National Offender Management Service

Information Risk Management Policy

This instruction applies to:-		Reference:-
NOMS HQ Prisons National Probation Service		**AI 08/2016** **PSI 06/2016** **PI 08/2016**
Issue Date	**Effective Date**	**Expiry Date**
11 May 2016	11 May 2016	N/A
Issued on the authority of	NOMS Agency Board	
For action by	All staff responsible for the development and publication of policy and instructions ☒ NOMS HQ ☒ Public Sector Prisons ☒ Contracted Prisons* ☒ Immigration Removal Centre's (IRCs) ☒ National Probation Service (NPS) ☐ Community Rehabilitation Companies (CRCs) ☐ Other Providers of Probation and Community Services ☒ Governors ☒ Heads of Groups ☒ NOMS Rehabilitation Contract Services Team **** If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***	
Instruction type	***legal compliance***	
For information	All information asset owners, information asset custodians, senior managers, delivery partners and third party suppliers.	
Provide a summary of the policy aim and the reason for its development / revision	This policy is a revision only and has been updated: • To extend the requirement for Information Risk Management to all NOMS, including HQ, Prisons and Probation. • To replace the word Risk Register template with an excel version.	
Contact	Information Management and Security Team Tel: 0300 047 6590 / Email: InformationmgmtSecurity@noms.gsi.gov.uk	
Associated documents	PSI 25/2014 – PI 19/2014 – AI 19/2014 IT Security PSI 24/2014 – PI 18/2014 – AI 18/2014 Information Assurance PSI 44/2014 – PI 61/2014 – AI 28/2014 - The Data Protection Act 1998; The Freedom of Information Act 2000; PSI 35/2014 - PI 28/2014 - Archiving Retention and Disposal PSI 13/2014, AI – 11/2014 NOMS Business Continuity Management Manual PSI 43/2010 AI 24/2010 – Security Vetting	

Replaces the following documents which are hereby cancelled: AI 04/2012 - PSI 16/2012

Audit/monitoring: Mandatory elements of instructions must be subject to management checks (and may be subject to self or peer audit by operational line management/contract managers/HQ managers, as judged to be appropriate by the managers with responsibility for delivery. In addition, NOMS will have a corporate audit programme that will audit against mandatory requirements to an extent and at a frequency determined from time to time through the appropriate governance

Introduces amendments to the following documents: None

Notes: ***All Mandatory Actions throughout this instruction are in italics and must be strictly adhered to.***

CONTENTS

1 Executive summary

Background

1.1 Reliable and accurate information management is critical to proper decision making across the Ministry of Justice (MoJ). Information can take many forms and may or may not have protective markings – from data sets containing personal information through to records of sensitive meetings, policy recommendations, prisoner / offender records, case files, correspondence and historical records.

- Information is the lifeblood of our organisation. It is a critical business asset that NOMS needs to protect and get the most value from to benefit the business.
- The management of information risk should be incorporated into all day-to-day operations. If effectively used it can be a tool for managing information proactively rather than reactively. It will enable NOMS to get the right information to the right people at the right time, and help avoid incidents where data is lost or improperly disclosed.

Desired outcomes

1.2 This policy sets out NOMS commitment to the management of information risk. It also sets out what prison establishments, headquarters groups and National Probation Service (NPS should do to manage information risk. In doing so, this policy supports the NOMS strategic aims and objectives and should enable employees throughout the organisation to identify an acceptable level of risk and, when required, use the correct risk escalation process.

Application

1.3 *Governors, Directors of Contracted Prisons, Heads of Groups, Deputy Directors of Probation, Information Asset Owners and Information Asset Custodians must be familiar with the policy.*

Mandatory actions

1.4 *Governors, Directors of Contracted Prisons, Heads of Groups, Deputy Directors of Probation, and Information Asset Owners must ensure that Senior Management Teams and Information Asset Custodians review and are aware of this policy.*

1.5 *All establishments, headquarters groups, and NPS Divisions must have an Information Risk Register in place that is reviewed on a quarterly basis that is recorded for audit purposes.*

Resource Impact

1.6 Initial completion of the risk register should take a group of senior managers between 1-2 hours, depending on the scale and/or complexity of the prison / HQ group / NPS Division.

1.7 Quarterly reviews should take no longer than 1-2 hours, depending on the number of actions identified, and new risks appended.

