April 2020

Contents

1 Overview

IL7 relies heavily on the use of information systems to conduct its business. This includesthe provision of critical national infrastructure, law enforcement and high-profile citizen-facing services. The systems hold and process substantial quantities of sensitive data, including information relating to national security and citizens personal data.

Information systems contain vulnerabilities that can be exploited to enable unauthorised access, modification or deletion of the information, or to deny access to the information or service. There are a number of motivated individuals and groups with a desire to attack these systems, including criminals, foreign governments and disgruntled employees. A compromise in the confidentiality, integrity or availability of these business services, information systems or the data held within them can have a detrimental impact on the United Kingdom, affecting the operation of its borders and the safety and livelihoods of UK citizens.

Cyber and information risk assurance activities establish confidence in the security of information systems and verify that the residual risks are in accordance with the organisational risk appetite. They define and assure the security measures in place, ensuring that these are effective through the creation and analysis of evidence that demonstrates that the required governance, standards, policies, process and procedures are in place. It is therefore essential that IL7 develops and implements a cyber assurance framework to provide confidence that its information, systems and services are secured at a level that is commensurate with its risk appetite and classification.

1.1 Purpose

This policy sets out the requirements by which IL7 shall develop and implement a cyber assurance framework to ensure that it not only protects its information and its systems, but also has the required confidence that the measures in place are effective.

1.2 Scope

The scope of this policy covers what IL7 will do to provide assurance that information and cyber risks across the organisation are being managed in accordance with the departmental risk appetite. It should be considered in conjunction with the Cyber Organisation and Governance and Cyber Risk Management policies.

1.3 Applicability

This policy applies to all IL7 staff, third party providers and Arms-Length Bodies (ALBs) developing, procuring or operating IT products, systems and services that are owned or managed by IL7, or store or process IL7 information.

2 Cyber Assurance Policy

The following requirements relating to cyber assurance will be adhered to at all times to ensure the protection of IL7 information technology resources.

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])
- SP08 Validation, Confidence and Assurance (Ref [2])

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 [3]:

CA-1	Assessment, Authorization and Monitoring
CA-2	Assessments
CA-5	Plan of Action and Milestones
CA-6	Authorization
PL-2	System Security Plan
PL-6	Security-related Activity Planning
PM-1	Information Security Program Plan
PM-3	Information Security Resources
PM-4	Plan of Action and Milestone Process
PM-10	Security Authorization Process
PM-14	Testing, Training and Monitoring

3 Cyber Assurance Framework Requirements

In establishing the cyber assurance framework, the CISO shall ensure that:

Policy ID	Policy Requirement
1.1.1	A cyber and information security risk assurance framework is developed and implemented, in accordance with the Cyber Organisation and Governance Policy (Ref [4]), that is consistent with the department's 'three lines of defence' assurance model and integrated with IL7 Assurance Framework.
1.1.2	Directorates are made aware of, and monitored to ensure that they carry out, their first-line-of-defence responsibilities to design and operate their information systems securely and to document the evidence that it is secure.
1.1.3	A central assurance process is documented, communicated and implemented consistently across IL7 directorates to provide an independent, centralised, second-line-of-defence risk assurance that departmental systems meet their cyber and information security requirements, are coherent with the departmental enterprise security architecture, and that the associated risks to that system are understood and accepted by the business in accordance with the risk appetite [NIST CA-6, PM-10].
1.1.4	A senior IL7 employee, at Director level or higher, authorises system or service operation, prior to providing live service or storing or processing live data or personal information [NIST CA-6].
1.1.5	A process is documented, communicated and implemented across the department to monitor and assess security controls, by analysing test results and conducting reviews and audits to assess effectiveness and compliance with policy. [NIST CA-1]
1.1.6	Cyber and information security assurance activities are conducted across the department's supply chain.

