Leaflet 5C

Building Cyber Secure by Design Capabilities

Contents

Scope

1. This policy applies to all Ministry of Defence (MOD) personnel involved in the definition, acquisition, development, maintenance, and disposal of information-based capabilities for the MOD. This includes but is not limited to networks, applications, services, information technology, operational technology, platforms and weapons systems. Further guidance can be found on the Secure By Design Portal.

2. The MOD defines Secure by Design as:

> "An approach that enables a culture of proactive risk management and appropriate security consideration throughout a capabilities' lifecycle by connecting cyber security principles, roles, processes, tools and techniques to achieve secure systems."

3. This policy outlines the MOD Secure by Design Principles and is informed by industry good practice from the National Cyber Security Centre's (NCSC) Secure Design Principles, three lines of defence security assurance model and National Institute of Standards & Technology (NIST) Cyber Security Framework.

4. At present MOD is in a transition period from accreditation to the Secure by Design approach. All projects starting now should follow the Secure by Design approach outlined in this document; those already in progress should continue to follow the accreditation process (see Annex A). Over time these ongoing projects will transition to Secure by Design. Note that the principles of Secure by Design apply equally to the process leading to accreditation. Delivery Teams currently undergoing accreditation should conduct a review of their activities against this policy and address gaps as appropriate and as advised by their Cyber Security Assessor.

5. The Secure by Design Principles are:

a. **Principle 1: Understand and Define Context** – Understand the capability's cyber security context and how it will use and manage MOD data while achieving its primary business/operational outcome(s).

b. **Principle 2: Plan the Security Activities** – Establish security workstream of the capability, perform initial planning including assessment of cyber threat and potential risks while defining clear security requirements, validation and verification.

c. **Principle 3: Implement Continuous Risk Management** – Embed cyber security risk management into existing programme governance as a continuous process.

d. **Principle 4: Define Security Controls** – Define, architect and implement security control requirements to address risks identified. Reuse existing services and patterns where they exist.

e. **Principle 5: Engage and Manage the Supply Chain** – Understand the supply chain role and risks posed, including how to ensure they meet their responsibilities and implement good security.

f. **Principle 6: Assure, Verify and Test** – Work with security experts to gain security assurance, test and validate throughout the capability's lifecycle.

g. **Principle 7: Enable Through Life Management** – Ensure continuous security monitoring and improvements, including ongoing assurance requirements are enabled, met and disposed.

Introduction

6. This policy sets out the requirements to build cyber security controls into MOD capabilities, systems and data. This policy enables a culture of proactive risk management and security consideration throughout a capability's lifecycle by using cyber security principles, roles, processes, tools and techniques to secure systems and data.

7. By being 'Secure by Design' Defence will ensure it is better protected from the very real cyber threat posed by our adversaries. The threat ranges from low level hackers, to organised crime and ultimately to nation state adversaries. The impact of a cyber-attack could be reputation damage, information loss, disruption to our operations or ultimately to destruction of capability including loss of life.

8. In order to deliver the Defence Board's objective of being cyber resilient while delivering the Defence Tasks[1] it is essential that all our capabilities sufficiently address the risks and therefore controls to ensure security are 'baked in' from inception and applied throughout its lifecycle.

9. This policy sets the mandatory requirements that must be applied to ensure Secure by Design is adopted throughout the capability lifecycle. Guidance on implementing this policy can be found on the Secure By Design Portal.

10. Yellow boxes in this document indicate mandatory requirements. Supplementary information for these can be found in the supporting text.

Roles and Responsibilities

11. There are specific roles and responsibilities outlined throughout the policy. These roles are:

a. **Capability Sponsors** are responsible for the sponsorship of the capability, its requirement development, concept of operation and ensuring the capability can address the risks in-service.

b. **Senior Responsible Owners (SROs)** are accountable for the delivery of cyber secure outcomes throughout the capability lifecycle.

c. **Delivery Team Leaders** are responsible for the development and delivery of capabilities.

d. **Capability Owners** are the in-service owners of the capability. Responsible for ensuring the capability's ability to protect relevant MOD data throughout its lifecycle.

e. **Commercial Officers** are responsible for the implementation of contract terms and conditions in the MOD.