(Approved for Publication)

Bryan Clark,
NOMS Senior Information Risk Owner (SIRO)
Director of Digital and Change, NOMS

2. Information Risk Management

2.1 Reliable and accurate information is critical to proper decision making in NOMS. This makes information a vital business asset that we need to protect. Information risk management provides this protection by managing risks to the confidentiality, integrity and availability of information to assist our business to function effectively.

2.2 Confidentiality means ensuring that only authorised people can get to our information

2.3 Integrity means ensuring that it is authentic, accurate and complete

2.4 Availability means that authorised people can access it when they need to, at the right times in the right ways

2.5 Keeping the **right** information for the **right period of time** is also very important and can help ensure we comply with a range of statutory responsibilities (e.g. Freedom of Information Act 2000, Public Records Act 1958 & 1967, Data Protection Act 1998), supply information when it's requested by, for example, high-profile public enquiries, and provide supporting evidence in the event of litigation against NOMS. For guidance refer to PSI 35/2014 – PI 28/2014 Archiving, Retention and Disposal.

Information Asset Owner (IAO)

2.6 *IAOs are responsible for the day to day use of information, which includes who has access to the information and risk management of their information.* They are usually Governing Governors, Heads of Group, and Deputy Directors of Probation, but may be other senior managers such as IT system owners involved in running their relevant business function.

2.7 *IAOs are responsible for making sure their business areas, delivery partners and third party suppliers with whom they work, have in place the arrangements needed to implement and maintain an effective information risk management policy.* The IAO may wish to appoint Information Asset Custodians (IAC) to work on their behalf, taking day to day oversight of assets and reporting back to the IAO on the changes to risks.

2.8 Further information about the role of the IAO and IAC can be found in Annex A of this document and Section 3 of PSI 24/2014 – PI 18/2014 – AI 18/2014 Information Assurance.

Information Risk Register

2.9 *IAOs must review information risks on a quarterly basis as part of the review of the establishment/business group/Division Information Asset Register and, where appropriate, escalate any risks to the Information Management and Security (IMS) Team at InformationmgmtSecurity@noms.gsi.gov.uk or by telephone on 0300 047 6590. As well as existing risks that have already been identified, the review must also consider forthcoming potential changes in services, technology and threats.*

2.10 Guidance on reviewing the Risk Register, and when to escalate, can be found in Annex B.

2.11 The IMS Team will decide whether it is appropriate to escalate any risks to the NOMS Senior Information Risk Owner (SIRO) (Definition in Annex A). *NOMS is required to provide a report on information risk annually as part of a MoJ annual assessment of information risk and the information received from the IAOs forms part of this report. Additionally NOMS is required to provide quarterly risk updates to the MoJ SIRO Board.*

2.12 *The IAO must ensure that any Information and Communications Technology (ICT) systems that hold protectively marked information are accredited according to government standards by a MoJ Accreditor. For further information on the accreditation process or to determine whether the ICT system is an accredited system contact the NOMS IMS Team.*

2.13 Information risk can present a real and current threat to NOMS as an organisation, and the people we work with – staff, contractors, and service users – as such, managing such risks is essential. Disciplinary action will be considered for any member of staff (including contractors, consultants, and suppliers so far as is feasible) who do not follow the mandatory actions set out in this policy, unless prior agreement to do so has been secured from the NOMS Senior Information Risk Owner (SIRO).

3. Compiling and Maintaining an Information Risk Register

3.1 *To provide evidence that the risks in their business area have been identified and that there are plans in place for managing them, the IAO must compile and maintain an Information Risk Register.* A well-organised and easy to understand Risk Register is fundamentally important. The register needs to provide enough information to the IAO to enable them to be able to identify and explain risk management decisions.

3.2 Each prison establishment, headquarters group, and NPS Division should already have an Information Asset Register (IAR) in place, as a Mandatory Action of PSI 24/2014 – PI 18/2014 – AI 18/2014 Information Assurance. The IAR can be used to help to identify the different types of information assets held and provide direction on the risk that a loss / compromise or lack of availability of that asset would have.

The Information Risk Register

3.3 A partially completed risk register template whose content you can adapt to fit your own business area can be found in Annex C. The draft entry has been provided to assist you but you will need to look at the information in each of the columns and consider the extent to which it is valid in your location. The format of the template is fixed.

