Ministry
of Defence

Industry Security Notice

Number 2018/01

Subject: The Defence Assurance Risk Tool (DART) Risk Balance Case (RBC) Process

Introduction

1. The purpose of this Industry Security Notice (ISN) is to outline the process for Industry personnel submitting Risk Balance Cases (RBC) relating to Information Risk within Defence via the Defence Assurance Risk Tool (DART) where authorisation is required at the MOD Senior Information Risk Owner (SIRO) level. DART has been introduced to enable MOD to register, triage and determine approaches to dealing with the Information Risk pertaining to Information and Communication Technolgy (ICT) systems that process MOD identifiable information. DART will help provide MOD with a mature understanding of the ICT security risks across the Department and its Industry partners through the information entered by MOD and Industry organisations.

2. Associated processes include ICT Accreditation, covered under ISN 2017/01, and the Defence Cyber Protection Partnership (DCPP) Cyber Security Model (CSM) certification.

Definitions

3. Throughout this document, the term ICT systems means any ICT systems that store, process or generate MOD identifiable information. ICT Systems comprises the equipment, infrastructure, hosting environments and their composite applications.

4. For the purpose of this document, MOD identifiable information includes all information where MOD has a responsibility for requiring security of the information, which includes any information that is deemed OFFICIAL or above.

HMG Requirements

5. The HMG Security Policy Framework (SPF)[1] sets out the Government Policy Priorities including that:

   a. All information that HMG deals with has value.

   b. All ICT systems that manage government information or that are interconnected to them are assessed to identify technical risks.

   c. Proportionate assurance processes will provide confidence that these identified risks are being properly managed.

6. The SPF further states that ‘Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level. This process will take full account of relevant statutory obligations and protections, including the Data Protection Act, Freedom of Information Act, the Official Secrets Act, Equality Act and the Serious Organised Crime and Police Act’, and mandates that organisations will have:

   a. A mature understanding of the security risks throughout the organisation, where appropriate this will be informed by the National Technical Authorities.

   b. A clearly-communicated set of security policies and procedures, which reflect business objectives to support good risk management.

   c. Mechanisms and trained specialists to analyse threats, vulnerabilities, and potential impacts which are associated with business activities.

   d. Arrangement to deterimine and apply cost-effective security controls to mitigate the identified risks within agreed appetites.

   e. Assurance processes to make sure that mitigations are, and remain, effective.

7. Departments (and partners handling HMG information) are required to consult the full range of policy, advice and guidance provided by the National Cyber Security Centre (NCSC) to shape their business specific approaches and to deliver policy priorities and mandatory security outcomes.

MOD’s Approach

8. Security and Risk management of MOD identifiable information on ICT systems is conducted through the accreditation process. In accordance with ISN 2017/01, all ICT must be either accredited or self-evaluated before being permitted to process, store or forward MOD identifiable information.

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

9. If you have an area of HMG policy you are unable to adhere to or a risk that exceeds TLB or MOD SIRO appetite after discussion with your accreditor, this is required to be recorded using the MOD Defence Assurance Risk Tool (DART). A Risk Balance Case (RBC) is submitted to request TLB and/or MOD SIRO approval. This provides MOD with improved visibility of risks to MOD and the supply chain.

10. The RBC aims to provide the necessary information to enable the MOD SIRO or delegated authority to make an informed risk balance decision by clarifying the following:

    a. Threats and risks have been properly assessed and the impact is understood.

    b. Risks have been eliminated where possible through pragmatic measures.

    c. Where a risk cannot be eliminated or a residual risk remains, it is managed appropriately and mitigated to an agreed level.

11. This decision will inevitably direct the originator (or associated stakeholder) of the RBC to conduct some form of follow-up action (ongoing risk analysis and/or treatment plan) which will include a predetermined review date.

