Contents

1. Introduction .......................................................................................................................... 3
   1.1. Why Risk Management is vital to SDD ................................................................. 4
   1.2. Purpose ..................................................................................................................... 4
   1.3. Scope ....................................................................................................................... 5
   1.4. Ownership ............................................................................................................... 5
   1.5. Definitions ............................................................................................................... 5
   1.6. Review .................................................................................................................... 5
2. Risk Management Process ................................................................................................. 5
   2.1. Communication and Consultation .......................................................................... 6
   2.2. Scope, Context, Criteria .......................................................................................... 7
       2.2.1. Scope - What is the activity? ........................................................................... 7
       2.2.2. Context - What is the activity about? ............................................................ 7
       2.2.3. Criteria - How is the activity measured? ....................................................... 8
   2.3. Risk Assessment ....................................................................................................... 8
       2.3.1. Risk Identification - What could go wrong? .................................................... 8
       2.3.1. Risk Identification - What could cause it to happen? .................................... 10
       2.3.2. Risk Analysis .................................................................................................. 10
       2.3.2.1. Controls ....................................................................................................... 10
       2.3.2.2 Control effectiveness .................................................................................... 11
       2.3.2.3. Likelihood and Consequence .................................................................... 11
       2.3.2.4. Likelihood: What is the chance of the risk event occurring? ................... 11
       2.3.2.5. Consequence: What are the impacts of the risk event?............................. 12
       2.3.2.6. Risk Level .................................................................................................. 13
   2.4. Risk Treatment ............................................................................................................ 15
       2.4.1. Mitigating the risk – WHS ............................................................................ 16
   2.5. Risk Owner ................................................................................................................ 17
   2.6. Monitoring and Review ............................................................................................. 18
   2.7. Recording and Reporting ......................................................................................... 18
       2.7.1. SDD Risk Register ......................................................................................... 18
       2.7.2. Reporting ....................................................................................................... 19
       2.7.3. Maintenance and Sustainment ....................................................................... 19
3. References and Legislation ............................................................................................... 20
   3.1. External Guidance .................................................................................................... 20
   3.2. Internal Guidance ..................................................................................................... 20
4. Reviews and approvals ..................................................................................................... 20
5. Summary of changes ......................................................................................................... 21
6. Glossary ............................................................................................................................. 22
   SDD Risk Tools – Control Effectiveness guide ................................................................. 23
   SDD Risk Tools – Likelihood guide .................................................................................. 23
   SDD Risk Tools – Consequence guide ............................................................................ 24
   SDD Risk Tools – Risk Matrix ......................................................................................... 25
1. Introduction

Defence manages risk because it helps set our strategy and helps us make better business decisions. By understanding and being prepared for risk events, Defence will:

- manage uncertainty
- create an environment where surprises are minimised
- reduce the likelihood and impact of events
- identify priorities
- make decisions with a sensible, risk informed approach.

For SDD, the value proposition of risk management is that it will provide:

- pathways to better customer service
- opportunities to attain better value for money
- less bad days for Defence and the Government
- Increased confidence in service delivery.

Defence is legislatively bound by the *Public Governance, Performance and Accountability Act 2013 (PGPA Act)*, which mandates that the accountable authority of a Commonwealth entity must establish and maintain appropriate systems and internal controls for the oversight of risk.

The Secretary of the Department of Defence is the accountable authority under the *PGPA Act*. The Secretary, in partnership with the Chief of Defence Force issued a Joint Directive - JD30/2015 to all Defence employees, Defence civilians, ADF members and contractors to ensure that risk management is approached consistently and integrated into all planning, approval, review and implementation processes.
In addition, Risks that may have a safety impact have specific requirements under the Work Health and Safety Act 2011. Defence has a primary duty to manage risks:

- By eliminating health and safety risks so far as is reasonably practicable
- If it is not reasonably practicable to eliminate the risks, by minimising those risks so far as is reasonably practicable.

1.1. Why Risk Management is vital to SDD

Risk Management is a crucial part of any decision-making process in Defence. While it is impossible to eliminate all risk, SDD recognise that active identification and robust management of risk is far more likely to be better prepare us to respond rapidly, to take advantage of an opportunity and avoid a risk, or to re-focus effort or minimise a risk impact, when things go wrong.

Risk management within SDD is about managing uncertainty and creating an environment where surprises are minimised. When our management of risk goes well it often remains unnoticed. When it fails, consequences can be significant and high profile.

For SDD, effective risk management can:

- Prevent damage to reputation
- Prevent loss of life/injury
- Protect assets
- Allow the delivery of services/products to our customers that meet their expectation
- Prevent disruption to Defence capability
- Reduce the legal liability and increase the stability of our operations
- Recognise and respond to opportunities
- Assist in creating a safer environment for staff
- Protect the environment
- Ensure compliance with relevant legal/statutory requirements
- Increase operational effectiveness and efficiency

1.2. Purpose

The Service Delivery Division Risk Management Framework (the Framework) defines SDD’s approach for managing risk.

The Framework defines the procedures, roles and reporting requirements for the management of risks for SDD, ensuring:

- risk management is an integral part of planning and decision making in SDD
- a consistent and simple method to managing risks across SDD
- strengthened governance, compliance and management practices
- accountability is assigned to those with risk management responsibilities
- adequate resources are allocated in support of the corporate goals and strategic objectives
- a formalised process to link risk to organisational objectives is clearly articulated.

The Framework supports Defence’s Enterprise level risk management.
1.3. **Scope**

The Framework is to be applied to all SDD activities where there is an impact to the SDD mission and will be utilised by all employees across SDD; and includes contractors, consultants and any others who act on behalf of SDD.

1.4. **Ownership**

This Framework is owned and endorsed by the First Assistant Secretary, Service Delivery Division, Estate & Infrastructure Group.

