Risk Governance Framework at Contact Energy

October 2025

The purpose of Contact's risk management framework is to assist with the integration of risk management into significant activities and functions in a consistent manner in order to create and protect value at Contact. Our Board has established a robust risk management framework which ensures that:

- appropriate systems are in place to identify material risks
- we understand the potential impacts of identified risks and that appropriate risk tolerance limits are set by the Board
- responsibilities are assigned to individuals to manage identified risks and that material changes to risk profiles are monitored.

Contact's risk management framework is comprised of (but not limited to) our Risk Management Policy, Board Risk Appetite Statements, Risk Management Guidance documents and is supported by a range of systems and tools which help with risk assessment and reporting.

Contact's risk management framework is based on the foundational principles, framework and process for managing risk as set out in ISO31000.

Risk Governance Framework with board level oversight

Responsibility for the risk management framework sits with the Board, supported by the Audit and Risk Committee which assesses the effectiveness of, and monitors compliance with, the framework. The integrated nature of our business means that current and emerging risks are assessed frequently and reported regularly to the Board to help inform their decision making. The Board plays a critical role in approving Contact's risk appetite and tolerance. More detail and specific responsibilities are set out in the Board Charter here.

Contact's Audit and Risk Committee operates under a written charter here. All Committee directors including the Committee Chair (who is not the Chair of the Board) are independent, non-executive directors. One of the Committee's key roles is to assist the Board to fulfil its responsibilities in relation to risk management. The Audit and Risk Committee responsibilities include ensuring that management has established a risk management framework in line with the Board's expectations which includes policies and procedures to effectively identify, treat and monitor principal risks, and regular reporting to the ARC and Board.

Specific responsibilities of the ARC include:

- assessing the effectiveness of, and monitoring compliance with the risk management framework, including legal and compliance risks, climate-related risks, cyber security risks and prevention of fraud;
- identification of fulsome reviews on significant risks for inclusion in the agenda of the responsible Board and/or Board Committee meeting, as considered appropriate;
- reviewing the effectiveness of systems for monitoring Contact's compliance with laws, regulations and Government policies and relevant government policies;
- reviewing the effectiveness of systems to identify, manage and monitor IT risks and protect personal information;
- monitoring progress on embedding climate-related risk responses into business practices;

- reporting to the board on progress with risk management work.

Contact's Risk Governance Framework includes dedicated operational risk management functions in line with the three lines of defence model as follows:

Operational risk ownership (first line of defence)

Operational risk management at Contact Energy is embedded within the first line of defence, where business units and operational teams are directly accountable for identifying, assessing, and managing risks as part of their day-to-day responsibilities. These front-line teams are closest to the operational environment and are therefore best positioned to detect emerging risks and implement timely controls. Risk ownership is clearly assigned at the business unit level, with roles such as risk owners, managers, and team leads responsible for maintaining effective control environments.

The first line is supported by a robust framework that includes documented risk controls, regular risk reviews, and integration with Contact's central risk management database. This system enables consistent tracking of risk treatment actions and control effectiveness across the organization. Risk Champions embedded within each business unit play a key role in facilitating risk discussions, supporting risk workshops, and ensuring alignment with enterprise-wide risk objectives. Their collaboration with the enterprise risk team ensures that operational insights are captured and escalated appropriately, reinforcing a culture of accountability and continuous improvement.

This approach aligns with the Three Lines of Defence model endorsed by the Institute of Internal Auditors, which emphasizes the importance of operational management as the first line in owning and managing risk. By empowering operational teams with the tools, training, and authority to manage risk, Contact ensures that risk management is proactive, embedded, and responsive to the dynamic nature of its business environment.

Risk Management and Compliance oversight (second line of defence)

Risk Management

Contact has a separate risk function led by the Head of Risk and Business Assurance and reporting directly to the Chief Financial Officer.

The enterprise risk team provides risk support, monitoring and expertise on a regular basis throughout the year to ensure risk management objectives are achieved. This includes maintaining the risk management framework, identification of emerging risks, running risk workshops, risk training, regular risk reviews from business unit up to leadership team level and ultimately reporting up to the Audit and Risk Committee.

Risk Champions from each of the various business units support risk management processes within each of their respective teams. The Risk Champions actively work alongside the enterprise risk team as part of the regular risk review process with the business units and respective leadership team members.

