Policy
(Board Approved)

Enterprise Risk Management and Business Resilience

Document Number – GOV-POL-37

Table of Contents

1.0 Policy Statement

Risk Management is about understanding and then managing Stanwell's response to its risk environment and taking action, where necessary, to ensure that risks are contained at acceptable levels, consistent with Stanwell's risk appetite, as outline in the Stanwell Risk Appetite Statement (GOV-POL-38). It incorporates systems, structures, processes and people that identify, measure, monitor, report and control/mitigate sources of internal and external risk.

Business Resilience incorporates and integrates emergency response, business continuity, disaster recovery, security and insurance, and is an important element of Stanwell's enterprise approach to risk management.

2.0 Purpose

The purpose of this Policy is to ensure the implementation of effective risk management and business resilience practices that will protect and create value and are consistent with strategy formulation, business planning and the achievement of Stanwell's strategic objectives.

3.0 Scope

This policy applies to Stanwell's directors, employees and to all contractors working for or at Stanwell (our people) in relation to all categories of risk and Stanwell's business activities.

4.0 Enterprise Risk Management

Stanwell has defined its desired risk culture as a robust values-based culture where risk management is seamlessly integrated into daily operations. Risk management is considered as everyone's responsibility and our people are required to align their activities with the strategic and operational objectives of the organisation.

Stanwell recognises that managing risk is fundamentally about creating and protecting value. Stanwell's risk management approach is characterised by the following principles:

- the objective of Stanwell's risk management practices is not necessarily to eliminate risk, but to understand and to take a measured level of risk commensurate to the value that is being protected or created;
- Stanwell applies a structured and comprehensive approach to risk management to ensure that it achieves consistent and measurable results;
- the risk environment is not static, therefore our people should be aware of and respond to internal or external changes and events in an appropriate and timely manner;
- risk management should be integrated into day-to-day decision-making and leverage existing forums and processes wherever possible;
- the quality of Stanwell's decision-making will be further enhanced by ensuring that the appropriate stakeholders are involved so as to leverage their knowledge, views and perceptions;
- decisions should be made using the best available information that considers both internal and external factors; and

  appropriate behaviour and risk culture are fundamental to the effectiveness of Stanwell's risk management practices and decision-making and our people are expected to familiarise themselves with the Stanwell's Enterprise Risk Management Framework (GOV-PROC-37) (ERMF) and apply its principles at all times.

Stanwell's Risk Appetite Statement assists our people to make risk-based decisions and to provide guidance in terms of the level of risk that the Stanwell is prepared to accept in pursuit of its strategic objectives and business plans and ensuring that an appropriate level of risk taking is applied across Stanwell's daily operations.

The ERMF provides the methodology for ensuring that risks are considered and addressed in a systematic and consistent manner. Whilst different types of risk require different risk management strategies and governance arrangements, the ERMF is the common framework through which any significant risks – as assessed using Stanwell's likelihood and consequence criteria (Risk Evaluation Matrix (GOV-STD-11) – should be escalated and monitored.

5.0 Business Resilience Framework

Stanwell defines business resilience as the ability of its business operations to anticipate, prepare for and rapidly respond to, adverse events while protecting employees, assets and Stanwell's reputation before, during and after an adverse event.

Stanwell recognises that effective business resilience is an important element of its enterprise approach to risk management and has established a business resilience framework that integrates the functions of crisis and/or incident management, emergency response, disaster recovery, business continuity security and insurance.

Figure 1 - enterprise risk management, crisis and incident management, emergency response, security management and insurance relationship

5.1. Business Continuity

At Stanwell, business continuity comprises of:

- ***Emergency response preparedness*** - the planning Stanwell engages in so that it can prepare for and rapidly respond to, an adverse event;
- ***Crisis and or incident management*** - the steps taken immediately by Stanwell after an adverse event has occurred;
- ***Disaster recovery*** - the actions taken by Stanwell to fail-over to secondary data centres in the event of a significant service interruption impacting on its technology infrastructure, communication networks and business processes; and
- ***Business continuity preparedness*** - the planning Stanwell engages in ensure that it can respond to and recover from an adverse event while continuing to maintain business critical functions.

Stanwell's Business Continuity Management Procedure (GOV-PROC-47) establishes the principles necessary for Stanwell to appropriately respond to an adverse event. The Procedure is underpinned by plans, processes, systems and tools to support Crisis Leadership, Incident Management, Emergency Response and the continuity of business critical functions.

Stanwell conducts regular reviews of its business continuity framework and tests its capability to respond by scheduling periodic business continuity exercises.

5.1.1. Information Technology (IT) Disaster Recover

Stanwell's Information Technology Disaster Recovery Plan (IT-DRP) is a comprehensive statement of consistent actions that are to be taken before, during and after an adverse event.

The primary objective of the IT-DRP is to minimise the effects on Stanwell including downtime and data loss, in the event that all or part of its Information Technologies are impacted by an adverse event.

Stanwell conducts annual testing of its disaster recovery capability to provide assurance that its technology infrastructure, communication networks and business systems can continue to operate in the event of a significant service disruption.

5.2. Security

Stanwell maintains a Security Management Framework (GOV-PROC-48) which seeks to moderate Stanwell's security exposures and vulnerabilities and to establish the appropriate response through:

- a comprehensive understanding of Stanwell's assets and their security vulnerabilities;
- detailed intelligence, threat analysis and the identification of security risks;
- robust security management standards and plans tailored to the specific security priorities, location and risk environment;
- building the ability of the organisation to respond to and recover from a security event;
- undertaking regular security audits; and
- a sustainable security culture across all of Stanwell's operating sites and corporate offices.