1.5. **Definitions**

Definitions applicable to the Framework is detailed in the **Glossary** on page 17.

1.6. **Review**

The Framework is reviewed annually (or ad hoc, if required) by the Directorate of Risk and Assurance (DRA). The purpose of the review is to determine:

- If there have been any changes to the risk management environment (e.g. changes to risk appetite or risk posture (via the Risk Matrix)
- If current risk tools are fit for purpose
- Whether the Framework is contemporary with current legislation, international standards and best-practice

2. **Risk Management Process**

SDD complies with the risk management process outlined in the **AS/NZS ISO 31000:2018**. The ISO underpins the Framework and guides how we effectively and efficiently manage risk at all levels of the SDD.

The SDD risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of all SDD business. It can be applied at strategic, operational, program or project levels.

Although the risk management process is often presented as sequential, in practice it is iterative. SDD risk management process is comprised of:

- **Communication and Consultation**
  Takes place in all stages of the risk management process. Assists stakeholders in understanding risk and involves different areas of expertise to feed information to facilitate risk oversight and decision-making

- **Scope, Context, Criteria**
  Defines the scope for the risk management process and sets the criteria against which the risks will be assessed

- **Risk Assessment**
  Is the overall process of risk identification, risk analysis and risk evaluation

- **Risk Treatment**
  Selecting and implementing options for addressing the risk
➢ **Monitoring and Review**  
* Takes place in all stages of the risk management process. Assures and improves the quality and effectiveness of process design, implementation and outcomes  

➢ **Recording and reporting**  
* Takes place in all stages of the risk management process. Documents and communicates risk management activities across SDD and provides information for decision-making

---

**Figure 1:** Australian Standard for Risk Management - Principles and guidelines AS/NZ ISO 31000:2018 Process

### 2.1. Communication and Consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.

Communication and consultation aims to:

- Ensure that relevant expertise is available and used through each step of the risk management process
- Provide sufficient information to facilitate risk oversight and decision-making
- Build a sense of ownership and inclusiveness among those affected by risk

Comprehensive assessment of risks requires effective stakeholder communication and consultation. This is an essential attribute of good risk management and, in practice, is a key requirement within all stages of the risk management process.
2.2. Scope, Context, Criteria

The purpose of establishing the scope, context and criteria is to customise the risk management process.

Defining the scope for the risk management process sets the criteria against which the risks will be assessed and enables effective risk assessment and the chance to identify appropriate risk treatments.

2.2.1. Scope - What is the activity?

The scope defines the subject of the entity or activity being considered.

When planning the scope, considerations include:

- Objectives and decisions that need to be made
- Outcomes expected from the step to be taken in the process
- What risk assessment tools will be used
- Resources required
- Responsibilities and how will be recorded
- Relationships to other activities

As an example, a scope can be described as either a task, activity, project, program, contract or a subject.

2.2.2. Context - What is the activity about?

Context are circumstances that form the setting of a risk event, so it may be understood.

As an example, risk context is like the background of a story. Without the background information in a story, you wouldn’t understand a lot of things about the characters in the story and the actions which they take as part of that story.

If you consider risks to be like characters in the story and you do not look at the context (the background) of the risks, you may fail to understand some important things about the risks themselves. Setting the context will help you to see the whole picture.

Context can be broken down into internal context and external context.

Internal context is any internal factors that influences objectives.

This can include governance, organisational structure, policies, objectives, and the strategies set to achieve them, internal resources and knowledge (e.g. money, time, people, processes, systems and technologies), and the risk tolerance and appetite of the Division.

External context is any external factors that influences objectives.

This can include legal, regulatory, environment, financial, technological, and economic environment, competitive environment analysis, and key drivers and trends having impact on the organisation’s objectives.
2.2.3. Criteria - How is the activity measured?

Risk criteria determines what should be measured in an activity and how, to give the best opportunity to evaluate the significance of risk to the topic. Risk criteria must be aligned to the scope and context of the activity.

2.3. Risk Assessment

To set risk criteria, the following should be considered:

- How consequences and likelihood will be defined and measured
- The type of uncertainties that can affect outcomes and objectives
- Consistency and relevance of measurements
- How the level of risk is to be determined
- The levels at which the risk is tolerable or requires escalation to Senior Executive

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

Risk Identification

The aim of risk identification is to find, recognise and describe risks that, if they occur, will have an impact on the goals and objectives of the SDD and more broadly, the Department. To capture the correct events, ask the following questions:

- What could go wrong?
- What would cause it to happen?
- What are the effects if it goes wrong?

Comprehensive identification of potential risk events is critical to the success of any risk assessment. It is important not be too narrow or constrained if capturing the risks. Care needs to be taken to ensure that wide variety of sources are engaged in this process to deliver the veracity of information required.

2.3.1.1. Risk Identification - What could go wrong?

In asking what could go wrong with a task or activity, risks need to be identified as potential events and described in such a way that they can actually be treated.

When identifying risk events consider the following questions:

- What might prevent the achievement of goals and objectives?
- What events or occurrences could threaten the intended outcomes?
- How and where a risk event could occur?
- What are the risks relating to the established context?
- What risks events have already occurred in the past and could they happen again?

