17 April 2026

National Security and Resilience Group
Department of Prime Minister and Cabinet
Via email: criticalinfrastructure@dpmc.govt.nz

Tēnā koe,

Protecting New Zealand communities from cyber risk

Powerco is one of Aotearoa's largest gas and electricity distributors, servicing urban and rural homes and businesses in the North Island through around 363,000 electricity connections and 113,300 gas connections. These energy networks provide essential services to over 1 million kiwis and will be core to Aotearoa achieving a net-zero economy in 2050. Information about Powerco is attached in section 5.

Cyber security is central to our operations. Like most critical infrastructure providers, manging cyber risk is an area of continual improvement as the risks change. The breadth of critical infrastructure providers, potential cyber risks and possible responses, is vast. A new regulatory framework to manage this collectively will be complex.

We have provided a response to the consultation document and questions in the attached document. Our summary views are:

All electricity services are vulnerable to cyber attack, but gas distribution is not	• For clarity, consistency, and to achieve the objective to "protect the lives and livelihoods of New Zealanders", all electricity distribution services should be within the definition of critical infrastructure • The potential impacts of a cyber attack on gas distribution networks are not comparable to electricity distribution networks, and do not need to be part of a regulatory framework for cyber security • Powerco has a considered and active approach to cyber security relevant for our operations, but there would be significant cost incurred to move it into a national regulatory framework.
Regulation needs to be proportionate and targeted to minimise costs	• Powerco would need to undertake considerable effort to align our framework with new regulation of the nature proposed • The consultation document is very light on detail of the regulatory proposals, and does not provide any cost benefit assessment. It is difficult for us to assess the implications and costs but costs are potentially significant. Robust cost benefit analysis is essential to ensure that the costs of options are proportionate to the anticipated value • Relying on voluntary mechanisms, existing processes, and information sharing will in many cases achieve improved cyber security. While regulation will likely be justified in

some areas, there are lower cost options available to achieve this such as extension of existing regulation of essential services. The consultation does not adequately assess options to justify the proposals which would add significantly to cost of energy at a time when energy affordability is already a challenge.

This submission does not contain any confidential information and may be published in full. If you have any questions regarding this submission or would like to talk further on the points we have raised, please contact Steven Jones (Steven.Jones@powerco.co.nz).

Nāku noa, nā,

Emma Wilson
Head of Policy, Regulation and Markets
POWERCO

Powerco comments: Critical infrastructure cyber security

1. Our infrastructure is vulnerable to cyber attack

1.1 There are cyber risks for all electricity network infrastructure

Powerco, like all other electricity distribution businesses (EDBs) is on a steep adoption trajectory for new technologies. Automation, remote monitoring, and digital management of our assets and operations is here now and will only increase over time. In addition to critical system components, we also hold significant sensitive customer data. These cyber risks are present for all 29 EDBs, it is not a matter of network length or number of connections.

Conversely, the gas distribution network is not subject to the same level of cyber risk and gas distribution businesses (GDBs) do not need to be subject to specific cyber regulation.

We comment further on the thresholds and definition of critical infrastructure in section 2.

1.2 Powerco's approach to managing cyber risk

Powerco manages cyber risk as a part of Powerco's risk framework. Our risk framework reflects our Board's agreed risk appetite, and focusses on our priorities as an organisation. This is different to a pure cyber focus in a national context, which is the subject of this consultation. For example, while we define our 'critical cyber assets' this is in our risk context, not that proposed in the consultation document.

Cyber risk is managed by Powerco's Information Security function through our enterprise risk framework, with risk identification, and detailed control mapping and control effectiveness assessment and assurance aligned to our organisation's priorities. The residual cyber risk is inclusive of components that are outside the scope of the national regulatory framework.

The consultation document is focused on cyber risk to delivery of essential services. As a commercial entity, our risks and responses have a much broader scope. For example, we hold and manage private customer data. This is not necessarily a 'component' that if disrupted would have a significant consequence for delivery of electricity services, but it is an aspect of our operations that requires careful protection in our risk management framework.

While we have a considered and active approach to cyber security relevant for our operations, it would not just be a matter of lifting this into a national regulatory framework (as indicated in the consultation). Powerco would need to undertake considerable effort to align our framework with new regulation of the nature proposed. Early clarity of the new regime will be very important, as well as certainty that the requirements will not change, for example through subsequent designation of entities or changes to obligations on entities by the Minister.

2. Defining critical infrastructure

2.1 Alignment of definitions across regulations

The Emergency Management Bill defines essential infrastructure providers (similar to lifelines) and essential infrastructure services. In that Bill, essential service is defined, but obligations are all directed to essential infrastructure providers as named in Schedule 3, rather than all entities that may deliver an essential service.

The proposal[1] in this consultation has similar, but not the same definitions as the Emergency Management Bill. The sectors included as essential services in this proposal also differ from the Emergency Management Bill, for example health and defence are not in Schedule 3 of the Emergency Management Bill. Alignment between the Emergency Management Bill and any critical infrastructure cyber security regulation is fundamental to ensure streamlined implementation and avoid confusion across these two overlapping regulations.

In our feedback on the Emergency Management Bill, we recommended removing the reference to suppliers from the list of essential infrastructure components. The functioning of organisations that provide for example, equipment or technical services to us, is less relevant in an emergency, and not a component for which an essential infrastructure provider has control. The same principle applies in defining components of critical infrastructure and obligations for the cyber security regulation.

