



**Australian Government**  
**Department of Defence**

# SAP Incident Management Guide



---

## Purpose

The purpose of this document is to provide broad guidance for the implementation of Incident Management in GEMS.

Incidents often require immediate make safe/good activities. All such activities take precedence over the process of documenting incident management in GEMS. This incident management process should be followed once initial danger has passed and immediate actions have occurred.

---

## Background

Historically Estate and Infrastructure Group (E&IG) has captured and managed environmental related incidents through formal processes. All other Incidents that contain an Estate related component are reported through various Defence mandated Incident management systems. E&IG manage these incidents through various ad-hoc processes which result mostly in reactive works.

The introduction of Defence SAP provides the opportunity to create a standardised E&IG Incident management system. The focus of the system will be on managing incidents to ensure the continued provision of estate and infrastructure services enabling capability preparedness.

Existing Defence mandated Incident management systems such as Sentinel, Defence Policing and Security Management System (DPSMS) will continue to be used to and will not be duplicated in SAP unless there is a specific investigation or impact necessitating it. The inter-relationship of these systems will be matured as E&IG expands implementation of the SAP module across the Group.

## Key Terminology

Term	Description
<b>Incident</b>	An Incident is an unplanned, undesired event that adversely affects the completion of a task and/or endangers the safe operation of the Defence estate and/or the environment.
<b>Incident Management</b>	Incident Management is the end-to-end process of recording, processing, investigating, undertaking corrective actions and closing incidents that relate to the Defence estate.
<b>Task</b>	A Task (notification) is a link used for quick access to the Edit Incident window. Tasks are available to multiple users from various functional areas by accessing the Work Overview item. Tasks may also be accessed via the Universal Work List (UWL).
<b>Asset</b>	An Asset is any item, object or structure that is a part of the Defence estate
<b>Release</b>	A Release is a substance (solid, liquid or gas) that is discharged into the environment during an incident.
<b>Notice of Violation</b>	<p>A Notice of Violation (NOV) could be in the form of:</p> <ul style="list-style-type: none"> <li>▪ a breach in legal obligations</li> <li>▪ a breach in policy</li> <li>▪ a non-conformance to a Defence guideline</li> <li>▪ a non-conformance to a Standard Operating Procedure (SOP).</li> <li>▪</li> </ul>
<b>Environmental Factor</b>	An Environmental Factor is an aspect of the estate's environment, such as the presence of threatened species, pests and weeds, and man-made aspects and impacts upon the environment such as the presence of Heritage Sites, Asbestos and Contaminated Sites.
<b>Health and Safety</b>	Health and Safety refers to the function where users can create and manage information about incidents and hazards related to the estate's assets and environment.

---

## Incident Management Process Overview

The incident management process covers the following key steps:

