Ministry
of Defence

JSP 892
Risk Management

Part 1: Directive

Foreword

Defence is a complex business and risk is inherently part of everything we do. How we take and manage risk determines our success, both in operations and in our activities that support them. We all make decisions on risk every day; the objective of risk management is to harness our collective knowledge of risk and to formalise, where it makes sense to, our approach to analysing and managing the more significant uncertainties we face that could affect the achievement of our objectives and delivery of our outputs.

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.

This policy sets out the principles and standards regarding risk management that we want to see adhered to throughout Defence. It provides a framework, with supporting guidance, to ensure that risk is managed robustly and to a consistent level of rigour, allowing informed decisions to be made by the right people at the right time. This policy will evolve as our needs and abilities develop over time. Please take the time to familiarise yourselves with it and to apply it to the conduct of your business as appropriate.

Jon Thompson

PUS

Preface

How to use this JSP

1. JSP 892 sets out the mandatory requirements for risk management activities within MOD. This JSP will be reviewed at least annually.

2. The JSP is structured in two parts:

a. Part 1 - Directive, which provides the direction that must be followed in accordance with statute or policy mandated by Defence or on Defence by Central Government.

b. Part 2 - Guidance, which provides the guidance and best practice that will assist the user to comply with the Directive(s) detailed in Part 1.

Coherence with other Defence Authority Policy and Guidance

3. Where applicable, this document contains links to other relevant JSPs, some of which may be published by different Defence Authorities. Where particular dependencies exist, these other Defence Authorities have been consulted in the formulation of the policy and guidance detailed in this publication.

Related JSPs	Title
JSP 525	Corporate Governance
JSP 503	MOD Business Continuity Management

Further Advice and Feedback – Contacts

4. The owner of this JSP is PUS. For further information on any aspect of this guide, or questions not answered within the subsequent sections, or to provide feedback on the content, contact:

Job title/e-mail	Project focus	Telephone
Director Defence Audit, Risk and Assurance	N/A	[redacted]

Contents

1 Risk Management Policy

1. This Risk Management Policy defines the strategy, principles and mandatory requirements for how risks are managed in MOD. This policy has been formally approved by the Defence Board.

2. Under the delegated model each TLB[1] and Defence Authority (DA) will continue to be responsible for ensuring they have appropriate risk management governance structures, processes and activities in place to effectively manage their risks. To ensure a common approach across MOD, each TLB/DA's approach will need to comply with both parts of this JSP.

3. The risk management framework described in this JSP is the over-arching authority for risk management in MOD. This JSP does not replace other MOD processes that identify and report risks (e.g. DCAR, Portfolio, Duty Holding etc.) and technical risk management activities in specialist fields (e.g. technical risk assessment directives in place for the Defence Safety Authority); these will need to continue to be complied with. However, any key risks identified through these processes should be reported to the Defence Board as described in this JSP.

4. The MOD risk management framework is aligned with the overarching principles of the HM Treasury's Orange Book but has been tailored to meet the specific needs of the Department.

What is Risk Management?

5. A risk is an expression of uncertainty. 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 Department.

The Risk Management Framework

6. The framework encompasses the risk management activities required to operate in an effective and consistent manner throughout the Department. These activities can be summarised in the following elements:

- Governance
- Process
- Training and Awareness
- Behaviours and Performance
- Assurance

[1] Throughout the document the term 'TLB' is used as shorthand and refers to the four Front Line Commands, DE&S, DIO and HOCS.

7. Note that elements of the MOD risk management framework, namely Training and Awareness and Behaviours and Performance are yet to be developed. Work is underway to embed a common framework by 2016.

Benefits of Effective Risk Management

8. Effective risk management supports:

- Informed decision making to deliver consistent and improved business performance, informed cost management, and avoidance of unwanted surprises.
- Successful management of risks to within acceptable levels, as a result of consistency and clarity in their accountability and ownership.
- An improved view of the key controls and mitigations that are in place to manage risks, whether they are operating as desired, and whether there are any gaps.
- A clear path for TLBs/DAs to communicate key risks[2] to the Defence Board, enabling the Defence Board to make informed decisions and oversee and challenge the management of those risks.
- A proactive, risk-aware culture across the Department.
- Assurance to the Defence Audit Committee (DAC) and Defence Board that effective processes are in place to identify, understand and manage key risks.

Risk Management Vision

9. The MOD vision for risk management is that all key risks to the achievement of our Strategic Objectives are identified, assessed and managed to within acceptable levels. To achieve this, an environment needs to be created where consideration of risk is embedded into MOD's culture, planning, decision making and business as usual activities in a common way.

10. The objectives of risk management are to:

- Identify and understand the risks that we face.
- Select and take the risks that give us the right benefits, and understand their impact on the Department.
- 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.

Principles

11. The key principles to support the delivery of the risk management approach are outlined below:

- It is the responsibility of all staff (as appropriate to their roles) to ensure they understand and comply with this policy and their defined risk management roles and responsibilities.
- A consistent risk management approach is used throughout MOD to identify and manage risks.
- There is a defined risk management governance structure with clear accountabilities within each TLB/DA. This is sufficiently communicated to staff within that TLB/DA.

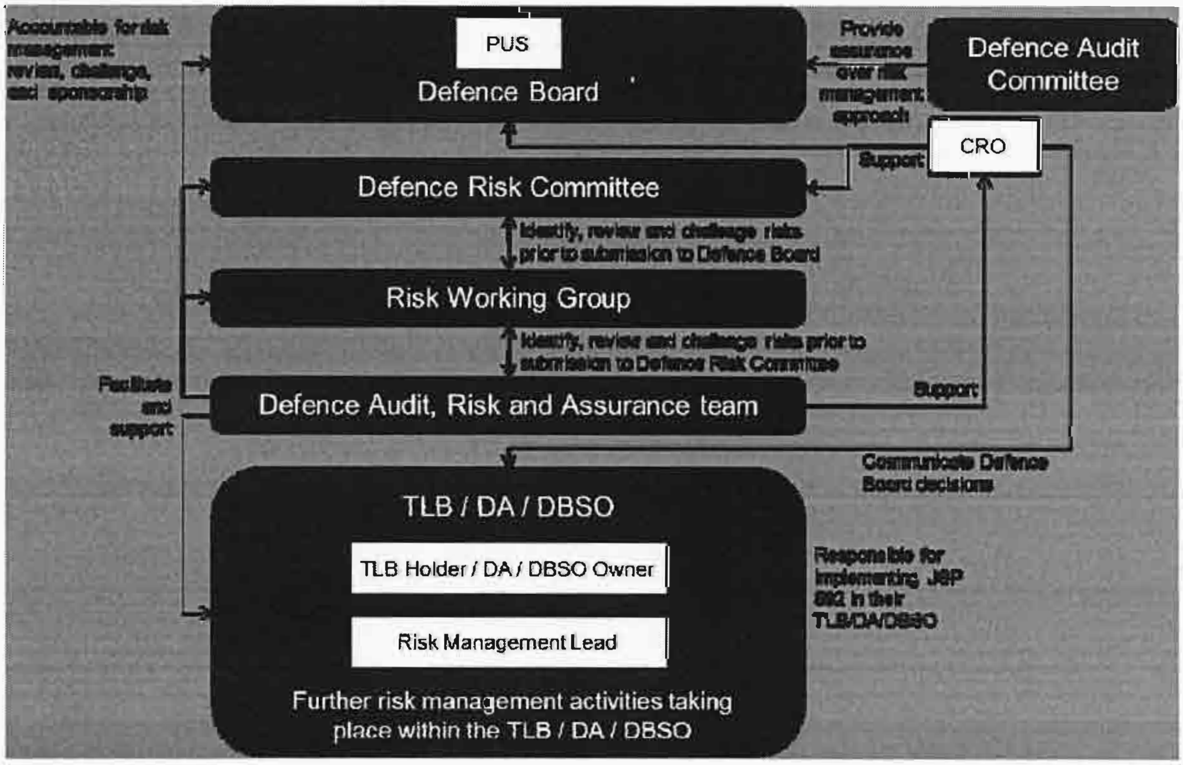
[2] The criteria for escalating risks to the Defence Board is set out in stage 4 of the risk management process.

- A common definition of risk and risk language is used consistently throughout MOD.
- The reporting and escalation of risk information is timely, accurate and provides coverage of the key risks to support relevant decision making at key levels of the Department. Risks identified and reported in other MOD processes will feed into the MOD risk reporting process.
- TLB Holders[3]/DAs are responsible for assuring that the risk management approach is operating effectively in their area and where it is not, rectifying this in a timely basis.
- Each TLB/DA is responsible for identifying and managing risks in its respective part of MOD; reporting and escalation of a risk does not necessarily pass on risk ownership or responsibility for management of that risk.

Governance Structure

12. To successfully embed risk management across MOD, the risk management process is supported by a governance structure that defines roles and responsibilities at each key level of the Department. The diagram below outlines the MOD risk management governance structure.

13. This JSP outlines a framework within which MOD risk management will operate; each TLB/DA must define their own risk management governance structure and risk management process specific to their area's needs and in alignment with this JSP. The TLB/DA roles and responsibilities described below are mandatory; TLB/DAs may choose to have additional risk management roles and responsibilities as appropriate.


Accountable for risk management review, challenge, and sponsorship
PUS
Defence Board
Provide assurance over risk management approach
Defence Audit Committee
CRO
Support
Defence Risk Committee
Identify, review and challenge risks prior to submission to Defence Board
Risk Working Group
Identify, review and challenge risks prior to submission to Defence Risk Committee
Facilitate and support
Defence Audit, Risk and Assurance team
Support
Communicate Defence Board decisions
TLB / DA / DBSO
TLB Holder / DA / DBSO Owner
Risk Management Lead
Further risk management activities taking place within the TLB / DA / DBSO
Responsible for implementing JSP 892 in their TLB/DA/DBSO

[3] Throughout the document the term 'TLB Holder' is used as shorthand and refers to the Heads of the Front Line Commands, DE&S and DIO.

Summary of Risk Management Roles and Responsibilities

Defence Board

14. PUS, supported by the Defence Board, is accountable for ensuring business risks are managed effectively across MOD and for maintaining a robust risk management framework and system of internal control (including owning the Risk Management Policy). PUS is not responsible for military operational risks and this JSP does not apply to the assessment and management of risks associated with the Armed Forces carrying out operations. To support PUS, the Defence Board's responsibilities are to:

1. Promote the effective delivery of the risk management approach (including demonstrating 'tone from the top' through on-going sponsorship, behaviours and communications).
2. Review all key risks submitted to the Defence Board on a quarterly basis:
   a. Challenge the validity of key risks and current response activities.
   b. Approve/reject the proposed approach to manage the risk.
   c. Challenge the completeness of the risk profile submitted.
3. Sign-off revisions to the risk management framework.

Defence Audit Committee (DAC)

15. As part of its wider remit the DAC is responsible for overseeing and scrutinising the effectiveness of MOD's approach to risk management and will:

1. Ensure PUS receives, from appropriate sources (e.g. Defence Internal Audit), a robust and independent view of the adequacy and effectiveness of the risk management process across the Department.
2. Endorse the internal audit plan and review the output of periodic reviews of key risk areas.
3. Assess how management is getting assurance on how risks are being managed and ensure focus on key areas of risk.

