Group Risk Management Policy

Policy statement

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

Policy purpose

The purpose of the Group Risk Management Policy is to set expectations, principles, and detail responsibilities for the management of risk which supports the achievement of SSE objectives, protects staff and business assets, and ensures financial sustainability.

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

Martin Pibworth

Chief Executive Officer

Doc Ref: PO-GRP-014

Version: 2.02

Effective Date: April 2026

Review Date: April 2027

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	• Risk appetite describes the nature and extent of risk the Group is willing to take to achieve strategic objectives. • The Board 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; can be effectively managed; and is in line with stakeholder expectations. • There is an expectation that each Business Unit defines its risk appetite and risk tolerance across relevant Principal Risks and/or risk categories (depending upon its priorities and operations) in a way that it is consistent with the Group risk standards.
Enterprise Risk Management Framework (ERM)	• The purpose is to help identify, assess, and analyse key business risks and minimise negative business impacts if those materialise. • Allows management to oversee a complete, integrated, organisation-wide level of risks. • Through Enterprise Risk Management, each Business Unit and Corporate Function can manage risks in the most appropriate way for its business activities and operations while meeting the risk management standards that have been set by the Board. • There is an expectation that risk management is embedded within key business processes and supports key decision making where appropriate. • The four stages of the Enterprise Risk Management framework are: o Risk Identification – there is an expectation that each Business Unit and Corporate Function identify potential risks from internal or external sources. Each Business Unit should identify its risks to achieve strategic objectives and each Corporate Function should identify its relevant Group wide functional risks. o Risk Assessment – there is an expectation that each Business Unit and Corporate Function analyse and evaluate its risks, identify significant changes, and measure the materiality and impact (aggregation) of risks.

	○ Risk Response – there is an expectation that each Business Unit and Corporate Function has adequate processes and controls in place to manage identified risks. An action plan should be developed which aligns to the risk response and must have an owner, who is aware of their role and responsibilities. ○ Risk Monitoring – there is an expectation that each Business Unit and Corporate Function conduct ongoing evaluations, communicates deficiencies, and sets Key Risk Indicators (KRIs). • There is an expectation that any risk acceptance or authority must be defined on a qualitative criteria and approved by the appropriate person(s) in line with the risk governance framework.
Risk Universe	• Provides all relevant risk categories to ensure all risks are considered and captured in a consistent manner. • The primary risk categories are: ○ Strategic and Market ○ Operational ○ Legal and Regulatory ○ Financial • There is an expectation that each Business Unit and Corporate Function advise the Group Risk Team of any changes in its risk exposures to ensure all risk categories can be captured.
SSE System of Internal Control (SoIC)	• An appropriate System of Internal Control will be maintained, in accordance with the requirements of the UK Corporate Governance Code, to support the business in meeting its objectives. • There is an expectation that each Business Unit and Corporate Function implement and maintain controls in adherence with the SoIC. • There is an expectation that each Business Unit and Corporate Function will complete the end of year Assurance Evaluation (Letter of Assurance Process) and present this to the CEO and FD in line with the agreed timetable.
Viability Assessment	• Consideration of the financial impact of severe yet plausible scenarios relating to each Principal Risk must be provided to inform decision making and ensure appropriate mitigation measures are applied and maintained. • There is an expectation that each Business Unit identifies, and analyses stress test scenarios based on individual Business Unit Principal Risks to substantiate disclosures on

	the viability of the Business Unit in the annual Business Unit Risk Report.

ROLES AND RESPONSIBILITIES

Risk management is the responsibility of everyone at SSE. 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.

Where we operate internationally, we will utilise our Group Policies as a default, subject to legal or regulatory requirements of the relevant international domain, and relevant local policies and supporting procedures.

The Board	• The Board are accountable to customers, investors, employees, and all other key stakeholders, and has ultimate responsibility for the effectiveness of SSE's management of risk. • 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") and approve the Group Risk Management Policy as proposed by the Group Risk Committee.
The Audit Committee (AC)	• Responsible for the monitoring and ongoing review of the effectiveness of SSE's risk management and System of Internal Control on behalf of the SSE Board. This includes all external risk disclosures and Viability Assessment.
The Group Executive Committee (GEC)	• Responsible for the implementation and operational effectiveness of the Board's strategies and decisions with respect to risk management.
The Group Risk Committee (GRC)	• Responsible for providing executive level oversight of Group level risks. This includes monitoring risks that are managed at Business Unit or Corporate Function level which have Group implications. • Review risk exposures across the Group by overseeing the controls and strategies employed to manage these risks. Ensuring and promoting an effective System of Internal Control and assessing that the correct mitigating controls and mechanisms are in place for managing all Group risks. • Constructively challenge and provide oversight for the ongoing effectiveness of the Group Enterprise Risk Management framework.

