

Auditing and assessing emergency operations

Purpose

- Verify the degree of compliance with emergency management (EM) plans, policies, procedures, risk assessments and relevant legislation
- Provide assurance that personnel are complying with requirements
- Identify issues and non-conformances for investigation and corrective action to prevent reoccurrence
- Identify opportunities for improving the management of emergencies
- Strengthen EM knowledge and capabilities through increased coaching opportunities

Types

- Assessments – conducted by personnel or teams completing the task usually using a standard checklist
- Internal (DPI) audits – by independent auditors not involved in the activity and usually coordinated at a State Coordination Centre (SCC) or Local Control Centre (LCC) level
- External audits – conducted by auditors external to Department of Primary Industries (DPI), usually contracted for a specific skill or reason, eg aircraft operator audits

Assessments

- Function officers (eg Operations Officer) are responsible for scheduling and managing assessments
- Non-conformances are to be addressed in a timely manner
- Systemic issues are to be elevated to the Incident Controller to be addressed

Planning audits

- Audits are managed by the Planning function. An Audit Coordinator may be appointed to ensure effective auditing of the emergency operations
- Engage function officers to determine high risk or problematic areas to be audited
- Develop an audit program to address risks
- Assign appropriate auditors and ensure Work Health & Safety processes are followed by all auditors

Preparation

Brief of the auditor should include:

- Unique identification number, audit title (short description of audit) and audit scope
- Contact details and location of auditees and time frame for audit completion
- Providing or arranging access to documents relevant to the audit, including copies of:
 - Audit report template
 - System documents relating to the audit scope and activities
 - Previous audit reports, corrective action documents, incident reports
 - Self or team assessment reports (if applicable)

The auditor should:

- Contact auditees and confirm the scope, date, time and likely duration of the audit
- Study the briefing documents
- Prepare the draft audit report including the checklist
- Plan how the audit will be conducted eg evidence required and how that will be obtained

Initial meeting

Auditor to conduct an initial meeting to confirm:

- The proposed audit plan (scope, activities and timeframe) with key contacts (usually the Site Supervisor at field sites, Officer In Charge at Forward Command Posts, Controller or relevant function officer at LCC and SCC)
- Proposed communication channels
- Logistics for site access and suitable meeting places
- Restrictions on site, required Personnel Protective Equipment and process to report hazards during the audit observations

Conducting the audit

- Gather information and evidence relating to the scope and audit criteria by employing questioning techniques, listening, examining documents and records, observing activities and inspecting facilities
- Record evidence on the audit form
- Evaluate the information against the documented system, establishing compliance (yes), partial conformance (part), non-compliance (no) or not applicable (NA) – record on the audit form
- Investigate the extent of any variation from the system requirements and the possible implications
- Conduct an exit interview with the auditees to:
 - discuss findings, highlighting areas of non-conformance and partial conformance
 - correct any errors documented during the observations
 - indicate recommendations that will be made on the report

Note 1: The auditor has no authority to insist on any changes to activities based on audit findings. The relevant supervisor/function officer/controller is responsible for assessing and implementing recommendations (if appropriate).

Note 2: If auditors become aware of serious breaches of legislation, criminal behaviour or serious non-compliance to DPI policies and Code of Conduct, a report should be made immediately to the relevant supervisor or function officer (depending who is involved in the breaches) and to the relevant controller (via the audit co-ordinator if appointed).

Note 3: If dangerous or life-threatening situation is observed by the auditor, the issue must be raised immediately with the local supervisor to enable corrective action to take place without delay. An incident notification report must be completed.

Reporting

- Internal audit reports should be completed using the Audit report template with associated paperwork and labelled photos
- External audit reports should address the key points from the Audit report template, ie summary of the general performance with respect to the audit scope, any non-conformities, recommendations or opportunities to improve
- Reports should be submitted within a week of conducting an audit

Audit responses

The relevant position (usually a function officer or support personnel) is required to:

- Consider the recommendations and any actions required including further investigations of issues. This should be done in consultation with personnel responsible for the activity.
 - Note 1: Recommendations do not have to be implemented but must be responded to with an explanation of non-implementation.
 - Note 2: It may also be possible only to implement some recommendations post response, requiring a note to that affect.
- Record the required actions in the 'response' column on the report
- Implement and track relevant actions
- Enter the date when relevant actions have been completed
- Enter name, position and date when relevant responses are completed
- Provide the audit coordinator with a copy of the audit with the completed responses (see note 1 and 2 above)

Further information

[Form – audit report template](#)

[Form – audit program template](#)

[Safe work method statements](#)

Incident notification form (Department of Industry intranet online form)