Risk Register

Business area	Information
Responsible officer	DCC as Senior Information Risk Owner (SIRO)
Period	Quarter 2, 2015/16

Identifier	Category	Risk description	Information Asset Owner / Delegate	Proximity / Frequency	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 0006	Operational efficiency & effectiveness	The Sexual Exploitation Investigation Unit (SEIU) has several standalone computers containing at least 13.5TB of digital information (including indecent images of children and related reports, BIL4); as this information is not backed up to the Force network equipment failure could result in permanent loss of evidential and intelligence information which impedes future serious crime investigations	Head of Public Protection / Det Insp, SEIU	2015	Med (3) u/k	Very high (5)	High (15)	⇔	Reduce the probability: • IS and InfoSec, with the IAD, to review the cause of the risk & develop a risk management plan	Limited
INF 0007	Operational efficiency & effectiveness	The Sexual Exploitation Investigation Unit (SEIU) has digital information (including indecent images of children and related reports, BIL4) stored on external hard drives kept at Holmes House; damage to or failure of those devices could result in permanent loss of evidential and intelligence information which impedes future serious crime investigations	Head of Public Protection / Det Insp, SEIU	2015	Med (3) u/k	Very high (5)	High (15)	⇔	Reduce the probability: • IS and InfoSec, with the IAD, to review the cause of the risk & develop a risk management plan	Limited

Identifier	Category	Risk description	Information Asset Owner / Delegate	Proximity / Frequency	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 0017	Operational efficiency & effectiveness	Control room operator error, or issues with the interface between Vision and Compact IT systems, results in information relating to missing persons reports not being made available when required by coordinators and divisional officers (approx. 1 in 4)	Head of Public Protection / Missing Persons Manager	Daily	Very high (5)	Med (3)	High (15)	NEW	Reduce the probability: • IS and EMSCU to engage the supplier to review the interface & identify cause • *CM to communicate correct recording of missing persons incidents to control room operators?*	Substantial
INF 0005	Judicial process	The Digital Image Evidence Unit (DIEU) has digital information (ie. CCTV, BIL 3) stored on standalone computers; as this information is not backed up to the Force network equipment failure could result in permanent loss of evidential information which impedes the prosecution of crime	Head of Crime Support / DIEU Manager	2015	Med (3) u/k	High (4)	High (12)	⇔	Reduce the probability: • IS and InfoSec, with the IAD, to review the cause of the risk & develop a risk management plan	Limited

Identifier	Category	Risk description	Information Asset Owner / Delegate	Proximity / Frequency	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 0016	Life & safety	A supervisor using the DMS system accesses the sensitive personal data (specifically information about health and absence) of another employee who they do not have line management responsibility for and which they are not authorised to do, potentially causing distress to an individual and in breach of the Data Protection Act	Head of HR & OD / Senior HR Partner	Daily	Med (3) u/k	Med (3)	Med (9)	⟺	Reduce the probability: • IAD to review the SyOps for DMS	Limited
INF 0018	Finances	Because EMCHRS-OHU do not share information on new starters' personal requirements, Contact Management is unable to plan for reasonable adjustments to be made, including application for funding to Access to Work, resulting in unnecessary costs and potential disruption to operations	Head of Contact Management / Ch Insp Contact Management	2016	High (4)	Low (2)	Med (8)	NEW	Avoid the risk: • HR to liaise with OHU regarding process to facilitate availability of information *Should this be a HR information asset risk?*	Reasonable

Identifier	Category	Risk description	Information Asset Owner / Delegate	Proximity / Frequency	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 0013	Crime & community safety	Technical failure results in temporary loss of Vision command & control IT system in the Force control room, compromising availability of information that impacts on service levels, management of response to incidents, public safety and reputation	Head of Contact Management / Business Systems Development Manager (CM)	Daily	Low (2)	High (4)	Med (8)	⇔	Reduce the probability: • Force core network replaced on 9 June – should improve resilience of control room ICT Contingency plan: • Established control room business continuity plans • Northern control room provides back-up site for longer-term interruptions	Reasonable
INF 0011	Life and safety	Sensitive personal information of a registered violent or sexual offender is disclosed to an individual or group in order to reduce risk of harm, but outside the scope of the MAPPA Guidance 2012, compromising its confidentiality and putting the offender at risk of harm	Head of Public Protection / Det Insp DPMU	Monthly	Very low (1)	Very high (5)	Low (5)	⇔	Avoid the risk: • Disclosure form to be revised in line with MAPPA Guidance 2012 & formally registered as a Force Form	Reasonable