It is common that there is confusion about what should be captured in a risk register and how it should be worded in a risk register. Badly framed risks can be very difficult to manage.
There are a number of traps we can fall into when trying to identify risks. Sometimes we fall into the trap of capturing “risks” that are either broad statements, causes or consequences. Common examples of this include:

<table>
<thead>
<tr>
<th>The too broad risk statement</th>
<th>The risk that is actually a cause</th>
<th>The risk that is actually a consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation damage</td>
<td>Lack of …. (funding, policy direction, maintenance, planning, communication)</td>
<td>Project does not meet schedule</td>
</tr>
<tr>
<td>Compliance failure</td>
<td>Ineffective …. (training, internal audit, policy implementation, contracts)</td>
<td>Department does not meet its stated objectives</td>
</tr>
<tr>
<td>Fraud</td>
<td>Insufficient …. (time and assets allocated for planning, resources applied)</td>
<td>Death/injury to staff</td>
</tr>
<tr>
<td>Environment damage</td>
<td>Inefficient …. (use of assets, procedures)</td>
<td>Loss of stakeholder confidence</td>
</tr>
<tr>
<td>Safety</td>
<td>Inadequate …. (training, procedures).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Poor…. (leadership, data storage, procurement practices).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inaccurate…. (records, data, recording of information)</td>
<td></td>
</tr>
</tbody>
</table>

These examples don’t describe the risk for it to be managed at any level.

**So what should our risks look like?**

They need to be events/incidents or activities.

When something goes wrong like a food poisoning outbreak in the mess or an unauthorised person entering the Defence Estate, it is always an event. After the event there is a post event analysis to determine what happened, why it happened, what could have stopped it happening and what can be done to try and stop it happening in the future. Risk management is no different – you are trying to anticipate and stop the incident before it happens.

If the risks in your risk register could not have a post event analysis conducted should it occur—then it is not a risk.
2.3.1.2. Risk Identification - What could cause it to happen?

In looking at causes, business areas must identify the source that might cause each risk event to happen.

Wording that would distinguish a cause from the risk may include:

- Lack of
- Ineffective
- Insufficient
- Inadequate
- Failure to
  - Poor
  - Excessive

The use of the above wording assists in determining a risk cause as opposed to a risk event.

Risk Analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk.

Risk analysis involves developing a detailed understanding of each risk and to establish its potential impact. An event can have multiple causes and consequences and can affect multiple objectives. Risk analysis should consider factors such as:

- assessing what existing controls are in place and how effective they are
- the consideration of the likelihood that a risk event will occur
- the plausible consequence/s if it does occur

2.3.2.1. Controls

A control is any measure or action that modifies or reduces a risk event occurrence or severity.

Controls include any policy, procedure, practice, process, technology, technique, method, or device.

When determining the Likelihood or the Consequence of a risk occurring, consideration must be given to existing control measures. Once the existing controls have been identified, the controls must be tested to evaluate their effectiveness.

Tip: Controls should be aligned to the causes.
Controls are split into three distinct types:

- **Preventative Controls** – aimed at preventing the risk event from occurring. Examples of preventative controls could include *plans, policies and procedures*.

- **Detective Controls** – used to identify failures in the preventative controls. Examples of detective controls could include *audits, investigations and stocktakes*.

- **Corrective Controls** – focused on minimising the consequences that arise from the risk event. Examples of corrective controls could include *Business Continuity Plans and insurance*.

2.3.2.2 Control effectiveness

With any control, assuming that because it is in place, it must work is poor business practice and will lead to risks being realised. The only way to determine a control’s effectiveness is to measure the effectiveness. This is done by asking:

- What are critical controls and are they effective?
- How do we measure and validate that effectiveness?

_N.B. all controls will need to have performance measures or key performance indicators attached to them._

<table>
<thead>
<tr>
<th>CONTROL EFFECTIVENESS RATING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective</td>
<td>Control is fit for purpose in addressing the causes of the risk event and is applied in a consistent manner. AND/OR Control is effective and has been tested across applicable circumstances and in accordance with contractual obligations. AND/OR Only minimal work (other than ongoing review and monitoring) can be done to strengthen the control.</td>
</tr>
<tr>
<td>Room for Improvement</td>
<td>Moderate amount of work is required to strengthen the control. AND/OR Control is fit for purpose in addressing the causes of the risk event but is applied in an inconsistent manner.</td>
</tr>
<tr>
<td>Not Effective</td>
<td>Significant work is required to improve the effectiveness of the control. AND/OR The control is not fit for purpose in addressing the causes of the risk event. AND/OR The control has not been tested or has been tested and is not effective across applicable circumstances or in accordance with contractual obligations.</td>
</tr>
</tbody>
</table>

Figure 2: SDD Control effectiveness table

2.3.2.3. Likelihood and Consequence

To determine the Likelihood and Consequence of each risk event, the SDD utilise the Division’s Likelihood and Consequence guide on pages 19-20. For risk assessments to be effective, a structured approach to assessing consequence is critical. Therefore, the level of consequence for each risk event is to be finalised for the seven categories in the SDD consequence guide.

2.3.2.4. Likelihood: What is the chance of the risk event occurring?

**Likelihood is the chance that something might happen.**

Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either quantitatively or qualitatively. There are many cases where the likelihood of a risk cannot be measured on frequency or probability.
The likelihood of these risks can instead be based on the effectiveness of the current control environment. For example, using the risk event of ‘worker exposed to unbonded/friable asbestos’ as a case study:

- The **likelihood** of this risk occurring (the worker being exposed to asbestos) is in no way going to be based on frequency or probability (how often the worker handles or is in the vicinity of asbestos).
- What will make this risk unlikely or rare in this case is the effectiveness of the control(s) (does the worker wear appropriate Personal Protective Equipment (PPE) when working with or around asbestos?).