12. Previously, RBCs have been subject to a cumbersome paper-based distribution process. Consequently, it has proven difficult to track progress and to prioritise effectively. Furthermore, each Front Line Command (FLC) and Main Business Unit (MBU) has its own procedure for dealing with those RBCs that fall within their SIRO's delegated authority, resulting in the lack of a Defence-wide view of where risks are held, how they are being addressed and whether Risk Appetites (the extent of the risk that is acceptable to a Business owner) are being correctly applied. In addition, it has not been possible to understand where cross-organisational commonality might exist in the nature and treatment of risks. In order to address these factors, it has been determined that the RBC process should be incorporated into DART.

13. The DART was introduced in June 2014 with the principle aims of:

    a. Providing an automated facility whereby users could register ICT that required MOD accreditation (generally referred to as a Target of Assurance or ToA) by answering a relevant set of questions.

    b. Enabling Defence Assurance and Information Security (DAIS), through the scoring and weighting that was applied to the given answers, to gain a picture of the risk and complexity of the ToA, thereby leading to an informed decision on the accreditation approach that should be applied and facilitating the effective management of workloads.

    c. Progressing tasks through a semi-automated workflow, that enables closer monitoring of the accreditation effort and a deeper understanding of priorities.

    d. Providing Head DAIS with a greater understanding of Information Risk across the accreditation space through improved informational availability.

14. Bringing the RBC process into DART will further enhance the Information Risk picture by providing the ability to link RBCs and ToAs. It will generate an improved understanding of the progress of each RBC and where any potential blockers might exist. In addition, it will enable far greater trend analysis, so that common risks can be identified and either Best Practice introduced or, where appropriate, outdated Policy amended. Overall, it will lead to a streamlined process that is far more responsive to changing circumstances and events.

Aim

15. The aim of this ISN is to:

    a. Notify companies, contractors and suppliers of the requirements for registering and progressing RBCs through DART.

    b. Raise awareness of the HMG SPF requirements and adoption of DART within Defence Industry.

    c. Help ensure that Risk Management is conducted in line with HMG Policy.

Issue

16. All RBCs requiring MOD SIRO approval are now to be submitted via the DART RBC module. An RBC can take one of two forms:

    a. Movement: Formerly known as a Fast Track RBC, this covers portable devices (laptops, PDAs, etc.) and the transportation of optical/magnetic media (Hard Disk Drives (HDD), DVDs, CDs, USB thumb drives etc) that are either not colour coded or are non-compliant with mandated encryption standards[2]. In these cases, a Hand Carriage/Movement Plan is required.

    b. Information: Formerly known as a Short Format Supplement 12, this covers all other instances where an RBC is required.

17. Where a requirement for an RBC has been identified, the information must be registered on DART. If you have not used DART before, then you will be required to register from the Home Page. Full details on how to navigate your way through DART may be found in the User Guides, which are available via the Help (**?**) icon at the top of every DART screen.

18. The registration of an RBC will necessitate your answering a series of questions. Please note that Progressive Disclosure applies, meaning that you will only be asked questions that relate to the type of activity you are undertaking. Until you have submitted your entry, you may continue to amend any of your answers.

19. DART assigns a unique 'Survey Response' identifier to each submission at the beginning of the process. Following submission, a Case ID in the format 'RBC-XXX' will be allocated, which is to be considered the primary reference number for the RBC.

[2] For guidance on encryption, see ISN 2017/08.

20. Ideally, every RBC should be linked to a ToA, although this is not a mandatory prerequisite to raising a case.

21. RBCs will be prioritised in accordance with their urgency. It is therefore important that an answer be provided to the question requesting the date by which the MOD SIRO decision is required. RBCs should be raised as soon as the need arises, and short-notice cases kept to a minimum.

