Group Risk Management and Internal Control Policy

Policy statement

SSE's policy is that everyone in the company has a responsibility for management of risks; that the risks to the business are understood and effectively managed; and that decisions must be made with full consideration of the risks involved.

Policy purpose

This policy outlines the principles and responsibilities which underpin SSE's approach to risk. It is designed to ensure that risks are taken and managed consciously, recognising that this is a necessary part of doing business.

This policy is owned by the Director of Group Risk and Audit and is one of a suite of group-level policies that promote a healthy business culture, guide decisions and actions as expected by the company's stakeholders, and make SSE a responsible company that people want to invest in, buy from, work for and partner with.

Ewan Currie
Director of Group Risk and Audit

Alistair Phillips-Davies
Chief Executive Officer

Doc Ref: PO-GRP-014

Version: 1.1

Effective Date: April 2021

Review Date: April 2022

POLICY PRINCIPLES

The following principles highlight how we expect the policy statement to be achieved, and should be used to guide behaviours, decision making and action:

Risk Appetite	• The Board of Directors set the Risk Appetite for the Group. The achievement of SSE's strategic objectives necessarily involves taking risk. SSE will however only accept risk where it is consistent with its core purpose, strategy and values; is well understood; and can be effectively managed; and offers commensurate reward.
Risk Management	• Everyone in SSE has a responsibility for the management of risk. To ensure success, it is critical that the risks to our business are understood and effectively managed. Decisions must be made with full consideration of the risks involved and in accordance with the procedures and guidance provided by Group Risk on behalf of the Board of Directors.
Compliance	• SSE conducts its business in a manner which is fully compliant with all relevant legislation, regulation and rules – both external and internal.
SSE System of Internal Control (SOIC)	• An appropriate system of internal control (SoIC) will be maintained, in accordance with the requirements of the UK Corporate Governance Code, to support the business in meeting its objectives. • SSE's SoIC consists of Governance, Strategic, Risk Management, Assurance, Standards & Quality Frameworks.
Business Continuity /Disaster Recovery	• SSE aims to minimise the potential impact of risk events and safeguard the delivery of our services by ensuring adequate Business Continuity and Disaster Recovery Plans are in place and are regularly tested. These plans are designed for the management of, and the recovery from, significant risk events.
Viability	• Consideration of the financial impact of severe yet plausible scenarios relating to each Principal Risk must be given to inform decision making and ensure appropriate mitigation measures are applied and maintained.
Insurance	• Insurance should be purchased for all statutory requirements and on an optional basis dependant on contractual obligations and risk appetite.
Business Separation	• SSE will apply appropriate measures to comply with business separation regulatory requirements (where

	applicable), including staff training of obligations and associated risks.

ROLES AND RESPONSIBILITIES

This policy applies to all SSE employees. We also expect employees of third parties and those working on our premises and with our employees to meet the same level of standards.

Everyone in SSE has a responsibility to identify and to protect the business from risks which could threaten the achievement of objectives or compromise the SSESET of values, and to operate in a manner which is compliant with all relevant legislation, regulation and rules

The **Board of Directors** is accountable to customers, investors, employees and all other key stakeholders, and has ultimate responsibility for the effectiveness of SSE's management of risk.

It is the responsibility of each of the **Managing Directors** (MDs) of SSE's Business Units and those **Directors** leading Corporate Service functions to ensure that the risk management procedures as provided by Group Risk are followed, that compliant processes are implemented, supporting documentation provided and that applicable business separation risks are adequately managed. MDs must also ensure that management responsibility and accountabilities for compliance are clear, supported by appropriate structures and lines of sight. Audit actions should be completed within agreed timescales and all control improvement actions, including those identified in the annual MD assurance evaluations, should be completed and monitored on an ongoing basis.

Managers are responsible for ensuring that their teams understand and comply with this policy and supporting procedures and complete any relevant training.

All employees must comply with the policy and supporting procedures and complete all relevant training.

The **Group Risk Manager** supports the Board of Directors in fulfilling its risk management obligations as set out in the UK Corporate Governance Code. The Group Risk Manager is responsible for providing risk management-related support to SSE businesses and for reporting SSE's approach and performance around risk management to stakeholders.