3.4 *You must include any additional risk descriptions and possible causes with business area specific risks and causes where necessary.*

3.5 *Prison establishments, NPS Divisions and HQ business areas must use the NOMS Information Risk Register template provided, which contains the following information:*

- a description of each risk expressed in terms of the potential or actual compromise associated with the risk and the cause (threat and vulnerability),
- an indication of the Information Assurance (IA) controls already in place to remediate each risk,
- a rating that reflects the likelihood of the risk being realised and is typically expressed in terms of the 'score' assigned by the risk assessment method used,
- a rating that reflects the business impact associated with the threat being realised is typically expressed in terms of the 'score' assigned by the risk assessment process,
- a description of the IA controls that the business group has or plans to implement to further control the risk (together with any additional actions or contingency arrangements that lessen the business impact if the risk is realised),
- a target date for implementing proposed IA controls or other plans to reduce the risk further,
- a target rating that reflects the score following the implementation of the further controls,

3.6 Detailed guidance on completing a risk register can be found in Annex B

3.7 The risk register template in Annex C can also be downloaded in Excel format from the IMS Team's page of the Intranet.

Escalating the Risk

3.8 *If a risk hits a certain 'score' it must be escalated to a specific management level*.

3.9 **NEW NUMBER** – If a risk is given a collective impact / likelihood score of 5 or above, it must be escalated to the IAO (where the IAO has delegated information risk authority to IAC's or other).

3.10 **NEW NUMBER** - If a risk *is given a collective impact/likelihood score of 9 or above, it must be escalated to the NOMS SIRO via the IMS Team. The NOMS IMS team can be contacted on InformationmgmtSecurity@noms.gsi.gov.uk or on 0300 047 6590.*

3.11 It is unlikely that a risk with a score of 15+ will be identified in either prison establishments, headquarters groups, or NPS Divisions that has not already been identified and included in the overall NOMS Information Risk Register. *However any new/existing risks which are identified as having a score of 15 or above must be escalated to the MoJ SIRO Board by the IMS Team.*

3.12 Further guidance on escalating risks to the appropriate level can be found in Annex B

3.13 *The Annual Information and Assurance Compliance Statement required under - PSI 35/2014 - PI 28/2014 - Archiving Retention and Disposal includes a statement giving assurance that your Risk Register is in place. The return of the Compliance Statement must be completed and sent electronically to the NOMS IMS team InformationmgmtSecurity@noms.gsi.gov.uk annually as per specific annual communications.*

4. Business Continuity Planning

4.1 The purpose of business continuity is to create the conditions that ensure a business can continue to operate even after an event that denies it access to its assets and information: this could be a server failure, a power cut, a fire or any other catastrophic event.

4.2 *To ensure business continuity is maintained across NOMS, all prison establishments must have in place a Contingency Plan for the loss of Prison NOMIS, and likewise with NPS Divisions for National Delius. The Governor / Deputy Director / IAO is responsible for contingency plans within their business area and must nominate suitable personnel for undertaking tasks identified in the plan. Whilst the IT service providers will be responsible for managing the resolution of the disruption, it is the responsibility of the IAO to make sure that all staff are aware of the contingency plans and have enough knowledge to implement them.*

4.3 *It is important that IAOs identify their local 'vital records'. These are information assets that are not held on the core networks (Quantum/OMNI) but have been identified as essential for the continuation of NOMS operations if, for example, stand alone IT systems and / or paper records cannot be accessed.*

4.4 *The plan must identify proposals for the recovery of business critical activities promptly and efficiently and include proposals for the protection of local 'vital records' and NOMS information assets.*

4.5 For guidance on putting in place suitable business continuity and contingency plans for ICT systems IAO's may wish to consult with their main IT supplier, and/or the NOMS Accreditor of that system as mentioned in PSI 25/2014 – PI 19/2014 – AI 19/2014 IT Security.

4.6 For staff in headquarters and regional offices PSI 13/2014, AI – 11/2014 NOMS Business Continuity Management Manual provides guidance on business continuity planning.