Defence Risk Committee

16. The Defence Risk Committee is chaired by PUS and meets on a quarterly basis. Its membership includes: VCDS, DG Fin, DCDS Mil Cap, CDP, CIO and a Board non-executive director to provide independent challenge and oversight. It is responsible for reviewing the risk management information that is consolidated by the Defence Audit, Risk and Assurance (DARA) team and reviewed by the Risk Working Group. The Committee will ensure the risk information is robust, accurate and complete, prior to reporting to the Defence Board (for questions to consider when reviewing risks see Part 2 of this JSP, Appendix D). Key activities are to:

1. Review the reported risks:
   a. Challenge the validity of risks and current response activities.
   b. Approve/reject the proposed approaches to manage the risks.
   c. Challenge the completeness of the risk profile submitted.
2. Confirm or recommend changes to the risk management information that is reported to the Defence Board.
3. Conduct deep dive reviews on risks as appropriate.

Chief Risk Officer (CRO)

17. The CRO is the most senior figurehead for risk management in MOD and the champion of risk management activities and behaviours. Key activities are to:

1. Act as the lead advisor to the Defence Board on risk management.
2. Provide support to Defence Board members, Defence Risk Committee members, TLB holders and DAs on risk management matters, providing high quality expertise and sound advice based on knowledge of the Department's operations, both military and civilian.
3. Challenge the management of MOD's key risks, including existing response activities and proposed further actions.
4. Facilitate and drive management discussions, decisions and strategies on risk at the Defence Board and TLB/DA level.
5. Monitor the performance of risk management across MOD.
6. Ensure appropriate mechanisms and processes are embedded to facilitate the collation of all types of risks across MOD.
7. Ensure that the Defence Board and the Defence Risk Committee receives a comprehensive view of the combined impact of risk that is being taken, and provide assurance that the risks are being actively managed.
8. Chair the Risk Working Group and communicate Defence Board decisions to the TLB/DAs where appropriate.
9. Communicate the importance and value of risk management and be visible as its sponsor.

Risk Working Group

18. The Risk Working Group is made up of Risk Management Leads from the TLB/DAs and is chaired by the Chief Risk Officer. It is responsible for reviewing the risk management information that is consolidated by the Defence Audit, Risk and Assurance (DARA) team, identifying any cross-TLB/DA risks, and allocating risk owners and further actions as necessary. The Group will ensure the risk information is robust, accurate and complete, prior to reporting to the Defence Risk Committee (for questions to consider when reviewing risks see Part 2 of this JSP, Appendix D). Key activities are to:

1. Review the validity of the risks submitted by the TLB/DAs, including ownership of risks and their severity ratings, using the MOD Risk Assessment Criteria.
2. Identify potential gaps in the Department's risk profile and conduct further analysis as appropriate (including cross-TLB/DA risk collation and aggregation).
3. Advise and assure that appropriate risk management actions to address submitted risks are planned, and review the implementation of any previously submitted and agreed actions.
4. Confirm or recommend changes to the risk management information that is reported to the Defence Risk Committee.

TLB Holder / DA

19. Responsible for implementing JSP 892 in their respective area of responsibility and ensuring that an appropriate risk management governance structure, process and activities are in place. Key activities are to:

1. Be responsible for the effective management of risks within their TLB/DA.

2. Review and challenge the scope, quality, completeness and validity of risk information (for questions to consider when reviewing risks see Part 2 of this JSP, Appendix D) submitted by their area to the DARA team in accordance with the defined Defence Board Risk Escalation Thresholds, as set out in Stage 4 of the risk management process.
3. Lead a top-down risk assessment exercise; the frequency should reflect key decision points in the planning and management cycles and should be at least annually.

TLB/DA Risk Management Lead

20. The TLB/DA Risk Management Lead will be appointed by the TLB/DA and may have desk level support. Key activities are to:

1. Actively support and champion the operation of effective risk management, providing risk advice, support and guidance, where required, to individuals and groups, including technical advice on the risk management process.
2. Ensure that the risk management process is being effectively executed, and that it is producing high quality risk information to inform business decision making.
3. Be responsible for collating and submitting robust and timely risk management information to the DARA team.
4. Disseminate top-down risk communications (e.g. from the Defence Risk Committee) to appropriate individuals.
5. Raise awareness and articulate the benefits of risk management.

The Defence Audit, Risk and Assurance (DARA) Team

21. The DARA team is responsible for supporting the operation of the MOD risk management framework. The DARA team reports into the MOD CRO. Key activities are to:

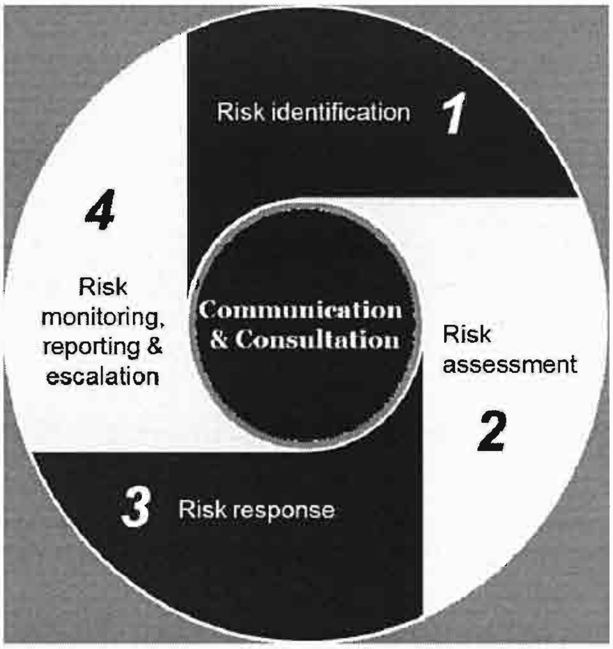
1. Facilitate the Defence Board annual strategic risk assessment exercise by providing research and analysis to help consider the broad range of risks facing the Department.
2. Coordinate risk submissions from TLB/DAs, and produce the Defence Risk Committee and Defence Board risk reports.
3. Provide DAC with updates on the key areas of risk focus.
4. Commission and deliver (as appropriate) risk management training to TLB/DAs. Own the risk management training.
5. Monitor the quality of submitted risk information and the performance of required risk management activities across MOD through quality reviews of reported risk data and conversations with TLB/DA representatives.
6. Review, challenge and provide advice on the quality of risk submissions (including tracking and challenging the status of risk response plans), and conduct further risk analysis e.g. collation and aggregation, as appropriate.
7. Coordinate and participate in the Defence Risk Committee meetings to promote a broad consideration of good practice risk management techniques, key risks / risk areas and identify any additional risks for escalation.
8. Facilitate knowledge sharing with TLB/DAs and act as a centre of excellence for risk management.
9. Raise awareness and articulate the benefits of risk management across MOD.

10. Drawing on practitioners' feedback, drive continuous improvement to the MOD Risk Management Framework by conducting an annual review and update, and update this JSP accordingly.

2 Risk Management Process

1. The risk management process comprises four main stages outlined in the diagram below. This section provides a high level description of the key activities of each stage.

2. Part 2 of this JSP should be used to support the development and embedding of the risk management process in TLB/DAs.


Risk identification
1
Risk assessment
2
3
Risk response
4
Risk monitoring, reporting & escalation
Communication & Consultation

3. Communication and consultation is a key factor in all stages of the risk management process, ensuring appropriate individuals are engaged to promote awareness and involvement e.g. individuals that can contribute to better understanding the nature and details of the risks, those who could be specifically affected by the risks, accountable decision makers and management etc.

Stage 1 – Risk Identification

4. The purpose of risk identification is to identify and describe the risks that could affect objectives and agree appropriate ownership. In doing so, it is necessary to establish the context and environment of the area within scope.

What is a Risk?

5. A risk is an uncertain future event that could affect the Department's ability to achieve its objectives.

Establishing the Context

6. To successfully identify and manage risks, it is important to consider the scope and objectives of the area under review.

Risk Description

7. A well-defined risk description is essential for effective risk management; it allows accurate assessment of, and response to a risk, and consequent prioritisation for action. The risk description must:

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

8. **A risk is:** a combination of a cause, an event and a consequence(s) and the description of a risk must enable a clear understanding of each of these three elements.

Understanding these elements helps inform risk assessment and response e.g. a business disruption event leading to financial loss could be caused by a key supplier failing or a flooded building; the risk severity and controls and mitigating activities applied would therefore differ.

Who Should Identify Risks, When and How?

9. Risk identification should be undertaken at all key management levels and in all parts of the Department. All TLB/DAs should regularly appraise their environment and activities to identify new risks as well as review existing ones. Each TLB/DA should have its own 'bottom-up' view of risk (identifying risk at the lowest levels of the Department and working up), which in turn is escalated, as necessary to the TLB Holder / DA. Additionally, the TLB/DA Boards should conduct a 'top-down' risk identification and assessment exercise (looking across or down from the highest levels of the Department, frequency to be aligned to the TLB/DA planning and management cycles of which it should be a part) to obtain a view of their key strategic risks. Risk identification activities need to cover all aspects of the Department and consider risks to the achievement of objectives as well as emerging risks.

10. A variety of techniques can be used to facilitate risk identification. Exercises to identify risks should involve relevant and/or impacted individuals and those that can provide the greatest insight on the risks in focus and their management, to facilitate open discussion and debate.

Risk Ownership

11. Once a risk has been identified, a Risk Owner must be allocated to provide a single point of accountability for the effective management of the risk. The Risk Owner:

- 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 (it does not need to be the TLB Holder/DA).
- is ultimately accountable for ensuring the identification of any changes to the risk, and that changes are appropriately managed and reported.
- is responsible for determining the risk severity (see Stage 2), developing the risk response and ensuring its implementation (stage 3), and complying with TLB/DA and MOD risk reporting procedures (see Stage 4).

Note: If a risk is identified that should be owned by an individual in another TLB/DA, ownership of the ongoing management of the risk should be transferred to the relevant individual; this needs to be communicated and agreed with the proposed Risk Owner.

12. **Minimum Risk Identification Requirements**

- The Defence Board must conduct a strategic risk assessment exercise as part of the planning and management cycle (at least annually) to determine a 'top-down' view of MOD's key risks.
- Each TLB/DA must provide a 'bottom-up' view of risks on a quarterly basis to the Defence Board by conducting a risk assessment exercise focused on their area and objectives. Only risks that exceed the Defence Board Risk Escalation Threshold (see Stage 4) will be submitted. All other risks do not need to be reported to the DARA team. The TLB Holder/DA will review and approve risks prior to reporting to the DARA team, who will then analyse and consolidate the risks and report them to the Defence Board via the Risk Working Group and Defence Risk Committee.
- Identified risks must be credible and reasonably foreseeable and have an element of uncertainty. This will include consideration of very high impact, low probability risks.
- Risk descriptions must contain a cause, event and consequence(s).
- Each risk must have an allocated Risk Owner.

Stage 2 – Risk Assessment

13. The next stage of the risk management process is risk assessment. Risk assessment should answer the following questions:

- What are the potential impacts of the risk and what is the likelihood of the risk occurring?
- 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?
- Is the level of risk acceptable or does it require further management actions?

Assessing the Impact and Likelihood

14. Risk assessment determines the significance of a risk by considering two factors: the potential impact(s) of the risk if it were to occur and the likelihood of the risk occurring. The impact and likelihood of a risk occurring needs to be measured in a consistent way in order to allow the size/significance of risks to be compared. A defined set of risk assessment criteria are used to allow comparison of risks across MOD (see Appendix A).

15. The MOD Risk Assessment Criteria is based on the impact and likelihood of risks materialising within a five year period. Risks that will not materialise in five years but require action in that time period should be described accordingly (e.g. a decision will need to be made next year to select a supplier, in order to prevent a capability gap in 8 years' time. In this case the risk event is that a supplier is not selected).

