Chapter 3 Risk Management

3.1 Introduction

The Service has adopted an enterprise risk management approach to the identification, management and evidencing of risks and issues affecting the Service, in compliance with the current Queensland Government requirements and internationally recognised standard (AS/NZS ISO 31000:2009).

The Enterprise Risk Management document can be found on the Strategic Risk and Business Continuity intranet page. This document has four chapters:

(i) Framework;

(ii) Appetite;

(iii) Risk assessment; and

(iv) Enterprise risk register.

Risk is the probability of something happening which may have an impact on the objectives an organisation wishes to achieve in a specified period e.g. the QPS Strategic Plan. The Service operates in a dynamic environment with both external and internal influences, some of which the Service is unable to control. This generates uncertainty and therefore risk.

Risk management is an integral part of all planning processes and should be applied to all activities. It is an ongoing activity that includes identification of new risks.

The Service has adopted the enterprise risk management approach whereby risk management is fully integrated into the management of the organisation.

3.2 Roles and responsibilities

Commissioner

The Commissioner is the accountable officer under the *Financial Accountability Act* and has the ultimate legislative responsibility and accountability for establishing and maintaining suitable systems of internal control and risk management.

Board of Management

The purpose of the Board of Management (BoM) is to endorse strategy, tone and risk appetite for the Service.

The role and responsibilities of the BoM are contained within s. 2.2: 'Purpose, Role and Responsibilities' of the Strategic Governance Manual (SGM).

Audit, Risk and Compliance Committee (ARCC)

The purpose of the ARCC is to scrutinise, challenge and oversee the Commissioners legislated management responsibilities.

The role and responsibilities of the ARCC are contained within s. 3.2: 'Purpose, Role and Responsibilities' of the SGM.

Strategic Risk Group – Chief Risk Officer

The Strategic Risk Group (SRG) has been established to provide risk management assistance, and training and coordination services to operational and executive Service managers.

The SRG is responsible for managing the Service Enterprise Risk Register and providing advisory support to the Senior Executive and ARCC each quarter, and to the BoM as required. The Chief Risk Officer will provide quarterly strategic risk management submissions to the ARCC for consideration and discussion.

The SRG will provide assistance and support to OICs, and the Senior and Executive Leadership teams. This includes the provision of Service risk management process and systems training.

Executive Leadership Team

The purpose of the Executive Leadership Team (ELT) is to influence and operationalise strategy and to drive performance.

The role and responsibilities of the ELT are contained within s. 4.2: 'Purpose, Role and Responsibilities' of the SGM.

Senior Leadership Team

Within their area of responsibility, district officers, commanders or directors are to:

(i) ensure there is an accurate evidence base of recorded risks within the Service Enterprise Risk Register (ERR). This risk management activity should occur once a month as a minimum as part of the monthly business management meeting (administration);

(ii) ensure all employees are aware of and comply with the Risk Management Framework, policy and procedures;

(iii) ensure the effective integration of risk management into planning, reviewing and reporting processes;

(iv) lead the risk management practice and ensure risk management resources and systems are established and maintained;

(v) escalate high or very high risks to the ELT;

(vi) consider operational risks that have been escalated, including treatments, to mitigate adverse impacts and maximise positive business opportunities;

(vii) review the adequacy and effectiveness of the controls and treatments, particularly for high or very high risks;

(viii) ensure relevant staff are appropriately trained in the risk management process.

The ERR must contain:

(i) a record of all risks escalated from the OIC or patrol group inspector;

(ii) a record of all risks identified at the district, command or director level;

(iii) a record of any action, treatments or controls applied to the risk;

(iv) where the risk is unable to be managed within the relevant risk tolerance level, escalation to assistant commissioner or deputy commissioner;

(v) the high, very high and strategic risks that will be the subject of ARCC discussions.

Patrol group inspectors and officers in charge

Compliance management, issues and risks that can be managed within the capabilities and resources of the divisional or unit OIC and/or locally with support of the inspector need not be recorded within the ERR.