5. Physical and Personnel Security

5.1 *Physical Security - All managers for prison establishments, NPS Divisions, and headquarters buildings must assess any physical security risks that affect the sites and environments in which ICT-based and paper-based information systems reside. They must ensure that IAOs (and ICT accreditors) are made aware of any assessed risks that affect them.*

5.2 *Personnel security - All staff must have the appropriate level of checking or 'vetting' needed to assure the reliability of each employee (including contractors) according to the sensitivity of the information that the member of staff has regular access to and the business impact that might arise if that employee discloses this information without authority.* Refer to PSI 43/2010 AI 24/2010 – Security Vetting for more information.

6. Delivery Partners and Third Party Suppliers

6.1 *NOMS Delivery Partners and Third Party Suppliers must identify and manage risks to all NOMS information assets that they have access to and/or control of, including escalating them via the necessary channels as outlined in this policy (via the IAO, the IMS Team and NOMS SIRO).*

6.2 *Any significant risks relating to NOMS information must be raised with the relevant point of contact and if required the relevant IAO, as outlined in this policy.*

Roles and Responsibilities

1. MoJ SIRO Board

1.1 SIRO means Senior Information Risk Owner. The Board is composed of all of the MoJ's Business Group SIROs and Executive Agency SIROs. The Board is chaired by the MoJ SIRO.

2. NOMS Senior Information Risk Owner (SIRO)

2.1 The NOMS SIRO has overall responsibility for all NOMS information assets which are held or owned by NOMS. The NOMS SIRO sits on the MoJ SIRO Board and provides assurance that all Information Asset Owners in NOMS are following their responsibilities. The SIRO is familiar with information risks and would lead the NOMS response in the event of a major data incident.

3. Information Asset Owner (IAO)

3.1 The Information Asset Owner is responsible for the creation, use, storage and sharing of the Information Assets for which they have been identified as the owner. *They must understand what information is held, what is added, removed and who has access and why.* They should use their knowledge to address risks to their Information Assets and ensure the Information Assets are fully used within the law and for the public good.

3.2 The Information Asset Owner for each asset (electronic or paper-based and items such as identity cards, DVDs and video tapes) should agree the general protective marking of standard documents/information and the appropriate arrangements to access the information.

3.3 *Information Asset Owners must follow the rules for dealing with information assets laid down by statute (including the Data Protection Act 1998 and the Human Rights Act 1998) as well as the minimum mandatory measures contained within this guidance.* They should also be aware of the overarching obligations imposed by the Official Secrets Acts and the Freedom of Information Act 2000.

3.4 Information Asset Owners are governing Governors, Deputy Directors of Probation or Heads of Function but may be other senior managers involved in running the relevant business area. They are responsible for the day to day use as well as the risk management of their information asset, and supporting the NOMS SIRO in carrying out their duties.

3.5 *Information Asset Owners must escalate substantial risks and issues through the NOMS Information Management and Security Team at InformationmgmtSecurity@noms.gsi.gov.uk or by telephone on 0300 047 6590.* These will be escalated to the NOMS SIRO if they cannot be resolved or guidance provided.

3.6 Detailed guidance for Information Asset Owners can be found in the Information Asset Owner Reference Guidance on the Information Assurance page of the NOMS Intranet, or from the IAO Welcome Pack available from the IMS Team.

3.7 The IAO may wish to appoint Information Asset Custodians to work on their behalf, taking day to day oversight of assets and reporting back to the IAO on the changes to risks. They will also be responsible for reviewing the risk register with the IAO on a quarterly basis.

4. Information Asset Custodians (IAC)

4.1 Information Asset Custodians are involved in the day to day use and management of information assets in a particular area, they will be appointed by the IAO to have responsibility for overseeing and implementing the necessary safeguards to protect the information assets and report back to the IAO on any changes to risks. The IAO will retain the overall responsibility.

4.2 Information Asset Custodians can be assigned where the business function contains a broad range of information assets, or is geographically dispersed. Acceptable uses of the IAC role are:

- Assigned to Head of Functions within Prison establishments (an example where broad range of assets will exist under the control of an IAO)
- Assigned to Operational Heads of LDU Clusters with range of responsibility for particular operational functions e.g. Courts, Victims, MAPPA, or with non-operational functions e.g. IT, Equality, Performance & Quality.
- Assigned to Controllers of Private Prisons (an example where the IAO sits in a NOMS HQ function with responsibility for Controller offices that are geographically dispersed).
- Other managerial roles with a local presence governed by a NOMS HQ Directorate, for example HR, Estates.