16. The Criteria can be tailored to be more relevant and useable to individual TLB/DAs as appropriate; however, when reporting risks to the Defence Board (see Stage 4), the MOD Risk Assessment Criteria must be used. Therefore it is advisable that any specific criteria defined by TLB/DAs are easily translatable or aligned to the MOD Risk

Assessment Criteria to avoid having to repeat assessment activities and introducing inefficiency in the approach.

Inherent, Residual and Target Risk Assessment

17. To understand the nature and potential size of a risk exposure requires its Inherent, Residual and Target risk positions to be assessed. This helps ensure 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.

18. **Inherent risk assessment** is the pre-mitigated assessment of the impact and likelihood of the risk and is based on the assumption that controls and mitigations that are currently in place and have a specific and significant effect on the risk do not exist or do not function as intended. This assessment determines a foreseeable or plausible worst case scenario for the risk.

19. **Residual risk assessment** is the current assessment of the impact and likelihood of the risk, and is based on how it is currently being managed. It assumes that the specific and significant controls and mitigations that are currently in place to manage the risk are working as intended.

20. **Target risk assessment** is the determination of the desired impact and likelihood levels for the risk, based on the amount of exposure the Department is comfortable accepting for the benefits it derives from taking the risk, and the feasibility and cost of further response activities.

21. All risks should be assessed on an inherent, residual and target basis, using the same impact and likelihood criteria. The three assessments, as well as the controls and mitigations, should be captured in a risk register. The risks reported to the Defence Board will be captured in the MOD Risk Reporting template (see Part 2 of this JSP, Appendix C).

22. When identifying and documenting controls and mitigations, the Risk Owner should describe the activities with sufficient detail to ensure they can be understood by all relevant stakeholders in order to allow review and challenge.

Stage 3 – Risk Response

23. Risk response establishes which risks require new or additional management actions, by comparing the residual risk position against the target risk position. A number of response options may be available to manage the risk; consideration should be given to the following five response types when deciding the most appropriate action: Terminate, Treat, Transfer, Tolerate and Take the opportunity (see Part 2 of this JSP for further information).

There are three possible outcomes from the risk response stage:

1. Maintain existing response activities, as residual risk is aligned to target risk or additional management activities are not feasible or cost effective.
2. 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.

3. Increase the level of risk (and hence possible benefits or cost savings) by either relaxing or removing controls and mitigations.

Risk Response Plans

24. Where the residual and target risk assessment positions are not aligned, appropriate response actions will need to be selected, documented in a risk response plan and then implemented in order to bring the residual position in line with the target 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, based on the inherent, residual and target assessments of the risk, and considering key aspects, such as the cost and feasibility of response plan actions.

25. A risk response plan should be developed with sufficient detail to ensure it can be understood by all relevant stakeholders, and the Risk Owner should allocate actions to individuals, as necessary, to ensure its implementation.

Stage 4 – Risk Monitoring, Reporting and Escalation

26. Once the risk response plan has been established and is being implemented, the next stage involves tracking and reviewing the risk to identify changes to it, inform management response, and track progress made against the response plan. Some risks will also need reporting to the Defence Board in line with the Defence Board risk escalation requirements.

Risk Monitoring

27. The Risk Owner should establish the frequency of review and monitoring for each risk, considering the needs of the TLB Holder/DA and other stakeholders, and document the monitoring activities in the risk register.

28. In addition to monitoring individual risks, TLB/DAs should also implement monitoring and review processes as appropriate to track the effectiveness of their risk management process.

Risk Reporting and Escalation

29. Risk reporting must be timely, accurate and reflective of the needs and understanding of the target audience. Risk reporting requirements should be discussed and agreed within each TLB/DA to ensure the risk information provided meets stakeholders' needs, can be integrated into regular management reporting and is aligned to strategic and operational activities.

30. Risk escalation is the upward notification of a specific risk due to: its significance, a change in its status (identified through risk monitoring), or an action to manage it. Note, risk escalation does not transfer risk ownership. Each TLB/DA should establish a process for the escalation of risks to the right level within the TLB/DA, including defined thresholds for risk escalation.

Defence Board Reporting and Escalation Requirements

31. On a quarterly basis the Defence Board will review, challenge (and where

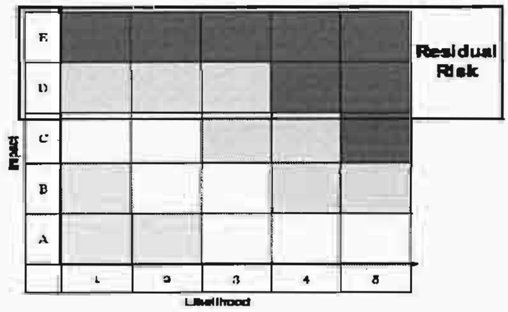
appropriate) provide feedback and guidance on the management of the key TLB/DA risks reported to them. To facilitate this process risks that exceed the defined Defence Board Risk Escalation Threshold (see below) will be submitted to the DARA team via the Risk Management Lead, using the MOD Risk Reporting Template (see Part 2 of this JSP, Appendix C). Note that although risk escalation does not transfer ownership of the risk to the Defence Board, TLB/DAs can request Defence Board action.

Defence Board Risk Escalation Threshold

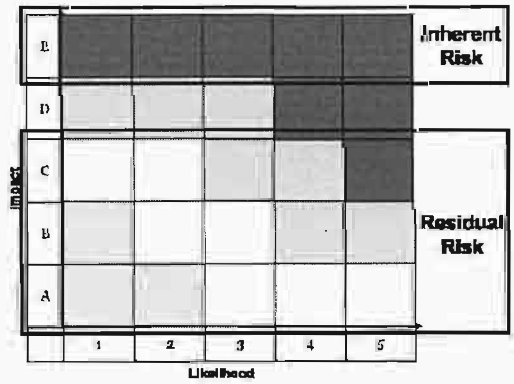
32. The Defence Board Risk Escalation Threshold is based on the MOD Risk Assessment Criteria (see Appendix A). There are five levels of risk impact severity, where E is the most severe, 'critical', and A is the least severe, 'minor'.

33. The risks to be submitted to the DARA team for escalation to the Defence Board are:

- risks with residual impact D or E and



- risks that have inherent impact E and residual impact A, B or C (i.e. a difference of 2 levels or more between the inherent and residual impact).



Ad-hoc Risk Escalation to the Defence Board

34. New risks identified outside of the Quarterly Defence Board Risk Reporting cycle that exceed the defined Defence Board Risk Escalation Threshold should be reported to the TLB/DA Risk Management Lead immediately, who will in turn submit the risk to the DARA team for escalation. For example, as part of routine risk monitoring, a Risk Owner may identify that a risk has deteriorated and subsequently requires escalation. The Risk Owner should immediately submit the risk for escalation and not wait for the next TLB/DA or Defence Board risk reporting cycle.

3 Further Information

Sources of Further Risk Management Information and Support

1. Further information on the MOD risk management framework and other supporting tools can be found through:

- Part 2 of this JSP that contains 'How to' guidance for each stage of the risk management process, and supporting templates.
- The Risk Management intranet page (currently under development).
- Contacting your TLB/DA Risk Management Lead.
- Contacting the DARA risk focal point o[redacted]

2. Please direct any requirements for training support to the DARA team. Work is currently underway to develop a MOD-wide risk management training course.

3. Your TLB/DA Risk Management Lead and the DARA team can also be contacted with any feedback on the MOD risk management framework and other supporting tools.

APPENDIX A – MOD RISK ASSESSMENT CRITERIA

The impact and likelihood of a risk occurring must be measured in a consistent way in order to allow the size/significance of risks to be compared. The MOD Risk Assessment Criteria measures risk impact and likelihood against five levels of severity and should be used, as a minimum, to assess all risks (on an inherent, residual and target basis) submitted to the Defence Board, although TLB/DAs are encouraged to use the criteria for the assessment of all risks.

Risk Assessment Likelihood Criteria

The below criteria should be used for measuring the likelihood of a risk occurring within the next five years.

The likelihood can be measured using any of the 3 likelihood criteria shown below: the probability percentage, the perceived approximate frequency, or based on how commonly it has occurred in the past. Note that based on the specific risk being assessed, one measurement scale may be more applicable than the others.

Where multiple scales are applicable, the assessment should be based on the scale with the highest likelihood. For example, if a risk has never occurred in MOD history but has a 30% probability of occurring, then the likelihood assessment should be documented as 3.

	Likelihood	Probability	Approximate frequency	Description
5	Very high	> 90%	Occurs at least once every 5 years	Is a common occurrence in MOD
4	High	51 - 90%	Occurs once every 5 - 10 years	Has occurred within MOD many times
3	Medium	26 - 50%	Occurs once every 10 - 20 years	Has occurred in MOD on several occasions
2	Low	11 - 25%	Occurs once every 20 - 50 years	Has occurred on a small number of occasions in MOD's history
1	Very low	≤10%	Occurs less than once every 50 years	Has occurred once / never in MOD history

Risk Assessment Impact Criteria

The below criteria should be used for measuring the total potential impact(s) of a risk, if it were to occur (not in-year only).

Where multiple impact areas are applicable, the assessment should be based on the area with the highest impact. For example, if a risk has a potential reputational impact of E and a financial impact of C, then the impact assessment should be documented as E.

	Financial	Reputational	Impact on outputs / capability	Health, safety & environment (not as a result of hostile action)
E Critical	[redacted]	[redacted]	[redacted]	[redacted]

D Severe	[redacted]	[redacted]	[redacted]	[redacted]

C Major	[redacted]	[redacted]	[redacted]	[redacted]
B Moderate	[redacted]	[redacted]	[redacted]	[redacted]

A Minor	[redacted]	[redacted]	[redacted]	● [redacted]

APPENDIX B – MOD RISK CATEGORIES

The MOD Risk Categories can be used as a guide to ensure a broad range of risks are considered during risk identification exercises. Additionally, the categories will be used by the DARA team to conduct risk consolidation and reporting analysis.

When assigning a category to a risk, assign it to the cause or event of the risk, not the consequence.

Risk Category and associated core MOD function	**Description** Any risks whose cause is related to…
Strategic, i.e. Direct	How MOD is managed, strategy, policies and compliance
Operational, i.e. Operate	Military operations
People, i.e. Generate and Develop	Recruitment, retention, training and development, engagement, culture and behaviour of military and civilian personnel
Capability, i.e. Acquire	The acquisition of equipment, systems and other items that the armed forces need
Infrastructure, i.e. Enable	All support services
Finance, i.e. Account	The accounting and reporting of defence activity and spending to Parliament and the public

APPENDIX C – RISK MANAGEMENT GLOSSARY

Term	Definition
Action owner	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.
Cause	The first part (of 3) of a structured risk description. It is the source or driver of the risk event e.g. the underlying conditions, circumstances or activities that could lead to a risk event occurring.
Consequence	The third part (of 3) of a structured risk description. It is the possible effects that the risk event would have on the achievement of objectives.
Control	An activity or measure that is expected to reduce the likelihood of a risk event occurring.
Emerging risk	New or evolving risks that are difficult to characterise or assess at this point in time due to limited information being available and/or prior experience of managing the risk.
Escalation	Required upward notification to a specified person or group of a specific risk, a change in its status or an action to manage it. Note risk escalation does not transfer risk ownership.
Frequency	The number of times it is expected that a risk event will occur over a specified period of time.
Impact	Estimate of the potential effect(s) of the consequences of a risk on the achievement of objectives and protection of values. Often assessed using a standardised scale that measures the impact of the risk on a range of Departmental assets e.g. finances, reputation etc.
Inherent risk assessment	Assessment of a risk's pre-mitigated likelihood and impact, i.e. when existing controls and mitigations that have a specific and significant effect on management of the risk are either not in place or fail when needed or fail to work as intended, in a manner that is credible and reasonably foreseeable. Inherent risk can be considered to be 'the reasonably foreseeable worst case scenario' for the risk.
Issue	An issue is an unplanned event or situation that has already occurred, or will definitely happen, which is certain to affect the achievement of business objectives. An issue must be addressed to negate or minimise its impact(s) on objectives.
Key Risk Indicator (KRI)	Information points and metrics that, when tracked, can provide early warning of a change in the status of a risk, allowing interventions to be made to avoid the risk occurring or reduce its impact. KRIs are leading in nature (i.e. telling you what could happen) and provide the opportunity to identify potential changes in a risk sufficiently far in advance to enable its effective management. The use of KRIs is not mandatory.
Likelihood	Estimate of the probability or frequency of a risk occurring in a specified time period, based on the description of its cause, event and consequences.
Mitigation	An activity or measure that is expected to reduce the impact of a risk event should it occur.
Near miss	A 'Near-Miss' is a risk event or set or circumstances that had the potential for significantly more severe consequences than were actually experienced e.g. jets coming into dangerous proximity but a mid air collision was narrowly avoided.

