APPENDIX 50

Enterprise risk management - Risk management overview

Energex regulatory proposal – October 2014

ENTERPRISE RISK MANAGEMENT

Risk Management Overview (RMO)

06 11 2013

Table of Contents

1. INTRODUCTION 3

1.1 PURPOSE OF THIS DOCUMENT 3
1.2 REVIEW OF THE RMO 3

2. RISK MANAGEMENT GOVERNANCE 4

2.1 BOARD OF DIRECTORS 4
2.2 BOARD COMMITTEES 4
2.3 SUBSIDIARIES 4
2.4 CHIEF EXECUTIVE OFFICER (CEO) 4
2.5 CHIEF FINANCIAL OFFICER (CFO) 5
2.6 EXECUTIVE MANAGEMENT TEAM (EMT) 5
2.7 GOVERNANCE, RISK, COMPLIANCE AND ASSURANCE 5

3. ENTERPRISE RISK MANAGEMENT (ERM) 6

3.1 ERM FRAMEWORK 6
3.2 RISK APPETITE 6
3.3 ERM POLICY SET 7
3.4 ERM PROCESS 7
3.5 INTERNAL AUDIT GROUP ASSURANCE PLAN 7
3.6 EXECUTIVE MANAGEMENT REPORTS 7

4. RISK MANAGEMENT 8

4.1 RISK MANAGEMENT METHODOLOGY 8
4.2 CORPORATE RISK PLAN– STRATEGIC 8
4.3 CORPORATE RISK PLAN– OPERATIONAL 8

5. BUSINESS CONTINUITY MANAGEMENT (BCM) 9

5.1 BCM FRAMEWORK 9
5.2 BCM PROCESS 9
5.3 BCPS 9
5.4 BUSINESS CONTINUITY EXERCISES 9
5.5 CORPORATE EMERGENCY MANAGEMENT PLAN (CEMP) 9

6. COMPLIANCE RISK MANAGEMENT (CRM) 10

6.1 COMPLIANCE RISK MANAGEMENT FRAMEWORK 10
6.2 CRM POLICY SET 10
6.3 CRM PROCESS 11
6.4 PERFORMANCE MEASUREMENT AND REPORTING 11

7. OTHER RISK MANAGEMENT FRAMEWORKS 12

7.1 OTHER RISK MANAGEMENT FRAMEWORKS AND AREAS OF FOCUS 12

1. INTRODUCTION

1.1 Purpose of this document	This Risk Management Overview describes the **Enterprise Risk Management (ERM)** systems adopted by the Board and management for managing Risk within Energex. It identifies the policies and procedures, processes and Controls that comprise the Risk Management and Control systems for managing material financial and non-financial Risks at a Group level. It is intended as a business reference document.
1.2 Review of the RMO	The Risk Management Overview (RMO) will be reviewed biennially, and updated as necessary by management. The RMO will be regularly monitored to identify any material changes and appropriate updates made as required.

2. RISK MANAGEMENT GOVERNANCE

2.1 Board of Directors	The Board is responsible for oversight of Energex's ERM Framework. Key responsibilities of the Board include: • setting Energex's Risk Appetite; • approving Enterprise Risk Management policies; • overseeing Energex's material Risks; and • oversight of the adequacy and effectiveness of Energex's ERM Framework.
2.2 Board Committees	These Committees are to provide oversight and recommendations and advice to the Board. The Audit and Risk Committee (ARC) has overall oversight of the Risk Management Framework, however other Board Committees have responsibility for advising the Board of specific Risk matters that are brought to the attention of these Committees in the course of the execution of their Charters.
2.2.1 Audit and Risk Committee (ARC)	The role of the ARC is to provide assistance and recommendations to support the Board in discharging its responsibilities for oversight of relevant matters, and in particular in relation to the following: • Financial Integrity; • Risk Management; • Effectiveness of Control Framework; • Ethics and Integrity; and • Assurance over Business Operations.
2.2.2 Regulatory Committee	This Committee has oversight responsibilities for Risk matters pertaining to the Regulatory Determination Project, response to issues within Energex's regulatory regime and management of Energex's staff establishment.
2.2.3 Network and Technical Committee	This Committee has oversight responsibilities for Risk matters in relation to network and technical aspects of Energex's electricity distribution business, including in relation to standards and work practices, network performance, Program of Work delivery and specific network related safety issues.
2.2.4 Remuneration Committee	This Committee has oversight responsibilities for Risk matters in relation to Energex's remuneration and employment policies.
2.3 Subsidiaries	Boards of Energex subsidiary companies are responsible for oversight of the management of business Risk as it directly relates to the operations of the subsidiary company.
2.4 Chief Executive Officer (CEO)	The CEO is ultimately responsible and accountable to the Energex Board for ensuring that policies, procedures, systems and Controls are operating effectively so that Risks are managed to a tolerable level within the commercial constraints of the business as required to achieve balanced commercial outcomes.

