



Defence
Safety Authority

DSA 01.5

Analysis



Foreword

This document explains how the DSA conducts analysis. It is subordinate to DSA 01 *The DSA Sub-Operating Model* and complements other documents in the DSA 01 series. Together, the DSA 01 series provides colleagues in the DSA and across Defence an understanding of how the DSA conducts its activity and what can be expected from its outputs.

This document is coherent with the Secretary of State for Defence's policy statement for Health, Safety and Environmental Protection (HS&EP) and the DSA Charter. Departmental HS&EP policies are detailed within the relevant Joint Service Publications¹. Should there be a conflict between these documents and the DSA 01 series, please contact the DSA (DSA-Enquiries@mod.gov.uk).

Organisation

The DSA was established in 2015 and its authority and independence comes from a Charter issued by the Secretary of State for Defence, appointing it as an independent regulator, investigator and assurer for HS&EP within Defence. The DSA's vision is to protect defence personnel and operational capability through effective and independent HS&EP regulation, assurance, enforcement and investigation.

The DSA's analysis is conducted across the organisation at individual, team and organisational levels:

- DSA Headquarters
- Defence Themed Assurance Branch (DTAB)
- Defence Accident Investigation Branch (DAIB)
- Regulators:
 - Defence Environmental Protection Regulator (DEPR)
 - Defence Fire Safety Regulator (DFSR)
 - Defence Land Safety Regulator (DLSR)
 - Defence Maritime Regulator (DMR)
 - Defence Medical Services Regulator (DMSR)
 - Defence Nuclear Safety Regulator (DNSR)
 - Defence Ordnance, Munitions and Explosives (OME) Safety Regulator (DOSR)
 - Military Aviation Authority (MAA).

¹ JSPs 815 and 816.

Purpose

The purpose of analysis in the DSA is to generate insight from data and information to inform decision-making. This will be based on clear direction, collection from appropriate sources, effective processing through analysis and validation, and targeted dissemination. The purpose of this document is to primarily explain how this relates to outputs and outcomes across the DSA, from information gathered during audits and investigations. It does not cover input business management related analysis in detail.

This analysis will follow the standards and guidance set out by the UK Government Analysis Function² and MOD Analysis Function. It has been declared to the MOD Intelligence Function and will be reviewed annually to ensure appropriate oversight and good governance.

DSA Analysis Function Management

Section 1 – DSA Governance Structure

The scope of analysis within the DSA is difficult to bound and define. Whilst there are some personnel in the DSA who are employed as analysts to conduct analysis, the nature of the work in the DSA means that all staff members conduct analysis. Utilising data and information to inform decisions and deductions is a constant activity, especially for an organisation such as the DSA which operates as the Third Line of Defence for HS&EP. This includes regulators and branches as they scrutinise significant volumes of information collected through audits and investigations, and within the Headquarters across a wide range of enabling functions.

Therefore, the DSA Analysis Function operates across the entire DSA governance structure shown in Figure 1. The analysis function in the DSA exists to support and enable each regulator or branch and link into the DSA higher-level governance structures and deliverables, as required.

² [Government Analysis Function \(GOV.UK\)](https://www.gov.uk/government/organisations/government-analysis-function).