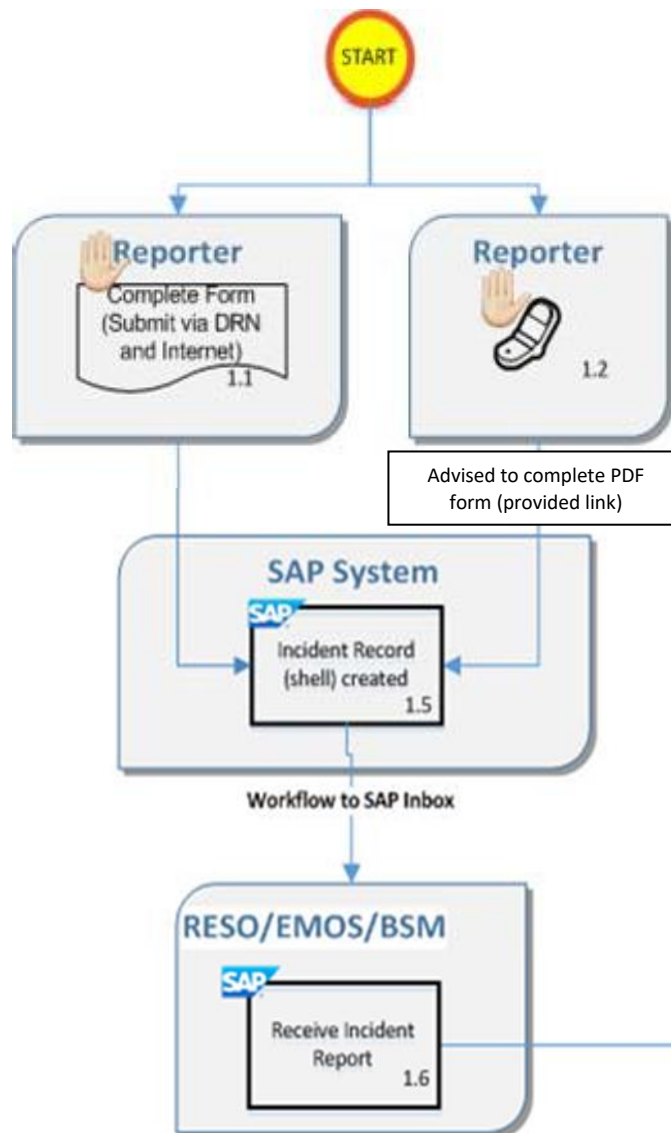
- Incident Occurs
- [off system- make safe/good] actions
- Incident Reported and recorded
- Incident is accepted or rejected
- Incident investigation if required
- Remediation activities/task undertaken
- Incident Closed
- Reporting – Operational and Analytical reports available

## Key SAP and Business Roles:

SAP Function			Business Function
<p><b>The Incident Reporter and Task Implementer</b> roles are the more ad-hoc users</p>	<p><b>Incident Reporter</b></p>	<ul style="list-style-type: none"> <li>Creates an Incident report</li> </ul>	<ul style="list-style-type: none"> <li>Direct Entry – Any SAP endorsed user</li> <li>via PDF:               <ul style="list-style-type: none"> <li>Any DRN User</li> <li>Any external user requires email forward to DRN user for automated upload</li> </ul> </li> </ul>
	<p><b>Task Implementer</b></p>	<ul style="list-style-type: none"> <li>Checks workflow notifications</li> <li>Carries out tasks needed</li> <li>Confirm tasks have been completed</li> </ul>	<ul style="list-style-type: none"> <li>EMOS (NPS/PDS) for Estate related works</li> <li>Any user appointed by the incident manager or investigator.</li> <li>Tasks may be managed off system and reported to the Incident Manager as Appropriate</li> </ul>
<p><b>Incident Manager and Incident Investigator</b> roles are the significant transactors within SAP</p>	<p><b>Incident Manager</b></p>	<ul style="list-style-type: none"> <li>Reviews, accepts or rejects the incident</li> <li>Gathers and records additional information such as: extent and complexity of damage, assets involved, breach of legal obligations, cost estimates.</li> </ul>	<ul style="list-style-type: none"> <li>Workflow to Incident Manager (RESO / BM)</li> <li>Environmental incidents – as per <a href="#">Defence Environmental Incident Reporting Guideline</a></li> </ul> <p>Can be on-forwarded to alternate Incident Manager (e.g. PD for management).</p>
	<p><b>Incident Investigator</b></p>	<ul style="list-style-type: none"> <li>Detailed investigation Identifies, records the likely drivers of the incident,</li> <li>Lessons learnt initiates tasks, work orders/ projects.</li> </ul>	<ul style="list-style-type: none"> <li>Any user appointed by the Incident Manager</li> <li>An SME in the area of investigation.</li> <li>The incident manager may also act as the investigator.</li> </ul> <p><b>Note:</b> Not all incidents require an investigation.</p>