The key focus of the framework is to apply security best practice to mitigate against security threats, identify and eliminate vulnerabilities and to demonstrate Stanwell's intent to comply with relevant regulatory and compliance requirements.

The framework also establishes an on-going and continuous process of improvement, enabling the security management program to develop and mature in alignment with Stanwell's strategic objectives.

5.3. Insurance

Stanwell chooses to utilise insurance as a risk transference mechanism (where appropriate) and to reduce the ultimate financial impact to the business should a serious event occur within the business.

Stanwell maintains a portfolio of insurance policies which aim to cover the types of business activities Stanwell undertakes on a day to day basis.

Stanwell regularly reviews its insurance coverage, insurers and deductibles as part of an annual renewal process.

6.0 Responsibilities

Position	Responsibility
The Board	Stanwell's Board has ultimate responsibility for risk management and for determining the appropriate level of risk that the Board is willing to accept (appetite) in the pursuit of Stanwell's strategic objectives. The Board is responsible for approving this policy, the Risk Appetite Statement, the Risk Evaluation Matrix (GOV-STD-11) and the Enterprise Risk Management Framework and for overseeing, reviewing and ensuring the effectiveness and integrity of Stanwell's enterprise risk management system and business resilience framework.
Audit and Risk Management Committee (ARMC)	The Stanwell Board has established the Audit and Risk Management Committee to assist the Board to oversee the process for identifying and managing significant business risks, business continuity, disaster recovery processes and insurance strategy. The responsibilities and delegated authority of the ARMC are detailed in the Board-approved ARMC Charter.
Chief Executive Officer (CEO)	Ultimate accountability for ensuring that Stanwell has identified and managed its significant business risks and has effective business resilience programs in place.
Executive General Managers	Each Executive General Manager is accountable for identifying and managing the significant risks of their division, ensuring enterprise risk management and business resilience activities in their divisions are effective and for having effective crisis management and business continuity planning in place.
Company Secretary	Accountable and responsible for the establishment, implementation, monitoring and review of Stanwell's enterprise risk management, business resilience and security management systems and frameworks.
Enterprise Risk and Resilience Team (ERRT)	Responsible for maintaining the effectiveness of Stanwell's enterprise risk management, business resilience and security management systems and frameworks. Performs the risk management second line of defence function for Stanwell which includes overseeing and independently challenging the 1st line of defence on and the monitoring of risk exposure. The Enterprise Risk and Resilience Team comprises of the Company Secretary, Manager Risk & Resilience and Principal Analyst, Risk & Assurance.
Financial Controller	Accountable and responsible for Stanwell's insurance strategy.
General Manager Information, and Technology	Accountable and responsible for Stanwell's Information Technology Disaster Recovery Plan.
Managers and Supervisors	Managers and Supervisors are responsible for evaluating their risk environment, to put in place effective controls and for monitoring the effectiveness of these controls.

Position	Responsibility
Our people	Our people are responsible for familiarising themselves with this Policy and the supporting procedures, processes and plans that affect their workplace activities, incorporating risk practices into their business activities and reporting and escalating all events, risk concerns, issues and breaches.

7.0 Review, Consultation and Communication

7.1. Review

This document is required to be reviewed on an annual basis.

7.2. Consultation

Board

Executive Leadership Team.

7.3. Communication/Requirements after Update:

This policy will be communicated to key internal stakeholders via GenNet. This policy is made publicly available on Stanwell's internet site www.stanwell.com in accordance with the Corporate Governance Guidelines for Government Owned Corporations.

This policy will be published on the intranet and available in Content Manager and Stanwell Controlled Documents.

All new employees will be advised of this policy as part of the induction process. Employees with responsibilities within the Crisis Management, Incident Management or Emergency Response Teams will undertake required training as outlined within the respective plans or subordinate documents.

8.0 Definitions

Not applicable.

9.0 References

- Environmental Protection Act 1994 & Regulation 2008
- Health & Safety Act 2011 & Regulation 2011
- GOV-PROC-47 Business Continuity Management Procedure
- GOV-PROC-48 Security Management Framework
- GOV-PROC-37 Enterprise Risk Management Framework
- GOV-PROC-59 Enterprise Risk Management Procedures and Guidance
- GOV-POL-38 Risk Appetite Statement
- GOV-STD-11 Risk Evaluation Matrix

10.0 Revision History

Rev. No.	Rev. Date	Revision Description	Author	Endorse/Check	Approved By
0	27.02.2015	This policy is a consolidation of the Risk Policy, Business Continuity Policy and the Security Policy.	K. Biggs	M O'Rourke	Board
1	16.02.2016	Annual review of Policy and inclusion of Risk Appetite Statement	K Biggs	M. O'Rourke	Board
	20.04.2016	Discussions with Rebecca Gurney stated the need to ensure that the full version of this Policy (incl Appendix 1) is not published to Stanwell.com. It was determined that a second copy would be made upon approval and Appendix 1 remote for publishing on the internet.	D. Wilkie		
2	23.01.17	Annual review of policy and updated to reflect changes in role titles and additional information on security approach.	R. Gurney	K. Biggs M. O'Rourke	Board
3	19.03.2018	Annual review of policy. Amended to reflect changes in responsibilities and the establishment of the Security Management Framework.	K Buckley	M O'Rourke	Board
4	21.05.2019	Annual review of policy. Amended to reflect the enhanced Enterprise Risk Management Framework and the establishment of the RAS as a stand alone Policy.	K Buckley	M O'Rourke	Board
5	20.05.2020	Annual Review of Policy. Minor updates to reflect current Enterprise Risk Management practices.	K Buckley	M O'Rourke	Board
6	21.5.2021	Annual Review of Policy. No amendments made.	K Buckley	M O'Rourke	Board