[1] Defence Tasks: How Defence Works, V4.2, December 2015, Para 83, Pg 24

f. **Delivery Team Security Leads**[2] are the individuals within the Delivery Team responsible for the overall design and implementation of security controls to mitigate the risks identified. They are the security SME on the Delivery Team.

g. **Cyber Security Assessor**[3] is responsible for second line assessment of Delivery Teams adherence to Secure by Design and relevant risk and security policies and standards. They coordinate between Delivery Teams dealing with similar security challenges to optimise solutions and minimise duplication of effort. They are responsible for consistent and coherent advice and support to relevant capabilities.

Governance

Policy ref: 5C-1

The Capability Sponsor must ensure a Senior Responsible Owner (SRO) is appointed to the project from the outset with the necessary skills and experience to fulfil the role.

The SRO must ensure:

a. All decisions regarding the capability's development and use are made in the context of the risk facing the MOD's data and capabilities, and its resultant impact should it be realised. This must include the security risk from supplier activities and the contractual arrangements;

b. A capability cyber risk appetite is defined and published for the Delivery Team before a Strategic Outline Case (SOC) is submitted; and

c. Delivery Teams are following the Secure by Design policy, or that accreditation activities are completed.

12. For capabilities planning security activities, this policy must be applied.

Policy ref: 5C-2

Capability Sponsor must ensure business cases, and where relevant, Joint Requirement Oversight Committee (JROC) submissions, adequately address security requirements. These must be funded and actioned through the capability's lifecycle.

Understand and Define the Context (Principle 1)

13. Understanding the cyber security context of a capability as early as possible in the capability lifecycle will ensure that Capability Sponsors, SROs and Delivery Teams can identify the cyber security activities required to deliver successful outcomes. This drives future planning, resourcing and costing accuracy.

[2] Previously known as the Security Assurance Co-ordinator (SAC)
[3] Previously known as the CyDR SACs and Accreditors and TLB Accreditor roles.

Policy ref: 5C-3

Capability Sponsors must have a clearly documented context, purpose and mode of operation for the capability. This must be handed over to the Delivery Team Leader for further development and maintenance. This should include:

a. Capability's use;

b. The risk appetite;

c. High level risks;

d. Who will operate the capability and the support requirements;

e. Data access, storage and processing requirements;

f. The role of suppliers; and

g. The capability's end-to-end operation and interdependencies.

Initial Cyber Security Risk Assessment

Policy ref: 5C-4

Capability Sponsors must ensure an initial cyber security risk assessment is completed and documented accordingly. This risk assessment must be used by the Delivery Team Leader to plan the security activities.

Define the Risk Appetite

Policy ref: 5C-5

The SRO must ensure that a capability risk appetite is defined and published, derived from the CyDR and FLC/TLB/EO Risk Appetite Statements as a minimum threshold.

14. The capability risk appetite may be lower than the FLC/TLB/EO risk appetite but must not be higher.

Capability Registration

Policy ref: 5C-6

Delivery Teams Security Leads must register their capability with Cyber Defence & Risk (CyDR) by recording the capability on the CyDR provided security support tool.

Plan the Security Activities (Principle 2)

15. The planning Principle is focused on establishing the security activities throughout a capability's lifecycle.

Policy ref: 5C-7

Delivery Team Leaders must:

a. Appoint a Delivery Team Security Lead who is suitably qualified and experienced (SQEP).

b. If needed establish a wider security team to provide advice and support. This team must be appropriately SQEP;

c. Establish security activities, including the assurance and testing approaches;

d. Establish a continuous risk assessment approach throughout the lifecycle;

e. Identify good practice controls, architecture and design;

f. Engage with key stakeholders to ensure security outcomes are understood and appropriately implemented throughout the lifecycle;

g. Embed security into governance, funding, delivery and engineering practices; and

h. Ensure the handover from Delivery Team to service management factors in the cost of maintaining security through life.

Security Approach

Policy ref: 5C-8

Delivery Team Security Leads must define the security approach, including the selection of a suitable risk assessment method and the identification of a control framework. They must ensure stakeholders understand their role in maintaining the security posture.