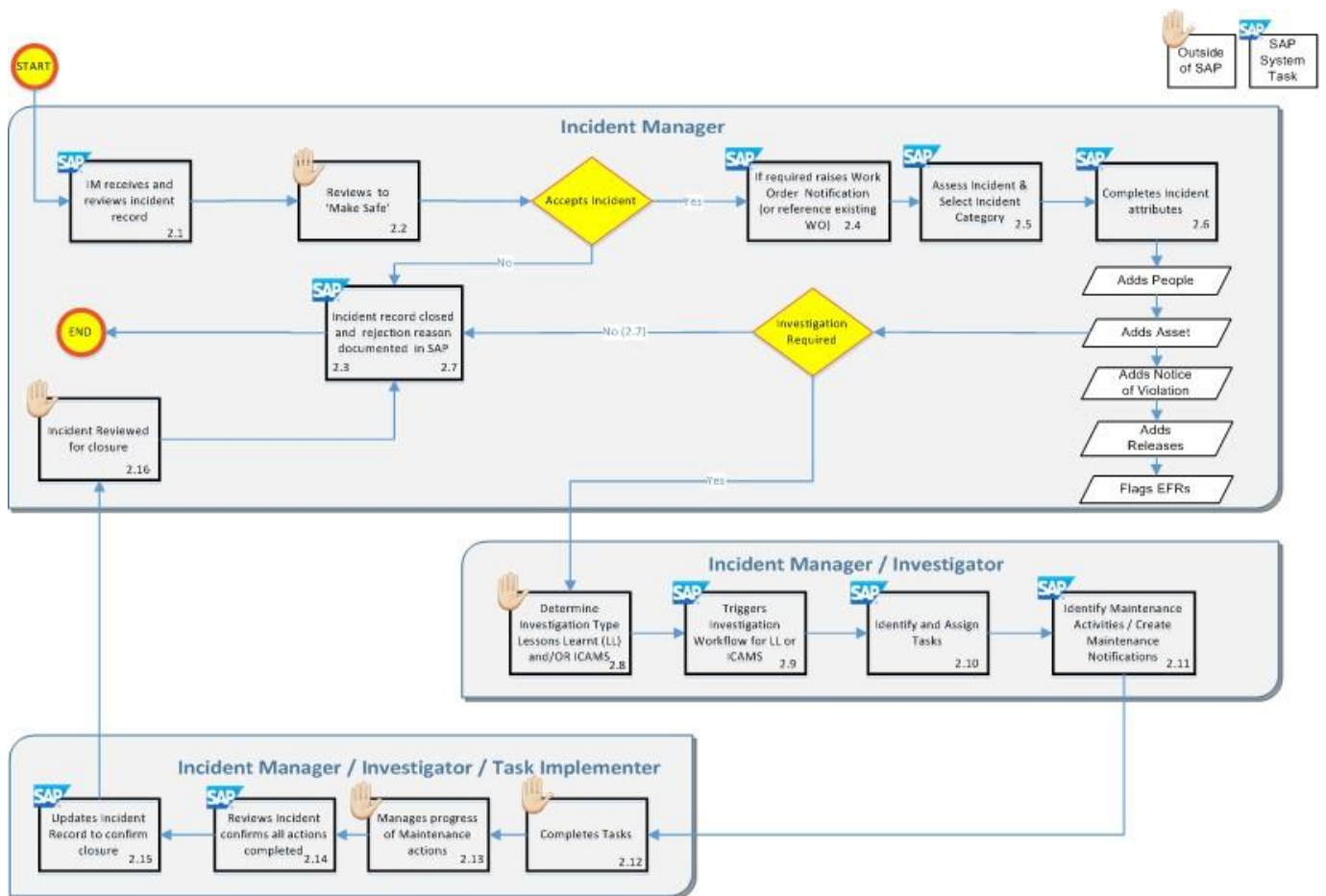
# Incident Management Process – Process

## 1. Incident Reporting and Recording



Step	Instruction	Guidance
1	<p>One of two methods can be used to report an incident:  An <b>Incident Reporter</b> completes the web-enabled PDF Incident form (via DRN or DEQMS); <b>Or</b>  An <b>Incident Reporter</b> calls the BSSC who records the incident.</p>	<p>The BSSC in most instances will advise the caller to complete an incident report form and send them a link.  A copy of the form is available at <b>Annex A.</b></p>
2	<p>On submission of a completed PDF form an email is generated and automatically updated to the SAP system and an incident record is created.</p>	<p>The completed incident report will be automatically uploaded to the SAP system on submission. This will trigger a workflow and notify system users that an incident needs to be actioned.</p>
3	<p>Notification of the incident is sent to multiple managers. Depending on the nature of the incident one of the managers will accept the incident and take on responsibility for managing and assessing it.</p> <p>Once accepted all sent incident report notifications are removed from the other SAP inboxes.</p>	<p>Where an incident does not fall within the remit of the current nominated managers, the BM should accept the incident and forward it to the relevant Product Director or Functional Lead.</p>
4	<p>Incident types include:</p> <ul style="list-style-type: none"> <li>▪ Environmental Incidents,</li> <li>▪ Fire (Structural and Bushfire)</li> <li>▪ Estate Only incidents</li> <li>▪ Capability/Infrastructure Failures</li> </ul>	<p>Definition of these incident types is being matured, broad guidance is available at <b>Annex C.</b></p>

## 2. Incident Processing, Investigation and Closure



Step	Instruction	Guidance
1	Once the manager accepts responsibility for the incident they become the Incident Manager (IM).	The manager considers actions already taken to make safe and determines whether any other immediate action is required.
2	<p>On review of the incident the <b>IM</b> may reject the incident and VOID it. In order to do this the reason must be recorded.</p> <p>If the <b>IM</b> accepts the incident as being valid, remedial action such as tasking or Work Order notifications may be created in the SAP system.</p>	<p>'VOID' means an incident has been reported that is considered either a duplicate record, or does not represent an valid incident. The record is not lost and its submission is still recorded on system.