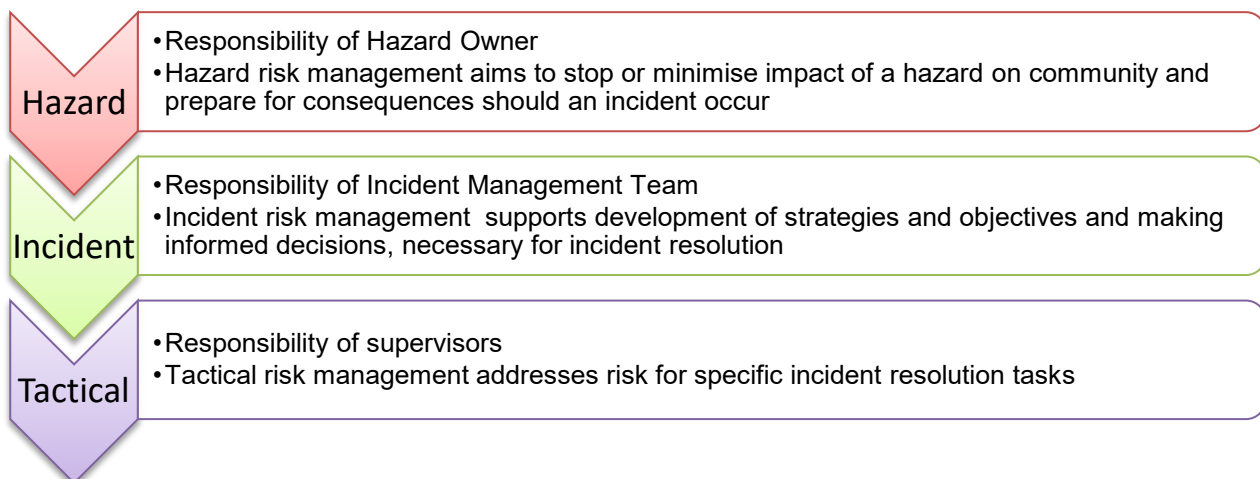# Risk management for emergencies

Effective emergency risk management minimises impacts on community through prevention, mitigation, and treatment.

Risk management is everyone's responsibility with particular onus on Hazard Owners, incident managers and supervisors. Risk management for emergencies occurs at three levels:

Hazard
- Responsibility of Hazard Owner
- Hazard risk management aims to stop or minimise impact of a hazard on community and prepare for consequences should an incident occur

Incident
- Responsibility of Incident Management Team
- Incident risk management supports development of strategies and objectives and making informed decisions, necessary for incident resolution

Tactical
- Responsibility of supervisors
- Tactical risk management addresses risk for specific incident resolution tasks

Hazard and incident level

Risk management supports prevention, mitigation, and planning. Risk management is required to identify areas of risk prior to and during an emergency response. Risks and the associated control activities are then incorporated into the planning and decision-making processes.

Completing the Hazard and incident risk assessment template

Numbers below correspond to cells on the template. Referenced tables are in the template.

1. Succinctly identify the risk. Update the footer (including the date and version) and filename with the risk.
2. Determine the context and parameters of the risk within which risks will be managed e.g., area, timeframe, or hazard.
3. Record the acceptable level of risk as determined by the risk owner i.e., the acceptable level of protection (ALOP). Further management actions will be required when estimated risk is higher than the acceptable level.
4. Number the risks sequentially.
5. Describe risks that contribute to the risk, applicable to the context.
6. Identify the risk owner, which can include one or multiple agencies, roles, industry organisations, and/or community groups. Do not enter individual's names, use their role.
7. Identify what may cause or contribute to the risk.
8. Describe the impact on the response/organisation if the risk occurs, i.e., consequence.
9. Rate the consequence for the area(s) of impact without control measures, i.e., the inherent consequence – Table 1.
10. Assess likelihood of risk occurring without control measures, i.e., inherent likelihood – Table 2.
11. Determine the inherent risk rating for the likelihood and consequence – Table 3.
12. List the existing control measures that mitigate each risk (using the hierarchy of controls).
13. Rate the residual consequence for the area(s) of impact based on the controls – Table 1.
14. Assess residual likelihood of the risk occurring based on control measures – Table 2.

15. Determine the residual risk rating (i.e., remaining risk after treatment which can contain unidentified risk) based on the likelihood and consequence – Table 3. Refer to Table 4 for acceptance of risk and monitoring criteria.
16. Identify risks requiring monitoring, due to level of risk in Table 4 and control effectiveness (Table 5).
17. State the overall residual risk with the agreed mitigations in place.
18. Provide a recommendation for risk tolerance to avoid, mitigate, accept, or share the risk, including any further management actions.
19. Enter the names, roles and agencies/organisations (if relevant) of people involved in the preparation of the risk assessment and the date completed.
20. Obtain approval from relevant role (Table 4); enter the name, role and date of approval.