2. RISK MANAGEMENT GOVERNANCE

2.5 Chief Financial Officer (CFO)	The CFO has overall responsibility for: • systems and frameworks for management of business Risk; • development and implementation of all Group financial Risk processes and structures, including market, credit and operational Risk strategies, structures and methodologies; • monitoring and control of credit risk systems, policies and procedures and management of credit risk arising from Group activities; • Group capital management; and • Recording, reporting of all financial transactions, preparation of accounts, financial reports and statutory returns.
2.6 Executive Management Team (EMT)	The EMT is accountable to the CEO and to the Board and is responsible for ensuring that Risks in their Divisions are managed to a tolerable level. Key Risk responsibilities include: • identifying material Risks to which Divisions are exposed; • analysing the Consequence of identified Risks to Divisional objectives and their Likelihood of occurrence; • developing cost-effective treatments and strategies to reduce where possible Risk Consequence and Likelihood to tolerable levels; • developing and implementing Monitoring processes to ensure that Risk Controls and strategies are working effectively and efficiently; and • developing and implementing reporting processes to provide the Board and CEO with timely and accurate information on Risks to which the Group is exposed and how management is performing in managing those Risks.
2.7 Governance, Risk, Compliance and Assurance	
2.7.1 Director Corporate Governance and Company Secretary	The Director Corporate Governance, reporting to the CFO, is responsible for the Corporate Risk and Compliance Group in the implementation of the Energex ERM Framework supporting the ERM Policy approved by the Energex Board.
2.7.2 Corporate Risk and Compliance Group	The Corporate Risk & Compliance Group promotes, champions and continuously improves the ERM Framework. In addition, the team routinely prepares reports to the Energex Board, Committees and EMT to provide information on the management of Risk and to facilitate the development and implementation of Risk Management policies, processes, systems and Controls.
2.7.3 Internal Audit	The role of Internal Audit within the Energex Group is to provide an independent, objective assurance and consulting activity, which is designed to add value and improve Energex's operations.
2.7.4 Management Committees	Management committees provide for cross-divisional communication and review of matters, including Risk Management responses in the specified area of focus for the respective management committees. See Section 7 for further details of other Risk Management Frameworks and focus areas..