The enterprise risk team at Contact has a focus on continuous improvement and as part of its planning for FY25 has developed an enterprise risk plan focussed on lifting Contact's risk capability and maturity and strengthening the second line of defence. Key activities include:

- Refreshing the risk appetite statements post the Contact 31+ strategy refresh

- Continued integration of climate related risk into our risk management framework
- Refreshing Contact's project risk matrix to support the renewable development pipeline
- Development of risk training including an e-learning risk 101 for new employees, quick guides to risk matrices and development of fraud risk training

Risk Champions from each of the various business units support risk management processes within each of their respective teams. The Risk Champions actively work alongside the enterprise risk team as part of the regular risk review process with the business units and respective leadership team members.

Compliance Oversight

Contact's legal team is responsible for compliance oversight, overseen by the General Counsel and Chief Corporate Affairs Officer. The team ensures adherence to laws, regulations and internal policies working closely with operational management to implement necessary controls.

The Contact Code of Conduct is our core policy document and it applies to everyone working for Contact, including the Board. It sets out our expectations for the standards of honesty, integrity, ethical behaviour and compliance with the Code of Conduct and policies it incorporates that we expect our people to meet.

Breaches of our Contact policies are reported monthly to the Chief Executive Officer and escalated through formal channels, including privacy breaches. Other parts of our compliance framework include the following:

- Key roles embedded within business units and providing specialized compliance and technical support in their respective fields.
- A Privacy Committee where dedicated privacy officers discuss breaches and privacy risk in order to strengthen controls and future compliance.
- Working Groups such as the Modern Slavery Working Group ensuring compliance with our Human Rights policy and consistency with our Modern Slavery Statement.
- Across both Retail and Generation and Trading various controls have been established in order to monitor compliance with legislative, regulatory and licensing requirements.

Independent Business Assurance Unit (third line of defence)

Our Business Assurance team fulfils our internal audit function and provides objective assurance of the effectiveness of our internal control framework. The team is based in-house and draws on external expertise where required.

The team brings a disciplined approach to evaluating and improving the effectiveness of risk management, internal controls and governance processes. We use a risk-based assurance approach driven by our risk management framework. The team has unrestricted access to all departments, records and systems of Contact, and to the Board Audit and Risk Committee, external auditor and other third parties as it deems necessary.

The team, overseen by the Audit and Risk Committee, has a strong mandate to perform agreed assurance programmes. The Head of Business Assurance meets quarterly with the Chair of the Audit and Risk Committee and separately with the whole Committee where required. Findings are reported to the Committee and Leadership Team (and where required, to the Health, Safety

and Environment Committee). Independence is an important feature of the team. It has a direct line to the Chief Executive Officer, Chief Financial Officer and the Audit and Risk Committee (and in extreme cases, to the Chair of the Board) where it considers that a significant issue should be reported.

The Governance Matters section (pages 74 – 77) of our latest integrated report provides more detail on our Risk Governance Framework at Contact Energy.

Risk Management Processes

Contact has risk management processes and strategies to promote an effective risk culture. Our Risk Management Policy and enterprise risk framework underpin risk management at Contact and ensure that we empower and support our people in identifying, assessing and managing risks by providing appropriate tools and processes.

Our risk management processes are embedded across the business including in our project delivery process, development of new initiatives through Mau Taniwha (our transformation programme), governance structures and day to day operations.

Our strategies to promote an effective risk culture are led by a dedicated enterprise risk team focussed on lifting the capability and maturity of risk management across Contact. In 2025 the team have delivered new risk training covering our risk matrices, fraud risk, Risk 101 and training videos on our risk management database. Further details in relation to our risk culture are outlined in the risk culture section below.