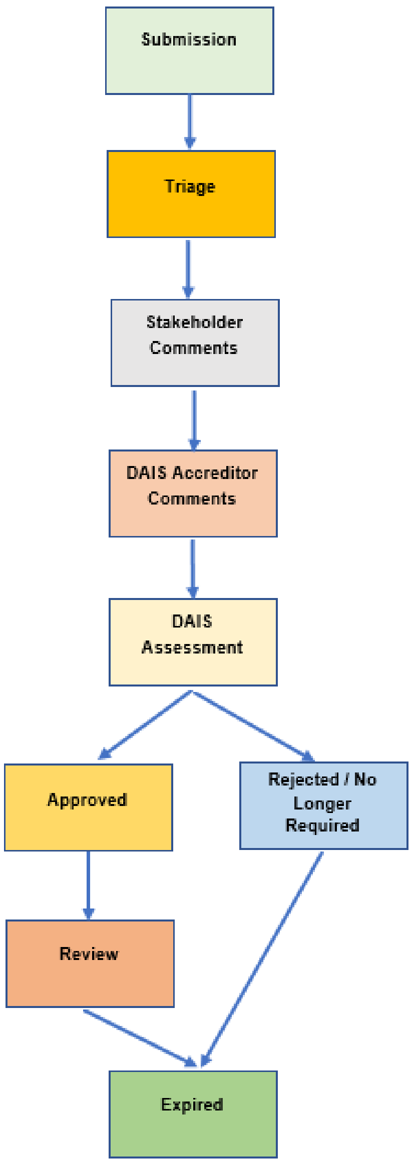
22. Once you have submitted the record, the submission will initially be scrutinised by the DAIS RBC Point of Contact (PoC). It will then be forwarded to the FLC/MBU PoC, who will coordinate the process of obtaining comments from the relevant stakeholders; e.g. Assurance Case Officers, FLC/MBU Accreditors, IT Security Officers (ITSOs), etc. Once this stage is complete, it will be submitted to a DAIS Accreditor and then to the DAIS RBC Advisor, who will liaise with the relevant Authority for approval.

23. At any stage in this process, you might be asked to provide further information via the workflow. In such cases, you should receive an automated E-Mail from DART, informing you that further action is necessary. However, it is always worth checking your RBC entry periodically to ensure that the submission has not been returned to you without your knowledge.

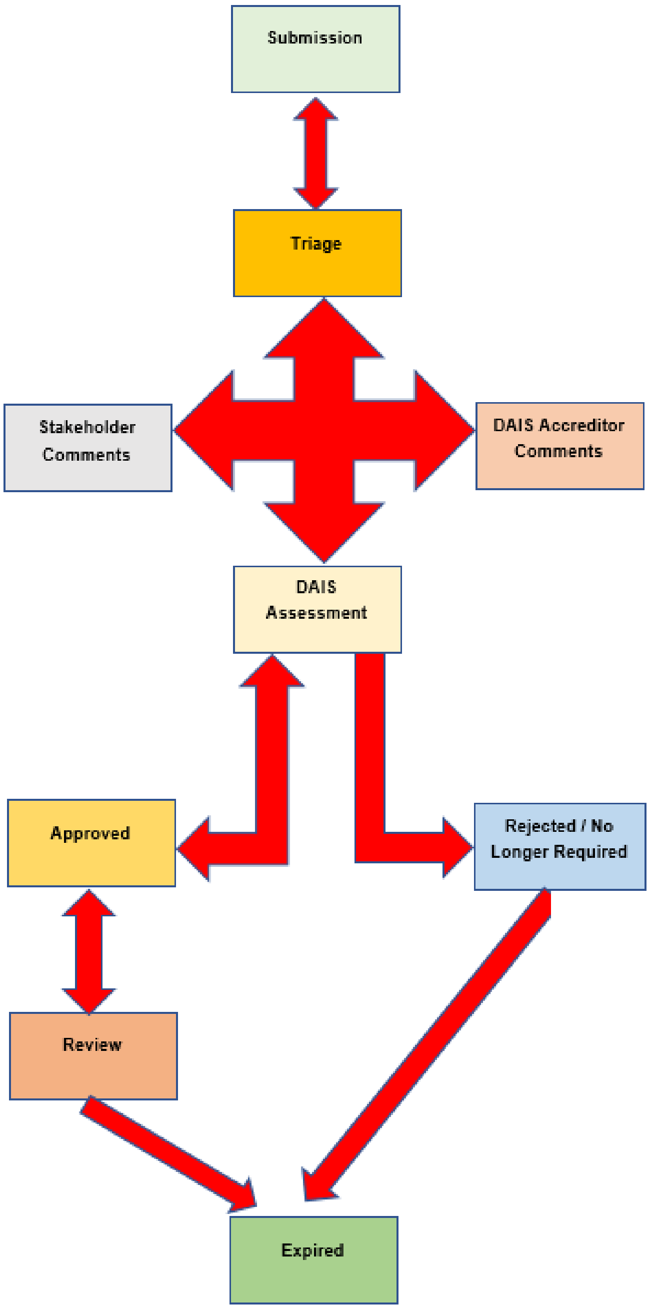
24. The timeframe for approval of an RBC is dependent on the complexity of the event, the number of stakeholders involved and whether the case needs to be returned to the originator for further details. RBCs will be prioritised in accordance with their urgency as specified in the submission.

