Policy
(Board Approved)
Public Version

Business Resilience and Risk Management

Document Number – GOV-POL-37

1.0 Policy Statement

Stanwell is committed to delivering a business resilience platform across all levels of the business and its implementation and maintenance is fundamental to Stanwell achieving its strategic objectives.

Business resilience for Stanwell incorporates and integrates risk management, business continuity, security and insurance.

2.0 Purpose

The purpose of this policy is to develop and strengthen Stanwell's business resilience and risk management practices by providing the structural framework in order to continue to meet Stanwell's objectives when faced by risks (including both opportunities and threats) and vulnerabilities.

Note: This document is not to be published to the external internet www.stanwell.com. A public version is to be created upon approval excluding Appendix 1 – Risk Appetite Statement. This is the responsibility of the Policy owners.

3.0 Scope

This policy incorporates the integration of a number of interrelated activities including business continuity, risk management, security and insurance. In delivery of this policy, additional business functions, such as Compliance and Regulatory Management and Information and Business Systems are incorporated into the business resilience and risk management corporation-wide approach.

The diagram below reflects Stanwell's optimal business resilience model.

In the development of Stanwell's Business Resilience and Risk Management approach, Stanwell will be well-positioned to create opportunities for benefit and to also respond to the negative consequences of an event. This will deliver improved outcomes based on informed decision making and resilience, including business continuity, security, and risk transference via insurance and corporation-wide risk management practices.

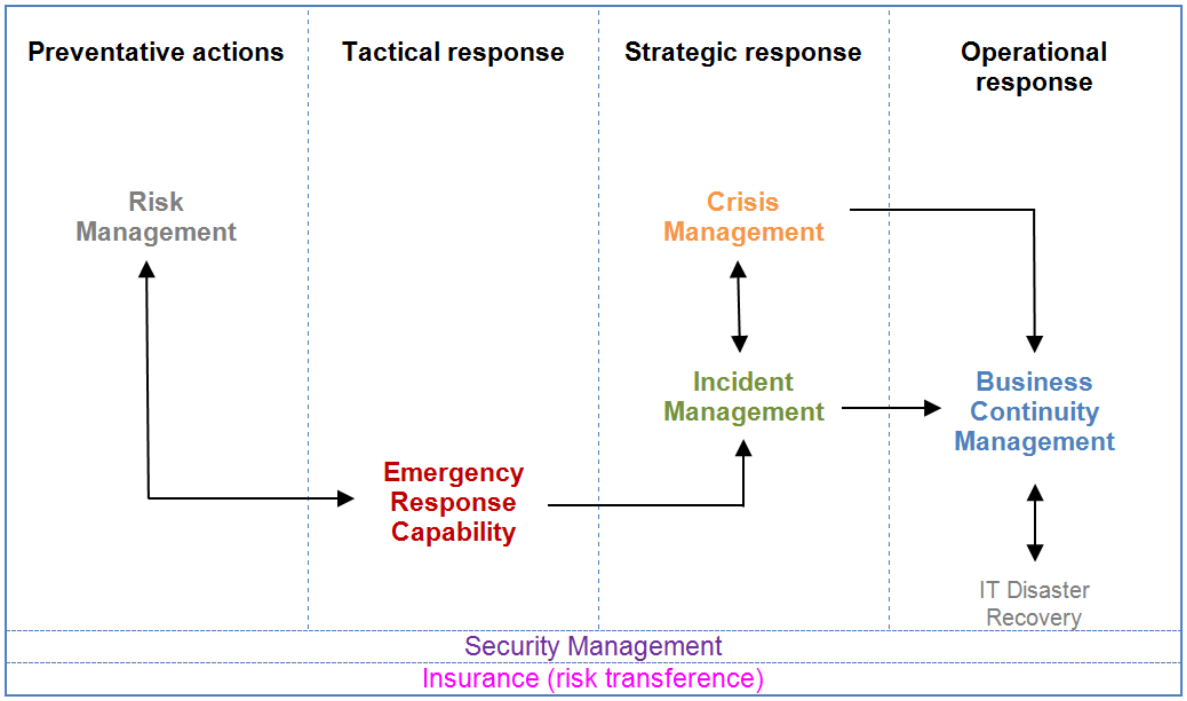
This policy applies to Stanwell's directors and employees and to all contractors working for or at Stanwell (our people) in relation to all categories of risk and Stanwell's business activities.

4.0 Content

This policy delivers a strategic methodology to Stanwell's business resilience which incorporates an organisation-wide approach to managing the risks and vulnerabilities which may impact on Stanwell's ability to achieve its strategic objectives.