Opportunity	An uncertain future event that could positively impact the Department's ability to meet or exceed its objectives.
Probability	A numerical description of the chance of a risk event occurring, usually described as a percentile figure. Note this is different to likelihood; likelihood is a broader term that encompasses probability, but also includes qualitative descriptions of the chance of a risk event occurring.
Residual risk assessment	Assessment of the current likelihood and impact, i.e. based on how a risk is currently being managed, assuming that the specific and significant controls and mitigations that are currently in place and have a direct effect on the likelihood or impact of the risk are working as intended.
Risk	An uncertain future event that could have an effect on the achievement of objectives. A risk consists of a cause, an event and consequence(s), and its magnitude is often expressed as a product of its impact and likelihood.
Risk aggregation	Grouping of risks which have a common cause or interdependency and when considered together have a greater impact than when considered separately e.g. failure of a common supplier to multiple projects.
Risk appetite	An expression of the types and amounts of risk the Department is willing or not willing to take or accept to achieve its objectives and aims to supports consistent, risk informed decision making across Defence. The articulation of risk appetite is not mandatory.
Risk assessment	Second stage of the risk management process that aims to determine the size / significance of a risk from an estimation of the likelihood of the risk occurring and the impact of the risk should it occur using a predetermined criteria.
Risk assessment criteria	The criteria used to determine the likelihood and impact level of risks, to ensure all risks are measured consistently and objectively.
Risk categories	Defined groupings of risk according to common qualities such as their nature and origin, cause or consequences. MOD risk categories are defined according to their origin and can be used to support consideration of a broad range of risks and used for Defence Board risk reporting analysis.
Risk collation	Grouping of risks that have the same or similar qualities e.g. by risk category, by common cause, event or consequence. Supports risk analysis and reporting activities.
Risk description	A description of the cause, event and consequence(s) of the risk to enable likelihood and impact to be assessed and effective controls and mitigations to be determined.
Risk event	An incident or occurrence arising from a cause, that could have consequences affecting the achievement of objectives.
Risk exposure	The amount of risk facing the Department (or TLB/DA, business unit, project etc.) at a point in time from a single risk event or multiple risk events.
Risk identification	First stage of the risk management process to determine all the risks that could significantly affect the achievement of objectives, based on consideration of the Department, its strategy and objectives, its operations, its resources and the external environment in which it exists
Risk owner	An individual who acts as the single point of accountability for ensuring the effective management of the risk.

	The risk owner should have an appropriate level of knowledge of the risk and the authority to be able to ensure the risk is managed sufficiently.
Risk profile	A population of identified and assessed risks that together represent the majority of key risks faced by an organisation and/or its subsidiary components at a point in time.
Risk register	A repository for capturing and recording risks and associated information.
Risk response	The approach / action / decision taken on how to manage a risk where the residual risk position does not align to the target risk position. There are five types of Risk response: terminate, treat, transfer, tolerate and take the opportunity.
Risk response plan	The additional activities planned to further reduce the likelihood and/or impact of a risk beyond its current residual position. Plans detail specific deliverables, accountabilities and timelines for completion.
Severity	A measure of the risk's importance. It is used to compare the relative size/ significance of risks and is determined by combining the likelihood and impact of the risk.
Take	Action taken to exploit an opportunity; undertaking an action or managing a set of circumstances to increase the likelihood of realising a positive outcome or upside.
Target risk assessment	Target risk assessment is the determination of the desired impact and likelihood levels for the risk, based on the amount of exposure the Department is comfortable in accepting for the benefits it derives from taking the risk, and the feasibility and cost of further response activities.
Terminate	Exiting the activities giving rise to risk as the risk is unacceptable. Avoiding / eliminating the risk by deciding not to start or continue with the activity that gives rise to the risk, or by doing something differently e.g. substitution of an alternative step or activity.
Tolerate	No action is taken to affect risk likelihood or impact. This means the current risk exposure is accepted. This usually results from taking the risk in order to pursue an opportunity or achieve a benefit/return, or retaining the risk by informed decision.
Transfer	Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk with another party. Common techniques include outsourcing activities to the private sector or purchasing insurance products (Note: transferring does not necessarily eliminate or remove accountability or the effects of the risk e.g. outsourcing a process may not reduce the reputational impact to MOD if something goes wrong).
Treat	Action taken to reduce risk likelihood or impact, or both through: • Changing the likelihood through implementing additional controls, or • Changing the potential impacts through implementing additional mitigations.
Trend	The outlook for, or expected change in, the exposure of a risk over a given time period e.g. increasing, decreasing, stable.

Ministry of Defence

JSP 892 Risk Management

Part 2: Guidance

JSP 892 Pt 2 (V1.0 Jul 15)

Foreword

Part 2 of this JSP provides guidance in accordance with the policy set out in Part 1 of this JSP; the guidance is sponsored by PUS. It provides policy-compliant business practices which should be considered best practice in the absence of any contradicting instruction. However, nothing in this document should discourage the application of sheer common sense.

Preface

How to use this JSP

1. JSP 892 sets out the mandatory requirements for risk management activities within MOD. It provides a common approach to risk management for use by all members of the Department, as appropriate to their roles. This JSP will be reviewed annually.

2. The JSP is structured in two parts:

a. Part 1 - Directive, which provides the direction that must be followed in accordance with statute or policy mandated by Defence or on Defence by Central Government.

b. Part 2 - Guidance, which provides the guidance and best practice that will assist the user to comply with the Directive(s) detailed in Part 1. This guidance is aimed at practitioners, subject matter experts and individuals with specific risk management responsibilities in the Department, though will be useful to anyone who wishes to understand more about MOD's approach to risk management.

Coherence with other Defence Authority Policy and Guidance

3. Where applicable, this document contains links to other relevant JSPs, some of which may be published by different Defence Authorities. Where particular dependencies exist, these other Defence Authorities have been consulted in the formulation of the policy and guidance detailed in this publication.

Related JSPs	Title
JSP 525	Corporate Governance
JSP 503	MOD Business Continuity Management

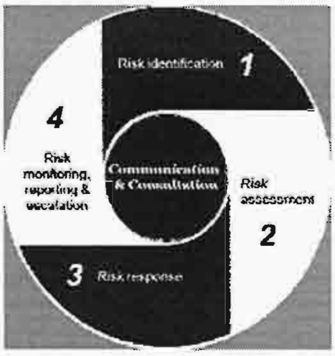
Further Advice and Feedback – Contacts

4. The owner of this JSP is PUS. For further information on any aspect of this guide, or questions not answered within the subsequent sections, or to provide feedback on the content, contact:

Job title/e-mail	Project focus	Telephone
Director Defence Audit, Risk and Assurance	N/A	[redacted]

Contents

1 How to Conduct Risk Identification


Risk identification 1
4
Risk monitoring, reporting & escalation
Communication & Consultation
Risk assessment
2
3 Risk response

Summary

A. Establishing the Context
B. How to Identify Risks
C. How to Describe and Capture Risks
D. Approaches to Identifying Risks
E. Risk Categories
F. Tips for Identifying Risks

1. This section explains how to identify a risk, which includes establishing the context of the area under review, identifying and characterising the risks that could affect objectives and agreeing appropriate risk ownership.

A. Establishing the Context

2. Establishing the context is about 'setting the scene' to provide focus, insight and ideas in support of risk identification, and should be performed as a precursor to identifying risks.

The approach described below highlights typical areas to consider when establishing the context.

Review and Understand Objectives and Values

3. Consideration should be given to the MOD Strategic Objectives, your TLB[1]/Defence Authority (DA) Strategic Objectives and how these are further cascaded to your team's objectives. Any uncertain future event that could affect the achievement of an objective, partly or completely, should be identified as a risk if it is credible and foreseeable.

4. **Establish the Internal and External Context**

- Review the internal environment in which the Department/TLB/DA operates and seeks to achieve its objectives. For example, consider core processes, activities and dependencies, or changes to the Department's structures and ways of working, e.g. a transformation programme or entry into new theatres/operations.
- Consider how key external drivers, trends and changes can impact the achievement of objectives. For example:
  - the decisions of key stakeholders (e.g. Treasury)
  - the geopolitical environment
  - the economy
  - the defence industry and supply chain, and
  - regulatory requirements.

[1] Throughout the document the term 'TLB' is used as shorthand and refers to the Front Line Commands, DE&S and DIO

B. How to Identify Risks

5. The risk identification stage provides a structured approach to understand how the objectives identified in establishing the context may be affected by risk. This is done by generating and recording a comprehensive list of risks.

What is a Risk?

6. A risk is an uncertain future event that could affect the Department's ability to achieve its objectives. A risk:

- is forward-looking (not a current issue)
- has an element of uncertainty
- could affect the achievement of objectives
- must be credible and foreseeable, and
- can have both positive and negative effects.

7. A risk leading to a potentially positive impact on objectives is classified as an Opportunity. Please note that this Guidance focuses on the identification and management of risks that can have a negative (downside) impact on objectives; however, the same process and activities can be applied to identifying and managing opportunities (upside).

C. How to Describe and Capture Risks

8. The risk description must be sufficiently detailed and precise so that it is possible to determine whether the risk has actually occurred or not at a point in time, and to enable an accurate assessment of its impact and likelihood, as well as decisions on its response to be made.

9. **A risk is:** a combination of a **cause**, an **event** and a **consequence**. The description of a risk must enable understanding of these three components.

Cause
- Causes are the sources of the risk event – the reason why the risk could happen. These can include conditions, circumstances, drivers, and activities that may result in the risk event occurring.
- Causes can be internal or external to MOD.

Risk Event
- Incidents or occurrences that arise from a cause that could have an effect on the achievement of objectives, or cause harm or loss.
- Consider events that can happen that may impact people, processes, systems, assets and the external environment in your analysis.

Consequence(s)
- Effects arising from the risk event, if it occurs, that could affect the achievement of objectives.
- Measured through estimating the impacts on assets and objectives, e.g. finances, reputation, ability to deliver outputs/capability.

Risks should be captured in a risk register (a repository for capturing risk information).

Example Risk Structure and Descriptions

10. "As a result of <cause>, <**an uncertain future event**> may occur, which could lead to <consequence(s) on objectives>"

Note the below are example risks and are not intended to depict actual MOD risks.