25. As the diagram below indicates, each stage can potentially be revisited multiple times until the authority is satisfied that risks have been sufficiently mitigated and that the necessary information is available to enable them to reach an informed conclusion:

Linear Process



Complex Process



Points to Note

26. Currenty, DART is used only to process RBCs that require MOD SIRO approval. However, there exists the aspiration to expand its use to also encompass those cases that fall within the delegated authority of FLC and MBU SIROs.

    The information entered into DART regarding an RBC must not exceed OFFICIAL SENSITIVE level. In the circumstances where the information in the RBC exceeds OFFICIAL-SENSITIVE you should look to register the RBC on DART with a skeleton record for audit and tracking progress. Further details are likely to be required off-line in the SECRET tier. A SECRET version of DART is being considered.

27. DART is currently only accessible to users who possess connectivity to the Restricted LAN Interface (RLI). For any Industry partners who are unable to link to the tool, an off-line form is available on the DAIS.gov.uk site. This, along with the aforementioned classification restriction, are the **only** circumstances where an off-line submission will be accepted.

28. In the event that an existing RBC needs to be resubmitted for either of the following reasons, the resubmission is to be completed via DART:

    a. Any change that affects a risk previously approved by MOD SIRO.

    b. The review date is due and the activity that triggered the risk is still required.

Development of DART

29. Development of DART will continue, including the addition of modules covering other risk-related activities undertaken by DAIS. Feedback from industry to support the development of DART is welcome and should be forwarded by email to the DAIS RBC team (ISSDes-DAIS-RBC@mod.gov.uk).

Action by Industry

30. To follow the requirements of this ISN and apply the process for raising RBC requests and obtaining RBC approvals with immediate effect.

Validity / Expiry Date

31. To be reviewed annually in consultation with stakeholders.

MOD Point of Contact Details

32. Any queries or issues should be forwarded in writing by email to the DAIS RBC team: Email: ISSDes-DAIS-RBC@mod.gov.uk. This email should not be used for OFFICIAL-SENSITIVE unless it has been confirmed that TLS encryption is active between MOD and the company sender/recipient and that the email will land on a system accredited as suitable for OFFICIAL-SENSITIVE information.

33. Companies who know they have an appropriate connection may send OFFICIAL-SENSITIVE email using: - iss-des-dais-rbc@diif.r.mil.uk.

34. OFFICIAL-SENSITIVE may also be discussed on 01480 52451 4564 or 01480 446311, but inquiries should be submitted via E-Mail wherever possible. Companies connected to the RLI can find further guidance concerning the online operation of DART in the DART User Guide, which may be found under the question mark (**?**) at the top of each DART page.

Address:

DAIS Contact Point
X007 Bazalgette Pavilion
RAF Wyton
Huntingdon
Cambs. PE28 2EA