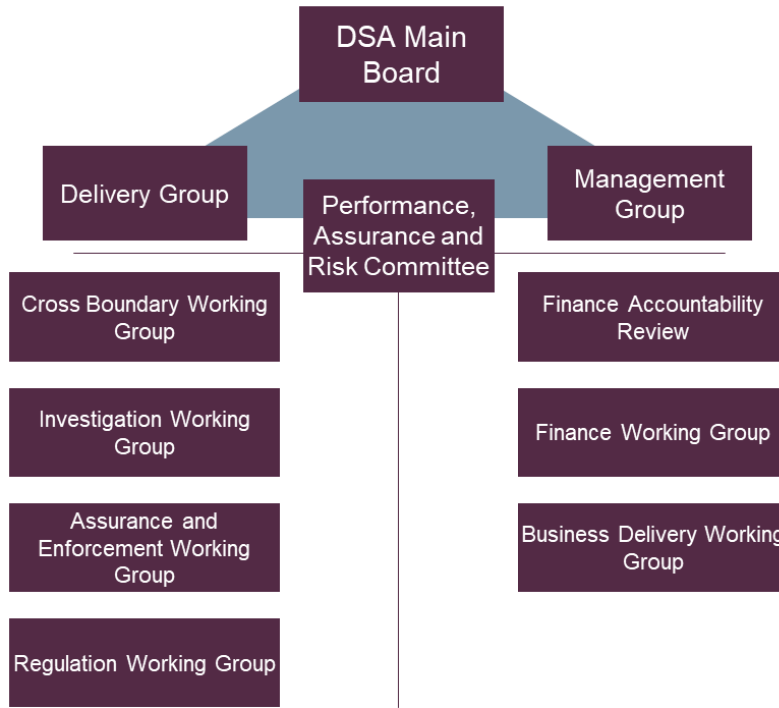


Figure 1: DSA Internal Governance Structure

Embedded throughout the DSA governance structure are several formal and informal processes that provide collection, processing and dissemination routes for DSA Analysis [see Figure 2]. These processes outline how information flows from one area to another and how the ecosystem of safety and environmental analysis work together.

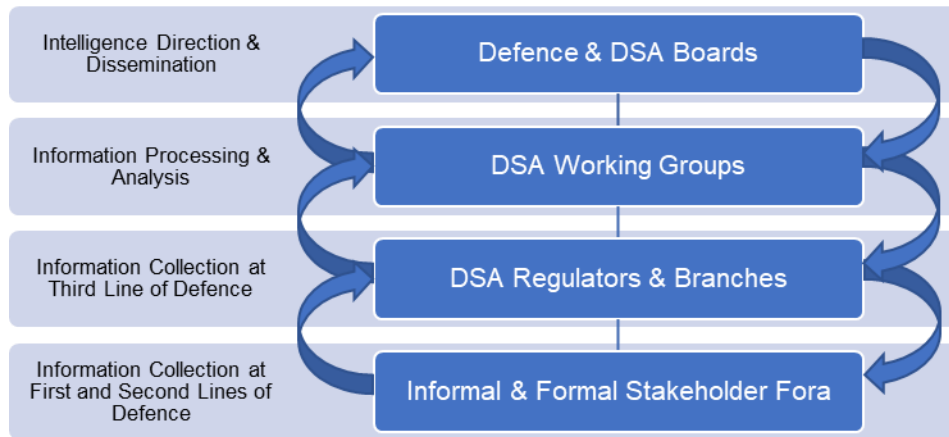


Figure 2: DSA Information Flow

From an outputs and outcomes perspective, the primary governance structure tasked to focus on the output of all analysis across the DSA is the Cross Boundary Working Group. It collates information from across the regulators and branches, as well as the wider defence community, to identify common themes or concerns that should be raised to the Delivery Group or Main Board, at which further direction can be provided to drive activity. The DEPR Coordination Group is similar, but specifically collates EP information from across the regulators and defence community to cohere EP information and thematic identification. Themes raised to the Main Board that require further escalation may be

discussed with the Second Permanent Secretary or at the Defence Safety & Environment Committee.

Section 2 – Process

The process undertaken by the DSA follows the widely-adopted and well-understood Intelligence Cycle (NATO, 2016) — Direction, Collection, Processing and Dissemination [Figure 3]. This process provides a clear link between what the DSA focusses on, how capabilities are employed to undertake collection activities, the processing and analytical resource then apportioned to that information, and how that information is disseminated in order to achieve safer and more environmentally responsible outcomes for Defence. It does not generate intelligence in the traditional sense, instead the DSA generates what is termed HS&EP intelligence.