<table>
<thead>
<tr>
<th>LIKELIHOOD RATING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Almost Certain** | • The risk event has occurred more than once in Defence in the last 12 months.  
• All critical controls associated with the risk are weak and/or non-existent.  
• Without control improvement, it is very likely that the risk event will eventuate. |
| **Likely** | • The risk event has occurred more than once in Defence over the last 5 years but no more than once in the last 12 months.  
• Nearly all critical controls associated with the risk are weak.  
• Without control improvement it is more likely than not, that the risk event will eventuate. |
| **Possible** | • The risk event has occurred once in Defence in the last 5 years.  
• Some critical controls associated with the risk are rated as ‘Effective’.  
• If there is no control improvement, the risk event may eventuate. |
| **Unlikely** | • The risk event has occurred in Defence but not within the last 5 years.  
• Nearly all critical controls associated with the risk are rated as ‘Effective’.  
• The effectiveness of the risk controls means that it is likely that the risk event eventuating would be caused by external factors not known to Defence. |
| **Rare** | • The risk event has never occurred in Defence.  
• All critical controls associated with the risk are rated as ‘Effective’.  
• The effectiveness of the risk controls means that it is likely that the risk event eventuating would be caused by external factors outside of Defence control. |

Figure 3: SDD Likelihood Guide

*N.B. The likelihood rating names may vary on different systems*

2.3.2.5. Consequence: What are the impacts of the risk event

**A consequence is the outcome of an event and has an effect on objectives.**

A single event can generate a range of consequences, which can have both positive and negative effects on objectives.

The best way to determine the consequences of a risk event is by determining the **most plausible outcome** against each of the categories (impacts) in the SDD consequence guide.

For example, if a hundred people had a slip, trip or fall in the workplace, which resulted in an injury - statistically about 90% of those are either going to have an **insignificant or minor injury** (it is extremely unlikely that someone will die, i.e. a severe consequence).
In a large organisation such as Defence, it is almost certain there will be slips, trips or falls over a period of time. If we were to take the worst-case scenario and assess the consequence as severe (i.e. death) our risk would be rated as Very High. In that case, it would be well above the SDD risk tolerance and would be prohibitive to have the requisite controls in place.

The lesson out of this is, rather than determining the worst-case consequence, ask “what is the most plausible consequence?” This will make assessed risk levels more credible, and, the decisions based on these risk levels, more appropriate.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>No emotional impact. Event managed internally by Defence – no intervention required. No stakeholder impact.</td>
<td>Event managed by Defence public relations staff. Stakeholder conflict but minimal impact on defence operations.</td>
<td>Event managed through Defence public relations processes. Loss of key stakeholder confidence. Media coverage of event.</td>
<td>Event requires interaction by Defence public relations and senior Defence officers. Loss of key stakeholder confidence. Negative impact on ministerial government and/or senior Defence officers. Media coverage of event.</td>
<td>Event requires intervention by Secretary or Minister. Wide loss of stakeholder and community confidence Secretary or Minister resignation. Sustained detrimental media coverage at international level. Security via royal commission or similar level inquiry.</td>
</tr>
</tbody>
</table>

Event causes no disruption to core Defence operations. Minimal local intervention required. | Event causes minimal disruption of core Defence operations, causing minor delays of the fundamental objectives times. Event causes internal management of resources to Defence operational priorities. | Event causes noticeable level of disruption of core Defence operations, causing ended delays of key fundamental objectives times. Event causes reduction of resources to Defence operational priorities. | Event causes significant levels of disruption to core Defence operations, causing major delays to fundamental objectives times, exacerbating major management resources. Event causes major management of resources to Defence operational priorities. | Event causes full disruption of core Defence operations, creating a catastrophic breakdown of fundamental objectives. Event requires complete revision of defence operational priorities. |

No financial impact. Event managed internally by Defence staff – no intervention required. | Event triggers minor financial loss or damage. Event managed by Defence property, finance and/or legal staff. Event results in financial impact of $1,000 – $25,000. | Event triggers limited financial loss or damage. Event activity monitored through Defence property, finance and/or legal staff. Event results in financial impact of $10,000 – $250,000. | Event triggers significant financial loss or damage that requires Defence resources. Event activity managed through such activity, and/or managed by senior Defence officers. Event results in financial impact of $1 million – $20 million. | Event triggers major financial loss or damage and may result in major court action/mediation. Event results in financial impact of more than $20 million. |


No immediate damage, contained spillage. Fully recoverable with minor impact on the environment. The impact will take less than 15 days for the response to be fully recovered. | Normal damage to the environment. The impact will take less than 2 years to fully recover or in-built only require minor repair. | Limited damage is caused to the environment with a possibility it is recoverable. The impact will take up to 10 years to recover. | Medium damage is caused to the environment with a possibility it requires repairs. The impact will take up to 20 years to recover. | Extensive and irreversible damage is caused to the environment. Off. Limited repairs are to a significant environmental area or off the Environment Protection and Biodiversity Conservation Act 1999 (from which it will take more than 10 years to recover. |

Event is a near-miss where an injury does not occur. Minor injury or illness that is detected in the employee but not at a regulated health examination, with or without follow-up treatment. Minor injury or illness that is treated in the workplace (e.g. by a registered health professional) with or without follow-up treatment. | Injury or illness causally connected to the incident that, if the employee had received timely medical attention would have been registered as a minor injury or illness. | Serious injury or illness requires immediate admission to hospital as an inpatient and/or partial permanent disability, or 10 or more days of restricted work. Serious injury or illness requires immediate admission to hospital as an inpatient and/or partial permanent disability, or 10 or more days of restricted work. | Severe injury or illness requires immediate admission to hospital as an inpatient and/or partial permanent disability, or 10 or more days of restricted work. Severe injury or illness requires immediate admission to hospital as an inpatient and/or partial permanent disability, or 10 or more days of restricted work. | Loss of life or total permanent disability (injured and/or psychological), or 10 or more injuries or illnesses classified as severe. |


Figure 4: SDD Consequence Guide

N.B. The consequence rating names may vary on different systems

2.3.2.6. Risk Level

The combination of the likelihood and consequence rating determines the severity of the risk. To determine the overall risk level for a risk event, the likelihood and consequence scores for the risk are formulated with the SDD risk matrix on page 25.
Risk Evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to:

- Consider risk treatment options
- Undertake further analysis to better understand the risk
- Have no further action
- Maintain existing controls
- Reconsider objectives

2.3.3.1. Risk Appetite: What is the acceptable level of risk for SDD?

The risk appetite is set at MEDIUM for SDD. Risks that sit at a low or medium level are within the SDD risk appetite, and are able to be accepted at the Directorate level. As the risk level reaches High or Very High, the risk requires risk escalation to the DRA and the executive team.