Failure of the base inventory system at site X results in the permanent loss of inventory data in TLB Y**, due to poor system maintenance**	- Impact on outputs / capability
Insufficient investment in effective cyber security allows a third party to gain illegal access to the MOD network to misappropriate operationally sensitive data, leaking information on the internet, putting X number of personnel at risk and resulting in severe reputational damage	- Health, safety & environment - Reputational
Failure to sign contract X by agreed deadline causes supplier Y to pull out of the arrangement and delays the activity launch of project Z by 2 months	- Financial - Impact on outputs / capability
A significant improvement in the UK economy combined with civil servant/military salary freezes causes a 20% loss of staff from Operational Pinch Points in TLB X, leading to the inability to meet standing commitment Y	- Impact on outputs / capability (Manpower)

D. Approaches to Identifying Risks

11. Risks can be identified through a number of approaches. A combination of 'top-down' (looking across or down from the highest levels of the Department) and 'bottom-up' (identifying risk at the lowest levels of the Department and working up) risk identification is required to ensure a complete understanding of the Department's risk profile.

12. A common risk identification approach involves conducting interviews to capture relevant TLB/DA members' views on risks to their area of the Department. The interviewer then collates and analyses all the risk information and facilitates a broader team workshop to debate the risks and their prioritisation. The MOD Risk Categories (see section E and Appendix B) should also be used as a prompt to help consider of a wide range of risks.

Risk Identification Timeline

13. Defining the time period during which a risk could occur is important as it will influence what risks are identified, and how they are assessed e.g. the risks identified and their associated severities when considering a 12 month timeframe are likely to be significantly different compared to those over a 10 year timeframe. Risks escalated to the Defence Board should be considered in the context of the risk materialising within a five year period. TLB/DAs may choose to use a timeframe more appropriate to them (e.g. the timeframe for a project will be the duration of the project), when not submitting risks as part of the Defence Board risk reporting.

14. Identifying risks that could occur over a longer time period is often described as identifying emerging risks. By their nature, these risks are often less well understood or characterised at this time and not typically captured in bottom-up risk assessment exercises, as data may not currently exist to facilitate their understanding. Additional techniques, such as horizon scanning (e.g. a specific exercise focused on identifying risks that may emerge outside of the period which is the focus for the standard identification exercise) can provide a more effective approach and should be considered on at least an annual basis as a corollary to the standard 'event' driven risk identification techniques.

15. Once a risk has been identified, a Risk Owner must be allocated to provide a single point of accountability. The Risk Owner is responsible for ensuring the effective management of the risk.

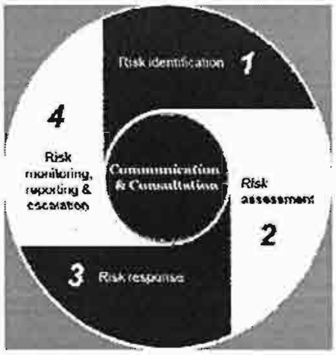
E. Risk Categories

16. When identifying risks, the MOD Risk Categories (see Appendix B) are a useful tool to help ensure a broad range of different types of risks are considered, as well as facilitate risk analysis. Risks submitted as part of the Defence Board risk reporting must reference the MOD Risk Categories.

F. Tips for Identifying Risks

- Do not identify an issue as a risk – an issue is already happening or has happened, therefore has no uncertainty and so is not a risk.
- When considering risks to achieving objectives, do not simply describe the opposite of the objective.
- Some risks can have a very low likelihood of occurrence, but remember they must be credible and foreseeable to be identified and captured.
- Be as specific as possible in describing risks.
- When identifying risks, consider near misses. A near miss is a risk event or set of circumstances that had the potential for significantly more severe consequences than were actually experienced e.g. jets coming into dangerous proximity but a mid air collision was narrowly avoided, a fatality that could have resulted from an equipment failure but no one being injured this time.
- When identifying risks, try to involve not only people in your immediate team but other stakeholders that have insight into the risk or could be affected by it, as they can often provide helpful views on your risks.
- Remember not to state impacts as risks, use the cause, event, consequence approach to describe the risk properly.
- Consider any dependencies, milestones, activities, timescales and resources (such as people, assets and technology) that will be used to achieve objectives.
- Use existing risk registers as a prompt only after your first attempt at identifying risks, otherwise there is the danger that these will stop creative thinking and become your risk profile. Use the risk categories to challenge that all areas of risk have been considered.
- When identifying risks, do not limit yourself to risks that have already occurred in the past, but consider risks that may occur in the future for the first time or have been experienced by other organisations or nations.

2 How to Assess Risks


Risk identification
1
Risk assessment
2
3
Risk response
4
Risk monitoring, reporting & escalation
Communication & Consultation

Summary

A. Understand the Size/Significance of the Risk
B. Risk Assessment Criteria
C. How to Assess Inherent, Residual and Target Risk
D. Worked Example of a Risk Assessment

1. A consistent basis for assessing risk is required to allow reliable measurement and comparison of risks, inform our focus on the most significant risks, and prioritise our investment in resources for their management. It also helps determine who needs to be notified of the existence of a risk and the approach needed to monitor it.

A. Understand the Size/Significance of the Risk

2. Risk assessment determines the significance of a risk by considering two factors: the potential impact(s) of the risk if it were to occur and the likelihood of the risk occurring.

Impact

3. The impact of a risk is established by considering its potential effects on the achievement of Departmental objectives. As objectives can vary widely in their nature and significance, a standard measurement scale is typically used to consistently evaluate risks. The risk description will provide a summary of the risk consequences; their impact on objectives can be measured using defined quantitative and/or qualitative criteria.

Likelihood

4. The likelihood of a risk occurring is determined by estimating the probability or expected frequency of the risk occurring in a given timeframe, and is reflective of the risk description (its cause, the risk event and consequence(s)). The likelihood can be expressed in both qualitative and/or quantitative terms.

B. Risk Assessment Criteria

5. A defined set of risk assessment criteria should be used to assess risks, to allow like-for-like comparison. The MOD Risk Assessment Criteria measure risk impact and likelihood against five levels of severity using the following areas:

Impact: Financial, reputational, impact on outputs/capability, and health, safety & environment.

Likelihood: Percentage probability of occurrence, qualitative descriptors, frequency of occurrence in a five year period.

The MOD Risk Assessment Criteria can be found in Appendix A.

C. How to Assess Inherent, Residual and Target Risk

6. Understanding the true nature and potential size of a risk exposure requires its Inherent, Residual and Target risk positions to be assessed, considering the effects of controls and mitigations.

7. Controls are activities and measures that reduce the likelihood of a risk occurring. Mitigations are activities and measures that reduce the impact of a risk, should it occur.

Note: there are several different types of controls (e.g. detective, preventative, directive and monitoring – further guidance is available in section D); consideration should be given to the most appropriate types and combinations of controls to best manage a risk.

Inherent Risk Assessment

8. The assessment of risk on an inherent basis involves the assessment of the pre-mitigated impact and likelihood of the risk. This is based on the assumption that controls and mitigations that are currently in place and have a specific and significant effect on the risk do not exist or do not function as intended. This assessment determines a foreseeable or plausible worst case scenario for the risk.

Why Assess Inherent Risk?

9. Assessing risk on an inherent basis provides a view of how bad a risk could be if the existing controls and mitigations in place did not exist or do not work as intended. This is important as, when compared to the residual risk exposure, it provides an understanding of the amount of reliance being placed on current response activities, focusing scrutiny and challenge by management on their effectiveness and adequacy in light of potential worst case consequences. Where there is significant reliance on the existing controls and mitigations, the effectiveness of these controls and mitigations, and the Department's compliance with them should be tested on a regular basis.

Residual Risk Assessment

10. The assessment of risk on a residual basis involves the assessment of the current impact and likelihood of the risk based on how it is currently being managed. It assumes that the specific and significant controls and mitigations that are currently in place to manage the risk are working as intended.

Why Assess Residual Risk?

11. Residual risk assessment tells us the current severity of a risk's exposure if existing controls and mitigations to manage it are in place and working as intended. In addition to helping direct the focus of management towards those that are most significant (after taking response activities into account), the difference between inherent and residual also helps inform the assurance focus and determines the reporting/escalation requirements.

Target Risk Assessment

12. The assessment of risk on a target basis involves the determination of the desired impact and likelihood levels for the risk, based on the amount of exposure the Department is comfortable in accepting for the benefits it derives from taking the risk, and the feasibility

and cost of further response activities. It is not always desirable or possible to try to avoid or reduce some types of risk; the objective of risk management is to ensure that the right benefits are achieved in return for taking/accepting certain types of risks.

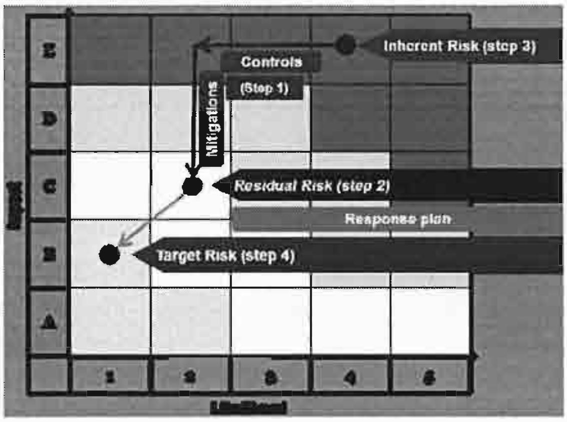
13. Target risk is a proxy for risk appetite, at an individual risk level. Risk appetite is an expression of the types and amounts of risk an organisation is willing to take or accept as it seeks to achieve its objectives and aims to support consistent, risk informed decision making.

The articulation of an organisation's risk appetite can provide decision makers with an understanding of the type and amount of risk that is acceptable/unacceptable, to ensure that the right risks are being taken for the right ,benefits. MOD does not use risk appetite; however if TLB/DAs would like further information on its use, they should first contact the DARA team.

Why Assess Target Risk?

14. Determination of target risk positions allows understanding of whether current residual risk positions are acceptable or require further management action.

The illustration below shows the three different risk positions (inherent, residual and target) and the effect of the controls and mitigations:



How to Assess a Risk

15. Once a risk has been identified and appropriately described (cause, event and consequence(s)), the following steps should be carried out, to assess the severity of the risk.

16. Step 1 – Establish the controls and mitigations currently in place

Detail all significant controls and mitigations that are specifically applied to actively manage the risk at present and consider their effectiveness:

- What component(s) of the risk do they affect, how and by how much e.g. fully prevent a cause leading to an event?
- Are they independent or rely on other processes or activities to work?
- How reliable are they - could they fail or not be available when needed? If so how often will this be the case?

- What are their limitations - will they only work up to a certain threshold of risk severity?
- If one fails is there back up?

Where a new risk is identified, there may not be any controls or mitigations in place.

Note: The focus should be on the identification of controls and mitigations that are specifically in place to manage the risk and have a significant effect on its management. Generic informal activities, e.g. calling the fire brigade if there is a fire, should not be included.

17. Step 2 – Assess the residual position

Taking account of controls and mitigations, estimate the residual risk size. What are the likelihood and impact values of the described risk occurring based on the effectiveness of the controls and mitigations considered in the previous step? Consider:

- How often does the risk cause occur that could lead to the described event and consequence? E.g. is it always in the background or periodic?
- The reliability of the controls working as intended; are they always in place and effective?
- The effectiveness and reliability of mitigations.

18. Step 3 – Assess the inherent position

What would the likelihood and impact of the described risk be if all current controls and mitigations did not exist? Consider:

- All the controls and mitigations already captured in step one, the effect they would have on the risk (step 2) and imagine none of them were in place.
  - What could happen?
  - How severe could the impact be and what is the credible worst case scenario for the risk?
- How likely is it that the risk would occur? Is the likelihood the same as the cause? I.e. is it constant or intermittent?