</p> <p>Valid incidents where no further action is required can be immediately CLOSED. This will apply to many smaller incidents where all make good actions have been completed and there is no lasting impact, work requirements or requirement for investigation. The incident manger will simply have to complete details within the incident record prior to closure.</p>



<p>3</p>	<p>The <b>IM</b> assesses the incident and selects an incident <b>category</b>.</p> <p>The Incident Manager also updates the following incident <b>attributes</b>:</p> <ul style="list-style-type: none"> <li>▪ Damage to Asset</li> <li>▪ Notice of violation</li> <li>▪ Releases</li> <li>▪ EFR's (Environmental Factor Records)</li> </ul>	<p>The current category structure is being reworked. For now IM's are to choose the category that is best suited to the incident – mindful that all WHS category incidents must be reported in sentinel.</p> <p>SAP provides guides on updating attributes.</p>
<p>4</p>	<p>The <b>IM</b> decides whether the incident needs to be investigated.</p> <p>If no investigation is required, the incident record is <b>CLOSED</b>.</p> <p>Once again a reason why must be included before the incident can be closed.</p>	<p>The incident manager may also be the incident investigator.</p>
<p>5</p>	<p>If an investigation is however needed the <b>IM</b> assigns an Incident Investigator via a Work Overview item within the SAP system.</p> <p>The <b>Incident Investigator (II)</b> examines the processed Incident record completed by the Incident Manager and determines the Investigation Type – SAP provides two types:</p> <ul style="list-style-type: none"> <li>▪ <b>Lessons Learned (LL)</b></li> </ul> <p>A critical part of contributing to the correct methods of managing incidents affecting assets on the Defence estate and could also be used to improve existing Standard Operating Procedures (SOPs).</p> <ul style="list-style-type: none"> <li>▪ <b>Incident Cause Analyses Method (ICAM )</b></li> </ul> <p>The root cause of incidents is categorised to allow consistency across investigation records and provide trend analysis in reporting.</p> <p>Post investigation the incident investigator or manager may raise further tasks (which include activities or work order notifications) as remediation items.</p>	<p>It is not expected that Sentinel WHS investigations will be replicated in SAP.</p>