16. Delivery Team Security Leads should select a risk method that is adequate for the complexity and risk facing the capability. Security risk must be translated into appropriate language to allow the business to make an informed decision and must be recorded in the capability's risk register.

17. A focused threat assessment may be required to develop the risks. This should be informed by Defence Intelligence threat assessments.

18. Delivery Team Security Leads should select relevant security control frameworks, e.g. NIST, based on the scope and breadth of the capability. This should be in terms of the

technology it utilises, the process it requires and the culture and behaviours needed to support it.

Policy ref: 5C-9

Delivery Team Leaders must document the security approach in a Security Definition and Management Document (SDMD), see Annex B. This document must be maintained during the life of the capability and transferred to the Capability Owner prior to the capability entering service.

Implement Continuous Risk Management (Principle 3)

19. Cyber security risk management is the mechanism used for risk decisions to be taken and for the SRO and Delivery Team to understand what risks need to be addressed and managed.

Policy ref: 5C-10

SROs must ensure that cyber risks are actively managed throughout the capability lifecycle to ensure delivery is within defined MOD risk appetite, capability delivery risk management and underpinned by JSP892 (Risk Management).

20. Risk analysis should be continuous throughout the capability lifecycle, this may be assured by specialist cyber security teams through routine assessment.

Policy ref: 5C-11

Delivery Team Leaders must ensure that cyber risk assessments are carried out and documented in a risk register and regularly reviewed. They should consider the capability's interaction with other capabilities.

21. The risk register must:

a. Be created, maintained and managed throughout the capability's lifecycle;

b. Include all controls used to mitigate risks;

c. Indicate a clear accountable owner for all risks; and

d. Identify the risk to be transferred and managed as the capability goes into service.

22. To provide oversight, guidance, and analysis across multiple capabilities and allow for MOD to understand systemic risk. The Risk Register must be made available to specialist cyber security teams, 3rd line auditors (e.g. Defence Internal Audit, CyDR), Infrastructure and Projects Authority (IPA) and TLB security teams.

Review Frequency

Policy ref: 5C-12

Delivery Team Security Leads must perform regular reviews of cyber risk with the Delivery Team Leader and where required Cyber Security Assessors. The minimum frequency of these must be appropriate to the risks identified but must be quarterly as a minimum.

Define Security Controls (Principle 4)

23. Understanding the capability's context and security goals will inform the security architecture and proportionate control selection.

Policy ref: 5C-13

Delivery Teams Leads must ensure capabilities are designed with NCSC Good Design Guidance (Annex C) in mind and use MOD approved architectural design patterns and standard tooling as default where this is available and applicable.

24. Existing processes, knowledge, standards and technologies should be identified, assessed and reused where possible to avoid duplication of effort.

Control Identification

Policy ref: 5C-14

Delivery Team Leaders must select appropriate controls to mitigate security risks to ensure compromise and disruption from cyber-attack is difficult, detection is easy and impacts are reduced.

25. All controls must be implemented at a level that is proportionate for the criticality of the capability and the data used. Delivery Teams can use control frameworks (such as NIST SP800-53, ISO27000 series) to help understand relevant control options.

Engage and Manage the Supply Chain (Principle 5)

26. MOD relies on an extensive supply chain to deliver and maintain its capabilities. The security of a capability will only be as good as the security requirements defined in the contract that delivers that capability. The Delivery Team Leader on behalf of the SRO owns the relationship with the supplier and associated risks posed to the data used.

27. Delivery Team Leaders should foster a secure by design culture in the supply chain.

Policy ref: 5C-15

Delivery Team Leaders must ensure supply chain security risks are adequately addressed throughout procurement and in all contractual arrangements. These include handling MOD data, providing services, developing, manufacturing and/or implementing capabilities. This must include, as a minimum:

a. Through life capability security requirements;

b. Application of the DCPP[4] processes; and

c. Tender evaluation of security approaches.

Policy ref: 5C-16

Commercial Officers must ensure contracts include:

a. Clear and unambiguous through life security requirements, including the unencumbered transfer of data at contract end,

b. DEFCON 658 or equivalent;

c. The right to access information relevant to a security investigation; and

d. Penalties, recovery and remedial actions to be applied in the event of a security breach. (See DEFCON 514).