Risk review

Risk reporting regularly takes place with the Leadership Team and Audit and Risk Committee (ARC). Risk reporting to the ARC includes identification of top enterprise risks, a description of the risks, the current risk rating, as well as controls and risk treatment actions. The table below sets out two of Contact's top enterprise risks and mitigating actions:

Risk Category	Description	Magnitude	Likelihood	Risk Rating	Actions and Mitigations
Financial, Partners & Stakeholders	There is the risk of government intervention in the wholesale market due to security of supply concerns and/or electricity price pressures	Critical	Unlikely	High	Continuing to build out our renewable development portfolio in order to meet demand, maintenance programmes for our Thermal fleet to maintain firming capacity until the energy transition is complete, increased battery storage, increased demand response and other alternative products to manage security of supply.
People Safety and Wellbeing, Partners & Stakeholders, Financial	There is the risk of harm, serious injury or death due to a degradation or failure of health, safety and wellbeing controls resulting in fines or penalties, remediation costs or reputational damage.	Critical	Unlikely	High	Mitigations include continuous improvement of all controls, a variety of tools including our StayLive Competency Tool, capturing learnings in our 'knowledge well", scaleable learning tools, being learnings to life for our people.

Risk appetite

Contact Energy's risk appetite statements define the amount and type of risk we are prepared to pursue, retain or take in pursuit of achieving our strategy and objectives. The statements align to our Contact 26 Strategy and ensure that our risk appetite enables growth and does not hinder our ability to achieve our objectives.

The risk appetite statements are reviewed periodically with the Board in line with the strategy setting process and are also tested retrospectively against business activities to test divergence from risk appetite. The Enterprise Risk team is in the process of updating our risk appetite statements in line with the Contact 31+ strategy refresh that is currently underway. As part of this process, the enterprise risk team have been sitting alongside the Board as they have developed the new strategy to capture the Board's thoughts and comments around risk appetite.

Our risk appetite statements are translated or operationalised into the enterprise risk matrix across Contact's 5 risk categories – People, Safety and Wellbeing, Compliance, Environment, Financial Performance, Customers, Partners & Stakeholders.

Our enterprise risk matrix is our on the ground risk management tool and provides guidance on actions required and escalation pathways where risks are assessed as outside of risk appetite.

Risk exposure review process

Regular reviews are undertaken of Contact's risk landscape to ensure Contact is reviewing its risk exposure and can continue to deliver on its strategic objectives. This is achieved through:

- A regular risk review process is held with the various business units across Contact. Teams are specifically asked to scan both the internal and external environments for any changes or emerging trends. These changes are incorporated into existing risks or recorded as new risks.
- Quarterly risk reviews are held individually with Leadership Team members to review their existing risks as well as reviewing any new or emerging risks. Risks rated high and above are regularly monitored for active management by the Leadership Team.
- Interviews are held with key stakeholders including board members, leadership team members and tier 3 leaders annually as part of the development of the annual risk and business assurance plans. Stakeholders are specifically asked about changes to the internal or external environment and emerging risks that may impact Contact's risk landscape.
- The enterprise risk team regularly attend training, development and education session on new and emerging risks in New Zealand and the energy sector.
- Refer to pages 76-77 of our 2025 Integrated Report for more details on Contact's process for reviewing its risk exposure.

Risk management process audit

An audit of the strength of our entity level controls was undertaken in June 2024 by a qualified internal auditor. The strength of our entity level controls was assessed against the risk assessment component of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control - Integrated Framework May 2013 (Framework). This is an internationally recognised principles-based framework covering the design, implementation and evaluation of the effectiveness of an organisation's entity level controls.

The risk assessment component included four underlying principles, one of which covered the assessment of the methods, tools and processes used in identifying, evaluating, controlling, monitoring and reporting risks.

In addition, a gap analysis was undertaken by the Head of Business Assurance against ISO31000, the findings of which were used to develop the 2025 annual risk plan and risk continuous improvement programme.

Risk Culture

Risk management education for non-executive directors

Contact has developed a programme for the purposes of inducting new board members with the intention of ensuring board members are brought up to speed quickly in order to meet their governance obligations for Contact. Risk is part of this programme including key enterprise risks specific to Contact Energy as well as essential company and board information and the energy industry. The programme is administered by Contact's board secreteriat and is regularly updated to align with best practice. David Gibson participated in the programme with his appointment in 2024.