OICs, managers and supervisors are responsible in their area of responsibility for;

(i) escalating at level risks or issues that cannot be managed to the superintendent/equivalent for recording and management within the ERR. Any risk that is of concern needs to be escalated to the SLT to enable management and resolution. This escalation process is an opportunity to resolve risks and issues outside the control of the OIC;

(ii) maintaining a record of any risk that has been identified and escalated to be actioned. It is not advocated for OICs to record normal management and/or compliance matters within a local risk register. Station compliance regimes need to be managed as required by the 'Compliance performance checklist report' and should be recorded in the appropriate registers as outlined; and

(iii) maintaining a local risk register that evidences:

(a) escalated risks being managed at superintendent or equivalent level;

(b) identified risks that require additional treatments or controls to be applied to reduce the risk profile; and

(c) ongoing risks to operations that require evidence of management.

3.3 Reporting requirements

The Service is required to maintain and record risks at a Service wide level. To comply with this requirement each district and command is responsible for maintaining a local version of the Service Enterprise Risk Register (ERR) at district officer level. It will be the responsibility of the district officer to ensure that all risks are recorded and managed in the ERR. Risk escalated from a group or equivalent functional unit to the district officer will be recorded within this ERR.

Risks are to be escalated to the ELT if they cannot be mitigated or treated at the senior leadership level. The ESC Strategic Risk Group via the Chief Risk Officer will coordinate with the ELT to ensure accurate recording, management and reporting of all identified strategic risks.

It is not advised to record normal management and/or compliance matters within a local risk register. Station compliance regimes need to be managed as required by 'Compliance performance checklist report' and should be recorded in the appropriate registers as outlined.

It is imperative that all identified business risks are recorded, managed, treated, controlled or escalated and evidenced within the ERR.

The risk management activity should occur as part of the monthly business management meeting. The enterprise risk register must be updated and managed monthly at a minimum.

3.4 Document retention

Risk management documents, including enterprise risk registers and working papers are to remain at the relevant work unit and stored electronically where practicable. The documents are to be retained in a secure location for seven years in accordance with the General Retention and Disposal Schedule.

The seven-year retention period commences on the date that the newest version of the document/s and enterprise risk register is submitted. Previous versions should also be retained to demonstrate the rationale for the change in the risk and as electronic working papers.

It is the responsibility of the Chief Risk Officer to manage the retention of the Service Enterprise Risk Register for the Service, ELT and SLT. Officers in charge are to manage the divisional risk register under local arrangements.

3.5 Business continuity planning

Business continuity considerations in risk management planning

To ensure a minimum consistent level of readiness throughout the Service, it is essential that business continuity risks are addressed by all OICs and managers. Risks are to be viewed from a worst-case scenario perspective (i.e. a total loss of a resource, asset or system). Planning for worst case scenarios will assist in dealing with lower impact incidents.

To assist officers in preparing their business continuity plan (BCP), ESC has prepared a QPS Business Continuity Planning Guide available through the Strategic Risk and Business Continuity webpage of the Service Intranet.

All OICs and unit managers are to assess their work areas and determine the extent to which they provide or support the delivery of Service objectives.

All areas of the Service should consider having a BCP so if an adverse event occurs, members will be aware of the contingency plans to be adopted.

ORDER

QP 1039: 'Business Continuity Plan (BCP)' is to be utilised by all OICs and unit managers when preparing and updating their plan.

OICs and unit managers are to ensure their work unit's BCP address the loss of:

(i) use of accommodation;

(ii) energy;

(iii) information technology/communications (phone/radio/computer network);

(iv) staff; and

(v) transport (where appropriate to the work unit).

In preparing the BCP, OICs and unit managers should:

(i) plan for loss due to natural disasters and extreme weather conditions, including cyclone and inundation;

(ii) identify other specific resources, assets or systems critical to their ability to deliver work unit objectives and activities; and

(iii) include these in their BCP.