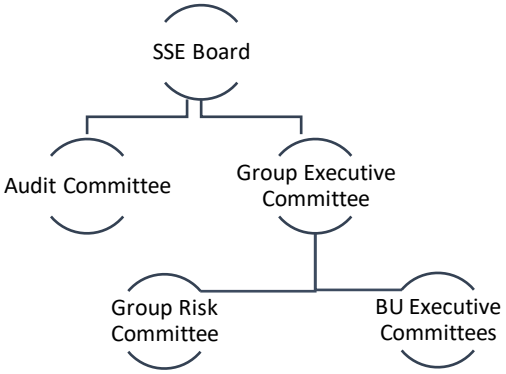
Group Audit work with the business to understand the key risks and controls of the Group, and to examine and evaluate the adequacy and effectiveness of SSE's risk management activities and controls.

Group Compliance performs independent reviews to assess the level of compliance in the business with key regulatory and legislative obligations, providing advice and guidance where appropriate.

Subject Matter Experts provide advice on changes or additions to external legal and regulatory rules.

In order to facilitate business separation adherence and reporting the SSEPD Board has internally appointed a dedicated **Business Separation Compliance Officer** (BSCO).

GOVERNANCE



The **SSE plc Board** and **Group Executive Committee** are responsible for the oversight for this policy including the approval of any changes to the policy. This policy is reviewed annually as part of an evaluation process.

The Board will determine the nature and extent of the risks which SSE is willing to take to achieve its objectives (SSE's "Risk Appetite").

The **Audit Committee** is responsible for the monitoring and ongoing review of the effectiveness of SSE's risk management and internal control systems.

The **Group Executive Committee** is responsible for the implementation and operational effectiveness of the Board's strategies and decisions in respect of risk management.

The **Group Risk Committee** supports the Policy Owner and ensures that the policy is adhered to through awareness and monitoring of policy implementation. Incidents and breaches are reviewed and where appropriate opportunities for improvement are actioned.

The **Business Unit Executive Committees** are responsible for the identification of risks and corresponding mitigations (including Business Continuity and Disaster Recover Plans) that are Principal to its Business Unit and that these risks are monitored on an ongoing basis and, reported and escalated in line with the Governance Framework.

TRAINING

Appropriate training is seen as key mitigation against risk across the Group and all mandatory training should be completed in a timely manner when required. SSE has a mandated Ethics and Compliance elearning programme for key topics to ensure we are all aware of our responsibilities for doing the right thing.

Our Auditors maintain their skills to provide effective assurance of business risk mitigations.

The Leadership Blueprint includes the need to anticipate future risks and their impact, and the need to take measured risk in the pursuit of future value.

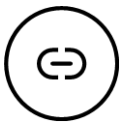
SPEAKING UP

SSE takes pride in its reputation as a responsible company with a strong commitment to always do the right thing. SSE's core values – Safety, Service, Efficiency, Sustainability, Excellence and Teamwork – guide the actions employees take on the Company's behalf and the "decision tree" in the Guide to Ethical Business Conduct for SSE Employees helps people through ethical dilemmas.

The achievement of SSE's strategic objectives necessarily involves taking risk. SSE will however only accept risk where it is consistent with its core purpose, strategy and values; is well understood; and can be effectively managed; and offers commensurate reward. Safety is SSE's first value and it has no appetite for risks brought on by unsafe actions, nor does it have any appetite for risks brought on by insecure actions including those relating to cyber security.

If you see or hear something that falls short of our expected high standards of ethical conduct and compliance you should be able to discuss it with your manager or a Speak Up Ambassador, but when that is not possible you are encouraged to raise issues with SafeCall through the following channels:

- Phone: 0800 915 1571 (UK) 1800 812 740 (Ireland)
- Email: sse@safecall.co.uk
- www.safecall.co.uk/report



SUPPORTING DOCUMENTS

The Risk Blueprint provides clear, practical guidance to help all employees fulfil their risk management obligations and derive value from doing so in order to aid the successful delivery of objectives.

Additional documents available to provide further guidance and support can be found on the Document Library:

- Group Risk & Audit
- Group Compliance

The policies and procedures relating to all risk management activities including SHE, Cyber Security, Large Capital Projects, Fraud, Bribery and Anti-Corruption should be adhered to at all times.

To ensure that our legal and regulatory obligations (in particular) are fully understood and adhered to, these must be identified and documented. An obligations database (iComply) has been developed and is maintained by Group Compliance to support this.

Further information can also be found on SSEnet:

- Group Risk
- Group Compliance
- Group Audit
- Insurance

DEFINITIONS

SSE defines **risk** as any event or circumstance which has the potential to threaten the achievement of our objectives or compromise the SSESET of values.

External obligations include legislation, regulation, industry codes and government policies.

Internal obligations include company mandated policies, standards, procedures, values, rules and codes of conduct.

Comments and feedback on this policy and its application are welcome.

Please contact kim.mcmanus@sse.com