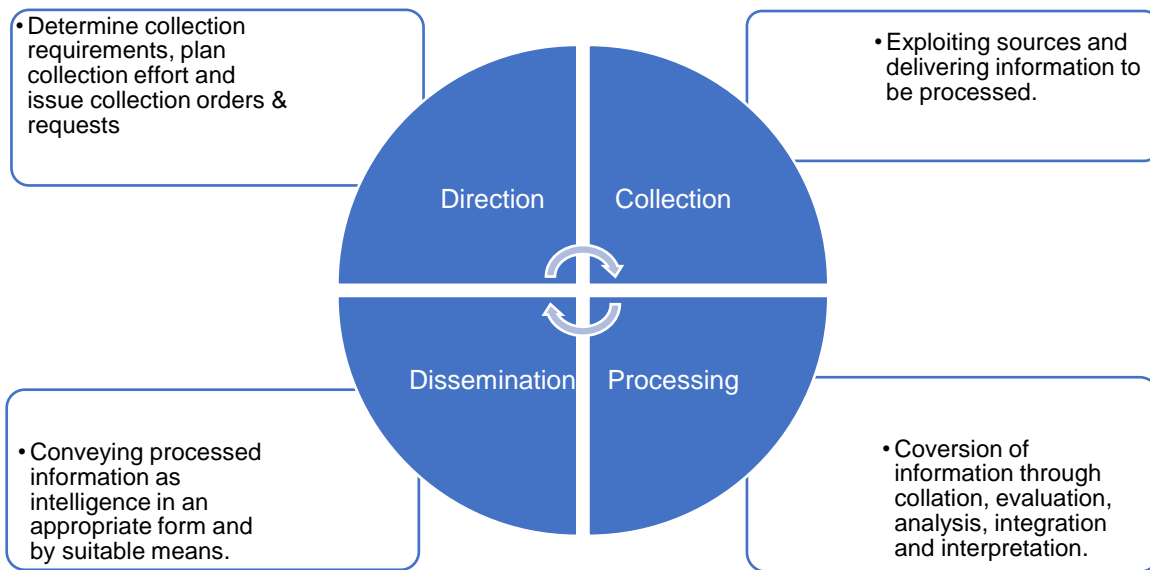


Figure 3: The Intelligence Cycle (NATO, 2016)

Direction

The DSA operates a largely disaggregated structure through the appointment of regulator and branch heads. The regulators are empowered to operate within their respective domains, either solely or in conjunction with other regulators. Therefore, it is the regulator heads that provide direction to their teams to collect the required information and data within their domain. This activity may be in accordance with DSA higher level direction or in reaction to a specific risk, theme of concern, or finding within their respective domain. The two branches operate slightly differently: DAIB is directed to undertake investigations by DG DSA as the convening authority; whilst DTAB is directed to conduct audits against specific themes identified by DG DSA and ratified by the Defence Safety and Environmental Committee.

Where further central DSA collection and analysis direction is needed it will be provided by the Delivery Group or DSA Main Board. It is at these fora, where a more detailed picture is available to the DSA Senior Leadership Team, that more strategic direction can be provided. This direction is then imparted at the Delivery Group, Working Groups or

more routine meetings but the working groups are not empowered to provide direction for follow-on activities.

Direction is essential to focus the capabilities of the DSA. This may include which themes are of the greatest concern and should be investigated further, or where a single DSA regulator or branch identifies a theme of concern, and a more pan-DSA position needs to be established. Alternatively, should the theme be well developed already, direction could be provided to commence a pan-DSA audit on a specific organisation, area of policy or functional discipline utilising capabilities from many regulators and branches.

The DSA Annual Assurance Report provides insight into areas of concerns and themes from the previous reporting year. Looking forward, it can therefore be used as extant direction to all regulators and branches in the DSA to focus their collection and analytical resource. Updated annually, the themes in the report highlight the areas that the DSA would propose are of most concern to the department.

Collection

The DSA conducts extensive collection activities aligned to the direction received. This can be achieved through assurance and audit activities, investigations, enforcements, stakeholder engagement, attendance at Defence Organisations' health, safety and environmental committees, whistleblowing from across Defence or internal in the DSA, data from outside the DSA such as claims data, incident reporting tools, high-level DG engagement, the Defence Safety and Environment Committee and, of course, the self-assessments and domain reports that feed the DSA Annual Assurance Report.

These collection activities are augmented by a larger range of more informal activities that all provide the regulators and branches with an extensive collection capability at the Third Line of Defence. The DSA will also leverage the collection undertaken by the First and Second Lines of Defence to further enhance their analysis. The collection architecture that feeds the analysis in the DSA is, therefore, extensive and reaches across Defence. Ensuring that this information is provided up the chain of command in a way that can be interrogated at all Lines of Defence is critical and relies on effective processing and dissemination.