	• Provides assurance to the Group Executive Committee, Audit Committee, and the Board that risks are being managed effectively across the Group. • Responsible for the endorsement of the Group Risk strategy, policy, processes, and procedures. • Endorses and proposes to the Board the Group risk appetite statement (both internal and external). • Endorses all external risk disclosures including Annual Report content, Viability Assessment and Review of Effectiveness of the System of Internal Control.
Energy Markets Risk Committee (EMRC)	• Responsible for reviewing the adequacy and effectiveness of SSE's risk management policy, framework and systems as appropriate for the identification, assessment, management, monitoring and reporting of Energy Markets risks. • Approve changes to the methodologies used in calculating exposures in commodities and counterparty credits.
Group Risk Team	• Supports the Group Risk Committee through the completion of a detailed assessment of Group level risks, either current or emerging, to allow consideration of how effectively these are being managed. • Provides detailed analysis to the Group Risk Committee on Group level risks, including risks recorded at Business Unit or Corporate Function level which have Group implications, risks that are interconnected and where risks are recorded in multiple Business Units. • Performs 'constructive challenger' role through interactions with Committees, Business Units, and Corporate Functions. • Delivers all statutory and Board committee responsibilities including Group Principal Risk Process, Viability Assessment, Directors and Strategic risk disclosures as part of Annual Report for SSE plc. • Sets risk management standards for SSE acting as a Centre of Excellence supporting each Business Unit and Corporate Function. • Collaborates with, coaches, and supports all stakeholders to embed effective risk management across SSE, providing proactive and accessible education and training materials.
Managing Directors of SSE's Business Units and Directors leading	• Accountable for ensuring appropriate risk governance is in place within the Business Unit or Corporate Function, supported by risk hierarchy.

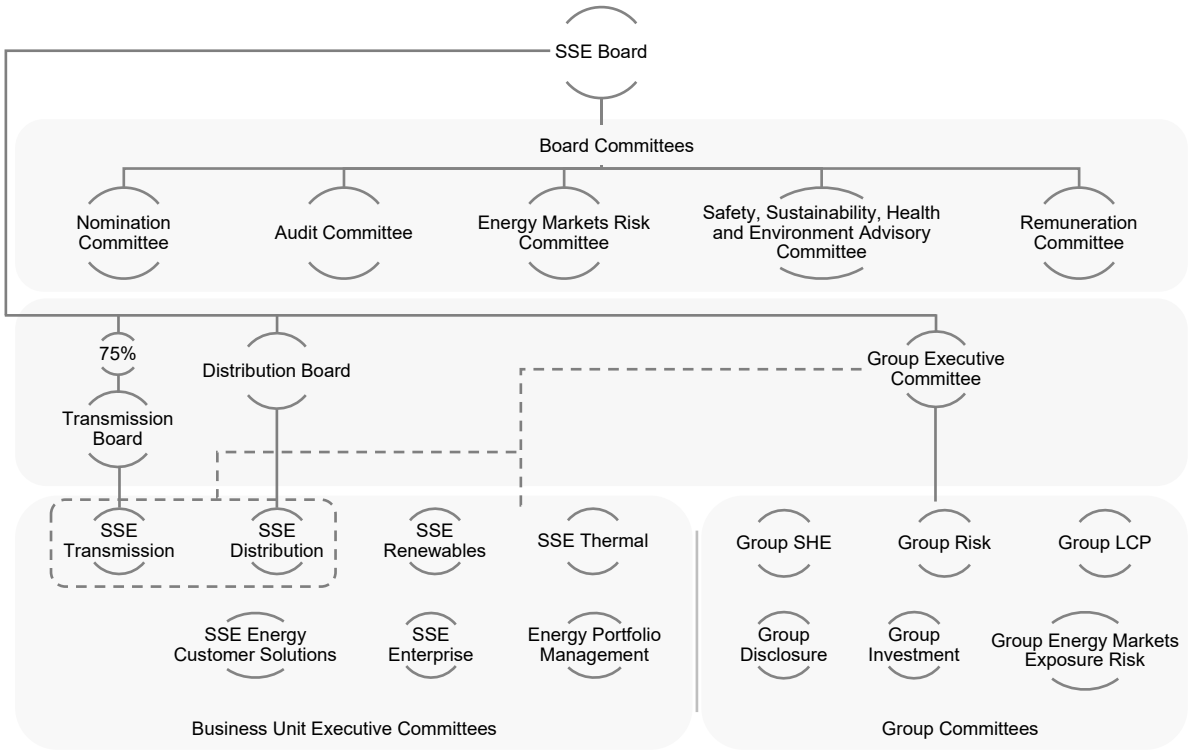
Corporate Service functions	• Responsible for supporting the implementation of the Enterprise Risk Management framework within the Business Unit or Corporate Function, ensuring that methodologies, tools, and techniques are followed in line with Group policies and procedures. • Ensuring the risk register remains relevant and up to date in accordance with the agreed risk universe. • Providing necessary information in relation to the monitoring and reporting of risks in line with the Group Risk Management Policy. • Completing the end of year Assurance Evaluation (Letter of Assurance Process) and presenting this to the CEO and FD in line with the agreed timetable. • Ensuring audit actions are completed within agreed timescales and that all control improvement actions are in place with ongoing monitoring, including those identified in the end of year Assurance Evaluation.
The Business Unit Executive Committee (Exco) Members and Corporate Function Leadership Team Members	• Responsible for establishing a risk governance framework, including a risk hierarchy, within its Business Unit or Corporate Function. • Responsible for establishing, communicating and effective implementation of the Enterprise Risk Management framework, methodologies, tools, and techniques within its Business Unit or Corporate Function. • Responsible for assessing and reviewing risks at Business Unit or Corporate Function level, ensuring appropriate action is taken and effective controls are in place to manage/mitigate risks. • Responsible for the monitoring of risks on an ongoing basis at the appropriate frequency and communicating to the Group Risk Team.
Group Audit	• Group Audit are an objective, independent function set up to review and assess the effectiveness of internal controls and risk management across SSE.
Safety, Health and Environment Committee (SHEC)	• Responsible for providing executive oversight and assurance that health, safety, and environmental risks are being effectively managed across the Group.
Large Capital Projects Committee (LCPC)	• Responsible for providing executive oversight and assurance that large capital project risks are being effectively managed across the Group.