Contact has an ongoing board education programme covering a variety of topics including risk based topics. During 2025, the directors received updates and training on the following key areas of risk:

- Real-life simulation of a Cyber attack
- Training on the XRB Climate Risk Disclosures
- Quarterly deep dives covering topics in relation to Contact's top enterprise risks

Focussed training on risk management principles

The foundational principles set out in ISO3100 are incorporated into our risk training programme. It is customised, uses the best available information, integrated and a variety of different mediums are utilised including quick guides, on-line modules, video tutorials and personalised training. The focussed training on risk management principles undertaken throughout Contact includes:

- Bespoke risk training which is integrated and tailored to different business units (depending on their level of maturity in risk management) as part of the regular business unit risk review process, risk workshops or on request.
- All employees at Contact are also required to complete regular mandatory training in respect of privacy risk, the code of conduct, security awareness and health and safety risk.
- Employees at Contact managing specific types of risk including commodity risk, credit risk, legislative risk (including the Fair Trading Act 1986, securities trading and competition law) are required to undertake regular, mandatory risk training.
- New inductees to Contact are provided with access to Contact University which includes our risk training programme mentioned above. This includes our Risk 101 module (covering Contact's risk appetite statements, information on identifying, assessing and managing risk, our matrices and risk acceptance criteria)
- The enterprise risk team actively promotes a culture of availability and all risk training material recommends talking to the risk team if more assistance or personalised training is required.
- Training and development on risk assessment, analysis, and management in the Generation and Trading side of the business as part of systematic risk management processes that are based on industry standards and good practice. This training and development is driven by defined senior roles responsible for discipline risk oversight.

Incorporation of risk criteria in the development of new products and services

The development of any new energy product for our customers involves a comprehensive risk assessment, encompassing environmental, commercial, commodity, legal, and health and safety risks. Any significant risks identified are documented and managed throughout the product development lifecycle to ensure they are maintained within risk appetite.

Contact goes even further and is developing products that are specifically designed to reduce some of Contact's material risks. A good example is Our Good Plans which help manage the risk of security of supply around periods of peak demand and reduce the need for fossil fuel generation. By offering free or discounted energy during off-peak hours, customers are incentivised to shift load, reducing the risk around security of supply and environmental risk.

Offering financial incentives tied to meeting risk-related goals.

The CEO and Executive Team remuneration is reviewed by our Board each year. The Board works closely with and is advised by Contact's People Committee. The total remuneration is made up of a fixed remuneration component, which includes cash salary and other employment benefits, and pay for performance remuneration containing short term incentives (cash and equity awarded through deferred share rights) and long-term incentives (equity awarded through performance share rights.

The FY25 corporate scorecard outlines corporate performance metrics that deliver the pay for performance remuneration. The performance metrics within the corporate scorecard are designed to address some of our primary risks as well as incentivise delivery of our strategic goals.

For example, one of Contact's top enterprise risks is around the risk of harm due to a degradation or failure of health, safety and wellbeing controls. The FY25 corporate scorecard contains a 20% weighting for Safety & Wellbeing targets in order to manage this risk. This covers targets specifically in relation to health, safety and wellbeing training, leadership site walkarounds, critical risk control failures and observations and incidents. A copy of the full scorecard can be found in the 2025 Integrated Report on page 82.

Two important long-term (3-5 years +) emerging risks that Contact identifies with the most significant impact on the business in the future are as follows:

	Emerging Risk 1	**Emerging Risk 2**
Name	Global Instability	Energy Disruption opportunity
Category	Geopolitical	Technological
Description	There is the risk of increasing global instability due to the escalating hostilities in multiple regions, economic uncertainty, the threat of misinformation and 3 billion people worldwide heading to the electoral polls	There is the risk Contact misses an 'energy disruption' opportunity with the increasing pace of technological, product and market change exceeding Contact's current vision/expectations due to excessive internal/industry focus resulting in lower future returns.
Impact	Potential increased fuel costs, supply chain constraints, project delays to our renewable development pipeline and loss of stakeholder confidence.	Loss of strategic and market relevance as a result of not identifying and leveraging the right opportunities, failure to adapt and loss of shareholder value, lack of preparedness for the future landscape and inability to decarbonise as quickly as competitors.
Mitigating Actions	Supply chain mapped and overlaid with areas of conflict, maintaining supplies of critical spares, strengthening procurement guidelines and policies, strong inventory planning and	Robust risk management strategy that incorporates future trends in the decision-making process, building relationships with emerging energy technology companies and startups, continuing board and senior executive study tours, monitoring of offshore developments with energy companies

	management, strategic stockpiling, focussed attention on global events and developments.	transitioning to renewables, building capability and knowledge within Contact to identify and stay informed on energy disruption trends