19. Step 4 – Assess the target risk position

Is the current residual risk position acceptable or are the desired impact and likelihood values different? When establishing the target risk position, the following should be considered:

- What are the benefits and opportunities presented by taking the risk? Do they justify the size of the exposure?
- Is the current risk position 'unacceptable'? Given the feasibility and cost of actions to reduce the position, what is acceptable for this risk?
- How important is the objective that the risk could impact?
- Are there internal rules and policies related to the risk area?
- Are there external regulatory and legal requirements that MOD must comply with?

Stakeholders affected by the risk should be consulted when establishing the target position.

D. Worked Example of a Risk Assessment

20. **Risk:** A downturn in the UK economy causes Company X, the only supplier of critical equipment Y to become insolvent, resulting in significant disruption to operations

21. Step 1 – Establish the controls and mitigations currently in place

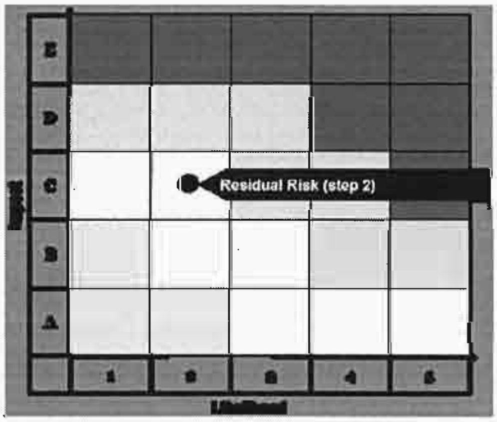
Controls (reduce the likelihood):

- Financial due diligence during supplier selection
- Monthly operational KPI checks
- Regular contact of sourcing staff with supplier

Mitigations (reduce the impact if the risk were to occur):

- Business continuity planning has identified an alternative provider and describes a process for transition
- Spares are warehoused

22. Step 2 – Assess the residual position

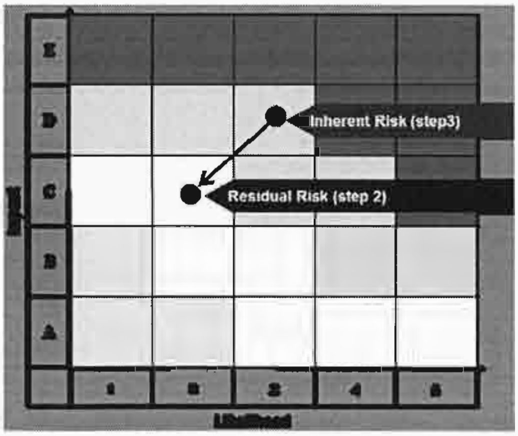


The residual risk position: C2

This is taking the following controls and mitigation information into consideration:

- Warning signals are identified but the lead time provided does not allow us to fully avoid disruption to operations.
- Alternative supplier experiences teething troubles in exactly understanding our needs and scaling up to meet demand and spares are exhausted in this time resulting in some disruption being suffered.

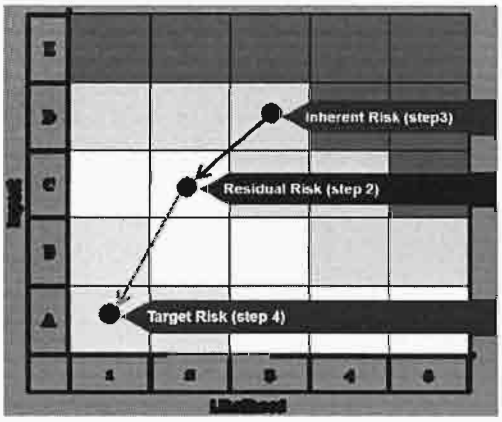
23. Step 3 – Assess the inherent position



The inherent risk position: D3

Insolvency comes as a complete surprise and results in total disruption of X operational activities at the facility for 3 months before an alternative supplier can be sourced and production resumed.

24. Step 4 – Assess the target risk position



Considering the residual risk position, the impact and likelihood is not acceptable.

Target Risk: A1

3 How to Respond to Risks

Risk identification
1
4
Risk monitoring, reporting & escalation
Communication & Consultation
Risk assessment
2
3
Risk response

Summary

A. Evaluating the Need for Risk Response
B. How to Prioritise the Risks that Require a Response
C. Identifying and Selecting Risk Response Options
D. Developing a Risk Response Plan

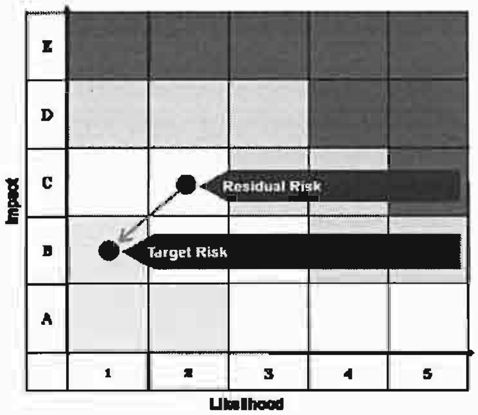
1. The purpose of risk response is to establish which risks require new or further management action by comparing the residual risk position against the target risk position. Where the two assessment positions are not aligned, appropriate actions will need to be selected and implemented to bring the residual risk position in line with the target risk position.

A. Evaluating the Need for Risk Response

2. Once the target risk position has been established, it should be compared against the residual risk position in order to understand if a risk response is required. There are three possible outcomes:

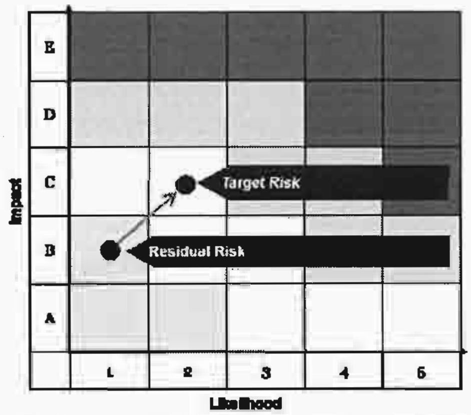
i. The residual risk score is greater than the target risk score

3. **Action required:** Reduce the level of risk exposure to an acceptable level by developing and implementing a Risk Response Plan that will reduce the risk exposure to the target position.



ii. The residual risk score is smaller than the target risk score (e.g. the risk is over controlled)

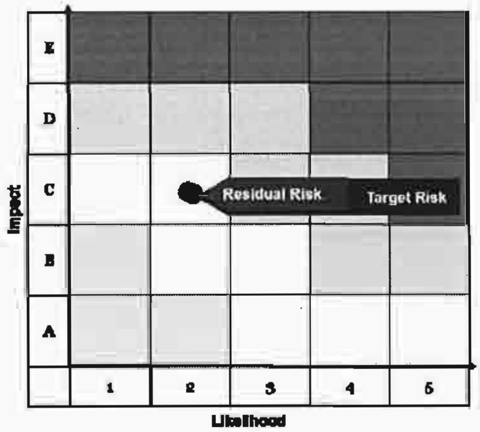
4. **Action required:** Consider increasing the level of risk exposure by relaxing or removing controls and mitigations until risk exposure is aligned with target position. This can realise cost savings on existing responses, but should always be thoroughly evaluated and signed-off by appropriate management before enacting.



Note: Where the benefits or returns for taking the risk are attractive, an increase in exposure by taking more of the risk is also an option, e.g. concentrating supply with a third party to secure better terms.

iii. The residual risk score is the same as the target risk score

5. **No further action required:** Maintain and monitor existing controls and mitigations as residual risk is aligned to target risk. No response plan required.



B. How to Prioritise the Risks that Require a Response

6. If multiple risks require a response, it may be necessary to prioritise the order in which the risks are managed due to time and resource constraints. The following points should be considered when prioritising risks for response:

- Risks that have the greatest residual risk impact. Likelihood should be a secondary consideration after impact for prioritisation as it can be the more subjective measure in risk assessment.
- Risks with the largest difference between residual and target risk positions.
- Risks with a large difference between inherent and residual, where management want more levels of control as current controls may not be reliable.
- Consideration of feasibility, cost, resources and time required to further manage the risk (see section C below).
- The prioritisation / importance of the objective that will be affected, should the risk occur.
- Risk owners and TLB/DA management priorities and focus.

C. Identifying and Selecting Risk Response Options

7. A risk response needs to be considered for all risks where the residual risk position is greater than the target risk position (example A.i. above) and the Risk Owner and/or respective management decides whether and what risk response is required to manage the risk. The Risk Owner should evaluate risk responses based on a consideration of their effectiveness, cost and feasibility.

8. Risk response options can be grouped into the following types:

Risk response type	Examples
Terminate Exiting the activities giving rise to risk as the risk is unacceptable	- Avoiding/eliminating the risk by deciding not to start or continue with the activity that gives rise to the risk, or by doing something differently e.g. substitution with an alternative step or activity.
Treat Action taken to reduce risk likelihood or impact, or both	- Changing the likelihood through implementing additional controls. - Changing the potential impacts through implementing additional mitigations.
Transfer Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk	- Common techniques include outsourcing activities to the private sector or purchasing insurance products (Note: transferring does not necessarily eliminate or remove accountability or the effects of the risk e.g. outsourcing a process may not reduce the reputational impact to MOD if something goes wrong).
Tolerate No action is taken to affect risk likelihood or impact. This means the current risk exposure is accepted	- Taking the risk in order to pursue an opportunity or achieve a benefit/return. - Retaining the risk by informed decision.
Take the opportunity Action taken to exploit an opportunity	- Undertaking an action or managing a set of circumstances to increase the likelihood of realising a positive outcome or upside.

9. Where Treat is selected as the appropriate risk response type, consideration should be given to the different types of controls and mitigations available and the overall control environment created to manage the risk. The following factors should be considered:

- Effectiveness of the proposed response in actually reducing the likelihood and/or impact of the risk.
- Efficiency of the proposed response compared to other options (e.g. automated vs manual controls):
  - Automated controls are controls that are designed to operate automatically (without intervention) and are generally more reliable and resource efficient than manual controls.
  - Manual controls are controls designed to operate using human involvement and interpretation (and are therefore exposed to human error).
- Reliability of the proposed controls and mitigations i.e. could it fail when needed or not work as intended – if so how likely is this?

- The type of control required. Should the controls be preventative or detective, transactional or entity level? Typically a combination of all 4 types creates the most robust control environment:
  - Preventative controls are designed to prevent risks from materialising in the first place (e.g. authorisations / approvals).
  - Detective controls are designed to detect risks that have materialised (e.g. comparison with actual results against budget, investigation of exception reports).
  - Transactional controls are controls designed to be ordinary activities that are undertaken as part of day-to-day operation.
  - Entity level controls are dependent on the culture and behaviours, determined by the tone from the top of an organisation.
- Efficiency and reliability of multiple proposed controls and mitigations options working together.
- Cost and resource requirements of the proposed response.
- Timeframe to implement the response compared to how rapidly a response is needed:
  - Are there quick wins that are very effective, reliable and/or an efficient risk response option with low resource/cost requirements?
  - Is it necessary to develop a high cost but highly effective, reliable and/or efficient response option?
- TLB/DA's ability to implement the proposed response i.e. is it feasible?

Obtaining a better understanding of the existing controls / mitigations, and fine tuning them, may well be the most effective course of action to improve how a risk is addressed.

D. Developing a Risk Response Plan

10. A risk response plan should be prepared once the risk response options have been assessed, prioritised and the appropriate risk response(s) determined.

11. The plan should be reviewed by the Risk Owner (if not the preparer) to consider whether its implementation will change the residual risk position to align it with the target risk position. If the residual and target positions do not align, consideration needs to be given as to whether the risk response plan needs to be adjusted or if the target risk position is appropriate. If the target risk position is appropriate but unachievable with the current response options available, the risk should be escalated in line with TLB/DA requirements; if the risk breaches the Defence Board Risk Escalation Threshold then it will also need to be escalated to the Defence Board (see section on escalation).