6	<p>Once the <b>II</b> completes the investigation they will notify the IM via SAP workflow. The <b>IM</b> manages the progress of the maintenance actions and reviews and confirms the completion of all actions by:</p> <ol style="list-style-type: none"> <li>1. Ensuring the investigation is not marked as <b>In Process</b> and that the investigation/s are displayed as Complete</li> <li>2. Verifying that there are no outstanding action tasks or maintenance notification tasks relating to the Incident</li> <li>3. Confirming that completed tasks can be marked as <b>Closed</b></li> </ol>	<p>There are strict closure rules within the SAP module that must be followed to allow the incident to be closed out in the system.</p>
7	<p>The <b>IM</b> updates the incident record to confirm closure and closes the incident Record in the SAP System.</p>	<p><b>NOTE:</b></p> <p>Once the investigation process is completed the status is set to <b>CLOSED</b>.</p> <p>All Incident records can still be viewed and accessed after the incident is closed.</p>

---

## Incident Management Reporting

There are two types of analytical reports available through the Reporting functional area in Defence SAP that can be utilised to perform incident related analysis:

### **Dashboard Reports**

Gives a broad overview of incident activities and provide graphical representations of data providing graphical displays such as bar charts and graphs

### **Analysis Reports**

Produces a list of items that fall within specific parameters, or a list of specific aspects of a report. The reports display data in different formats, and both types of reports can be customised by setting different filter options. Analysis reports are different to Dashboards as the parameters e.g. date, time, location must be set in the prompts window before the report can be viewed.

The reports provide a broad overview of Incident activities and can be customised by setting different filter options.

Work will commence with the Product Directors and Functional Leads to determine the reports required for SDD and it is expected this will further drive the nature of incidents that will be captured.

---

## Support and help

For further support on SAP system processes to the SAP Incident Management system guides available at:

<http://drnet/dsrg/GEMS/InterfaceAssets/GEMSGateway.aspx#AccTngTraining>

<http://easrsn159.eas.mil.au/gm/cabinet-1.25.501>

For environmental incident reporting:

[Defence Environmental Incident Reporting Guideline](#)

For Business Process support please visit the DEQMS website at:

<http://intranet.defence.gov.au/estatemangement/lifecycle/IncidentManagement/Default.asp>

---

## Annex A:

### **Incident Report form**

A web-enabled copy of the form is available at:

<http://intranet.defence.gov.au/estatemangement/lifecycle/IncidentManagement/Default.asp>

# Report Incident



Australian Government

Department of Defence

## E&IG GEMS - Incident Management & Reporting

### Scope

This form is only for reporting Estate related incidents, including Environmental incidents. For details on how to report all other incident types go to -

<http://drnet/AssociateSecretary/AFCD/Incident-Reporting/Pages/Home.aspx>

If required, further instructions on reporting an environmental incident are available on:

Intranet - <http://intranet.defence.gov.au/estatemangement/lifecycle/IncidentManagement/Environment.asp>

Internet - <https://www.defence.gov.au/estatemangement/lifecycle/IncidentManagement/Environment.asp>

Tip - The PDF incident report form contains hover-over instructions on how to complete each field.

### Form Details

#### What happened and which immediate actions have been carried out?

**Title:** A short description of the event e.g. Diesel Spill hyphenated with a short location description e.g. Fire Training School, RAAF Base Amberley - [Diesel Spill - Fire Training School, RAAF Base Amberley]

**Description of Events:** What, where, when, and why. Include the following specific information for the incident types below:

- Fuel Spill - Material spilt, estimated quantity in litres, receiving environment (air/water/ground), land ownership if not Defence.
- Vegetation/wildlife/community/wetland impacts - EPBC conservation status of affected matter.
- Notice of Violation (breach of legislation, compliance requirement or policy) - issuing authority, date, type of breach e.g. EPBC condition of approval breached, ECC condition not met, or management order from local government.
- Resource usage - material, volume, circumstance.
- Waste/dumping - materials, circumstances if known.