3. ENTERPRISE RISK MANAGEMENT (ERM)

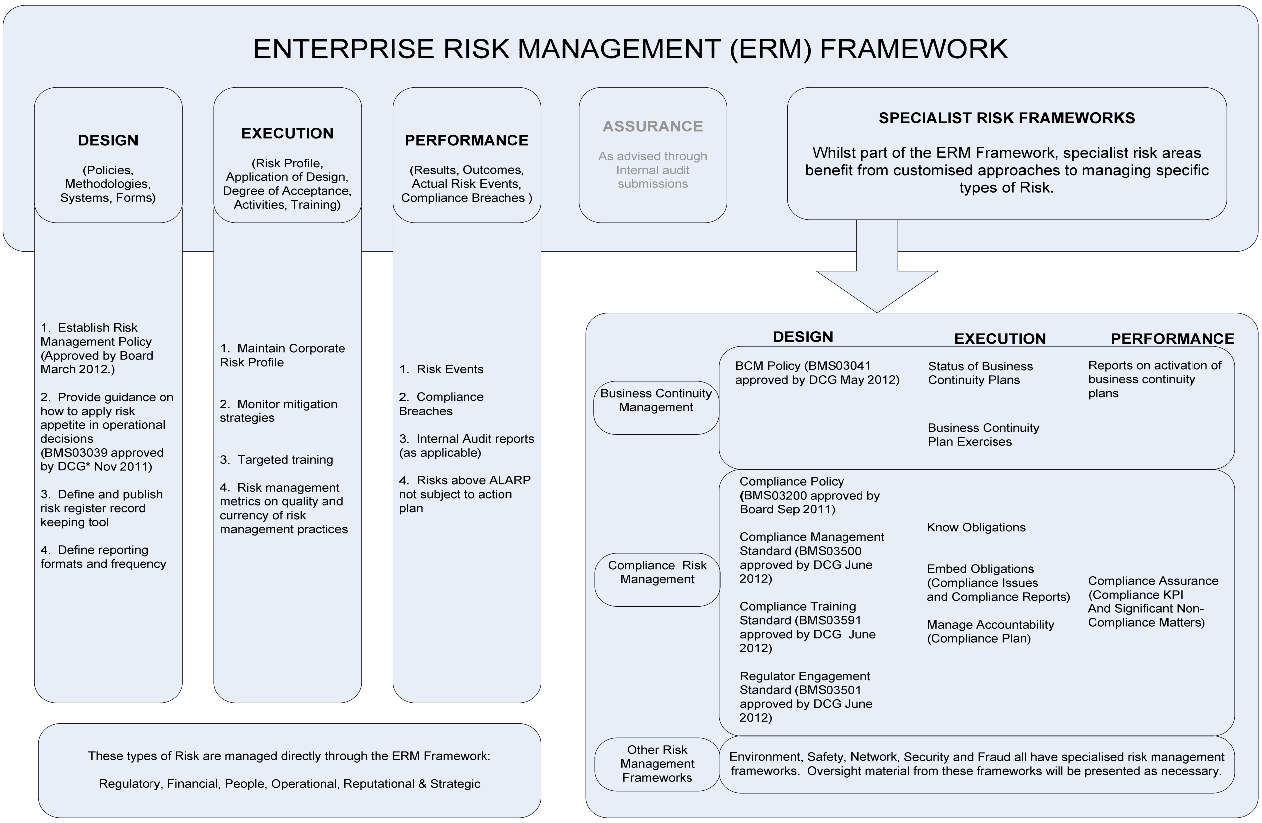
3.1 ERM Framework

Energex's ERM Framework comprises a common risk language for the Group and clearly defined risk accountabilities. The ERM Framework is diagrammatically represented below.

The ERM Framework forms an integral component of Energex's corporate governance framework.

Energex has adopted AS/NZS ISO 31000:2009 'Risk management–Principles and guidelines' (ISO 31000), including ISO Guide 73:2009 'Risk management–Vocabulary', as a guiding reference in the development of the Energex Enterprise Risk Management Framework and Standard.

Whilst the ERM framework provides the overarching structure for the management of Risk within Energex, it also benefits from integrated specialist Risk frameworks, as set out in the diagram below. The specialist Risk frameworks of **Business Continuity Management (BCM)**, **Compliance Risk Management (CRM)** and **Other Management Risk Frameworks** are discussed in Sections 5-7.



ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK

DESIGN

(Policies, Methodologies, Systems, Forms)

1. Establish Risk Management Policy (Approved by Board March 2012.)

2. Provide guidance on how to apply risk appetite in operational decisions (BMS03039 approved by DCG* Nov 2011)

3. Define and publish risk register record keeping tool

4. Define reporting formats and frequency

EXECUTION

(Risk Profile, Application of Design, Degree of Acceptance, Activities, Training)

1. Maintain Corporate Risk Profile

2. Monitor mitigation strategies

3. Targeted training

4. Risk management metrics on quality and currency of risk management practices

PERFORMANCE

(Results, Outcomes, Actual Risk Events, Compliance Breaches)

1. Risk Events

2. Compliance Breaches

3. Internal Audit reports (as applicable)

4. Risks above ALARP not subject to action plan

ASSURANCE

As advised through Internal audit submissions

SPECIALIST RISK FRAMEWORKS

Whilst part of the ERM Framework, specialist risk areas benefit from customised approaches to managing specific types of Risk.

These types of Risk are managed directly through the ERM Framework:

Regulatory, Financial, People, Operational, Reputational & Strategic

	DESIGN	EXECUTION	PERFORMANCE
Business Continuity Management	BCM Policy (BMS03041 approved by DCG May 2012)	Status of Business Continuity Plans Business Continuity Plan Exercises	Reports on activation of business continuity plans
Compliance Risk Management	Compliance Policy (BMS03200 approved by Board Sep 2011) Compliance Management Standard (BMS03500 approved by DCG June 2012) Compliance Training Standard (BMS03591 approved by DCG June 2012) Regulator Engagement Standard (BMS03501 approved by DCG June 2012)	Know Obligations Embed Obligations (Compliance Issues and Compliance Reports) Manage Accountability (Compliance Plan)	Compliance Assurance (Compliance KPI And Significant Non-Compliance Matters)
Other Risk Management Frameworks	Environment, Safety, Network, Security and Fraud all have specialised risk management frameworks. Oversight material from these frameworks will be presented as necessary.		