5. Local Information Manager (LIM)

5.1 The Local Information Manager (LIM) role is enforced in the policy on Retention, Archiving and Disposal and takes a lead role in specifically the archiving of information, its length of retention, and the destruction of information once it's no longer required. The LIM should be supported by a Deputy.

6. The Information Management and Security (IMS) Team

6.1 The IMS Team is a central function in NOMS HQ. The team aims to provide information risk management to deliver business benefits and efficiency savings, reduce information risk and facilitate compliance with information legislation.

6.2 The team's role is to enable, monitor and develop Information Assurance Maturity and Compliance within NOMS and contracted service providers. The team also owns and maintains the NOMS Information Risk Register and provides written advice to the NOMS SIRO on the security and use of NOMS assets.

Annex B

Information Assurance Risk Management Process

Risk management is an iterative process. It encompasses the following stages: Identification, Assessment, Manage, Monitoring, and when appropriate Escalation.

There are various risk management frameworks and methodologies, relating for example to project management or health & safety, but they all commonly contain these main stages.

A Risk Register that provides enough information to explain risk management decisions will enable the IAO to monitor and manage the risks within their business group.

A partially completed risk register template that you may wish to adopt and amend to fit your business group can be found in Annex C. This draft has been provided to help you to prepare your local document.

In order to complete it you will need to look at the information in each column and consider the extent to which it is true in your location and provide an appropriate risk rating.

You must include any additional risk descriptions with business area specific risks, causes and mitigating actions and also include the possible consequences of the risk being compromised where necessary.

The risk register template in Annex C can also be downloaded in Excel format from the IMS Team's page of the Intranet.

Stage 1 - Risk Identification:

1.1 *Situations where risks must be identified may take many forms, for example:*

- *Preparation to develop a new Information Communication Technology (ICT) based or paper-based information systems,*
- *Regular reviews under 'business as usual' arrangements for maintaining IA compliance, and*
- *Work to address a change of requirement.*

1.2 The starting point in these examples is risk analysis: being clear on what information assets fall within scope of the assessment and the importance of those assets to the business (or the impact of loss of confidentiality, integrity or availability).

1.3 Each prison establishment, business group, and NPS Division should already have an Information Asset Register in place. This can be used to help to identify the different types of information assets held and to provide direction on the risk to the organisation that a loss / compromise of that asset would have. Some examples of information assets are:

- Staff and HR Details
- Official Correspondence
- Prisoner / Offender records and reports
- Financial budgetary information
- Litigation or caseworking files

1.4 Once you have considered the information assets that might be at risk you need to identify the 'risk description' which is the form that the compromise / loss might take. The following suggestions are some of the factors that you might want to consider as 'risk descriptions' when completing your own register. This list is only for guidance and you might identify different or additional descriptions that are more appropriate in your own business area:

- Inappropriate disclosure of personal material
- Theft, loss or unauthorised access to information (paper records should be considered as well as electronic and systems)
- Ineffective or insecure information sharing
- Records retained for the wrong length of time
- Failure to create or locate reliable records as evidence of business decisions and activities
- Poor management of information risk
- Stand alone IT systems that are not supported or accredited

An identified risk that warrants recording in the Risk Register may be very specific to a situation, function, or process. Example risk descriptions may be:

- Sending referral information electronically to X delivery partner is not done so using secure methods
- Mobile working performed by X post, critical to HR processes, is done so using a locally-procured non-accredited IT device.

1.5 Once you have identified the 'risk description', the next step is to identify the organisations, the people, or the events that pose a threat to your information assets. The following are just a few of the possible causes of information loss / compromise but you need to consider which of these are true in your business area and update the Risk Register to reflect this:

- Lack of awareness and training
- Absence of information sharing agreements
- Password sharing
- Documents sent to incorrect address or lost/compromised during transmission
- Dishonesty
- Inappropriate storage
- Records retained unnecessarily result in large volumes of data to be searched.
- Unavailability of business continuity plans

1.6 An important part of the risk identification process for IT systems is through the accreditation process. Further information on this process can be found in PSI 25/2014 AI 19/2014, PI 19/2014 IT Security.

Stage 2 - Assessing the Scale of Risk:

2.1 Assessing a risk involves evaluating two factors, these are:
The Impact to the organisation or persons where the compromise/loss to occur, and

The Likelihood of the risk being realised, taking into account the working environment and past experience.