4 Cyber Assurance Implementation Requirements

In implementing the cyber assurance framework, CISO shall ensure that:

Policy ID	Policy Requirement
1.1.7	The GRA Secure By Design process (Ref [5]) is monitored and implemented across the department.
1.1.8	Security architectures and designs are assured in accordance with the departmental enterprise security architecture and approved design patterns.
1.1.9	The GRA Cyber and Information Risk Assurance (Ref [6]) and GRA Controls Assessment and Monitoring (Ref [7]) processes are monitored and implemented across the department.
1.1.10	The system or service Risk Statement is signed off by a IL7 employed[1] Risk Assurer, along with the Senior Responsible Owner (SRO) [NIST CA-6].
1.1.11	If agreement in 5.3.4 cannot be reached, risks are escalated through to the CISO and ultimately ExCo through defined cyber governance channels in accordance with the Cyber Organisation and Governance Policy (Ref [4]). [NIST CA-6, PM-10].
1.1.12	All cyber assurance activities and outputs shall be documented. The documentation shall include a single document that provides a concise overview of the security controls, risks and assurance activities associated with a solution (system or service), with explicit reference to further documentation that provides a full description in order to provide a full record of evidence to justify risk decisions. [NIST PL-2, PL-6].
1.1.13	Directorates use a standard template to develop information and cyber security assurance documentation for products, systems and services, to enable consistency for assurance activities and outputs across the department [NIST PL-2].
1.1.14	Actions and milestones for Directorates to remediate residual risks or policy non-compliance are monitored and carried out. [NIST PM-4].
1.1.15	Common controls that are relied on by information systems and services developed across the business are identified, documented and assured [NIST PM-1].

[1] In the event that the Risk Assurer is a contractor, it will be signed off by an appropriate civil servant in the line management chain, following the recommendation(s) and guidance from the Risk Assurer.

Policy ID	Policy Requirement
1.1.16	An inventory of all cyber assurance documentation is maintained, to provide an assurance record that justifies risk management decisions, to be used in the event of any subsequent breach.

5 Directorate Assurance Requirements

Directorates shall ensure that:

Policy ID	Policy Requirement
1.1.17	They engage with the Governance Risk and Assurance (GRA) function at the start of any activity to procure, develop or modify any information product, system or service.
1.1.18	The GRA Cyber Assurance Processes (Refs [6], [8], [9], [7] and [10]) are followed for all information systems and services.
1.1.19	All activities to procure, develop or modify an information product, system or service are undertaken in compliance with IL7 Cyber Security Policy.
1.1.20	All products, systems and services follow the GRA Secure By Design process (Ref [5]) to ensure that information and cyber security is considered throughout their lifecycle.
1.1.21	Products, systems and services are developed in accordance with the departmental enterprise security architecture and using approved security design patterns and products where appropriate.
1.1.22	A senior IL7 employee, at Director level or higher, authorises system operation prior to providing live services or using live data or personal information, through sign-off of the Risk Statement, in accordance with the risk appetite and the GRA Cyber and Information Risk Assurance process (Ref [6]). [NIST CA-6].
1.1.23	Risk Statements authorising any system providing live services or using live data or personal information must be signed-off by a GRA Risk Assurer in addition to the sign off provided in 1.1.22.
1.1.24	Plans are developed, documented and implemented to monitor and assess security controls throughout the product, system or service lifecycle, in accordance with the GRA Controls Assessment and Monitoring Process (Ref [7]). [NIST CA-2].
1.1.25	Accurate and up-to-date risk assessment and assurance information is made available in a timely fashion to support the GRA assurance activities, in accordance with the GRA Cyber and Information Risk Assurance process (Ref [6]).
1.1.26	Information and cyber security assurance documentation is developed and maintained throughout the product, system and service lifecycle, using GRA defined templates as required. [NIST PL-2].

Policy ID	Policy Requirement
1.1.27	Directorates will ensure that sufficient budget is allocated in system and service acquisition for specialist expertise to ensure the demonstrable security of the solution. [NIST PM-3].
1.1.28	Where information and cyber security assurance activities identify residual risks or policy non-compliance, a plan containing actions and milestones will be developed and implemented to undertake the necessary remediation activities [NIST CA-5].
1.1.29	They liaise with the department's Cyber Security Operations Centre at the start of the lifecycle and agree and implement an appropriate onboarding plan.
1.1.30	Cyber security testing and monitoring activities are conducted in accordance with the Protective Monitoring (Ref [11]) and Security Testing Policies (Ref [12]), and with the GRA Secure By Design (Ref [5]), GRA Controls Assessment and Monitoring (Ref [7]) and GRA Cyber Resilience Testing (Ref [13]) processes. [NIST PM-14].
1.1.31	Actions and milestones to remediate residual risks or policy non-compliance are identified, documented, carried out and monitored [NIST PM-4].
1.1.32	System security maintenance activities are in place to achieve assurance prior to go-live, including Asset Management, Change Management and Incident Management. See Operations Security Policy (Ref [14]).

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 [15])

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.