**Immediate Actions:** Detail any immediate response actions e.g. Barricades erected to prevent further damage, absorbent material and spill kit deployed, works immediately stopped, environmental officer notified etc.

#### When did it happen?

**Date:** DD/MM/YYYY format - 30/01/2020

**Time:** 24 hour time format - 1300

**Incident Rating:** If known, specify the consequence (Insignificant to Severe) of the incident based on the highest impact category in the E&IG Risk Management Framework. Do not use the 'Dangerous' category. WHS aspects should be reported in the appropriate system(s).

#### Where did it happen?

**Region:** The Region - e.g. Queensland

**BSA:** The Base Service Area - e.g. Brisbane

# Report Incident

---



Australian Government  
Department of Defence

**Location:** The Property - e.g. Gallipoli Barracks

**Location Description:** Where possible, specify any asset or equipment affected and the location relative to that item e.g. Northwest corner Building 32. For remote or difficult to describe sites provide the name or description of the general location e.g. Freshwater Beach, and where possible provide geographic coordinates including the datum and projection (e.g. WGS84) of the coordinates and the source of coordinates e.g. Training Area Special map or GPS.

*Note that the incident manager will need to provide a sketch of the location for GED.e GEMS mapping. The Location Description should be sufficient to allow a reasonable sketch to be made, or a sketch of location can be attached to the incident PDF using the left-hand menu on the PDF browser. Please indicate in the Location Description if a sketch has been attached to the form.*



# Report Incident

## Reporting Person

Personnel Number:	<input type="text"/>		
First Name:	<input type="text"/>	Last Name:	<input type="text"/>
Organization Unit:	<input type="text"/>	Address:	<input type="text"/>
Phone:	<input type="text"/>	E-Mail:	<input type="text"/>

## What happened and which immediate actions have been carried out?

Title *:	<input type="text"/>
Description of Events:	<input type="text"/>
Immediate Actions:	<input type="text"/>

## When did it happen?

Date *:	<input type="text" value="24/06/2020"/>	<input type="text" value="00:00:00"/>	<input type="text" value="AUSACT-Australia Capital Territories"/>
	<input type="checkbox"/> Time Unknown		

## Where did it happen?

Region *:	<input type="text"/>	Incident Rating	<input type="text"/>
BSA *:	<input type="text"/>		
Location *:	<input type="text"/>		
Location Description:	<input type="text"/>		

## Who witnessed the incident?

Personnel Number:	<input type="text"/>		
First Name:	<input type="text"/>	Last Name:	<input type="text"/>
Organization Unit:	<input type="text"/>	Address:	<input type="text"/>
Phone:	<input type="text"/>	E-Mail:	<input type="text"/>

*I accept accountability for all information provided in this Incident Reporting Form and I confirm that the information provided is accurate, detailed and represents a full disclosure of all facts available to me at the time of lodgement of this form.*

## Annex B:

SAP Workflow nominated incident managers:

Person	Email	Role
Glenn Hewton	<a href="mailto:glenn.hewton@defence.gov.au">glenn.hewton@defence.gov.au</a>	RESO
Heath Rosen	<a href="mailto:heath.rosen@defence.gov.au">heath.rosen@defence.gov.au</a>	BSM
Kerrie Lock	<a href="mailto:kerrie.lock@defence.gov.au">kerrie.lock@defence.gov.au</a>	RESO
Paul Screen	<a href="mailto:Paul.screen1@defence.gov.au">Paul.screen1@defence.gov.au</a>	BSOM
Rebecca Worrall	<a href="mailto:Rebecca.WORRAL@defence.gov.au">Rebecca.WORRAL@defence.gov.au</a>	RESO
Richard Poli	<a href="mailto:richard.poli@defence.gov.au">richard.poli@defence.gov.au</a>	RESO
Sam Stead	<a href="mailto:samuel.stead@defence.gov.au">samuel.stead@defence.gov.au</a>	RESO
Stephen Marazes	<a href="mailto:EMOS-Manager.BNE@defencegov.au">EMOS-Manager.BNE@defencegov.au</a> <a href="mailto:stephen.marazes@defence.gov.au">stephen.marazes@defence.gov.au</a>	EMOS