2.3.3.2. Risk Escalation: How do we escalate the issue?

High and Very High risks will be escalated to the DRA to manage with the executive team. This is to ensure that management, who have the accountability and authority, can make clear risk informed decisions.

The process of risk escalation allows decision makers to tolerate the risk or apply further risk treatment as required (please see Risk Treatments for further information). It is important to note that all levels below the approving authority for a risk should be aware of the risk i.e. for a Very High risk the DRA, FAS SD, SES Band 1, EL2, and EL1 should all be aware.
Continuous reporting of the High and Very High level risks to the Program Governance Board will be undertaken on a quarterly basis by the DRA.

![SDD Risk Escalation & Review Model](image)

**Figure 6: SDD Risk Escalation & Review model**

### 2.4. Risk Treatment

Risk treatment is the action taken in response to the risk evaluation, where it has been agreed that additional mitigation activities are necessary. Risk treatments are assessed to determine if they are adequate to bring the residual risk levels to a tolerable or appropriate level include, but are not limited to:

- **Avoiding the risk**
  - Seeks to treat the risk by avoiding the event that would lead to the risk.

- **Mitigate the risk**
  - Development of an action plan to reduce the likelihood and/or consequence by addressing identified causes

- **Share the risk with other stakeholders**
  - Involves transferring part of a risk to another stakeholder that can also treat the risk

- **Accept the risk**
  - Accept the consequences should the risk occur.
Risk may be accept or retained for many reasons. Examples of this may include:

- no treatment options available
- the treatment costs more than the consequences
- the potential to realise certain objectives or opportunities

Choosing the most suitable treatment requires balancing the cost and effort of implementation against the benefits resultant from additional risk mitigation. In some cases, further treatment may be unfeasible or unaffordable and the residual risk may need to be accepted.

Where a risk sits above the SDD risk acceptability level of MEDIUM and the decision has been made to accept the risk, it is imperative it be recorded in the areas risk register, together with the reasons for the decision not to treat the risk.

2.4.1. **Mitigating the risk – WHS**

When a hazard is identified, the Hierarchy of control (below) is used as the system to eliminate or mitigate the risk of exposure to certain hazards.

The hierarchy of control is a systematic approach to managing safety in the workplace by providing a structure to select the most effective control measure/mitigating strategy to reduce risk.

When mitigating a risk relating to health and safety, following this hierarchy leads to the implementation of inherently safer systems and practices. The hierarchy has six levels of mitigating controls and includes:

- **Eliminate** – removes the hazard of the danger completely
- **Substitute** – controls the hazard by replacing it with a less risky way to achieve the same outcome
- **Isolate** – separates the hazard from the people at risk
- **Engineering controls** – making physical changes to lessen any remaining risk *(e.g changes/additions to machinery for added protection)*
- **Administrative controls** – applying administrative measures to lessen the risk – *(e.g installing signs)*
- **Personal Protective Equipment (PPE)** – using protective equipment to lessen the risk – *(e.g wearing protective mask, safety goggles etc)*
N.B – You must always aim to eliminate a hazard, which is the most effective control. If this is not reasonable practicable, you need minimize the risk by working through the other alternatives in the hierarchy.

2.5. Risk Owner

Without a risk owner it is difficult to manage any risk. In identifying a risk owner, a risk owner must have the following:

- Knowledge of the environment of where the risk can occur
- The responsibility and accountability for the risk
- The authority to apply resources (people, funding) to mitigate the risk

While there can be only one lead owner, responsibility can be shared with others who have an active role for managing / treating / controlling the risk.

Risk sharing comprises transferring part of the risk to another, such as transferring an activity or a consequence.

An example of this related to Defence may include the risk of a ‘Tree falling on a defence asset or person’.

While the Directorate of Estate, Environment and Energy Service Delivery own that risk in Defence, they share that risk with:

- The contractors
- Our insurers
- Our base management
Why?

- Because the contractors are responsible for delivering the activity and carry impacts if the risk was realised
- Because the insurers wear financial consequences if the risk was realised
- Because our base management are responsible for managing base operations, delivering base plans and assist in the identification, investigation and resolution of service delivery inconsistencies on bases and carry impacts if the risk was realised.

Sharing risk does not mean that the lead ownership has been transferred.

2.6. Monitoring and Review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes.

Risks change over time and all risk documentation should be treated as ‘live’. Priorities can change quite quickly and so can the level and types of risks contained within the documentation.

Monitoring and review is integral to successful risk management and entities may wish to consider articulating who is responsible for conducting monitoring and reviewing activities. Key objectives of risk monitoring and review include:

- detecting changes in the internal and external environment, including evolving organisational objectives and strategies
- identifying new risks
- ensuring the continued effectiveness and validity of the risk and its controls
- seeking to improve the understanding and management of any identified risk
- seek strategies to improve the quality and integrity of information to assess any risk
- learn from any successes and failure in the risk management process

Continuous monitoring and reviewing of operational risks ensure that new risks are detected and managed, action plans are implemented and stakeholders are kept informed. The availability of regular information on operational risks can assist in identifying trends, likely trouble spots or other changes that have arisen.

2.7. Recording and Reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms in SDD. Recording and reporting aims to:

- communicate risk management activities and outcomes across SDD
- provide information for decision-making
- improve risk management activities
- assist interaction with stakeholders, including those with responsibility and accountability for risk.