2.2 The assessment of these factors helps you to decide on the overall severity of each risk, this means that they can be prioritised and resources focused on the most serious.

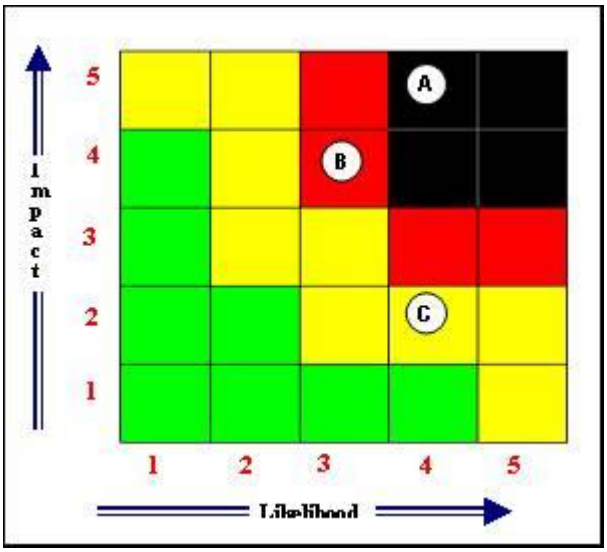
2.3 The table below illustrates what score is attached to each level for both impact and likelihood. Once you have decided on the scores they are multiplied together to give the overall risk score.

2.4 For example:

- A risk is determined to have a 'significant detrimental effect in the long term' would have a score of High (4).
- It is then judged the likelihood of this occurring is unlikely giving a score of Low (2).
- This is multiplied to give a total risk score of 8.
- This score is then used to determine if the risk needs escalating.

Scale	IMPACT	LIKELIHOOD
5 Very High	Prevents achievement of NOMS objectives or has highly damaging impact on NOMS operational effectiveness or reputation.	> 80 % **Almost Certain**
4 High	Significant detrimental effect on achievement of NOMS corporate objectives in the longer term. National media criticism.	51 – 80 % **Probable**
3 Medium	Impacts at local level on elements of efficiency, output and quality which impacts on the outcome of long term NOMS corporate objectives. Potential for negative local media coverage	21 – 50 % **Possible**
2 Low	Impact at local level on short term goals within their objectives without affecting long term achievement of NOMS corporate objectives.	6 – 20 % **Unlikely**
1 Very Low	Minor and containable impact on achievement of local (establishment / business area) objectives.	< 5 % **Very Unlikely**

Risk scores can be shown on a matrix:



Risk **A**: *Very High* Impact (5), and *High* Likelihood (4), giving a score of 20;
Risk **B**: *High* Impact (4), and *Medium* Likelihood (3), giving a score of 12;
Risk **C**: *Low* Impact (2), and *High* Likelihood (4), giving a score of 8.

2.5 The risk scores are used to decide if the level of risk is acceptable or if further action to mitigate is required (e.g. controls, escalation and/or contingency plans), and whether escalation is necessary.

Stage 3 - Managing the risk:

3.1 *There are generally four options that the IAO must consider when deciding how to manage the identified risk.*

3.2 The first one is 'treating the risk' which is done by applying one or more Information Assurance controls to reduce the likelihood of the risk being realised or lessen the impact if the risk is realised. Examples of these controls could be:

- Implementing the mandatory actions in PSI 24/2014 AI 18/2014 PI 18/2014 - Information Assurance
- Implementing the mandatory actions in PSI 35/2014, PI 59/2015 - Archiving Retention and Disposal
- Using the Government Classification Scheme PSI 12/2014 AI 10/2014 PI 04/2014.
- Investigation of incidents and lessons learned
- Training and awareness

3.3 The second option is 'removing the risk', this is done by finding another way to achieve a business objective; for example returning protectively marked documents to the originating department rather than storing them within NOMS.

3.4 Another possible option to consider is 'transferring the risk', for example to a more appropriate function IAO, or by outsourcing services. For the latter example, it is important to recognise that even if it is possible to transfer responsibility for managing a risk to an organisation other than NOMS, the consequences of a risk will rest wherever the business impact associated with it being realised is felt. *The legal basis for sharing information and appropriate contractual provisions and arrangements to ensure compliance with control requirements must be in place.*

3.5 Finally the IAO could decide that 'tolerating the risk' is the most appropriate action. This is usually done where:

- the financial cost of mitigation is too great,
- where the likelihood of the risk being realised is low,
- where the impact on the organisation if the risk is realised is low or else
- where the business benefit is high.