## Annex C:

### Incident Types – Deployment 1

#### **Environmental Incidents**

Existing policy and business processes remain extant, guidance is obtained from the Defence National Environment Standard – Environmental Incident and Reporting Management. Further information is available at:

<http://wwwdev/estatemangement/lifecycle/IncidentManagement/environmentestate.asp>

#### **Fire**

There are currently several Fire Incident management systems. It is anticipated that in the longer term all Estate and Infrastructure related fire events will be recorded using the Defence SAP Incident system. As the Defence SAP incident system is implemented it is expected that guidance will mature. For the immediate future the following guidance is offered:

Bushfire:

For deployment 1 it is expected that the current Bushfire Event processes will remain extant. If a bushfire is reported using the incident form, then the incident record should be completed within the incident module and a respective EFM Fire Event record created. There may be cases where, an investigation is required if this is the case then the investigation should be carried out within the incident management module.

Other Fires:

Other fires – considered to structural or equipment related and not within the scope of Bushfire or range fires should have incident records created. This will assist in identifying the type and nature of fires, with the aim of providing clearer guidance on recording fire incidents.

#### **Estate Only Incidents:**

The formal definition of an estate related incident is yet to be agreed. E&IG currently does not capture in one system incidents that have an impact on Defence Estate or Infrastructure. The aim is to have a single ERP that captures the cost and nature of Defence Estate related incidents, Defence SAP will be that system.

The scope of Incidents as agreed with the DGWHS is that SAP will only record Estate related incidents with all incidents related to an injured person being in Sentinel. Any incidents that have both an injury and estate impact may be logged in both systems.

The caveat to this is:

The SDD executive has endorsed that where an injury related incident has occurred and the remediation is routine and not complex then a work order may be raised and the sentinel reference number recorded. There is no requirement to duplicate the incident and record it in SAP. There is still work to be done in defining the thresholds for routine and complex, however if an investigation is required and is not supported through the current sentinel processes, then a SAP Incident must be logged.

It is expected that the EMOS/RESO/BSM will consult with each other and determine what Estate related incidents are reported in SAP.



## **Capability and Infrastructure Failure**

Service Level Partnering Arrangements (SLPA):

There are SLPAs between E&IG and each Service and Group. Each Service and Group articulates their specific requirements and services. The scope of the SLPA is to establish:

- Standard E&IG products and services schedule to allow visibility of and accessibility to E&IG partners.
- Basis for E&IG to deliver products and services within a financial framework that provides transparency and accountability.
- Service level prioritisation input by E&IG partners.
- Governance arrangements to ensure national consistency of products and services in line with Defence priorities whilst also being responsive to local requirements.
- Transparency in performance and a commitment to achieve agreed quality assurance levels.

Details on each SLPA can be found at:

<http://drnet/dsrg/DSAA/Pages/Service%20Level%20Partnering%20Agreement%20and%20Service%20Offer.aspx>

It is intended that when there is a failure or disruption to capability/infrastructure delivery as outlined in the respective Groups/Services SLPAs then the incident will be logged so that the information is able to be analysed and used for a variety of purposes.

For deployment 1 it is expected that Senior Managers within the Brisbane BSA will have an understanding of the infrastructure and capability that is required by their stakeholders. It is where these fail that incidents will need to be raised.