3.2 Risk Appetite

Within the objective of achieving balanced commercial outcomes (as contained within the Energex business planning objectives and goals), the Energex Board has adopted 'As Low As Reasonably Practicable (ALARP) within business constraints' in the determination of its Risk Appetite.

3. ENTERPRISE RISK MANAGEMENT (ERM)

3.3 ERM Policy Set

Policies create the Framework for reflecting the plans and intentions of the Board and management. Compliance with Policies is monitored by the various Board and Management Committees. Principal policies that underpin the Group's ERM Framework are:

3.3.1 Enterprise Risk Management Policy

The ERM Policy is a formal statement of the Board's approach to Risk Management. The Enterprise Risk Management Policy is approved by the Board and is reviewed annually by management and the ARC.

3.3.2 Enterprise Risk Management Standard

The ERM Standard outlines the process of Risk Management to be used to support decision-making at Energex. It is regularly reviewed for currency and updated as required.

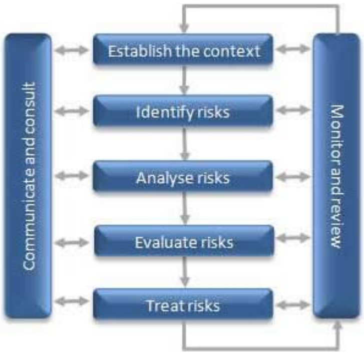
3.3.3 Enterprise Risk Management Manual

The ERM Manual is the primary document detailing the Risk Management process at Energex. Other subsidiary frameworks (e.g. Compliance, Safety etc.) come under this overarching document. Also reviewed regularly and updated as required.

3.4 ERM Process

The ERM Process is concerned with the identification, analysis, evaluation, treatment, monitoring and reporting of all Risks to which Energex is exposed.

Consistent with the good practice guidelines, Energex's ERM Framework addresses the identification and management of Risk through the following process:



Risk Management includes an assessment of Level of Risk, which is used to rank and prioritise actions, monitoring and reporting.

3.5 Internal Audit Group Assurance Plan

Prior to the commencement of each financial year, Internal Audit Group (IAG) prepares a plan of assurance activity for Energex for endorsement by the ARC, which is subsequently referred to the Board for approval.

3.6 Executive Management Reports

The EMT receives and provides feedback on the following reports:

- Controls Environment;
- Compliance Risk;
- Operational Risk;
- Strategic Risk, and
- Oversight of the Enterprise Risk Framework.

4. RISK MANAGEMENT

4.1	**Risk Management Methodology**	Managers are required to understand the operational and strategic Risks to which the business is exposed, assess the exposures and implement necessary mitigators in a cost-effective manner. The methodology adopted to satisfy this requirement is based on a structured approach to Risk profiling, as detailed in the ERM Standard and the ERM Manual. Essential components of the Risk Management Methodology used by the business are: • Risk Registers (regularly refreshed by the business to aid management decision-making) • Risk Management Reporting – (evidencing ownership, relevance and progress of Risk Management Controls) • Assessment of both the Inherent and Residual Levels of Risks • Rolling Corporate Risk Plans (to evidence awareness of Risks that may affect the business from both near and long-term perspectives).
4.2	**Corporate Risk Plan– Strategic**	The Corporate Risk Plan (CRP)–Strategic shows the strategic key Risk factors identified in the "Strategic Direction Towards 2030" document and the Corporate Plan. The CRP-Strategic demonstrates that Energex has a considered and well defined forward view of Risk and is taking action today to position the business for challenges of the future.
4.3	**Corporate Risk Plan– Operational**	The Energex Corporate Risk Plan (CRP)–Operational reports the outcome of the monitoring and reporting processes used to inform the most material Risks of the organisation to the EMT, the Energex Board and Energex's shareholders. The CRP–Operational is built from both top-down and bottom-up perspectives of Risk to ensure alignment between the strategic, longer-term view and the operational, immediately actionable view. This component is used in business planning, refreshed through monthly Risk Reporting and feeds into the Statement of Corporate Intent.