2.7.1. SDD Risk Register

All business areas are required to establish and maintain systems relating to risk and control as required by the PGPA Act.

The SDD Risk Register is the approved divisional tool used to capture these operational inherent and residual risks within different business areas. It also allows SDD to assess the risk.
in context with the overall Departmental strategy, and records controls and treatment details of those risks.

For further information on how to complete a risk register please view the SDD Risk Management Handbook. The SDD risk register is available on Objective, under “SDD Risk Register”. It can be also found on the intranet as part of the Defence Estate Quality Management System, under ‘‘SDD Risk’ at:


2.7.2. Reporting

Reporting is an integral part of our governance and will enhance the quality of dialogue with stakeholders and support senior management and oversight bodies in meeting their responsibilities. Factors to consider for reporting include, but are not limited to:

- differing stakeholders and their specific information needs and requirements
- cost, frequency and timeliness of reporting
- method of reporting

Risks need to be identified, assessed, controlled and reported by central owners within the controlling SDD Directorates. This process can be summarised by the following steps:

1. SDD Business areas self-identify and capture risks for service/products and identify controls through the development of an SDD risk register.
2. SDD Business areas send completed/reviewed risk registers to the DRA at intervals, dependent on the level of risk.
3. DRA evaluates SDD Business areas risk registers and offers guidance/direction on risk identification, rating and controls.
4. DRA provides feedback to SDD Business areas, in order to identify and monitor risk rating and control effectiveness for future reporting cycles.
5. DRA reports to Senior Executive, via the Program Governance Board (the Board) every three months regarding areas, numbers and specific types of high-level/visibility risks within E&IG.

2.7.3. Maintenance and Sustainment

One of the key intents of the PGPA is to ensure risk management is an integrated element of Commonwealth business activity. To that end, the Framework has been consciously drafted to provide utility as a key tool in supporting and informing SDD business activity.

DRA will liaise with relevant SDD business areas on a quarterly basis to assist them to continue to maintain contemporary risk information and the necessary risk management capability to do so. In addition, this engagement will ensure the Board has oversight of the current state of SDD’s risk liability through the reporting governance referred to at 2.7.2 point 5.

The mutual obligation for SDD business areas is that they must sustain vigilance over their risk management responsibilities on an on-going basis. Business areas need to be attendant to SDD’s principles of risk management as an integrated component of business activity.

For example, business areas need to sustain the effort to be open to the identification of new risks. Should one be identified, it must be assessed, articulated in the relevant Risk Register and escalated to the relevant authority, if required. This would be conducted at the time of discovery instead of waiting until the next quarterly process facilitated by DRA.
3. **References and Legislation**

There are multiple references to related material in the Service Delivery Division Framework, including internal policies and external guidance.

### 3.1. External Guidance

- The *Public Governance, Performance and Accountability Act 2013* (PGPA Act)
- Commonwealth Risk Management Policy (CRMP)

### 3.2. Internal Guidance

- Joint Directive – *JD30/2015*
- E&IG Risk Management Framework

4. **Reviews and approvals**

This document has been reviewed and approved by the personnel listed in the below table. Evidence of the approvals must be retained in accordance with Information Management policy.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tobias Seldon</td>
<td>Director Risk and Assurance</td>
<td>11 Jun 2019</td>
<td>Initial Approver</td>
</tr>
<tr>
<td>Jason Armstrong</td>
<td>Assistant Secretary Service Delivery Division</td>
<td>25 Jun 2019</td>
<td>SES Endorsement</td>
</tr>
<tr>
<td>Monique Hamilton</td>
<td>Acting First Assistant Secretary Service Delivery Division</td>
<td>11 Jul 2019</td>
<td>SES Final Approval</td>
</tr>
</tbody>
</table>
### 5. Summary of changes