Where a potential risk is 'tolerated', it is more important to have the right reporting channels and monitoring processes, in order to identify if the risk does occur.

Stage 4 – Monitor and Escalate:

4.1 An ongoing programme of monitoring, inspection and testing is required by risk owners which validates and provides evidence that the IA controls used to manage risks remain effective.

4.2 *An annual Information and Assurance Compliance Statement is required under PSI 35/2014 - PI 28/2014 - Archiving Retention and Disposal, the statement must be completed on an annual basis and includes a statement giving assurance that your Risk Register is in place.*

4.3 *In addition to this, the IAO must carry out a quarterly review of the information risks. As well as existing risks that have already been identified, the review must also consider forthcoming potential changes in services, technology and threats. Reviews must be discussed at local SMT level and minuted*. This will be checked as part of the Internal Assurance Audit process.

4.4 *Where the risk relates to ICT-based information systems: Business groups must use Her Majesty's Government's (HMG) accreditation process to assess, treat, validate and verify risk to all ICT-based information systems on which their business operations depend*. For further

information on the accreditation process or to determine whether the ICT system is an accredited system please refer to PSI 25/2014 AI 19/2014, PI 19/2014 – IT Security, or contact the NOMS IMS Team.

4.5 *If a risk hits a certain score it must be escalated to a specific management level. This is set out below;*

- **Very High (I/L 20-25) MOJ Board via the Corporate Risk Register**
- **High (I/L15 - 19) SIRO Board through the NOMS IMS Team**
- **Med (I/L 9 - 14) NOMS SIRO through the NOMS IMS Team**
- **Low (I/L 5 - 8) Information Asset Owner**
- **V. Low (I/L 1 - 4) Can be managed at Business Group level**

4.6 How does it work in practice? The description below illustrates the step by step process.

Where a risk is identified and escalated to the IAO:

- Step 1 (Identification) – A senior manager as an Information Asset Custodian (IAC) for their specific function identifies a risk to information resulting from an established operational process. They arrange for a Risk Register entry by defining the information assets affected, a risk description, and the threat.

- Step 2 (Assessment) - The IAC assesses the risk in terms of Impact and Likelihood. This is achieved using the IAC's detailed knowledge of the information asset, what damage the risk could cause, and the likelihood of that risk taking place. Following the scoring method in this policy, the risk score is 6, which requires escalation to the IAO. So the IAC informs the IAO of the details captured in the Risk Register along with actions that, with the IAO's agreement, the IAC will take to mitigate.

- Step 3 (Manage) – The IAC identifies, plans, and carries out actions to mitigate against the risk. They treat the risk by introducing new controls within their operational processes.

- Step 4 (Monitor) - At the next Senior Management Team (SMT) meeting, Information Assurance is on the agenda, in which the Risk Register is reviewed. For this particular risk entry, the IAC provides an update to the IAO including actions taken, the current risk rating as a result of the action, and recommends that the item is closed. The IAO is in agreement. Review of the Risk Register along with other points relating to IA is minuted.

Where the risk needs escalation beyond the IAO:

- Step 1 (Identification and Assessment) – The IAO identifies and defines a risk to information. After assessment, the collective impact / likelihood score is greater than 9, which as per policy, needs escalation to the NOMS IMS Team for the attention of the SIRO.

- Step 2 (Manage) – The IMS Team informs the NOMS SIRO of the escalated risk through the NOMS Risk Register along with supporting advice. The SIRO reviews the situation and makes a decision on mitigations and actions, along with agreeing whether the risk scoring is appropriate, target dates, and risk owner.

- Step 3 (Monitor) – The SIRO asks for the IAO to be the designated risk owner to oversee the required activities in order to reduce the risk profile. Monthly updates are provided to the SIRO in order to monitor developments.

4.7 It is worth remembering that when risks are escalated and assessed at the next management level, that the level of impact is likely to be moderated as objectives and responsibilities widen. Therefore, a risk identified at local level may often (although not in all cases) have a lower impact upon the overall NOMS business objective.

Annex C

Information Risk Register Template

The Information Risk Register Template can be found via the following link - https://www.gov.uk/government/publications/information-risk-management-psi-062016-pi-082016