Stanwell recognises that business resilience is dynamic and emerges from the complex interaction between a wide range of business processes. To achieve business resilience, Stanwell has established a business resilience framework that integrates the functions of business continuity, security, insurance and risk management.. This alignment supports the knowledge, expertise and skills of its people to develop, implement and maintain a robust and appropriate business resilience and risk management program for the corporation.

The diagram below details the relationship between risk management, business continuity (including crisis, incident, disaster recovery and emergency response), security and insurance.



4.1. Business Continuity

Business continuity planning provides assurance that Stanwell has a sound degree of resilience should it be required to respond to and recover from a crisis while continuing to maintain business critical operations. Stanwell conducts annual reviews of its business interruption risks and implements appropriate planning to mitigate those risks.

The business continuity management program includes the Business Continuity Procedure (GOV-PROC-47), Crisis Management, Incident/Emergency Management, and critical function continuity response capability, which is underpinned by plans, processes, systems and tools. . . Business continuity plans are tested by periodic business continuity exercises.

Information Technology (IT) Disaster Recovery

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.

4.2. Security

Stanwell maintains a security management framework 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 resilience 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.

4.3. Risk Management

This policy defines risk management as a part of Stanwell's governance framework, articulates the responsibilities for the management of risk and ensures Stanwell uses its risk management capabilities to maximise value from assets, projects and other business opportunities.

Stanwell promotes a risk-aware corporation-wide culture in all decision making.

Through the skilled application of high quality, integrated risk analysis, our people will utilise risk effectively in order to enhance opportunities, reduce threats and to sustain our competitive advantage.

Stanwell recognises that risk is an integral and unavoidable component of our business and is characterised as both an opportunity and a threat to the achievement of objectives. Stanwell has adopted a combined "top-down" "bottom-up" approach to risk management, which focuses on both setting the strategic direction and implementation of a robust control framework across the entire business. Stanwell is committed to:

- managing all risks in a proactive and effective manner;
- behaving as a responsible corporate citizen, protecting employees, customers, contractors and their property, as well as the community and the broader environment from unnecessary injury, loss or damage;

- achieving its corporate objectives by seeking opportunities to improve the business and optimise risk management; and
- finding the right balance between the cost of control and the risks it is willing to accept as the legitimate grounds for earning reward.

Stanwell's Risk Appetite Statement (Appendix 1) articulates the significant risks to which Stanwell is exposed and details the extent to which those risks will be accepted. The Board monitors Stanwell's adherence to the Risk Appetite Statement and the broader risk management process.

Stanwell's approach to risk management (adopting the principles of ISO:31000) is to:

- be commercially focussed and create value;
- have risk as an integrated part of health and safety, environmental, asset, operational and project management and strategic planning processes;
- ensure that risk management is tailored to the requirements of Stanwell and dynamically reviewed using the mechanisms defined within the Board Risk Oversight Model;
- take human and cultural factors into account;
- be transparent and inclusive via the corporate-wide risk management tool; and
- facilitate continual improvement of the organisation and its control frameworks.

To support this approach, risk analysis is applied to all facets of the business by management at appropriate levels, following the principles as set out in the corporation-wide Risk Management Framework (GOV-PROC-37) and utilising the Risk Evaluation Matrix (GOV-STD-11) to assess risk.

4.4. 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.

5.0 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 in the pursuit of Stanwell's strategic objectives. The Board is responsible for approving this policy and the Risk Evaluation Matrix (GOV-STD-11) and is responsible for overseeing, reviewing and ensuring the effectiveness and integrity of Stanwell's enterprise risk management system. The Board is responsible for the strategic direction, approval, governance and monitoring of business resilience within Stanwell in consultation with the Audit and Risk Management Committee, Chief Executive Officer and Executive Leadership Team.
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.

Position	Responsibility
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 and for having appropriate crisis management and business continuity planning in place.
Company Secretary	Accountable and responsible for the establishment, implementation and review of Stanwell's enterprise risk management, business resilience and security management frameworks.
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.
Our people	Our people are responsible for familiarising themselves with this Policy and the supporting strategies, 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.

6.0 Review, Consultation and Communication

Review:
This document is required to be reviewed at a minimum, every 2 years.

Consultation:
Executive Leadership Team

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 TRIM.

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.

7.0 Definitions

Not applicable

8.0 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-STD-11 Risk Evaluation Matrix
- GOV-PROC-37 Risk Management Framework

9.0 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 urgent 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