April 2020

Contents

1 Overview

Organisations are increasingly reliant on IT systems to deliver a wide range of business functions and services and typically have an extensive IT estate. This heavy reliance on IT, coupled with the ever-increasing and evolving threat landscape that looks to compromise IT systems, places Organisations at significant risk of compromise from cyber-attack. IL7 handles, processes and stores substantial quantities of sensitive information, and in the event of a compromise this could have an impact on national security and public safety and also cause financial (e.g. from ICO fines) and reputational damage to the department.

To manage the risk posed, it is necessary for IL7 to define and implement a robust information and cyber risk management framework to identify, assess and ultimately manage the risk to its information, systems and services. It is essential that IL7's information and cyber risk framework is integrated and aligned to IL7's general risk management processes to ensure a holistic and effective approach to risk management within the organisation. The framework for managing information and cyber risk should be communicated throughout IL7, and make clear that the management of information and cyber risk is the responsibility of the whole organisation and all its staff, not just IT or security functions.

1.1 Purpose

This policy sets out the requirements by which IL7 shall develop and implement a robust information and cyber risk management framework.

1.2 Scope

The scope of this guideline covers what IL7 should do to manage information and cyber risks across the organisation. It should be considered in conjunction with the Cyber Organisation and Governance and Cyber Assurance policies.

1.3 Applicability

This policy applies to all IT systems and services that are owned or managed by IL7, or store or process IL7 information. It should be followed by all IL7 staff, third parties and service providers that have responsibilities to manage or use these systems or services, including arm's length bodies.

2 Cyber Risk Management Policy

2.1 Policy and Controls

This policy is written to ensure that the outcomes of the following Cyber Security Principles are met;

- SP01 Governance and Risk Management (Ref [1])

This policy is one of several that are required to support principles above.

This policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 [2]:

RA-1	Risk Assessment Policy and Procedures
RA-3	Risk Assessment
RA-4	Risk Assessment Update
PM-2	Information Security Program Roles
PM-9	Risk Management Strategy

3 Cyber and Information Risk Management Framework Requirements

The CISO shall ensure that:

Policy ID	Policy Requirement
1.1.1	An information and cyber risk management framework, supported by policy and processes, is developed, implemented and maintained that addresses organisational, business and system level cyber risk, aligned to wider departmental risk policy [NIST PM-9].
1.1.2	The information and cyber risk management framework is reviewed and updated, at least annually and whenever there is a major change to wider departmental risk management policy [NIST PM-9].
1.1.3	Risk management activities shall be embedded into decision making processes at all levels and across all functions of the department.
1.1.4	A cyber risk assessment process is developed, maintained and implemented to ensure consistent and appropriate risk management across the department [NIST RA-1].
1.1.5	The cyber risk assessment process shall enable appropriate methodologies to be adopted, in accordance with NCSC guidance, provided they meet the policy requirements.
1.1.6	Robust and proportionate risk assessment and management activities shall be carried out, aligned to recognised security and risk management frameworks (e.g. ISO27005, NIST SP-800 series).
1.1.7	Cyber risk assessments and risk management activities conducted within the department shall consider the latest threat intelligence from both internal and external sources and vulnerability information.
1.1.8	A comprehensive understanding of the threat and vulnerability landscape is developed by gathering and analysing threat intelligence, through the use of credible and reliable information sources (e.g. NCSC and CiSP), monitoring and active cyber defence activities.
1.1.9	Continual activities are undertaken to keep the understanding of the threat and vulnerability landscape up to date.

Policy ID	Policy Requirement
1.1.10	A routine risk reporting cycle is in place for risk escalation from the business up to ExCo, aligned with existing IL7 risk reporting and the Cyber Organisation and Governance Policy (Ref [4]).
1.1.11	A risk dashboard is developed and updated at least quarterly, identifying strategic information and cyber risk across the department.
1.1.12	Information and cyber security risks are reported in a defined common format, which shall be consistent with wider departmental risk processes.
1.1.13	Thresholds for the reporting and escalation of information and cyber security risk shall be defined, in accordance with the departmental risk appetite.