12. Any proposed plan will likely require approval and allocation of resources; Risk Owners should follow any relevant TLB/DA procedures for approval.

Allocating an Action Owner

13. When developing the risk response plan, it may be necessary to appoint an Action Owner(s), as some of the actions to respond to the risk may not be within the remit of the Risk Owner. The Action Owner is responsible for ensuring individual or multiple 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 accountability for the risk.

4 How to Monitor, Report and Escalate Risks

Risk identification 1
4
Risk monitoring, reporting & escalation
Communication & Consultation
Risk assessment
2
3 Risk response

Summary

A. Risk Monitoring
B. Risk Reporting and Escalation
C. Defence Board Risk Reporting Cycle

1. Capture, tracking (monitoring) and review of risk information is required to be able to identify changes to risks and notify management of those changes to support understanding and decisions on response.

A. Risk Monitoring

2. TLB/DAs should implement monitoring and review processes to track the status of individual risks, aggregated risks and the effectiveness of their risk management process. Risk monitoring provides management with the necessary risk information to:

- detect changes in risk profile and status of risks, supporting decisions on prioritisation, escalation up the management line, and response activities
- allow challenge and oversight on the completeness and quality of the risk information produced and the robustness of the risk management approach (see Appendix D for questions to consider when reviewing risks)
- ensure that risk responses are effective and efficient in both design and operation
- monitor the progress of risk response plans
- obtain further information to improve the identification and analysis of risks and
- analyse and learn lessons from risk issues / incidences, changes, trends, management successes and failures.

3. The Risk Owner should establish the frequency of review and monitoring for each risk. Regular risk monitoring enables the Risk Owner to:

- confirm that the controls and mitigations implemented to manage the risk are operating effectively
- adjust controls and mitigations as required
- ensure response plans are delivered against committed dates and outcomes
- identify changes to the risk including deterioration in status or circumstances that can affect risk impact and likelihood, and escalate as necessary and
- ensure any significant changes to the risk are reported or escalated to the appropriate levels.

Key Risk Indicators

4. Key Risk Indicators (KRIs) are forward looking information points and metrics that when tracked can provide an early indication of a change in the status of a risk and enable timely interventions to be made to either avoid a risk occurring or reduce its severity if it does. MOD does not mandate the use of KRIs; however the Defence Audit, Risk and Assurance (DARA) team can provide further guidance upon request.

B. Risk Reporting and Escalation

5. Risk reporting is the set of activities that enables risk information to be captured, documented, communicated and understood by others in a consistent way. At this stage in the risk management process all the risk information, including a summary of risk response plans, should be documented in a risk register.

Risk Reporting

6. The purpose of risk reporting is to present risk information in a consistent and timely manner (frequency to be determined by management needs, risk severity and dynamics) to provide management with appropriate visibility and understanding of risks to:

- inform decision making
- enable further analysis and
- provide oversight and challenge.

Note: risk reporting can also be used to inform assurance providers of where they need to focus their reviews.

Risk Analysis

7. A key focus for risk analysis is to identify the most significant risks facing the TLB/DAs and the Department, on both an inherent and residual basis to enable prioritisation of management focus and inform decision making. Some risks will have similar characteristics and/or may be identical in nature and accordingly can be collated to present in summary form. Other risks may have common causes which can lead to multiple risk events occurring. Collation and aggregation can provide additional and valuable insights into the Department's risk profile.

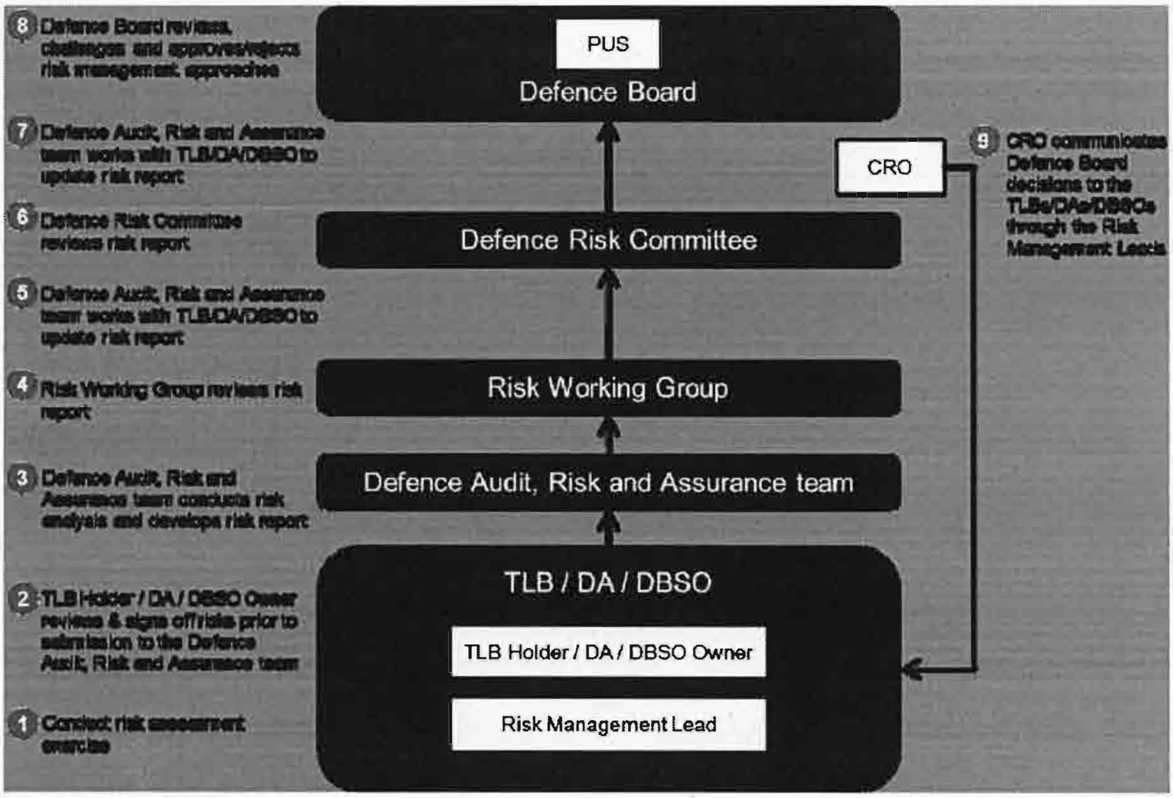
C. Defence Board Risk Reporting Cycle

8. On a quarterly basis, each TLB/DA conducts a risk assessment exercise. The risks that meet the Defence Board Escalation Threshold are recorded in the MOD risk reporting template and, following review and sign off by the TLB Holder/DA, are submitted to the DARA team.

9. The DARA team collate the risks received, conduct risk analysis and produce the Defence Board Quarterly Risk Report. The Risk Working Group review and challenge the key risks identified and conduct further analysis as required. The DARA team work with the TLB/DAs to make any necessary changes to the Defence Board Quarterly Risk Report. This is then reviewed by the Defence Risk Committee, who may also request further changes, before being presented to the Defence Board.

10. The Defence Board review and challenge the risks, approve or reject the proposed approaches to further manage the risks, and conduct deep dive reviews as appropriate. The CRO communicates the Defence Board's decisions to the TLB/DAs through the relevant Risk Management Leads.

The diagram below sets out the key steps for the Defence Board risk reporting cycle:



8 Defence Board reviews, challenges and approves/rejects risk management approaches

7 Defence Audit, Risk and Assurance team works with TLB/DA/DBSO to update risk report

6 Defence Risk Committee reviews risk report

5 Defence Audit, Risk and Assurance team works with TLB/DA/DBSO to update risk report

4 Risk Working Group reviews risk report

3 Defence Audit, Risk and Assurance team conducts risk analysis and develops risk report

2 TLB Holder / DA / DBSO Owner reviews & signs off risks prior to submission to the Defence Audit, Risk and Assurance team

1 Conduct risk assessment exercise

9 CRO communicates Defence Board decisions to the TLBs/DAs/DBSOs through the Risk Management Leads

APPENDIX A – MOD RISK ASSESSMENT CRITERIA

The impact and likelihood of a risk occurring must be measured in a consistent way in order to allow the size/significance of risks to be compared. The MOD Risk Assessment Criteria measures risk impact and likelihood against five levels of severity.

Risk Assessment Likelihood Criteria

The below Criteria should be used for measuring the likelihood of a risk occurring within the next five years.

The likelihood can be measured using any of the 3 likelihood criteria shown below: the probability percentage, the perceived approximate frequency, or based on how commonly it has occurred in the past. Note that based on the specific risk being assessed, one measurement scale may be more applicable than the others.

Where multiple scales are applicable, the assessment should be based on the scale with the highest likelihood. For example, if a risk has never occurred in MOD history but has a 30% probability of occurring, then the likelihood assessment should be documented as 3.

	Likelihood	Probability	Approximate frequency	Description
5	Very high	> 90%	Occurs at least once every 5 years	Is a common occurrence in MOD
4	High	51 - 90%	Occurs once every 5 - 10 years	Has occurred within MOD many times
3	Medium	26 - 50%	Occurs once every 10 - 20 years	Has occurred in MOD on several occasions
2	Low	11 - 25%	Occurs once every 20 - 50 years	Has occurred on a small number of occasions in MOD's history
1	Very low	≤10%	Occurs less than once every 50 years	Has occurred once / never in MOD history

Risk Assessment Impact Criteria

The below Criteria should be used for measuring the total potential impact(s) of a risk, if it were to occur (not in-year only).

Where multiple impact areas are applicable, the assessment should be based on the area with the highest impact. For example, if a risk has a potential reputational impact of E and a financial impact of C, then the impact assessment should be documented as E.

	Financial	Reputational	Impact on outputs / capability	Health, safety & environment (not as a result of hostile action)
E Critical	[redacted]	• [redacted]	[redacted]	• [redacted]

D Severe	[redacted]	• [redacted]	[redacted]	• [redacted]

C Major	[redacted]	• [redacted]	[redacted]	• [redacted]
B Moderate	[redacted]	[redacted]	[redacted]	• [redacted]

A Minor	[redacted]	[redacted]	[redacted]	[redacted]

APPENDIX B – MOD RISK CATEGORIES

The MOD Risk Categories can be used as a guide to ensure a broad range of risks are considered during risk identification exercises. Additionally, the categories will be used by the DARA team to conduct risk consolidation and reporting analysis.