28. Further detail can be found in JSP440 Pt 2, Leaflet 6A (Contract and Project Security).

Assure, Verify and Test (Principle 6)

Policy ref: 5C-17

Delivery Team Leaders must demonstrate to the SRO and Cyber Security Assessor that security risks are adequately mitigated and deliver within the stated Risk Appetite. This must be carried out throughout the lifecycle before MOD data is used and before capabilities 'go live'.

29. Annex A details the conditions for accreditation decisions and the role of the SRO in approving 'go live'.

30. Where the capability interacts with third parties outside of the MOD coordination between relevant authorities is required.

[4] https://www.gov.uk/guidance/defence-cyber-protection-partnership.

Policy ref: 5C-18

Delivery Team Leaders must ensure:

a. Security requirements and controls are validated and verified at the most appropriate design points in the capability's lifecycle; and

b. Acceptance tests must evaluate the security controls and functions.

Non-conformances must be addressed before the capability can handle MOD data.

Policy ref: 5C-19

Delivery Team Leaders must ensure findings from security tests, including vulnerability analysis, are reviewed and appropriately acted upon. These must be made available to Cyber Security Assessors for reference and pan-defence vulnerability analysis.

31. Where possible Delivery teams should seek to make security testing repeatable through automated testing or integrate as part of wider 'bug bounty' process.

Enable Through Life Management (Principle 7)

32. Security does not stop once the capability is deployed. To ensure that capabilities remain resilient, vulnerabilities are fixed promptly and the security posture is maintained a continuous assessment of security performance is needed.

Policy ref: 5C-20

SROs must implement a through life approach to security utilising the Defence Lines of Development (DLOD) approach and a culture of learning from experience (LFE). They must demonstrate that they are actively seeking security improvements.

Policy ref: 5C-21

On behalf of the SRO, Capability Owners and Delivery Team Leaders must continuously reassess capability risks against functional changes, vulnerabilities and threats. They must act promptly to establish a mechanism to maintain the security posture of the capability.

Annex A – Accreditation

1. Accreditation is the assessment of an information-based capability, target of accreditation (TOA), against its security requirements, resulting in the acceptance of residual risks in the context of the business requirement.

Risk Acceptance

2. Residual risks must be at the level as to satisfy the stated risk appetite (See Policy 5C-5). Where risks have been identified that are outside the stated risk appetite approval must be sought from the appetite owner.

Accreditation Types

3. An Accreditation decision will be issued in the form of a letter signed by the SRO declaring that they are content with the residual risk. Before making their decision the SRO will be informed by the Cyber Security Assessor. The decision will be one of the following: Full, Interim and Conditional.

Interim Accreditation

4. Where a capability does not wholly meet the security requirements and or controls defined, because of a phased system development, an Interim accreditation may be granted. This must be of limited duration and scope. The Delivery Team Leader must satisfy the SRO of the planned activities to address this shortfall before Interim Accreditation may be granted

5. An Interim Accreditation Certificate will be issued for a short period, normally three to six months, after which a review is required for renewal. Continual renewals are not acceptable as a substitute for Full Accreditation. Interim Accreditation will not be extended beyond the initial six-month period without approval from Hd CySAAS.

Conditional Accreditation

6. When security controls are deemed weak or ineffective on in-service capabilities (generally caused by increased threats, vulnerability or from unscheduled minor changes), a Conditional Accreditation can be issued. The Delivery Team Leader must satisfy the SRO of the planned activities to address this shortfall before Conditional Accreditation may be granted

7. Conditional Accreditation can also be used in a planned manner for short duration installations such as Prototype/Demonstrator systems and quick notice deployments, where the full accreditation effort would be disproportionate.

8. In view of the increased risk being taken in such circumstances, the Accreditation Certificate signed by the SRO will itemise the shortfalls.

9. A Conditional Accreditation Certificate will be issued for a short period, normally three to six months, after which a review is required for renewal. Continual renewals are not acceptable as a substitute for Full Accreditation. Conditional Accreditation will not be extended beyond the initial six-month period without approval from Hd CySAAS.

10. Conditional Accreditation will not normally be allowed in a networked environment where such a decision could lead to unacceptable risk(s) being spread to the rest of the community, or where third party controlled or released information is stored or processed on the system(s).