Information Security and Privacy Committee (ISPC)	• Responsible for providing executive oversight and assurance that cyber and information security risks are being effectively managed across the Group, including operational security.
Anti-Corruption and Financial Crime Committee (ACFCC)	• Responsible for providing executive oversight and assurance that financial crime risks are being effectively managed across the Group.
All Employees	• All employees must comply with this policy and supporting procedures and complete all relevant training. • Everyone in the company has a responsibility for the management of risk.

GOVERNANCE

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

The Board-agreed division of responsibilities across key areas of SSE's governance framework is shown in the below structured governance pathways. Within SSE's governance framework dedicated committees have specific responsibilities for risk management described in the roles and responsibilities in the next section.



TRAINING

Appropriate training is seen as a 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.

The two learning paths are:

1 Training for all employees (based on Risk Methodology set within the Risk Blueprint document).
2 Specific training for groups of users for the Risk Management System (Group 1 – Input only into system, Group 2 – Input and report users and Group 3 – reporting only users).

Learning paths are designed to enable delegates to:

- Understand the purpose and principles of Enterprise Risk Management.
- Understand the need for risk assessment and management.
- Consider different methods to assess the level of risk.
- Identify common areas of risk and vulnerability.
- Define risk and the importance of risk assessments.
- Use practical tools to set SMART goals and risk management plans.

The Leadership Blueprint:

- Includes the need to anticipate future risks.
- Identify future opportunities and their impact.
- Allows measured risks in the pursuit of future value.

SPEAKING UP

Employees can discuss anything that falls short of our expected high standards of ethical conduct and compliance, with their line or any other manager within the business. Alternatively, any concerns can be raised internally at Speakup@sse.com or externally through SafeCall using:

- Phone:
  - UK - 0800 915 1571
  - Ireland - 1800 812 740
  - All other countries +44 800 915 1571. If you are more comfortable speaking in your own language, an independent telephone interpreter will be made available.
- Email: sse@safecall.co.uk
- www.safecall.co.uk/report

Any wrongdoing brought to light through the Whistleblowing Policy will result in internal disciplinary procedures, possible dismissal and criminal prosecution of individuals involved.

SUPPORTING DOCUMENTS

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

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

- Group Risk & Audit
- Risk Universe
- Risk Scoring Matrix
- Risk Governance Framework
- Risk Appetite Statement
- Viability Statement Procedure
- Risk Definitions

There are a suite of group-level policies and procedures relating to all risk management activities that should always be adhered to.

To support that our legal and regulatory obligations (in particular) are fully understood and adhered to, (iComply) captures the rules at risk across the SSE Group and provides a means to communicate and manage change to those obligations.

Further information can also be found on SSEnet:

- Group Risk and Audit