Ministry of Defence

DCS Risk Management Policy Directive

7.1.4

DCS Jul 23 v2.0

General

Authorisation	COS DCS
Senior Responsible Owner	Head DCS
Point of Contact	DCS POLRA
Next Review Date	Jul 26
Annexes	Annex A: Likelihood and Impact Criteria
	Annex B: Risk Register Example
Related Policy/Guidance	JSP 892 Risk Management
	ACSO 1109
	DCS SHEF Directive

Introduction

1. Defence Children's Services (DCS) and specifically Hd DCS are mandated by Defence to ensure that the organisation has an effective and robust risk management process in place, that risks are being identified and managed to within acceptable levels, and that, as a by-product, the risk management process is producing high quality risk information to inform business decision making. This DCS Directive complements, but does not replace, direction detailed in JSP 892: Risk Management. Elements of the JSP will be repeated in this Directive for consistency.

2. The MOD defines risk as 'an uncertain future event that could affect the Department's ability to achieve its objectives'. Risk management is the set of activities that enables the identification, assessment, management and communication of risks throughout the organisation and up through the chain of command as necessary.

3. Risks are separate to issues which are events that have already occurred, or will definitely happen, which are certain to affect the achievement of stated objectives. The risk management process defined in this policy will be used to manage risks and issues, however, issues should be manged as part of business-as-usual tasks and routine performance management activities.

Aim

4. Risk management is not about avoiding risk or being risk averse, nor should it be performed simply as a 'tick box' compliance activity. Effective risk management allows us to understand and optimise the benefits and value we can generate from calculated risk taking as well as helping us to avoid unwanted surprises. The aim of this Directive is to provide a framework of guidance to DCS Services on the identification, recording and reporting of risks, to ensure that risk is managed robustly and with a consistent level of rigour, allowing informed decisions to be made by the right people at the right time. The approach is both 'top-down' and 'bottom-up'.

Roles and Responsibilities

5. **Head DCS**. Hd DCS is responsible for managing, holding and accepting risk at the 1* level, and maintaining a robust risk management framework and system of internal control (including owning the Risk Management Directive).

    a. Responsible for the effective identification and management of risks to within acceptable levels in relation to any risks that could:

        i. Affect the ability to successfully deliver stated strategic objectives.

        ii. Impair the ability to comply with Defence Policy and Directives.

    b. Review risks presented at the 1* level for Hd DCS ownership.

    c. Challenge the validity, scope and completeness of key risks and current response activities, including ownership and severity ratings.

    d. Identify cross-Service or cross-agency/organisation risks requiring additional stakeholder engagement.

    e. Approve/reject proposed approaches to manage the risk. Review implementation of any previously submitted and agreed actions. Conduct deep dives if necessary.

    f. Identify and elevate risks as necessary to the 2* level (GOC RC).

6. **Chief of Staff (COS) DCS**. COS DCS will oversee the HQ Risk & Issues register on behalf of Hd DCS.

    a. Lead the Risk Review at weekly Command Groups as part of the Standing Agenda.

    b. Elevate risks on behalf of Hd DCS to the 2* level via monthly RC Risk Review Board and the Quarterly Performance and Risk Reporting (QPRR) mechanism.

7. **RC-DCS-POLRA**. POLRA will manage the HQ Risk & Issues register on behalf of Hd DCS.

    a. Maintain the HQ DCS Risk & Issues at the 1* level.

    b. Facilitate and support Service level Risk and Issue management.

8. **Assistant Heads (AH)**. AH's are to identify, track and manage Service risks at their level.

    a. Identify and understand individual Service risks.

    b. Select and take the risks that provide the organisation with the right benefits and understand their impact.

    c. Take action to monitor, manage and report the risks we do not want to be exposed to, ensuring our resources are effectively and efficiently prioritised and used.

    d. Lead Service Risk Reviews at appropriate intervals, but no less than monthly, to ensure organisational risks are captured.

    e. Maintain Service Risk & Issues Registers.

    f. Elevate risks to the 1* level as required during weekly Command Groups.

g. Create a proactive and risk-aware culture amongst teams to ensure that risk is embedded into planning, decision making and business as usual activities in a common way.