<table>
<thead>
<tr>
<th>Version</th>
<th>Details</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Original Version</td>
<td>R. Farrar (Consultant)</td>
<td>18 Dec 2012</td>
</tr>
<tr>
<td>1.1</td>
<td>Acronym/Title Amendments</td>
<td></td>
<td>23 May 2013</td>
</tr>
<tr>
<td>1.2</td>
<td>Document Review</td>
<td></td>
<td>14 Aug 2013</td>
</tr>
<tr>
<td>1.3</td>
<td>Document Review</td>
<td></td>
<td>26 Aug 2013</td>
</tr>
<tr>
<td>1.4</td>
<td>Document Review</td>
<td></td>
<td>30 Oct 2013</td>
</tr>
<tr>
<td>1.5</td>
<td>Document Review</td>
<td></td>
<td>30 Oct 2013</td>
</tr>
<tr>
<td>1.6</td>
<td>Document Review</td>
<td></td>
<td>18 Mar 2014</td>
</tr>
<tr>
<td>1.7</td>
<td>Inclusion of SDD Corporate Risk and Product and Service Managers</td>
<td></td>
<td>28 Mar 2014</td>
</tr>
<tr>
<td>2.0</td>
<td>Document Review (Transition to ESD RMF)</td>
<td>R. McClelland (AD Risk Governance)</td>
<td>04 Jul 2015</td>
</tr>
<tr>
<td>2.1</td>
<td>Terminology Update</td>
<td></td>
<td>19 Oct 2015</td>
</tr>
<tr>
<td>2.2</td>
<td>Terminology Update</td>
<td></td>
<td>18 Feb 2016</td>
</tr>
<tr>
<td>2.3</td>
<td>Terminology Update</td>
<td></td>
<td>30 Mar 2016</td>
</tr>
<tr>
<td>2.4</td>
<td>Terminology Update</td>
<td></td>
<td>01 July 2016</td>
</tr>
<tr>
<td>2.5</td>
<td>Update Authority Table and Corporate Objectives</td>
<td></td>
<td>07 Sep 2016</td>
</tr>
<tr>
<td>2.6</td>
<td>Update Directorate from DSPRP to DPM</td>
<td></td>
<td>06 Jul 2017</td>
</tr>
<tr>
<td>3.0</td>
<td>Document Review (Transition to SDD RMF)</td>
<td>M. Watson (AD DRA)</td>
<td>11 Jul 2019</td>
</tr>
</tbody>
</table>
6. Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td></td>
<td>Outcome of an event affecting objectives</td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td>Any process, device practice or other action that improves the management of a risk</td>
</tr>
<tr>
<td>Enterprise Risk</td>
<td></td>
<td>The key risks used to achieve Defence’s strategic objectives</td>
</tr>
<tr>
<td>Hazard</td>
<td></td>
<td>A situation or thing that has the potential to harm a person</td>
</tr>
<tr>
<td>Inherent Risk</td>
<td></td>
<td>Level of risk if no or failed controls in place</td>
</tr>
<tr>
<td>Likelihood</td>
<td></td>
<td>The chance of a risk happening</td>
</tr>
<tr>
<td>Residual Risk</td>
<td></td>
<td>Level of risk if effective measures and controls are in place</td>
</tr>
<tr>
<td>Risk</td>
<td></td>
<td>Possible events that, if they occur, will impact on corporate goals and strategic objectives</td>
</tr>
<tr>
<td>Risk appetite</td>
<td></td>
<td>The level of risk an entity is willing to accept or retain in order to achieve its objectives</td>
</tr>
<tr>
<td>Risk culture</td>
<td></td>
<td>The set of shared attitudes, values and behaviours that characterise how an entity considers risk in day-to-day activities</td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td>The application of coordinated activities and processes to control organisational risk</td>
</tr>
<tr>
<td>Risk Owner</td>
<td></td>
<td>Person or entity with the accountability and authority to manage risk</td>
</tr>
<tr>
<td>Risk Register</td>
<td></td>
<td>A repository for recording each risk and its attributes, evaluation and treatments</td>
</tr>
<tr>
<td>Risk tolerance</td>
<td></td>
<td>The level of risk-taking that is acceptable in order to achieve a specific objective or manage a category of risk</td>
</tr>
<tr>
<td>Risk Treatment</td>
<td></td>
<td>Process to modify risk</td>
</tr>
</tbody>
</table>
# SDD Risk Tools – Control Effectiveness guide

<table>
<thead>
<tr>
<th>CONTROL EFFECTIVENESS RATING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Effective**                | - Control is fit for purpose in addressing the causes of the risk event and is applied in a consistent manner.  
- Control is effective and has been tested across applicable circumstances and in accordance with contractual obligations.  
- Only minimal work (other than ongoing review and monitoring) can be done to strengthen the control. |
| **Room for Improvement**     | - Moderate amount of work is required to strengthen the control.  
- Control is fit for purpose in addressing the causes of the risk event but is applied in an inconsistent manner. |
| **Not Effective**            | - Significant work is required to improve the effectiveness of the control.  
- The control is not fit for purpose in addressing the causes of the risk event.  
- The control has not been tested or has been tested and is not effective across applicable circumstances or in accordance with contractual obligations. |