Identifier	Category	Risk description	Information Asset Owner / Delegate	Proximity / Frequency	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 0012	Compliance	Employees' personal information, stored on the Cyclops IT system hosted by Leicestershire Police, is accessed without authorisation by Leicestershire Police, Derbyshire Constabulary or GSA employees, in breach of the Data Protection Act	Head of HR / Senior HR Manager	Daily	Very low (1)	High (4)	Low (4)	⇔	Reduce the probability: • Set up a data processing agreement with Leicestershire Police & Derbyshire Constabulary • *Is data processing included in the contract with GSA?*	Limited
INF 0014	Compliance	Personal information obtained via CCTV at Force premises is disclosed to an unauthorised person, compromising its confidentiality in breach of the Data Protection Act	Head of Assets / Building Surveyor	Next 12 months	Very low (1)	High (4)	Low (4)	⇔	Reduce the probability: • Policy & disclosure form to be produced to advise & support Assets dept staff in management of CCTV information	Reasonable
INF 0001	Operational efficiency & effectiveness	Audio / video recordings stored on discs / removable media are passed to CPS and then lost within their offices, accidentally compromising availability of evidential information that needs to be re-sent, causing delays to the judicial process & impacting on day to day work of the DIEU	Head of Crime Support / DIEU Manager	Daily	Low (2)	Low (2)	Low (4)	⇔	Reduce the probability: • Staff handbook detailing Force processes now in use • Working group with CPS to address on-going issues	Substantial

Identifier	Category	Risk description	Information Asset Owner / Delegate	Proximity / Frequency	Probability	Impact	Rating	Trend	Response plan	Risk rating confidence
INF 0004	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	Director of Intelligence / DIU Manager	Before Sept 2015	Very low (1)	High (4)	Low (4)	⇔	Reduce the probability: • Temporary storage solution set up by IS (no back-up facility) • Project to relocate DIU to FHQ & utilise back-up capability / IS support (delayed until Sept 2015)	Reasonable

Closed risks

Identifier	Risk description	Reason for closure	Date closed	Closed by
INF 0002	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	Force policy changed to deny access using employees' own devices; Force owned laptops issued to users as required; risk avoided	February 2015	FIAB
INF 0003	With only a short term storage solution in place, equipment failure results in accidental compromise to availability of evidential information contained within the Airwave & telephony archive, impacting on the efficiency and effectiveness of the judicial process	Storage issues resolved to enable retention in line with Force policy; risk reduced to acceptable level	March 2015	IRMG
INF 0015	A complaint is made to the ICO for not completing a Subject Access Request [DPA 6389/14] in accordance with the Data Protection Act, resulting in an enforcement notice; the required HR file is believed to be stored at Iron Mountain in one of approx. 300 un-catalogued boxes	Risk assessed as Low due to no response from holding letters sent; risk accepted	April 2015	IRMG
INF 0010	System security vulnerabilities within Windows XP following expiry of MS support enable an external hacker to deliberately compromise the confidentiality, integrity and / or availability of multiple Force information assets	Windows 7 project completed; risk considered minimal and acceptable	June 2015	IRMG

Identifier	Risk description	Reason for closure	Date closed	Closed by
INF 0009	Continued use of Windows XP results in the national accreditor denying the Force permission to connect to the national Public Services Network (PSN), removing access to valuable information assets which reduces operational efficiency and effectiveness	Windows 7 project completed; risk avoided	June 2015	IRMG
INF 0008	A user who has been inactive for more than 6 months, and therefore should have had their access suspended in accordance with the PNC User Manual, accesses information on the Police National Computer (PNC), compromising its confidentiality	Business objects search now set up & in use by system administrators to manage user access in line with PNC Manual	June 2015	System Administrator / IRMG