Policy
(Board Approved)

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 and operational 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 is the public version of this document and excludes Appendix 1 – Risk Appetite Statement. If you require access to a full version, please contact 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 approach to Stanwell’s business resilience which reflects a corporation-wide approach to managing the risks and vulnerabilities which may impact on Stanwell’s ability to maintain operations.

Stanwell understands that as a government owned corporation that has critical infrastructure assets, business resilience is crucial to ensuring continuity of electricity supply and meeting stakeholder expectations.

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 adopted a business resilience framework which brings business continuity, security, insurance and risk management together. 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 and emergency), security and insurance.
4.1. Business Continuity

Business continuity management for Stanwell is aimed at ensuring that Stanwell can maintain or return to business as usual (within predetermined timeframes) after a disruption, major incident or a crisis. Stanwell achieves this by building resilience into existing business functions to prevent or minimise the likelihood of these events occurring and developing plans to minimise the impact to Stanwell’s business should they occur.

The business continuity management program includes the Business Continuity Procedure, Crisis Management, Incident/Emergency Management and a Functional Continuity Response capability underpinned by plans, processes, systems and tools. These subordinate documents detail clearly defined objectives, roles, responsibilities and action plans to ensure Stanwell is effective and efficient in the management of any business disruption, event or crisis that may occur.

*Information Technology (IT) Disaster Recovery*

As a key component of Stanwell’s continuity and resilience response, Stanwell has in place a documented process to recover and protect Stanwell’s information and technology infrastructure should an unplanned and unanticipated event occur.

Stanwell’s IT Disaster Recovery Plan (IT-DRP) is a comprehensive statement of consistent actions that are to be taken before, during and after an 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 operations and/or computer services are rendered unusable. Requirements for the IT-DRP are incorporated into Stanwell’s business continuity processes and specifically the Corporate Office Incident Management Plan.

4.2. Security

Stanwell’s commitment is delivered through the adoption and implementation of the following security measures and by building resilience and security capabilities into all aspects of its operation including:

- proactively managing security threats/risks to health and safety of employees, contractors and visitors;
- Information, Records and Systems and Tools Security;
- protection of Stanwell’s physical infrastructure; and
- communication channels with Government agencies.

Stanwell’s security management program includes the Security Procedure. This procedure details clearly defined objectives, roles, responsibilities and action plans to ensure Stanwell is effective and efficient in the management of any security related issues or events that may occur.

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 possible) 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

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Board</td>
<td>Stanwell’s Board retains the ultimate responsibility for risk management and for determining the appropriate level of risk that the Board is willing to accept in the conduct of Stanwell’s business activities. The Board is responsible for approving this policy and the Risk Evaluation Matrix and is responsible for overseeing, reviewing and ensuring the effectiveness and integrity of Stanwell’s risk management system. The Board is responsible for the strategic direction, approval, governance and monitoring of business continuity, security and risk management within Stanwell in consultation with the Audit and Risk Management Committee, Chief Executive Officer and Executive Leadership Team.</td>
</tr>
<tr>
<td>Audit and Risk Management Committee (ARMC)</td>
<td>The Stanwell Board has established the Audit and Risk Management Committee to assist the Board to oversee the business continuity, security, disaster recovery, insurance and risk management activities. The responsibilities and detailed administrative duties of the ARMC are detailed in the Board-approved ARMC Charter. The ARMC will monitor and if necessary make recommendations to the Board in respect of the adequacy and effectiveness of Stanwell’s Business Continuity</td>
</tr>
<tr>
<td>Position</td>
<td>Responsibility</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chief Executive Officer (CEO)</td>
<td>Ultimate accountability to ensure the organisation has robust and effective business continuity, security, insurance and risk management strategies designed to minimise risk to Stanwell while protecting its asset and ensuring business resilience.</td>
</tr>
<tr>
<td>Executive General Managers</td>
<td>Each Executive General Manager is accountable for appropriate crisis management and business continuity planning in their division.</td>
</tr>
<tr>
<td>General Manager – Corporate Services</td>
<td>Accountable to the Chief Financial Officer for the implementation, review and management of Stanwell’s risk management, business continuity, security and insurance programs, including associated reporting to the Executive Leadership Team and the Board. Responsible for reviewing and updating the Corporate Crisis Leadership Plan and associated Incident Management Plans and documentation. Responsible for establishing and maintaining best practice governance frameworks that are appropriate and effective for Stanwell and which meet governance requirements. Responsible for promoting and educating Managers and Supervisors about governance practices including risk management, business continuity, security and insurance, and how they enable and support the achievement of corporate objectives.</td>
</tr>
<tr>
<td>General Manager Information and Business Systems</td>
<td>Oversee the development and execution of an enterprise-wide disaster recovery and business continuity plan for business critical information and business systems.</td>
</tr>
<tr>
<td>Managers and Supervisors</td>
<td>Managers and Supervisors are responsible for ensuring effective implementation and maintenance of this policy and the supporting strategies, procedures and processes.</td>
</tr>
<tr>
<td>Our people</td>
<td>Our people are responsible for familiarising themselves with Stanwell’s Policy and the supporting strategies, procedures, processes and plans that affect their workplace activities, incorporating risk practices into their business activities and reporting and escalate all events, risk concerns, issues and breaches.</td>
</tr>
</tbody>
</table>
6.0 Review, Consultation and Communication

Review:
This document is required to be reviewed by the General Manager – Corporate Services at a minimum, every 2 years.

Key stakeholders within relevant functional areas will be consulted as well as the Executive Leadership Team.

Stanwell’s risk, business continuity and security management approach is also periodically reviewed by the General Manager – Corporate Services, in consultation with the members of the Executive Leadership Team to ensure that the program remains efficient and effective and is appropriate to Stanwell’s needs.

Consultation:
General Manager Corporate Services
Insurance Specialist
Principal Advisor – Risk, Continuity and Security

Communication/Requirements after Update:
This policy will be communicated to key internal stakeholders via GenNet. General awareness training in relation to the application of this policy is provided to new starters during induction and via an on-line training tool.

This policy is made publicly available on Stanwell’s internet site [www.stanwell.com](http://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 Crisis Management Framework document or subordinate document.

Persons named in section 5.0 Responsibilities and Authorities above will be advised of any amendments to this policy. Should amendments to this policy require updates to subordinate documents, those updates will be communicated according to the Communication Plan of each subordinate document.

7.0 Definitions

Not applicable

8.0 References

- Environmental Protection Act 1994 & Regulation 2008
- Health & Safety Act 2011 & Regulation 2011

9.0 Revision History

<table>
<thead>
<tr>
<th>Rev. No.</th>
<th>Rev. Date</th>
<th>Revision Description</th>
<th>Author</th>
<th>Endorse/Check</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>27.02.2015</td>
<td>This policy is a consolidation of the Risk Policy, Business Continuity Policy and the Security Policy.</td>
<td>K. Biggs</td>
<td>M O'Rourke</td>
<td>Board</td>
</tr>
<tr>
<td>1</td>
<td>16.02.2016</td>
<td>Annual review of Policy and inclusion of Risk Appetite Statement</td>
<td>K Biggs</td>
<td>M. O'Rourke</td>
<td>Board</td>
</tr>
<tr>
<td></td>
<td>20.04.2016</td>
<td>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. This approach was communicated to the CEO and Secretariat.</td>
<td>D.Wilkie</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10.0 Appendix 1: Risk Appetite Statement

This is the public version of the Business Resilience and Risk Management Policy. The public version of this policy excludes the Risk Appetite Statement due to the sensitivity of information. If you require access to a full version of this policy please contact the policy owners.