Processing

Once collected, most information is processed within the regulators and branches. This first stage analysis is fundamental to ensure that information collected is stored in a way that can be interrogated and structured so that it is useable, analysed effectively to extract insight and then packaged prior to dissemination. Each regulator and branch adopt their own processing activities based on the ways of working in their team. Much of how this is conducted will depend on the complexity of the domain, the size of the team, resource available, digital architectures and the weight of information that needs processing. This is a daily activity for most teams in the DSA and the HQ-led governance structure often has very little to do with this routine activity; instead, the DSA relies on its teams operating within their respective regulatory domains.

At the DSA level, the main forum for processing pan-DSA information collected by the regulators and branches is the Cross Boundary Working Group, with the DEPR Coordination Group providing an information processing function for EP data. Information fed into the Cross Boundary Working Group as a theme of concern, location or

organisation, is discussed during the meeting, cross referenced with other regulators and branches and scrutinised for accuracy. The product utilised to structure outcomes-related information from this Working Group is the DSA HS&EP Intelligence Picture (more in dissemination). It does so through the Defence Risk and Assurance ‘Assurance Map’ (see Figure 4) by capturing risks, or themes, and then massing evidence against each one to identify assurance levels to identify whether the deficiency is at the First, Second or Third Line of Defence, or possibly all three.

The DSA Assurance Map has two main parts: first, to categorise the themes against the level of risk it poses to Defence; and second, to assess the level of assurance where Defence applies controls to manage risks. The purpose of outlining the risk assessments for themes is to enable the DSA to prioritise themes accordingly. Low risk themes or those that are the sole purview of a single regulator may be monitored but not included in the DSA HS&EP Intelligence Picture.

A	B	C			D i, ii, iii						E		F		
Risks	Risk Category	Risk Assessment Likelihood Criteria			Levels of Assurance within Lines of Defence						Overall Levels of Assurance		Other Information		
					First Line of Defence		Second Line of Defence		Third Line of Defence						
Risk Description	E.g. DBR 1, DBDR 1.1, Strategy, People etc	Inherent Rating	Residual Rating	Target Rating	1LOD Assurance Level	1LOD Assurance Activity	2LOD Assurance Level	2LOD Assurance Activity	3LOD Assurance Level	3LOD Assurance Activity	Overall Assurance Level	Overall Target Assurance Level	Key findings and issues/assurance gaps	Status	Provenance
<Theme>															

Figure 4: DSA Assurance Map

Dissemination

The DSA disseminates the outcomes of its analytical work in several ways, many of which have already been discussed in the preceding section. These dissemination channels enable the DSA to operate effectively as Defence’s Third Line of Defence for HS&EP.

First and foremost, the most important mechanism for dissemination of the DSA’s analysis is the DSA Annual Assurance Report, as mandated by the DSA Charter. This report is compiled utilising self-assessments from all Defence Organisations, regulator domain reports, the Directorate of Defence Safety Functional Report, input from the DAIB and DTAB, as well as many other sources of information. It is hosted on gov.uk and is disseminated widely across Defence for fact-checking and consultation prior to release. Its content is subsequently discussed at higher-level MOD boards and meetings as required. Due to such a wide dissemination and open availability to the public, its dissemination can result in questions that normally require secretariat support.

Secondly, the output of the DSA’s analysis is disseminated more dynamically and routinely by the DSA senior leadership team, regulator and branch heads and team members on a routine basis during many formal and informal meetings and engagements. This may include regulator stakeholder engagements, attendance at HS&EP committee meetings, DG-level engagements and the Defence Safety and Environmental Committee.

Thirdly, the regulators and branches have their own individual formal dissemination routes for products and outputs. For example, this includes distribution of regulations, audit reports, investigations, enforcement activities and other correspondence as part of

their regulatory or investigative work. Regulators and branches will disseminate reports following the inclusion of an audit or investigation. This will include the outcome of much analysis and is a formal record of the DSA's position on a particular topic.