Approval of a business continuity plan

OICs and unit managers are to provide their BCP to their next level manager for approval in accordance with s. 3.3: 'Reporting requirements' of this chapter.

Accessibility of business continuity plans

OICs and unit managers are to ensure that BCPs are stored locally at the work unit (e.g. in hard copy and on a computer desktop) and off site where it is readily accessible by the next level manager (e.g. in hard copy and on a district office file server).

Testing and maintenance of business continuity plans

Testing and maintenance of the recovery process documented in a BCP provides management with assurance that the plan is effective. It is important that each component is individually tested, however it is not recommended the BCP be tested as a whole as this would be resource intensive and may affect normal operations.

ORDER

OICs and unit managers are to undertake testing of potential identified disruptions in their individual BCP annually, during the period 1 July to 30 June each year. QP 1040: 'Business Continuity Plan (BCP) – Test & Results Sheet' is to be used.

Loss of accommodation ..... 12 monthly

Loss of energy ..... 12 monthly

Loss of information technology and communications ..... 12 monthly

Loss of staff ..... 12 monthly

Loss of transport ..... 12 monthly

OICs and unit managers are to consider applying the tests provided below to their BCP within the testing cycle.

Type 1	Walkthrough self-assessment	Discussion stepping participants through each part of the BCP during development, review or update.
	A Type 1 test should be facilitated by the OIC/manager or designated member responsible for developing, reviewing or updating the BCP.	
Type 2	Supervised walkthrough	Facilitated scenario-based discussion to test the BCP.
	A Type 2 test requires direct supervision by the BCP Coordinator or delegate.	
Type 3	Process or plan simulation	Simulated 'real life' environment scenario
	A Type 3 test should be conducted by a facilitator who develops a relevant and believable scenario conducted in 'real time' with unfolding information throughout the test. Scenarios in a Type 3 test are to be relevant, realistic and conducted in 'real time' with unfolding information throughout the test.	
Type 4	Full end-to-end simulation	Full scale test under a simulated 'real life' environment or activation of a BCP during an actual disruptive event
	A Type 4 test exercise requires approval from an assistant commissioner and is only recommended for fully mature BCPs.	

3.6 Work health and safety considerations

Legislative compliance

The *Work Health and Safety Act* (WHSA) establishes a requirement for the Service to provide a balanced and nationally consistent framework to secure the health and safety of workers and workplaces. Sections 17, 19 and 27 of the WHSA impose numerous responsibilities on certain persons within a workplace including, but not limited to:

(i) eliminating or minimising risks to health and safety;

(ii) a primary duty of care upon the Commissioner to ensure the health and safety of all persons is not put at risk and the provision of a work environment without risks; and

(iii) ensuring appropriate processes within the workplace to eliminate or minimise risks;

so far as is reasonably practicable.

An integrated approach to work health and safety risk assessment should be adopted with all management or operational requirements.

All members are to be mindful of their obligations under the WHSA and adhere to the relevant policy as outlined in Safety and Wellbeing Policies on the Service Intranet. WHS risks are to be identified and addressed by OICs, managers and supervisors in line with risk management practices. WHS hazards that are not addressed and pose a significant risk to station/establishment should be recorded and managed in accordance with s. 3.3: 'Reporting requirements' of this Manual.

Reporting procedures

OICs and managers are to address health and safety risks as part of the normal risk management process and liaise with their local health and safety network to ensure that health and safety issues are appropriately controlled.

OICs and managers should refer to the Safety and Wellbeing Hazard Management Policy on the Service Intranet for managing health and safety hazards and associated risks.

If the hazard can be managed at local level in line with WHS framework and legislation, there is no requirement to manage the hazard via the ERR. If the hazard becomes a significant risk that cannot be adequately treated through that process and there is a major concern / danger of death or serious injury, the WHS issue is to be managed via ERR.