Tactical risks

Tactical risk management relates to specific events, tasks or operations that are conducted at a tactical or command level and are used to enhance planning processes. Some tasks may involve multiple risk assessments to address different risks associated with the task. For example, transporting carcasses have health and safety risks to operators and biosecurity risks, each with different areas of impact and treatment.

Task risk assessments:
- are required when stipulated in operating procedures
- should be conducted or reviewed prior to a task being undertaken

Completing the Task risk assessment template

Referenced tables are in the template.
1. Task - Identify the task, e.g., Maintaining biosecurity entering and exiting properties
2. Context – Determine the context of the risk, including parameters, conditions or boundaries within which risks will be managed e.g., a specific property, type of property, area or region.
3. Risk factors/causes - identify what may cause or contribute to the risk.
4. ALOP - Record the acceptable level of risk as determined by the risk owner. Further management actions will be required when residual risk is higher than the acceptable level.
5. Specific risk – Identify the specific risk
6. Area(s) of impact - List area(s) of impact from Table 1. Multiple areas of impact can be incorporated in a single risk assessment or each area of impact may have individual risk assessments. Areas of impact may be clarified if required e.g., health & safety – hearing.
7. Inherent risk - Evaluate the inherent risk profile using the likelihood, consequence, and risk rating tables – Tables 1, 2 and 3. The area of impact will provide a guide to the consequence rating. If multiple areas of impact are included on a single risk assessment and give different consequence ratings, it may be practical to split into separate risk assessments. Alternatively, use the greatest consequence measure.
8. Risk controls - List (using a numbered list) the current risk controls. These controls should be included in the task procedures where relevant and should take account of hierarchy of control.
9. Residual risk (is the remaining risk after treatment and may contain unidentified risk). Re-assess the risk profile after treatments are applied using Tables 1, 2 and 3.
10. State the overall residual risk with the agreed mitigations in place and control effectiveness (Table 5).
11. Provide a recommendation for risk tolerance to avoid, mitigate, accept, or share the risk, including any further management actions, including monitoring.
12. Prepared by and date - Enter the names, roles, and agencies/organisations (if relevant) of people involved in the preparation of the risk assessment and the date completed.
13. Obtain approval from relevant role (Table 4); enter the name, role, and date of approval.

Definitions

Term	Definition
Acceptable level of protection (ALOP)	Level of risk (Table 4) accepted by the risk owner as determined by the risk assessors at the start of the risk assessment process.
Context	Defining parameters within which risks will be managed and sets the scope for the risk management process.
Hazard Owner	A Hazard Owner is the DPI role accountable for an emergency response and initial recovery operations in their area of responsibility. Refer to the [Emergency Response and Recovery Manual](#) for more details.
Risk owner	Person or entity (e.g., agency, organisation, division) with accountability and authority to manage risk. Risk owners are required to regularly monitor control effectiveness, and risk ratings to confirm impact of any changes in risk.
Risk tolerance – 1. Avoid 2. Mitigate 3. Share 4. Accept	An organisation's readiness to bear the risk after treatment in order to achieve its objectives. If the assessed risk level is above the acceptable/tolerable level for that category of risk, then treatment may be required. If it is equal to or below the acceptable/tolerable level for that category of risk, then the risk can be accepted. Delegations must be followed for the acceptance of risks. There are four broad treatment options available for mitigation of identified risks. 1. Avoid - Avoid the event that would lead to the risk. 2. Mitigate – Reduce likelihood and/or consequence. 3. Share - Share responsibility for management of an activity for which risk has been identified to another party or transfer certain consequences (usually financial) to another party. 4. Accept/Retain - Risks are accepted or retained when: • There are no treatment options available • The level of risk meets the residual target outlined in the context • The level of risk is above the target level; however, an informed decision is taken to accept risk at that level • Risk treatment would cost more than the consequences of the risk.
Risk treatment	Process of selection and implementation of measures (i.e. controls) to modify risk using the hierarchy of control. The purpose of risk treatment is to manage the likelihood and consequence of the identified risks by limiting their impact.

Further information

- Australian / New Zealand Standard for Risk Management Principles and Guidelines, AS/NZS ISO 31000:2018
- [Code of practice: How to manage work health and safety risks](#)
- Enterprise risk management framework (IND-P-207)
- [NSW Treasury *Internal Audit and Risk Management Policy for the NSW Public Sector,* TPP15-03](#)