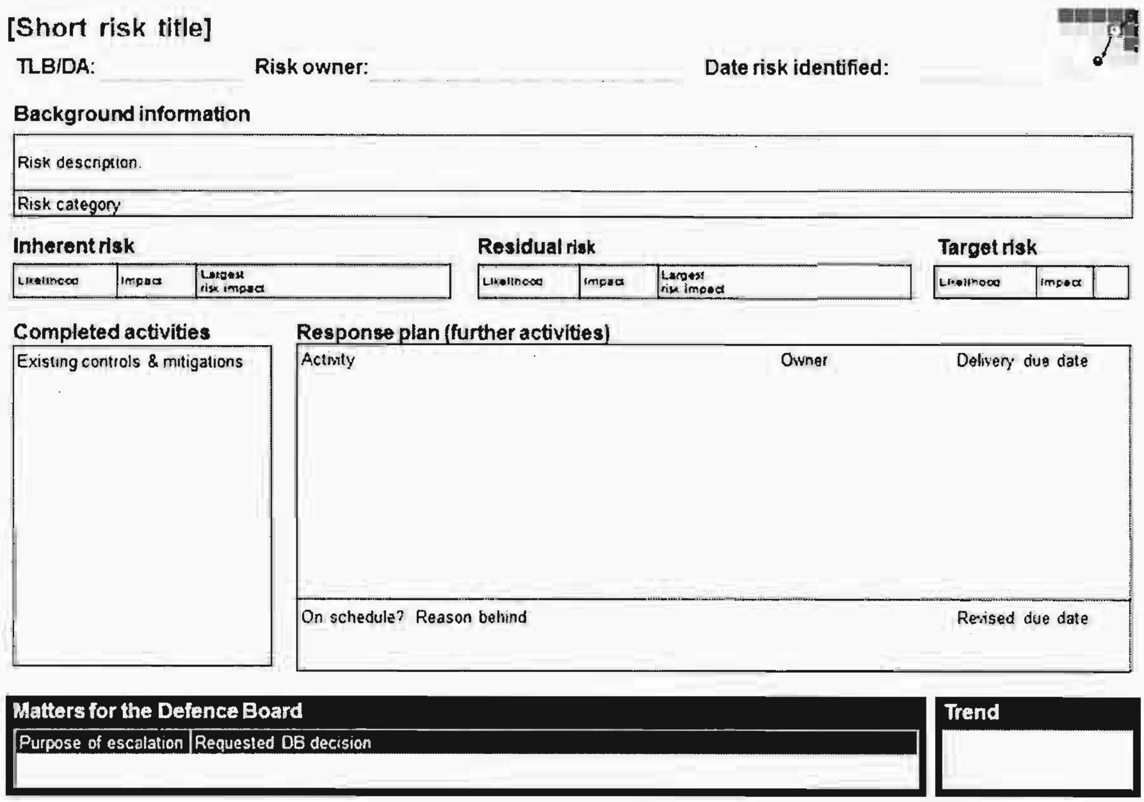
When assigning a category to a risk, assign it to the cause or event of the risk, not the consequence.

Risk Category and associated core MOD function	**Description** Any risks whose cause is related to...
Strategic, i.e. Direct	How MOD is managed, strategy, policies and compliance
Operational, i.e. Operate	Military operations
People, i.e. Generate and Develop	Recruitment, retention, training and development, engagement, culture and behaviour of military and civilian personnel
Capability, i.e. Acquire	The acquisition of equipment, systems and other items that the armed forces need
Infrastructure, i.e. Enable	All support services
Finance, i.e. Account	The accounting and reporting of defence activity and spending to Parliament and the public

APPENDIX C – RISK REPORTING TEMPLATES

The MOD risk reporting template is used for TLB/DAs to report risks that meet the Defence Board Escalation Threshold to the DARA team. Below is a screenshot of the template. The template can be found on the intranet JSP landing page.

The DARA team will consolidate the TLB/DA submissions to create the Defence Board Quarterly Risk Report.



[Short risk title]

TLB/DA: Risk owner: Date risk identified:

Background information

Risk description.

Risk category

Inherent risk

Likelihood	Impact	Largest risk impact

Residual risk

Likelihood	Impact	Largest risk impact

Target risk

Likelihood	Impact	

Completed activities

Existing controls & mitigations

Response plan (further activities)

Activity	Owner	Delivery due date
On schedule? Reason behind		Revised due date

Matters for the Defence Board

Purpose of escalation	Requested DB decision

Trend

APPENDIX D – QUESTIONS TO CONSIDER WHEN REVIEWING RISKS

The following is a list of questions that leadership may wish to consider when reviewing and challenging the risks reported to them.

Risks

1. Are all the principal risks you'd expect to see, here? If not, which are missing?

   a) Based on TLB/DA Board briefing papers, are there other risks to be considered?

2. Are the risks described correctly? Is their nature clear?

3. Are the right owners assigned to the risks?

Risk Assessment

4. Do you agree with the risk assessment ratings?

Current Controls and Mitigations

5. Do you have confidence that the existing controls and mitigating activities in place are fit for purpose and reliable? Are they specific and significant to the risk? Do they bring the inherent risk level to the residual risk level?

Target Risk Exposure

6. Do you agree with the target risk level? What are the benefits and opportunities presented by taking the risk? Do they justify the size of the exposure?

Response Plan Activities

7. Are the planned risk response activities appropriate (e.g. use of resource, effort, timeframe to completion) and will they enable the achievement of the target risk level?

8. Are the people with the right knowledge, skills and tools being assigned to undertake the activities?

9. Do you have evidence that planned activities are being completed on time?

Monitoring

10. Are you satisfied with how the risk is being monitored? Would it give us early warning of change and allow us to intervene?

Assurance

11. Is more assurance required to provide comfort that controls are working as intended?

Risk Correlation

12. Is there any risk correlation to consider? If one risk crystallises, could this increase the impact / likelihood of another risk or trigger any other risks to crystallise?

Lessons Learnt

13. Have any near misses occurred, or any risks occurred? If so, how and why? Did the controls and mitigating activities work as intended? Have we learnt from these risks / near misses?

APPENDIX E – RISK MANAGEMENT GLOSSARY

Term	Definition
Action owner	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.
Cause	The first part (of 3) of a structured risk description. It is the source or driver of the risk event e.g. the underlying conditions, circumstances or activities that could lead to a risk event occurring.
Consequence	The third part (of 3) of a structured risk description. It is the possible effects that the risk event would have on the achievement of objectives.
Control	An activity or measure that is expected to reduce the likelihood of a risk event occurring.
Emerging risk	New or evolving risks that are difficult to characterise or assess at this point in time due to limited information being available and/or prior experience of managing the risk.
Escalation	Required upward notification to a specified person or group of a specific risk, a change in its status or an action to manage it. Note risk escalation does not transfer risk ownership.
Frequency	The number of times it is expected that a risk event will occur over a specified period of time.
Impact	Estimate of the potential effect(s) of the consequences of a risk on the achievement of objectives and protection of values. Often assessed using a standardised scale that measures the impact of the risk on a range of Departmental assets e.g. finances, reputation etc.
Inherent risk assessment	Assessment of a risk's pre-mitigated likelihood and impact, i.e. when existing controls and mitigations that have a specific and significant effect on management of the risk are either not in place or fail when needed or fail to work as intended, in a manner that is credible and reasonably foreseeable. Inherent risk can be considered to be 'the reasonably foreseeable worst case scenario' for the risk.
Issue	An issue is an unplanned event or situation that has already occurred, or will definitely happen, which is certain to affect the achievement of business objectives. An issue must be addressed to negate or minimise its impact(s) on objectives.
Key Risk Indicator (KRI)	Information points and metrics that, when tracked, can provide early warning of a change in the status of a risk, allowing interventions to be made to avoid the risk occurring or reduce its impact. KRIs are leading in nature (i.e. telling you what could happen) and provide the opportunity to identify potential changes in a risk sufficiently far in advance to enable its effective management. The use of KRIs is not mandatory.
Likelihood	Estimate of the probability or frequency of a risk occurring in a specified time period, based on the description of its cause, event and consequences.
Mitigation	An activity or measure that is expected to reduce the impact of a risk event should it occur.
Near miss	A 'Near-Miss' is a risk event or set or circumstances that had the potential for significantly more severe consequences than were actually experienced e.g. jets coming into dangerous proximity but a mid air collision was narrowly avoided.

Opportunity	An uncertain future event that could positively impact the Department's ability to meet or exceed its objectives.
Probability	A numerical description of the chance of a risk event occurring, usually described as a percentile figure. Note this is different to likelihood; likelihood is a broader term that encompasses probability, but also includes qualitative descriptions of the chance of a risk event occurring.
Residual risk assessment	Assessment of the current likelihood and impact, i.e. based on how a risk is currently being managed, assuming that the specific and significant controls and mitigations that are currently in place and have a direct effect on the likelihood or impact of the risk are working as intended.
Risk	An uncertain future event that could have an effect on the achievement of objectives. A risk consists of a cause, an event and consequence(s), and its magnitude is often expressed as a product of its impact and likelihood.
Risk aggregation	Grouping of risks which have a common cause or interdependency and when considered together have a greater impact than when considered separately e.g. failure of a common supplier to multiple projects.
Risk appetite	An expression of the types and amounts of risk the Department is willing or not willing to take or accept to achieve its objectives and aims to supports consistent, risk informed decision making across Defence. The articulation of risk appetite is not mandatory.
Risk assessment	Second stage of the risk management process that aims to determine the size / significance of a risk from an estimation of the likelihood of the risk occurring and the impact of the risk should it occur using a predetermined criteria.
Risk assessment criteria	The criteria used to determine the likelihood and impact level of risks, to ensure all risks are measured consistently and objectively.
Risk categories	Defined groupings of risk according to common qualities such as their nature and origin, cause or consequences. MOD risk categories are defined according to their origin and can be used to support consideration of a broad range of risks and used for Defence Board risk reporting analysis.
Risk collation	Grouping of risks that have the same or similar qualities e.g. by risk category, by common cause, event or consequence. Supports risk analysis and reporting activities.
Risk description	A description of the cause, event and consequence(s) of the risk to enable likelihood and impact to be assessed and effective controls and mitigations to be determined.
Risk event	An incident or occurrence arising from a cause that could have consequences affecting the achievement of objectives.
Risk exposure	The amount of risk facing the Department (or TLB/DA, business unit, project etc.) at a point in time from a single risk event or multiple risk events.
Risk identification	First stage of the risk management process to determine all the risks that could significantly affect the achievement of objectives, based on consideration of the Department, its strategy and objectives, its operations, its resources and the external environment in which it exists
Risk owner	An individual who acts as the single point of accountability for ensuring the effective management of the risk.

	The risk owner should have an appropriate level of knowledge of the risk and the authority to be able to ensure the risk is managed sufficiently.
Risk profile	A population of identified and assessed risks that together represent the majority of key risks faced by an organisation and/or its subsidiary components at a point in time.
Risk register	A repository for capturing and recording risks and associated information.
Risk response	The approach / action / decision taken on how to manage a risk where the residual risk position does not align to the target risk position. There are five types of Risk response: terminate, treat, transfer, tolerate and take the opportunity.
Risk response plan	The additional activities planned to further reduce the likelihood and/or impact of a risk beyond its current residual position. Plans detail specific deliverables, accountabilities and timelines for completion.
Severity	A measure of the risk's importance. It is used to compare the relative size/ significance of risks and is determined by combining the likelihood and impact of the risk.
Take	Action taken to exploit an opportunity; undertaking an action or managing a set of circumstances to increase the likelihood of realising a positive outcome or upside.
Target risk assessment	Target risk assessment is the determination of the desired impact and likelihood levels for the risk, based on the amount of exposure the Department is comfortable in accepting for the benefits it derives from taking the risk, and the feasibility and cost of further response activities.
Terminate	Exiting the activities giving rise to risk as the risk is unacceptable. Avoiding / eliminating the risk by deciding not to start or continue with the activity that gives rise to the risk, or by doing something differently e.g. substitution of an alternative step or activity.
Tolerate	No action is taken to affect risk likelihood or impact. This means the current risk exposure is accepted. This usually results from taking the risk in order to pursue an opportunity or achieve a benefit/return, or retaining the risk by informed decision.
Transfer	Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk with another party. Common techniques include outsourcing activities to the private sector or purchasing insurance products (Note: transferring does not necessarily eliminate or remove accountability or the effects of the risk e.g. outsourcing a process may not reduce the reputational impact to MOD if something goes wrong).
Treat	Action taken to reduce risk likelihood or impact, or both through: • Changing the likelihood through implementing additional controls, or • Changing the potential impacts through implementing additional mitigations.
Trend	The outlook for, or expected change in, the exposure of a risk over a given time period e.g. increasing, decreasing, stable.