# SDD Risk Tools – Likelihood guide

<table>
<thead>
<tr>
<th>LIKELIHOOD RATING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| **Almost Certain**| - The risk event has occurred more than once in Defence in the last 12 months.  
- All critical controls associated with the risk are weak and/or non-existent.  
- Without control improvement, it is very likely that the risk event will eventuate. |
| **Likely**        | - The risk event has occurred more than once in Defence over the last 5 years but no more than once in the last 12 months.  
- Nearly all critical controls associated with the risk are weak.  
- Without control improvement it is more likely than not, that the risk event will eventuate. |
| **Possible**      | - The risk event has occurred once in Defence in the last 5 years.  
- Some critical controls associated with the risk are rated as ‘Effective’.  
- If there is no control improvement, the risk event may eventuate. |
| **Unlikely**      | - The risk event has occurred in Defence but not within the last 5 years.  
- Nearly all critical controls associated with the risk are rated as ‘Effective’.  
- The effectiveness of the risk controls means that it is likely that the risk event eventuating would be caused by external factors not known to Defence. |
| **Rare**          | - The risk event has never occurred in Defence.  
- All critical controls associated with the risk are rated as ‘Effective’.  
- The effectiveness of the risk controls means that it is likely that the risk event eventuating would be caused by external factors outside of Defence control. |
<table>
<thead>
<tr>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>No reputational impact. Event managed internally by Defence – no intervention required. No stakeholder conflict.</td>
<td>Event monitored by Defence public relations staff. Stakeholder conflict but minimal impact on stakeholder confidence.</td>
<td>Event actively managed through Defence public relations processes. Loss of key stakeholder confidence. Local media coverage of event.</td>
<td>Event requires intervention by Defence public relations and senior Defence staff. Loss of key stakeholder confidence. Negative impact on minister, government and/or senior Defence executives. Wide scale negative media coverage of event at national level. Event scrutiny by external agencies such as ANAO, resulting in adverse findings and recommendations.</td>
<td>Event requires intervention by Secretary or Minister. Wide loss of stakeholder and community confidence Secretary or Minister resignation. Sustained detrimental media coverage at international level. Scrutiny via royal commission or similar level enquiry.</td>
</tr>
<tr>
<td>Event causes no disruption to core Defence operations. Minimal local intervention required.</td>
<td>Event causes minimal disruption of core Defence operations, causing minor delays of key functions/activities/service times. Event causes minor realignment of resources to Defence operational priorities.</td>
<td>Event causes noticeable level of disruption of core Defence operations, causing extended delays of key functions/activities/service times. Event causes moderate realignment of resources to Defence operational priorities.</td>
<td>Event causes significant levels of disruption to core Defence operations, causing key functions/activities to break down. Event causes major disruption and activates program area’s business continuity/crisis management plans. Event causes major realignment of resources to Defence operational priorities.</td>
<td>Event cause full disruption of core Defence operations, creating a catastrophic breakdown of functions/activities. Unable to deliver Defence strategic objectives or execute Defence operational priorities.</td>
</tr>
<tr>
<td>No financial impact. Event managed internally by Defence staff – no intervention required.</td>
<td>Event triggers minimal financial/asset loss or damage. Event reported and monitored by Defence property, finance and/or legal staff. Event results in financial impact of up to $100,000.</td>
<td>Event triggers limited financial/asset loss or damage. Event actively monitored through Defence property, finance and/or legal staff. Event results in financial impact of $100,000 – $1,000,000 ($1 million).</td>
<td>Event triggers significant financial/asset loss or damage that exposes Defence resources. Event actively managed through court activity, and/or actively managed by senior Defence property, financial and/or legal staff. Event results in financial impact of $1 million – $10 million.</td>
<td>Event triggers heavy financial/asset loss or damage and may result in major court action/intervention. Event results in financial impact of more than $10 million.</td>
</tr>
<tr>
<td>No legal/regulatory impact. Minimal intervention required.</td>
<td>Event triggers legal liability with low impact potential. Event monitored by Defence legal staff. Event triggers investigation of Defence/Defence personnel from a Commonwealth regulatory or legal body. May require policy and/or process adjustments to correct issues.</td>
<td>Event triggers legal liability with medium impact potential. Event actively managed by Defence legal staff. Event triggers Defence/Defence personnel receiving a warning from a Commonwealth regulatory or legal body. Structured policy and/or process adjustments required to correct issues.</td>
<td>Event triggers legal liability with significant impact level. Requires intervention by senior Defence legal staff and court activity. Event triggers Defence/Defence personnel receiving a fine from a Commonwealth regulatory or legal body. Key policy and legislative gaps identified for correction.</td>
<td>Event triggers high-profile breach of law or major exposure to compensation claims (e.g. class actions) in the High Court. Senior Counsel and/or Ministerial intervention required. Event results in Defence/Defence personnel having to face criminal prosecution. Systematic failure of legislation, policy or process that allows high-volume operational errors, misconduct that affects operations or creates critical weaknesses in Defence controls.</td>
</tr>
<tr>
<td>Negligible damage, contained on-site. Fully recoverable with no permanent impact on the environment. The impact will take less than 6 months for the resource to fully recover.</td>
<td>Minimal damage to the environment. The impact will take less than 2 years to fully recover or it will only require minimal repair.</td>
<td>Limited damage is caused to the environment which is repairable. The impact will take up to 10 years to recover.</td>
<td>Extensive and irreversible damage is caused to the environment. OR Limited repairable damage is caused to significant environment area (as per the Environment Protection and Biodiversity Conservation Act 1999) from which it will take more than 10 years to recover.</td>
<td>Extensive and irreversible damage is caused to the environmentally significant area (as per the Environment Protection and Biodiversity Conservation Act 1999).</td>
</tr>
<tr>
<td>Event is a near-miss where an injury does not occur. Mental strain/anguish during event that requires no time off work and no counselling, but requires monitoring.</td>
<td>Minor injury or illness that is treatable in the workplace (first aid) or by a registered health practitioner, with no follow up treatment. Mental anguish/psychological repercussions that require minimal professional psychological treatment or time off work of up to two weeks. Suffers decreased self-confidence and work performance.</td>
<td>Injury or illness causing non-permanent disability, which requires non-emergency medical attention by a registered health practitioner, or 10 or more injuries or illnesses classified as minor. Mental anguish/psychological repercussions that require time off work of more than two weeks and require professional psychological treatment.</td>
<td>Serious injury or illness requiring immediate admission to hospital as an inpatient and/or partial permanent disability, or 10 or more injuries or illnesses classified as moderate. Suicidal ideation, self-harm or harm to others manifested. Severe mental anguish that requires significant psychological treatment. Requires extended time off work.</td>
<td>Loss of life and/or total permanent disability (physical and/or psychological), or 10 or more injuries or illnesses classified as major.</td>
</tr>
<tr>
<td>Event causes insignificant damage to integrity of SDD/E&amp;IG related data network or confidentiality of Defence information.</td>
<td>Event causes minor damage to integrity of SDD/E&amp;IG related data network or confidentiality of Defence information. Event triggers increased measures that reinforce security awareness, practice of security and safety drills.</td>
<td>Event causes moderate damage to integrity of SDD/E&amp;IG data network or confidentiality of Defence information.</td>
<td>Event causes major damage to integrity of SDD/E&amp;IG data network or confidentiality of Defence information. Event triggers an upgrade of the Defence Safebase Security Alert System to ‘Alert’. Additional access control measures; increased security messaging to all staff; preparation for emergency security controls; reduced activity on site.</td>
<td>Event causes severe damage to integrity of SDD/E&amp;IG data network or confidentiality of Defence information. Event causes an upgrade of the Defence Safebase Security Alert System to ‘Act’. Severe restrictions to access/locking of site; security measures to support escape, hide, tell; frequent emergency communications; evacuation and lockdown routines.</td>
</tr>
</tbody>
</table>
## SDD Risk Tools – Risk Matrix

<table>
<thead>
<tr>
<th>RISK MATRIX</th>
<th>INCONSEQUENTIAL</th>
<th>MINOR</th>
<th>MODERATE</th>
<th>MAJOR</th>
<th>SEVERE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>Low (Green)</td>
<td>Medium</td>
<td>High</td>
<td>Very High (Red)</td>
<td>Very High</td>
</tr>
<tr>
<td>Likely &amp; Possible</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Rare</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>