5. BUSINESS CONTINUITY MANAGEMENT (BCM)

5.1	**BCM Framework**	The Business Continuity Management (BCM) Framework covers the following activities: business continuity planning; disaster recovery planning; emergency management; incident management and business resumption planning. The business continuity structure includes: • **Tier 1**: A whole-of-Energex Corporate Emergency Management Plan (CEMP); • **Tier 2**: Business Continuity Plans (BCPs) for each critical function; and • **Tier 3**: Supporting BCPs for critical resources used by critical functions. Energex has adopted AS/NZS ISO 5050:2010 'Business continuity-Managing disruption related risk' as a guiding reference for the Energex BCM Framework. The methodology adopted to satisfy this requirement is based on a structured approach BCM, as detailed in the BCM Policy, BCM Standard and the BCM Manual.
5.2	**BCM Process**	Through the annual business planning process and the use of business impact analysis (Form 2945), we identify critical functions and critical resources required for the continuation of Energex core operations during a business disruption event. Business continuity is broader than just disaster recovery - it encompasses: **Emergency response**: the initial response to a disruption focused on the protection of people and property from immediate harm. **Continuity response**: planning for the management of disruption to minimise the impact and ensure the organisation continues to deliver customer value in the degraded state. **Recovery response**: re-establish full functionality to meet ongoing operational requirements and decommission workarounds undertaken as part of the continuity response. This information is then used to develop BCPs.
5.3	**BCPs**	The structure of the Business Continuity Plans at Energex has been implemented as a hierarchy in line with the Australian Standard guidelines for BCM (HB292). BCPs are developed, compiled and maintained in readiness for use in an incident to enable Energex to deliver critical products and services at predefined levels.
5.4	**Business Continuity Exercises**	BCPs are tested at least annually. Formal post-exercise reviews are an integral part of the exercise process to ascertain the lessons learnt and enable improvement.
5.5	**Corporate Emergency Management Plan (CEMP)**	The Corporate Emergency Management Plan (CEMP) is the primary mechanism to support the strategic response to major business disruption. It is a plan designed to be used by key decision-makers, led by the Duty Executive, in responding to a high impact event. As such, it is a key preparation in dealing with 'Black Swan' events (a.k.a. unknown, unknowns) that require urgent effective response.

6. COMPLIANCE RISK MANAGEMENT (CRM)

6.1 Compliance Risk Management Framework	The Energex Compliance Framework is a key tool for management, employees and external stakeholders to understand the Energex approach to Compliance Risk. The aim of the Framework is to support management in effective Compliance Risk Management across the organisation to enable Energex to demonstrate its commitment to relevant laws, codes, practices, standards, contracts etc.
6.2 CRM Policy Set	Australian Standard AS3806–2006 Compliance programs (AS3806) has been adopted as the model for achieving robust and credible Compliance Risk Management as part of the overarching ERM Framework. Policies create the framework for reflecting the plans and intentions of the Board and management. Compliance with Policies is monitored by the various Board and Management Committees. Principal policies that underpin the Group's Compliance Risk Management Framework are:
6.2.1 Compliance Policy	The Compliance Policy is approved by the Energex Limited Board and is reviewed annually by management against the expectations of Australian Standard AS3806 Compliance Programs.
6.2.2 Compliance Management Standard	The Compliance Management Standard is based on Australian Standard AS3806–*Compliance Programs* and provides guidance for the implementation of effective programs and systems that ensure Compliance Risks, obligations and requirements are understood and pro-actively managed.
6.2.3 Regulator Engagement Standard	The Regulator Engagement Standard sets out principles and protocols that apply to engagement with regulators and is designed to ensure there is a coordinated Energex-wide approach in all formal engagement with regulators.
6.2.4 Compliance Training Standard	The Compliance Training Standard sets out principles and protocols to be applied in designing and delivering training for Compliance obligations applicable to Energex.

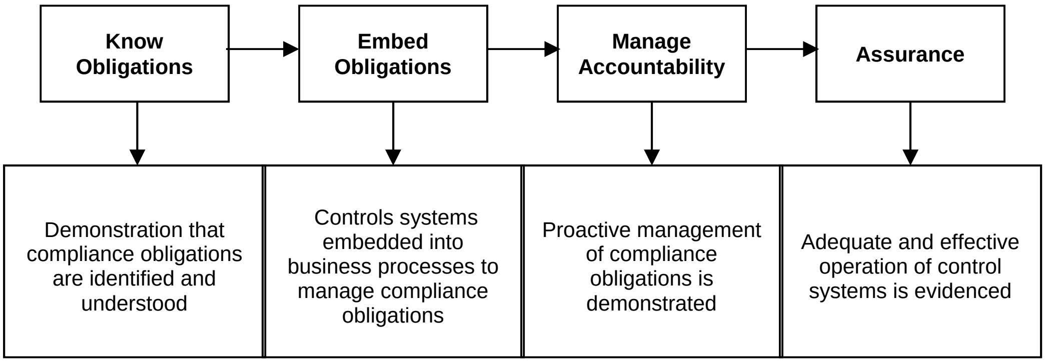
6. COMPLIANCE RISK MANAGEMENT (CRM)

6.3 CRM Process

Application of a Compliance Management Process is critical to ensuring Compliance objectives are achieved through a determined approach rather than through an assumed expectation that business units will be adequately compliant.

