Intercept and Escort Craft Project

Security Risk Appetite Statement

Version 1.1
23/02/2022

https://modgovuk.sharepoint.com/teams/1329/03Engineering/IEC Supporting Documentation/IEC - Risk Appetite Statement (REDACTED).docx

Authorisation and Approvals

Prepared by:	[redacted]	
Approved by:	[redacted]	
Authorised for issue by:	[redacted]	

Distribution List

Issued to:	Role

Version Control

Date Issued	Version	Author	Reason for Change
Nov 2020	1.0	[redacted]	
Feb 2022	1.1	[redacted]	Reviewed and Updated for ITN

References

Table of Contents

Navy Command Security Risk Owner's Appetite and Delegation

1. Security classification applied to assets provides for a baseline set of personnel (vetting), physical and information security controls, set out in the Defence Manual of Security, Resilience and Business Continuity (interpreted for the maritime environment through Navy Command Security Regulations) that offer an appropriate level of protection against a typical threat profile. The identified controls are cumulative - minimum measures for each classification provides the baseline for higher levels. They are intended to help Commanders and security staff determine appropriate security measures for the protection of infrastructure, ICT systems / services, and other assets at each level of the classification system.

They must be read in conjunction with the detailed policy, guidance and structured risk assessment methodologies set out in HMG and MOD guidance[1]. The indicative controls tables must be used as the basis for local security instructions and processes.

Some particularly sensitive information will attract additional markings to denote the need for further controls, particularly in respect of sharing. The impact of compromise of this information may be higher, but this does not imply that it will necessarily be subject to the threat model applicable to higher tiers.

Such information can be managed at the same classification level, but with a more prescriptive information handling model, potentially supported by extra procedural or technical controls to reinforce the need-to-know. The aim of additional technical controls is to manage the information characteristics that attract the additional marking for example enforcing access control, or technically limiting the number of records a user can view. These controls will be data and system dependent.

The use of additional control/handling measures has to remain a matter of judgement by the Information Asset Owner (IAO) or Senior Information Owner (SIO) of the information concerned. They are best placed to make an informed judgement on the balance between the increased assurance provided by control measures and the negative impact that the latter may have on timely and efficient delivery of business.

Care should be taken not to apply expensive security controls to information that is for public release, information on display, training materials (e.g. content of general courses), information already published by government, partner nations, or otherwise available such as in the Defence press and where corroborating the publicly available information is not an issue.

Where any security functionality or product is relied upon, there must be confidence that those products or functions are effective and are providing the protection that is expected of them. Within Navy Command the Principal Security Advisor conducts independent security assurance, on behalf of the Senior Security Risk Coordinator (SSRC), 2SL/DCNS, to ensure that products and functions are effective and proportionate to the classification of the assets and information they are used to protect.

<u>The OFFICIAL Domain</u>

The typical threat profile for the OFFICIAL classification is broadly similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend UK Government data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups.

[1] This includes the CESG IA Portfolio, CPNI guidance, JSP 440 CIS/ICT policy, JSP 604 and JSP 457.

My risk appetite in regard to information and assets within the OFFICIAL domain is Open[2].

I will:

Tolerate a level of loss or compromise of information provided steps have been taken to limit the volume and sensitivity.

Accept that there are times when the availability of information at a particular time/place is more important than limiting sharing to guarantee confidentiality.

Accept the risks to information associated with staff conducting some work using personal ICT provided that the risk to core information systems is not increased.

Accept that information systems and applications designed for OFFICIAL-SENSITIVE information are suitable for the storage and transmission of legacy RESTRICTED information.

I will not tolerate:

Widespread compromise or disruption of information systems.

Non-compliance with applicable legal, regulatory and international obligations.

Additional risks to assets or information owned by other organisations (e.g. OGD, NATO, foreign governments) that has been entrusted to MOD.

Compromise or loss of integrity of information in bulk or aggregated data sets.

Compromise or loss of integrity of assets or information that has serious impact on the effectiveness of current or future capability, prejudice investigations, operations, commercial arrangements or sensitive personal information.

Limitations on business effectiveness due to over-classification or due to a failure to declassify information after it is no longer sensitive.

A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or inappropriately disclosed. This subset of information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the 'need to know' principle or provide assurance that the information is under control.

IAO/SIOs are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate.

Personal Data

My risk appetite in this area is Minimalist[3]. I view the loss of control or breaches involving personal information as gross negligence.

[2] Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.).

[3] Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.

Commanders, IAO/SIOs are to ensure that they fulfil their obligations under the Data Protection Act 1998 (DPA 98).

Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Items Attractive to Criminal and Terrorist Organisations (ACTO)

ACTO items are those considered to be of immediate value to a criminal or terrorist. These items are split into 2 categories; Category 1 items are Arms, Ammunition and Explosives (AA&E) which present an immediate danger to Defence personnel or the public and Category 2, which are considered as ACTO but are not AA&E.

Recent serious incidents have brought the MOD's ability to safeguard items ACTO into sharp focus.

My risk appetite toward ACTO is Cautious[4].

Commanders and Asset Owners must:

Educate personnel about the importance of full and proper control of ACTO items.

Adopt a 'zero tolerance' approach with respect to Class 1 ACTO losses..

Have in place a regime of checks and audits, sufficiently frequent, independent and authoritative enough to deter and detect irregularities in the accounting of AA&E and ACTO.

Security Risk and Issue Management

In carefully controlled circumstances it may be appropriate to risk manage non-compliance with the baseline controls in order to capitalise on immediate business and/or operational benefits. This must be done through the Security Risk and Issue Management Framework processes detailed in Navy Command Security Regulations[5].

Organisations are required to assess the potential impact to the business in the event that specific risks are realised. This assessment should form part of a comprehensive risk assessment which considers Confidentiality, Integrity and Availability of information and assets independently. Classification only addresses the Confidentiality aspect of loss or compromise.

[4] Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward.

[5] For example: ACP 121 Classified Messages Transmitted in Plain Language (CLEAR).

There will be cases where information will be marked under GSC but there is a valid business reason why some of the standard security controls cannot be applied. Commanders, IAO/SIOs should assess risks involved in deviating from the baseline controls and ensure they are formally accepted at the correct level. Clear instructions must be provided to ensure that individuals understand the procedures and the limitations on which information sets a variation in controls applies to.

Security risks are to be managed in accordance with Navy Command Security Regulations. Risk assessed as scoring above 10 within the Security Risk Management (SRM) Framework is to be registered on the Command Risk Management application (Active Risk Manager – ARM). Risk scoring between 11 and 13 is to be managed at 1* level within the relevant Chain Of Command. Risk scoring above 13 is to be managed at 2* level within the relevant Chain Of Command.