4 Risk Executive Cyber and Information Risk Management Requirements

The Risk Executive shall:

Policy ID	Policy Requirement
1.1.14	Monitor and analyse risk from an organisation-wide perspective and ensure the management of risk is consistent across the department [NIST PM-2].
1.1.15	Own information and cyber security risk across the department, in accordance with the Cyber Organisation and Governance Policy (Ref [4]).
1.1.16	Advise ExCo on strategic information and cyber security risks and issues and related matters, escalating risks above the departmental risk appetite as appropriate.
1.1.17	Provide the focal point for all information and cyber risks that have been escalated by the business through directorate-specific governance channels.
1.1.18	Make information and cyber risk decisions at the departmental level, in accordance with the departmental risk appetite.
1.1.19	Provide assurance that the department's approach to information and cyber risk management is fully integrated and coordinated with existing risk management policy, process, and governance.

5 Directorate Cyber and Information Risk Management Requirements

Directorates shall ensure that:

Policy ID	Policy Requirement
1.1.20	All significant information and cyber risks to the department's information assets and IT systems are identified, monitored and managed.
1.1.21	The cyber risk appetite is defined, documented and published in accordance with the Cyber Organisation and Governance Policy (Ref [4]) and GRA Risk Appetite Setting Process (Ref [5]), and used to inform risk management activities.
1.1.22	Information and cyber risk assessments are conducted for their information systems and services in line with the GRA Cyber and Information Risk Assessment Process (Ref [6]). [NIST RA-1].
1.1.23	Information and cyber risk assessments are documented, maintained, communicated as appropriate, and reviewed and updated throughout the lifetime of a product, system or service in line with the GRA Cyber and Information Risk Assessment Process (Ref [6]). [NIST RA-3, RA-4]
1.1.24	Information and cyber risk assessments enable the monitoring, reporting management of information and cyber risks, establish security requirements, inform the selection of controls, support and maintain authorisation for operation, manage change, respond to the evolving threat and vulnerability landscape and inform continual improvements to the cyber posture. See Cyber Assurance Policy (Ref [7]), GRA Cyber and Information Risk Assessment Process (Ref [6]), Cyber and Information Risk Assurance Process (Ref [8]), Controls Section and Implementation Process (Ref [9]), Control Assessment and Monitoring Process (Ref [10]) and Threat and Vulnerability Management Process (Ref [11]).[NIST RA-1].
1.1.25	Information and cyber risk assessments identify the likelihood and impact of harm, covering unauthorised access, use, disclosure, disruption, modification or destruction of IT systems and services, or any information they process, store or transmit in line with the GRA Cyber and Information Risk Assessment Process (Ref [6]). [NIST RA-3].

Policy ID	Policy Requirement
1.1.26	Information and cyber risk assessments undertaken for systems and services shall identify a proportionate set of security controls linked to each risk, in accordance with the GRA Controls Selection and Implementation Process (Ref [9]).
1.1.27	Information and cyber risk management activities are linked to strategic business objectives.
1.1.28	All identified information and cyber risks shall have a risk owner, who is responsible for the monitoring and management of the risk.
1.1.29	Proportionate and appropriate mechanisms are implemented to manage identified information and cyber risks in accordance with the departmental risk appetite [NIST RA-3].
1.1.30	Cyber risk management activities include the ongoing monitoring and assessment of the effectiveness of the implemented security controls and their impact on the residual risks, in accordance with the GRA Controls Assessment and Monitoring Process (Ref [10]).
1.1.31	Information and cyber risk management decisions are documented in accordance with departmental policy and process [NIST RA-3].
1.1.32	Directorates follow the risk management and assurance processes defined by the CISO, in accordance with this policy and the Cyber Assurance Policy (Ref [7]).
1.1.33	Clear lines of escalation are established and documented for risks that exceed the defined risk thresholds in line with the GRA Risk Reporting and Escalation Process (Ref [12]).
1.1.34	Identified information and cyber security risks are reported and escalated when above the defined thresholds defined in accordance with the departmental risk appetite.

6 Exemptions, Exceptions and Breaches

6.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, please refer to the exemptions and exceptions policy (Ref [13])

6.2 Breach of Policy

IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in IL7 Disciplinary Procedure.

Breaches of this Policy by a third party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third party service provider and/or the cancellation of any contract(s) between IL7 and the third party service provider.

IL7 will refer any use of its IT resources for illegal activities to the Police.