Ministry of Defence

# Industry Security Notice

Number 2023/09 dated 21 July 2023

Subject: **Secure by Design Requirements**

## Introduction

1. This ISN is to inform the UK Defence Supply Base of the Secure by Design policy and approach which has been set out to ensure cyber secure delivery of capabilities.

2. It applies to the definition, acquisition, development, maintenance and disposal of information-based capabilities for MOD. This includes but is not limited to networks, applications, services, information technology, operational technology, platforms and weapons systems.

## Status

3. This ISN replaces ISN 2022/04.

## Issue

4. Secure by Design is being adopted by MOD. For new projects the Secure by Design approach outlined in this ISN should be followed. For MOD projects currently in progress suppliers should take advice from their Delivery Team concerning the transition plan.

## Background

5. The implementation of Secure by Design is intended to secure capabilities through continuous risk management. Ensuring that MOD capabilities are secure by design is crucial in achieving Defence Outcomes. Where capabilities are not designed and built with security in mind this can lead to serious consequences, up to and including loss of life.

6. Implementation of Secure by Design should produce the following outcomes:

   a. Threats are understood and security weaknesses are identified earlier in a project lifecycle, reducing costs and risks to delivery;

   b. Capabilities are more secure;

   c. Through life development and delivery of capabilities is more secure; and

   d. Capabilities are enhanced by applying modern cyber security practices.

7. The Secure by Design approach[1] is based upon the following seven principles (the requirements for which are set out within this ISN):

- **Principle 1: Understand and Define Context**
  Understand the capability's overall context and how it will use and manage MOD data while achieving its primary business/operational outcome(s).
- **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.
- **Principle 3: Implement Continuous Risk Management**
  Embed cyber security risk management into existing programme governance as a continuous process.
- **Principle 4: Define Security Controls**
  Define, architect and implement security control requirements to address risks identified. Reuse existing services and patterns where they exist.
- **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.
- **Principle 6: Assure, Verify and Test**
  Work with security experts to gain security assurance, test and validate throughout the capability's lifecycle.
- **Principle 7: Enable Through Life Management**
  Ensure continuous security monitoring and improvements, including ongoing assurance requirements are enabled, met and disposed.

# Roles and Responsibilities

8. The following roles and responsibilities are pertinent to the Secure by Design

---

[1] MOD's approach to Secure by Design is informed by industry good practice (from the National Cyber Security Centre's Secure Design Principles), three lines of defence security assurance model and National Institute of Standards & Technology (NIST) Cyber Security Framework.

approach:

- **Capability Sponsors**
  Responsible for the sponsorship of the capability, its requirement development, concept of operation and ensuring the capability can address the risks in-service.
- **Senior Responsible Owners (SROs)**
  Accountable for the delivery of cyber secure outcomes throughout the capability lifecycle.
- **Delivery Team Leaders**
  Responsible for the development and delivery of secure capabilities that support Defence Outcomes throughout the capability's lifecycle.
- **Capability Owners**
  The in-service owners of the capability, responsible for operating the capability to support Defence Outcomes.
- **Commercial Officers**
  Responsible for the implementation of contract terms and conditions in the MOD that ensure that security is enforced throughout the capability's lifecycle.
- **Delivery Team Security Leads[2]**
  The individuals within the Delivery Team responsible for advising Delivery Team Leaders on security and risk management.
- **Cyber Security Assessor[3]**
  Responsible for independent 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; and are responsible for consistent and coherent advice and support to relevant capabilities.

9. Industry partners must ensure they are aware of the individuals assigned to the above roles at the start of the project. Where a role is yet to be assigned, the Capability Sponsor must be contacted for advice.

# Governance

10. 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.

11. The SRO must ensure that:

---

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

a. all decisions regarding the capability's development and use are made in the context of the risk[4] facing MOD's data and capabilities, and its resultant impact should it be realised;

b. a capability cyber risk appetite is defined and published for the Delivery Team; and

c. Delivery Teams follow the Secure by Design requirements, or that accreditation activities are completed.

12. The Capability Sponsor must ensure that business cases, and any relevant submissions, adequately address security requirements. These must be funded and actioned through the capability's lifecycle.

# Principle 1: Understand and Define the Context

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.

14. 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, and should include the following as a minimum:

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**

15. 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**

16. The SRO must ensure that a capability risk appetite is defined and published, derived from relevant MOD risk appetite statements as a minimum threshold.

---

[4] this must include the security risk from supplier activities and the contractual arrangements.

**Capability Registration**

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

# Principle 2: Plan the Security Activities

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

19. Delivery Team Leaders must:

    a. Appoint and fund a Delivery Team Security Lead;

    b. where required, establish a wider security team to provide advice and support;

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

    d. establish a continuous risk assessment approach throughout the capability 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 through life, from initial development, in-service through to disposal; and

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

20. All individuals assigned to the project must be suitably qualified and experienced.

**Security Approach**

21. Delivery Team Security Leads must:

    a. define the security approach for the project, including:
        i. the selection of a suitable risk assessment method, which must be adequate for the complexity and risk facing the capability; and
        ii. the identification of a control framework (e.g. NIST) based on the scope and breadth of the capability (in terms of the technology it utilises, the processes it requires, and the culture and behaviours needed to support it);

    b. ensure that all security risks[5] are recorded in the capability's risk register and translated into appropriate language in order to allow the business to make an informed decision; and

---

[5] Where a focused threat assessment is required to develop the risks, the Capability Owner should be contacted for further support.

c. ensure stakeholders understand their role in maintaining the security posture.

22. Delivery Team Leaders must plan and document the security approach. This document must be maintained during the life of the capability and transferred to the Capability Owner prior to the capability entering service.

# Principle 3: Implement Continuous Risk Management

23. 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.

24. SROs must ensure that cyber risks are actively managed throughout the capability lifecycle to ensure delivery is within defined MOD risk appetite and capability delivery risk management.

25. Risk analysis should be continuous throughout the capability lifecycle. Projects must be able to evidence this.

26. 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.

27. 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.

28. The risk register is intended to provide oversight, guidance, and analysis across multiple capabilities and allow for MOD to understand systemic risk. As such, it 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**

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

# Principle 4: Define Security Controls

30. Understanding the capability's context and security goals will inform the security

architecture and proportionate control selection.

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

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

**Control Identification**

33. 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.

34. 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.

# Principle 5: Engage and Manage the Supply Chain

35. 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.

36. The Delivery Team Leader, on behalf of the SRO, owns the relationship with the supplier and associated risks posed to the data used; they should foster a secure by design culture in the supply chain.

37. 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[6] processes; and

c. Tender evaluation of security approaches.

38. 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;

---

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

c. The appropriate rights to allow the MOD to terminate the contract in the event of a breach (e.g. DEFCON 514); and

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

# Principle 6: Assure, Verify and Test

39. 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'.

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

41. Delivery Team Leaders must ensure that:

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

b. acceptance tests evaluate the security controls and functions; and

c. Non-conformances are addressed before the capability can handle MOD data.

42. 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.

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

# Principle 7: Enable Through Life Management

44. 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.

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

46. 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.

## Validity / Expiry Date

47. This ISN will expire when superseded or withdrawn.

## MOD Point of Contact Details

48. The point of contact in respect of this ISN is:

Info & Info-Cyber Policy Team
Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence
email: UKStratComDD-CyDR-InfoCyPol@mod.gov.uk (Multiuser).

## Annexes:

A. NCSC Good Design Guidance

## 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.