South Burnett
Regional Council

ENTERPRISE RISK MANAGEMENT FRAMEWORK

Corporate Plan

Strategic Priorities

Operational Goals and Objectives

Council

Mandate for ERM → Risk Management Policy

Executive Team

ERM Commitment and Strategic Approach → Embed Risk Culture Set Risk Appetite

Corporate Governance Manager Risk Management Coordinator

ERM Program Coordination → Develop ERM Plan Coordinate ERM Activities

All Management and Staff

ERM Process Implementation → Establish context, identification, analysis, evaluation and treatment of strategic, operational and project risks → Completion of risk registers

Audit Committee Risk Management Committee

Oversight Responsibility → Review of risk process

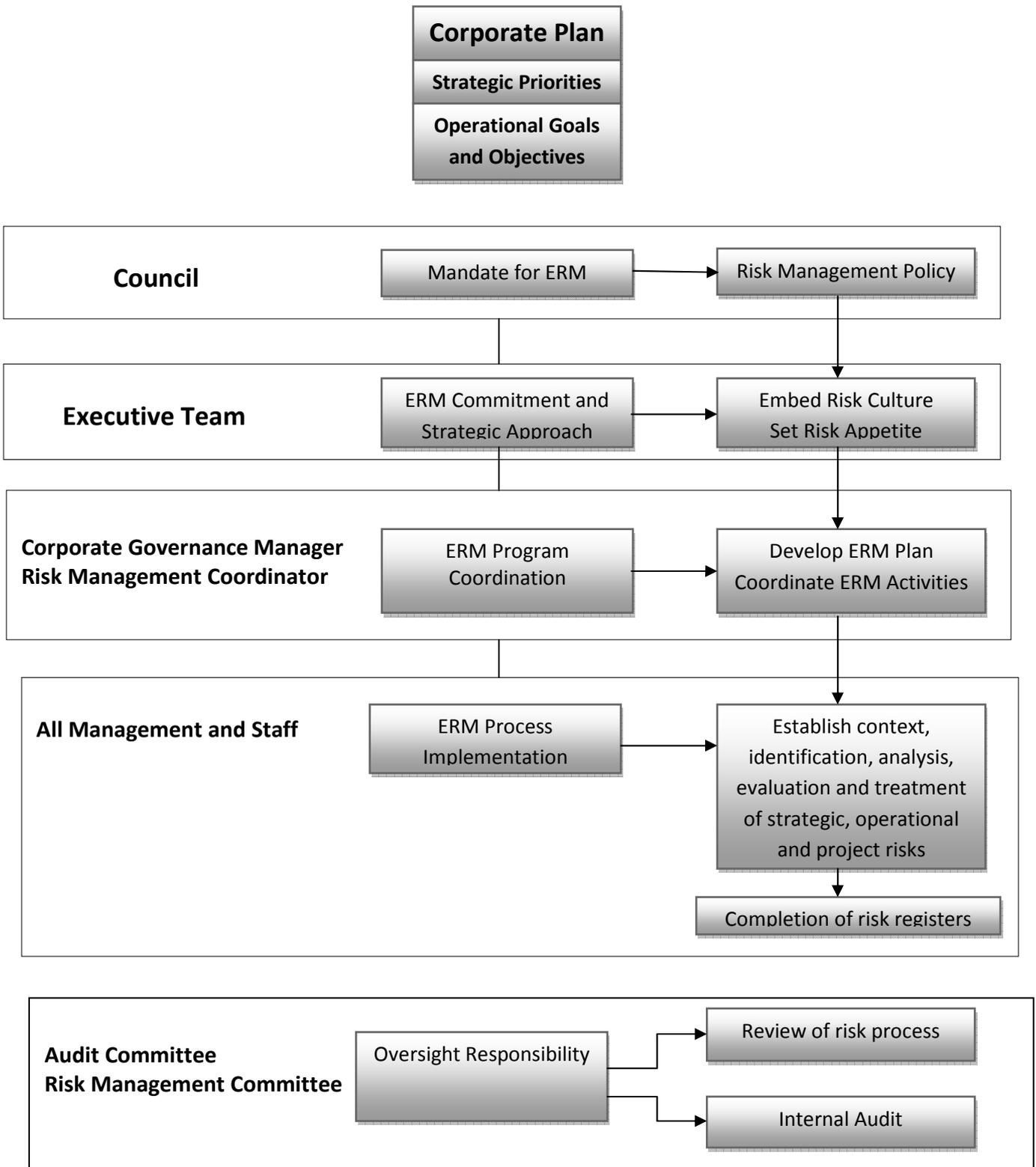→ Internal Audit

`

ERM Framework Description

Enterprise risk management (*ERM*) emerges from Council's intent to effectively and efficiently manage risks that may have an impact in the achievement of strategic priorities, goals and objectives as defined in the Corporate Plan.

The *ERM* Framework determines the accountability and authority for managing risk. It also specifies the responsibility for implementing the risk management process.

Council recognises that effective risk management is the responsibility of everyone in Council. Mandate for the implementation of enterprise risk management is granted by Council through the approval of the Risk Management Policy and Risk Management Committee Terms of Reference.

The **Executive Team** is responsible for promoting a strong culture and awareness of risk at all levels in the organisation. It will involve encouraging a risk informed workforce and demonstrating a commitment to *ERM*. The Chief Executive Officer provides direction in determining the strategic approach to risk and in setting the organisation's risk appetite.

The **Corporate Governance Manager and the Risk Management Coordinator** are responsible for developing the Risk Management Framework and Plan in consultation with the Risk Management Committee. The coordination of *ERM* activities, communication to all stakeholders, documentation of the internal risk policies and structures and the compilation of risk information and reports are the accountability of the Risk Management Coordinator. Providing training to internal stakeholders related to risk management also form part of the Risk Management Coordinator's responsibility.

The **Directors, Managers and Supervisors** need to develop a risk aware culture within their respective units and will be responsible for ensuring that employees implement risk management in their particular work areas and that the *ERM* process is integrated into their departments' operations and planning processes.   They will encourage honesty, openness and transparency in the reporting and escalation of strategic, operational and project risks.

Individual employees are responsible for understanding, accepting and implementing the *ERM* processes. Employees need to meet the key performance indicators stated in their position descriptions. Risk registers are to be completed upon conclusion of the risk process.

The **Audit Committee** exercises an oversight function over the risk management process. The scope of its responsibility includes the review and monitoring of the ERM Framework and Plan to ensure that these are up to date and relevant to Council Operations. The **Risk Management Committee** (RMC) provides feedback to the Audit Committee with regard to risk concerns and priorities. It also assists in the development, dissemination and implementation of the Risk Management Policy, Framework and Plan.

Internal Audit is responsible for the preparation of a risk based internal audit program in accordance with the appropriate professional standard and relevant legislation as stipulated in the Internal Audit Policy and Terms of Reference.   It will review the efficiency and effectiveness of internal controls within Council. The recommendations incorporated in the risk reports and internal audit reports are utilised in the strategic planning process for future Corporate Plans.

Reference: AS/NZS ISO 31000:2009 Risk management – Principles and guidelines