9. **Assistant Chief of Education Officers (ACEO)** ACEO's are to identify, track and manage Regional risks at their level.

    a. Identify and understand individual Regional Risks.

    b. Lead Regional Risk Reviews at appropriate intervals, but no less than monthly, to ensure organisational Risks are captured.

    c. Maintain Regional Risk & Issues Registers.

10. **Team Leaders (TL)**. TL's are to play an active role in the 'bottom up' approach of risk identification.

    a. Identify team risks and enter them on to the Service Risk Register with appropriate and sufficient detail.

    b. TL's discuss team risks with Service AH's/ACEO's during Team Risk Reviews as part of Team assurance meetings (no less than monthly)

    c. TL's act as Risk Owners or Action Owners as directed by AH's / ACEO's

11. **Head Teachers (Hds)** Hds are to play an active role in the 'bottom up' approach of risk identification.

    a. Identify school risks and enter them on to the Service Risk Register with appropriate and sufficient detail.

    b. Hd's discuss school risks with ACEO's/AH's during School Risk Reviews as part of school assurance meetings (no less than monthly).

    c. Hd's act as Risk Owners or Action Owners as directed by Service AH's / ACEO's

12. **Risk Owners.** A risk owner shall be appointed to every risk that is identified. The risk owner is the single point of accountability for the effective management of the risk and should be an individual (not a team or function), with an appropriate level of knowledge of the risk and the authority to ensure the risk is managed effectively.

    a. Ensure the risk is described accurately and clearly.

    b. Determine the inherent, residual and target risk level.

    c. Develop the risk response plan and ensure its implementation.

    d. Monitor the risk for any changes to its status, including its impact or likelihood, and the effectiveness of the existing controls and mitigations.

    e. Comply with risk reporting procedures.

13. **Action Owner**. An action owner is an individual responsible for ensuring risk responses are implemented in accordance with the risk response plan. The action owner has delegated authority from the risk owner who maintains the overall responsibility for the risk.

Risk Management Process

14. **Step 1 - Risk Identification.** The purpose is to identify and describe the risks that could affect strategic objectives and agree appropriate ownership.

15. **Risk Description**. A well-defined risk description is essential for effective risk management; it allows for accurate assessment of, and response to a risk event, and consequent prioritisation for action. A risk is a combination of a **cause**, an **event**, a **consequence(s)** and the description of a risk event must enable a clear understanding of each of these elements to help inform risk assessment and risk response. The risk description must:

    a. Be sufficiently detailed and precise so that it is possible to determine if and when a risk has actually occurred.
    b. Enable an accurate assessment of its impact and likelihood to enable decisions on responses to it to be made.

16. **Step 2 - Risk Assessment**. The purpose is to answer the following questions:

    a. What are the potential impacts of the risk and what is the likelihood of the risk occurring?
    b. Are there any activities or factors currently in place e.g. controls and mitigations that would reduce the impact of the risk if it occurred or its likelihood of occurrence?
    c. Is the level of risk acceptable or does it require further management actions.

17. **Assessing the impact and Likelihood**. A risk assessment determines the significance of a risk by considering two factors:

    a. The potential impact(s) of the risk if it were to occur
    b. The likelihood of the risk occurring.

18. To ensure common understanding across the MOD and ensure the impact and likelihood of a risk occurring is measured in a consistent way to allow for the size and significance of risks to be compare, a defined set of risk assessment criteria are to be used and these can be found at Annex A.

19. **Inherent, Residual and Target Risk Assessment**. To understand the nature and potential size of a risk exposure required its inherent, residual and target risk positions to be assessed. This ensures that risks receive the appropriate level of management focus and oversight, and assurance efforts are directed towards those risks that are key and have the greatest levels of reliance placed on controls and mitigations.

    a. **Inherent.** The pre-mitigated assessment of the impact and likelihood of the risk. Ignore any controls and mitigation in place – essentially the worst-case scenario.
    b. **Residual.** The current assessment of the impact and likelihood of the risk. Based on how it is currently being managed. Assumes controls and mitigations in place are working as intended.
    c. **Target.** The determination of the risk's exposure once any funded further response activities have been implemented and are working as intended.