Full Accreditation

11. Accreditation is usually granted for the following maximum periods, although factors other than classification should be taken into account:

a. OFFICIAL or equivalent - 5 years;

b. SECRET or equivalent - 3 years; or

c. TOP SECRET/STRAP or equivalent - 1 year.

12. Legacy systems are retained systems that were installed before current endorsed methodologies and security regulations were in force. If legacy systems are identified CySAAS must be contacted immediately to advise on the most appropriate accreditation action. The operation of unregistered/non-accredited capabilities to store, process, or forward classified, business or operationally critical data will be treated as a security incident.

13. Reaccreditation will be required when there is a change that adversely impacts on the security controls, affecting the risk profile. A proportionate change control process which assesses the security impact of each change must be established and appropriately governed by the Delivery Team Security Lead.

Joint Accreditation

Cross-government

14. Where the capability to be accredited crosses authority boundaries outside MOD, such as to international partners or Other Government Departments (OGDs), co-ordination between the relevant authorities is required.

International

15. NATO or Coalition documents may refer to Full Accreditation as ‘System Approval to Operate’ (SATO), and/or Interim Accreditation as ‘Interim Approval to Operate’ (IATO). Similarly, the term Designated Approving Authority (DAA) or System Approving Authority (SAA) will be encountered instead of Accreditor in NATO or Coalition documentation. NATO Policy is contained in the INFOSEC Management Directive for CIS AC/35-D/2005-Rev2.

Compartments

16. Where Compartmented Information is stored, processed or forwarded, Compartment Approval must also be sought. Accreditation of systems for STRAP information must comply with the HMG STRAP manual.

Annex B - Security Definition and Management Document

1. The Security Definition and Management Document (SDMD) must as a minimum:

   a. Define:

      (1) The use of the capability;

      (2) A description of the capability's relationship with and dependencies on other capabilities;

      (3) The Roles and Responsibilities involved in developing and managing the capability throughout its lifecycle including reporting points within CyDR;

      (4) External policies or standards that the capability needs to be compliant with and that will influence security e.g. air worthiness, safety, nuclear; and

      (5) The Stakeholders and any external requirements e.g. data protection, NCSC assurance requirements.

   b. Set out:

      (1) The risk and assurance approach for the capability with key decision points;

      (2) The overall approach to security considering the threat, vulnerabilities and risk assessment;

      (3) The role and structure of the supply chain and how supply chain risks will be managed; and

      (4) The cost and appropriate funding levels required to implement security controls.

Annex C – NCSC Good Design Guidance

1. The following should be considered during the capability design to ensure security compromise is made difficult:

a. Understand external input cannot be trusted;

b. Transform, validate, or render data input safely;

c. Reduce the attack surface;

d. Identify and gain confidence in crucial security controls;

e. Protect management and operations environments from targeted attacks;

f. Prefer tried and tested approaches;

g. Ensure all operations are individually authorised and accounted for;

h. Design for easy maintenance;

i. Make it easy for administrators to manage access control; and

j. Make it easy for users to do the right thing.

2. The following should be considered to ensure the capabilities are able to adequately detect and report malicious behaviour:

a. Collect all relevant security events and logs;

b. Design simple communication flows between components;

c. Detect malware command and control communications;

d. Make monitoring independent of the system being monitored;

e. Make it difficult for attackers to detect security rules through external testing; and

f. Understand 'normal' and detect the abnormal.

3. To make disruption to the capability difficult, the following should be considered as part of the capability design.

a. Ensure capabilities are resilient to both attack and failure;

b. Design for scalability;

c. Identify bottlenecks, test for high load and denial of service conditions; and

d. Identify dependencies on third parties and plan for the failure of that third party.

4. To reduce the impact of compromise following a breach to the capability, the following should be considered:

a. Use a zoned or segmented network approach;

b. Remove unnecessary functionality, especially where unauthorised use would be damaging;

c. Beware of creating a ‘management bypass’;

d. Make it easy to recover following a compromise;

e. Design to support 'separation of duties';

f. Anonymise data when it’s exported to reporting tools;

g. Don't allow arbitrary queries against your data; and

h. Avoid unnecessary caches of data