6.3.1 Energex 'KEMA' end-to-end Compliance Management Process

The AS3806 based end-to-end model for managing and improving Compliance at Energex comprises the following four pillars:


Know Obligations
Embed Obligations
Manage Accountability
Assurance
Demonstration that compliance obligations are identified and understood
Controls systems embedded into business processes to manage compliance obligations
Proactive management of compliance obligations is demonstrated
Adequate and effective operation of control systems is evidenced

Know Obligations: This pillar covers demonstrating that Compliance obligations applicable to Energex have been identified and understood.

Embed Obligations: This pillar deals with actions that business areas undertake to embed control systems into business processes to manage identified Compliance obligations and achieve desired outcomes.

Manage Accountabilities: This pillar deals with managing behavioural responses by providing employees with an understanding of their responsibilities and accountabilities in the proper application of embedded control systems.

Assurance: This pillar highlights how Compliance performance is monitored and measured, to evidence that the control systems are adequate and operating effectively to achieve positive Compliance management.

6.4 Performance Measurement and Reporting

Energex's Compliance management performance is measured through the '**Compliance Effectiveness Index**'.

The Index is a numerical representation of performance assessed using three metrics that together give a full picture of Compliance management:

Capability (50% weighting): Measures how mature or reliable are our Compliance Management systems. Self-assessments are undertaken within each Division based on 42 specific criteria aligned to AS3806.

Plan (50% weighting): This is an assessment by each division of progress towards achieving their Compliance Plan.

In the event of a **Confirmed Significant Non-Compliance** the Index, comprising of the sum of Capability and Plan scores, will be negatively moderated.

7. OTHER RISK MANAGEMENT FRAMEWORKS

7.1 Other Risk Management Frameworks and Areas of Focus	There are a number of other Committees and roles with the organisation that have Risk Management responsibilities under the corporate ERM framework. These include, but are not limited to the following:
7.1.1 External Auditors	The external audit is undertaken by external auditors on behalf of the Queensland Audit Office (QAO). The principal focus of external audit is to provide an opinion on the financial statements of Energex Limited and its controlled entities. Accordingly, the focus of QAO/KPMG is on those risks that have a direct impact on the financial statements. Regulators and other external bodies may conduct or require the commissioning of various additional independent audit activities to satisfy requirements or for accreditation purposes.
7.1.2 Risk and Compliance Coordinators	Each Division in Energex has coordinator(s) whose role includes: • championing/ promoting Risk Management within their Division • being the primary point of contact for their Division with Corporate Risk & Compliance (CR&C) Group • subject matter expert on use of Risk Management tools • compiling Divisional Risk Management Reports • liaising with CR&C Group, as necessary, on matters of Risk Management policy and practice • liaising with other Risk coordinators to ensure inter-dependencies are understood and easily handled • providing feedback on, and input to, corporate Risk initiatives.
7.1.3 Safety Council	The Safety Council is the peak workplace health and safety reference body responsible for setting safety strategy and policy, resolving high-level safety issues, reviewing safety performance data, reviewing safety management system audit results and reviewing incident investigations where the potential or actual severity requires its involvement.
7.1.4 Environment Council	The Environment Council is responsible for the regular monitoring of environmental exposures, review of incident trends, environmental initiatives, endorsement of recommendations for environmental improvement policies, programs and investments, as well as Compliance with environmental regulations.
7.1.5 Customer & Strategy Committee	The Committee provides a forum as a collective of the Senior and Group Manager Executives for development, application, oversight and communication of the strategies and policies applicable to Energex's regulatory and customer matters. The Committee receives reports on management's delivery of Energex's regulatory responsibilities and obligations.
7.1.6 Other Groups	There are a number of other specialised Groups within the organisation responsible for key Risks as identified in the Energex annual business plan. These are risks to corporate objectives as represeneted by Key Reporting Areas (KRAs).