20. **Step 3 – Risk Response.** Risk response establishes which risks require new or additional management options, by comparing the residual risk position against the acceptable position (As Low As Reasonable Practicable – ALARP). Typically, the risk response will fall into one or more of the following five categories: **Terminate**, **Treat**, **Transfer**, **Tolerate** and **Take** the opportunity.

21. **Risk Response Outcomes.** There are three possible outcomes from the risk response step:

a. Maintain existing response activities, as residual risk is aligned to the desired level of risk exposure or additional management activities are not feasible or cost effective. The risk is then held at the 1* level, or elevated to the 2* level i.e. Treat, Transfer or Tolerate.
b. Reduce the level of risk to an acceptable level by implementing a risk response plan. This could include stopping or changing the activity that gives rise to the risk i.e. Treat or Terminate.
c. Increase the level of risk (and hence possible benefits or cost savings) by either relaxing or removing controls and mitigations i.e. Take the opportunity.

22. **Risk Response**. Sufficient analysis and evaluation must be done to determine the nature and extent of risks that the MOD organisation is willing to take – its risk appetite and tolerance (at departmental or local levels) – will determine where and what additional action is required. Where the decision is made that the residual risk assessment position is not aligned to an acceptable level of risk exposure, appropriate actions are to be selected, documented in the risk register and then implemented in order to bring the residual position in line with the acceptable risk position. If multiple risks require a response, it may be necessary to prioritise the order in which risks are managed due to time and resource constraints. The risk response should be developed with sufficient detail to ensure it can be understood by all relevant stakeholders and given to a nominated **Risk Owner**. The **Risk Owner** can/should delegate actions out to **Action Owners** to ensure its implementation.

23. Step 4 – **Risk Monitoring and Reporting.** Once the risk response plan has been established and is being implemented, the Risk Owner must track and regularly review the risk to identify any changes to it, make any decisions about additional responses and track progress against the response plan. At Risk Reviews, AH's must assess all risks affecting the achievement of a set of objectives to identify any interdependencies or conflicts, and to confirm that their individual response plans are sufficient when viewed in relation to other risks.

24. **Risk Reporting**. The purpose of risk reporting is to provide Hd DCS and the Senior Leadership Team with information about the key risks facing their part of the organisation. This will enable decision making and enable the effective management and oversight of risks within their area of responsibility. Risk reporting can be upward, downwards or horizontal notification of a specific risk, or wider risk information. Typically risk reporting is intended to increase risk awareness, but should there be an additional purpose, the report owner should make this clear to the recipients.

a. Risks **MUST** be documented in a risk register. An example can be found at Annex B**.**
b. Risk reporting must be timely, accurate and reflective of the needs and understanding of the target audience. If a risk significantly deteriorates or a new severe risk is identified, the Risk Owner should not wait until the next reporting period, but raise to their TL or AH immediately.
c. Hd DCS will review all 1* risks weekly at Comd Gp and report strategic risks to RC on an ad-hoc basis and more formally through the quarterly QPRR process.

Risk Scoring Criteria

The likelihood can be measured using the probability percentage or based on how commonly it has occurred in the past. If multiple scales are being used, the assessment should be based on the scale with the highest likelihood i.e. if the probability is 30%, but it has only occurred once in the organisation's history, then the likelihood should be documented as 'medium'.

	Likelihood	Probability	Description
5	Very Likely (Very High)	>75%	Is a common occurence in the MOD.
4	Likely (High)	50% - 74%	Has occurred within MOD many times.
3	Possible (Medium)	30% - 49%	Has occurred in MOD on several occasions.
2	Unlikely (Low)	5% - 29%	Has occurred on a small number of occasions in MOD's history.
1	Very Unlikely (Very Low)	<5%	Has occurred once/never in MOD history.

