)	4	8	12	16	20
	Medium (3)	3	6	9	12	15
	Low (2)	2	4	6	8	10
	V low (1)	1	2	3	4	5
		V low (1)	Low (2)	Medium (3)	High (4)	V high (5)
		Probability				

Threat scoring matrix

Impact						
	V high (5)	25	20	15	10	5
	High (4)	20	16	12	8	4
	Medium (3)	15	12	9	6	3
	Low (2)	10	8	6	4	2
	V low (1)	5	4	3	2	1
		V low (5)	Low (4)	Medium (3)	High (2)	V high (1)
		Probability				

Opportunity scoring matrix

Confidence rating

The Confidence rating that is applied to each risk represents an evaluation of the source information used to assess the risk, as follows:

- Substantial – risk scoring is based on a significant amount of reliable data and / or intelligence
- Reasonable – risk scoring is based on some data and / or intelligence, but there are gaps or issues with reliability
- Limited – risk scoring is based on professional judgement alone