Finally, the DSA utilises the DSA HS&EP Intelligence Picture and Insights Brief as internal dissemination channels. They are internal products for use by the DSA to drive its activity and inform future analysis. The DSA HS&EP Intelligence Picture is owned by the DSA Chief of Staff (COS) who will direct any changes and actions to take. It is the responsibility of the DSA COS to ensure that it is updated and provided to the relevant stakeholders to inform and drive discussions. The purpose of the HS&EP Intelligence Picture is to:

- Provide the DSA with a single view of pan-DSA themes of concern. The DSA defines these themes as the underlying causes of issues (or symptoms) that may be seen across Defence. In that regard, they are cross-cutting and a single issue can be caused by multiple themes. It is these themes that drives the DSA HS&EP Annual Assurance Report.
- Provide the Cross Boundary Working Group and Delivery Group with a structure around which to have more focussed conversations about what future activity the DSA might need to take, either through a pan-DSA audit involving multiple DSA teams, a DTAB audit, investigation or perhaps high-level DG DSA engagement.
- Provide a high-level view but not complete view across the DSA, noting that DSA regulators and branches operate a similar process and generate an intelligence picture for their respective domain, which they then take action against unilaterally, explain in their submission for the Annual Assurance Report and discuss at stakeholder committees. There will be issues that exist at regulator level that are not included in the DSA HS&EP Intelligence Picture.

Section 3 – People

Effective analysis requires the right personnel structures, training and experience. Analysts require access to the right data, information and systems to be able to deliver timely and accurate reports. Through engagement with the relevant Functional leads, the DSA will develop its analytical capability by investing in the recruitment, development and retention of staff with the right skills and expertise to deliver credible analysis. Analysis conducted by other organisations, internal and external, will be used by DSA analysts where appropriate. Following common standards and guidance will allow DSA staff to exploit this analysis and incorporate findings into existing repositories. This will ensure the DSA is able to further improve its analytical maturity.

Section 4 – Technology

The DSA Digital Strategy is the primary delivery mechanism for the required technology to support the DSA analysis function. The strategy will deliver data capture tools that are standardised and rationalised to enable cross-organisational analysis and integrated insights. The data will be coherently structured, readily accessible and reusable for users internally and wherever possible externally. This will facilitate effective interrogation of

information through well-structured data and robust digital solutions to automate data input processes, thereby allowing analysts to focus on analytical activities to inform decision making.

Summary of changes

Date of change	Version	Author	Comments
21 July 2023	0.1	DSA-HQ-Ax-ATL	First draft.

References

- [1] NATO (2016), *Allied Joint Doctrine for Intelligence, Counter-Intelligence & Security*. Available at: [NATO >> DATA >> AJP2](#) (accessed 31 March 2023).
- [2] DSA (2022), *DSA Business Plan 2022-2023*. Available at: [DSA >> Strategy & Plans >> Business Plans >> Business Plan 22-23 >> Circulations](#) (accessed 31 March 2023).
- [3] DRA (2022a), *JSP 892 Part 2 Supplement 7 - Defence Risk and Assurance (DRA) Quarterly Risk and Assurance Mapping Report (Template Guidance)*. Available at: [MOD >> Head Office >> JSP 892 Part 2 Supplement 7](#) (accessed 31 March 2023).
- [4] HMT (2020), *The Orange Book: Management of Risk – Principles and Concepts*. Available at: [The Orange Book \(publishing.service.gov.uk\)](#) (accessed 31 March 2023).
- [5] DRA (2022b), *JSP 892 Part 2 Leaflet 2A - Defence Risk Assessment Criteria and Heat Map / Probability Impact Diagram (PID)*. Available at: [MOD >> Head Office >> JSP 892 Part 2 Leaflet 2A](#) (accessed 31 March 2023).
- [6] DRA (2022c), *JSP 892 Risk Management Part 1: Directive*. Available at: [MOD >> Head Office >> JSP 892 Part 1 Directive](#) (accessed 31 March 2023).
- [7] MOD (2016), *Defence Operating Model: How Defence is Organised*. Available at: [MOD >> Defence Operating Model >> How Defence is Organised](#) (accessed March 2023).