Table 1 - Risk Assessment Likelihood Criteria

Impact						
	E	17	22	23	24	25
	D	12	16	18	20	21
	C	7	10	14	15	19
	B	4	6	9	11	13
	A	1	2	3	5	8
		1	2	3	4	5
		Likelihood				

Table 2 - Heat Map

	Health, safety & environment (not as a result of hostile action)	Financial	Impact on outputs / capability/military operation	Reputational
D Severe	• Single death or injuries to multiple individuals which are life threatening and/or have a shortterm impact on normal way of / quality of life in a non-theatre environment. • Severe damage over a wide area and/or on a prolonged basis to a natural resource, including controlled waters, or geography requiring multiyear remediation. • Single incident causing a major environmental effect (EA Common Incident Categorisation Scheme - Cat 1). • Multiple incidents causing significant environmental effect (EA Common Incident Categorisation Scheme - Cat 2).	£1bn-£250m across delegated control total for 5 years. or 25% - 15% of in year budget for a Category A program.	Severe – severe constraint on the ability to deliver one or more DEO/DSOs.	• Severe short-term (less than 6 months) or moderate long term (at least the duration of the current political term) damage to strategically important international relationships, leading to a reluctance to enter into joint operations, share intelligence etc. • Severe short-term (less than 6 months) or moderate long term (at least the duration of the current political term) damage to the UK's international geopolitical agenda. • Concerted action in parliament questioning the actions of the Secretary of State for Defence. • Severe short-term less than 6 months or moderate long term, leading to damage to MOD perception. • Single high profile litigation against MOD.
C Major	• Single injury which causes permanent disability or permanent impact on way of life in a non-theatre environment. • Injuries to multiple individuals of a non-life threatening nature which have a short term impact on normal way of / quality of life in a non-theatre environment. • Moderate damage to an extended area and/or area with moderate environmental sensitivity (scarce / valuable environment) that requires months of remediation. • Single incident causing a significant environmental impact (EA Common Incident Categorisation Scheme - Cat 2).	£250m - £50m across delegated control total for 5 years. or 15% - 10% of in year budget for a Category A program.	Major – Major constraint on the ability to deliver one or more DEO/DSO's	• A negative questions posed to minister in parliament. • Short-term (less than 6 months) major outrage & protests from multiple a key campaign / activists / gatekeeper group.

	Health, safety & environment (not as a result of hostile action)	Financial	Impact on outputs / capability/military operation	Reputational
B Moderate	• Injuries to multiple individuals of a non-life threatening, non-permanent nature which require first aid only in a non-theatre environment. • Moderate damage to an area, and that can be remedied with MOD resources. • Multiple incidents causing minor environmental effect (EA Common Incident Categorisation Scheme - Cat 3).	£50m - £10m across delegated control total for 5 years. or 10% - 5% of in year budget for a Category A program.	Moderate – moderate constraint on the ability to deliver one or more DEO/DSOs	• Short-term (less than 6 months) major outrage & protests from multiple non-key campaign / activists / gatekeeper groups.
A Minor	• Injury of a non-life threatening, non-permanent nature which requires first aid only (in a non-theatre environment) • Limited short term damage to an area of low environmental significance / sensitivity • Incidents causing minor environmental impacts (EA Common Incident Categorisation Scheme – Cat 3)	£10m - £0m across delegated control total for 5 years. or Less 5% of in-year budget for a Category A program.	Minor – Minor constraint on the ability to deliver one or more DEO/DSO's	• Regional outrage & protests from non-key campaigner / activist / gatekeeper group

Table 3 - Risk Assessment Impact Criteria

Annex B to
DCS Risk Management Directive
Dated Jul 23

Example of a Risk Register

Serial Number	Owner	Manager	Statement of Risk	Inherent Likelihood	Inherent Impact	Inherent Score	Control/ Mitigation	Residual Likelihood	Residual Impact	Residual Score	Risk Response	Target Likelihood	Target Impact	Target Score	On/Near/Off Target	Comments
1																
2																
3																
4																