2.2 Thresholds in the energy sector need adjustment

The proposal is for critical infrastructure to only include electricity distribution services where the distribution service is above a threshold of 25,000 ICPs. The consultation Supplementary Document 2 suggests the reason for this threshold (in relation to electricity distribution) is not to exacerbate energy poverty by imposing costs that would be recouped across a relatively small population[2]. However, no assessment of cost is provided specific to the electricity distribution sector to understand if this is a reasonable conclusion. Due to the existing regulation of all distributors to produce asset management plans and report on expenditure and performance through information disclosure, additional cost imposed by the proposed measures could be minimised compared to some other sectors. Excluding some communities from the protection this regulation is seeking to achieve, will not be consistent with the objectives and principles for this proposal, as set out in the consultation Supplementary Document 1.

The proposal for gas distribution sets a threshold of 500,000 GJ/year. Unlike electricity distribution, this would capture all gas distribution businesses, including the smallest distributor with less than 10,000 connections. Unlike electricity networks, the gas distribution network is not subject to the same cyber risk as gas distribution systems are not remotely controlled or computerised in the way that electricity distribution systems are. The risk of interruption to gas services to customers from a cyber attack is low. While we manage our electricity and gas risks collectively in our enterprise risk system, gas distribution businesses (GDBs) do not need to be subject to specific cyber regulation. The consultation documents provide no explanation for including gas distribution services and we consider that there is no justification for the costs that would be imposed on GDBs.

[1] As summarised in the consultation document Figure 3
[2] DPMC Consultation Supplementary document 2, page 11.

The description of the services and thresholds proposed to be captured in the definition of electricity and gas critical infrastructure is inconsistent between the Supplementary Document and the Consultation Document. The detailed description in Supplementary Document 2 (page 10-12) refers to "electricity distribution businesses" with more than 25,000 ICPs, rather than a network with more than 25,000 ICPs. And for gas, this description references "distribution pipeline" that conveys more than 500,000 GJ/year, rather than a distribution business that conveys this volume. Elsewhere in the consultation material it references "electricity distribution services" or "gas pipeline services". The definition needs to be consistent and clear if it relates to a network/pipeline area, or a distribution business volume. For example in both Powerco's electricity and gas businesses, we have separate discontinuous network areas which are reported separately for our regulated information disclosures, as well as reporting for Powerco as a whole.

While there may be a case[3] in sectors other than electricity for a threshold to reduce compliance costs, in our view, for clarity, consistency, and to achieve the objective to "protect the lives and livelihoods of New Zealanders", all electricity services should be within the definition of critical infrastructure and no gas distribution services should be included.

Electricity services are changing. Powerco is on a path to become a distribution system operator by 2030 with more of a role in coordination of supply and demand at a local level, in addition to traditional network services. The consultation document refers to electricity distribution services as defined in section 54C of the Commerce Act 1986 which is an identifier for EDBs, but not necessarily for all components that will provide essential electricity services in the future.

As noted above, early clarity of the new regime will be very important, as well as certainty around the entities and services subject to requirements. We do not agree that the Minister can override set thresholds – either you have a threshold or you don't, and if you do it must be clear and certain.

2.3 Critical infrastructure of national significance

The proposal is that a "very small subset" of critical infrastructure components would be designated of national significance. However, the nature of this subset is not defined and examples of the core components not provided. It is therefore not possible to comment on the benefits or implications of having additional requirements for these components.

It is our assumption that components of our electricity distribution service and gas distribution services would not be classified as nationally significant.

[3] Although there is no evidence provided to justify this based on costs.

3. Cyber defences that are proportionate to the risk and minimise cost

We agree that there are costs associated with enhancing cyber security, and investment ahead of disruptions will provide better value than the costs faced with disruption from an event. Robust cost benefit analysis must be completed to ensure that the costs of any proposed regulation are proportionate to the anticipated value. We are concerned that costs of proposals may be significant, and the consultation material does not demonstrate that lower cost options have been assessed. For example, all of the measures could be incorporated into the emergency management regulatory framework, using existing processes and powers rather than another, parallel, regulatory system.

3.1 Information sharing

Measure 1: Allow government to collect specific information from critical infrastructure entities

We understand that the Minister is seeking improved understanding about critical infrastructure. A description of Powerco's operations, infrastructure components, and ownership is largely available through our asset management plan, information disclosures, public information on our website and lifeline group information. It is very difficult to understand from the consultation document what the extent of information requirement may be, how this would be managed to align with, and not duplicate, existing information disclosure, and the costs/benefits of this measure.

We do not oppose this proposed measure but strongly recommend that it be designed to complement existing measures and any additional information requests are very targeted and directly related to cyber risk management rather than critical infrastructure in general.

We are aware of various attempts at mapping critical infrastructure dependencies. Including in the 2023 Emergency Management Bill, and various initiatives regional emergency management groups have started[4]. There are many challenges in achieving robust, consistent and meaningful mapping of dependencies. We fully support improved coordination between critical infrastructure providers, and mapping dependencies is the first step in this. Ideally, this should be a joint exercise between those dependant critical infrastructure providers (probably at a regional scale), not a matter of individual entities submitting information to the Minister which is how the proposal appears. Requirements around this 'mapping' require careful consideration to be workable while also being targeted at cyber risk and not something with a much bigger scope. This is an area that could be achieved through the new emergency management legislation.

It is unclear if information on interdependencies will be a matter for Measure 1 (individual entity view), Measure 2 (voluntary shared view), or Measure 3 (mandated shared view). With the reliance of all other sectors and entities on electricity systems (rather than the reverse), we are concerned about the disproportionate effort that will be required by EDBs to respond to queries from entities or the Minister about dependencies and provide this information in an appropriate form. We would like to see more clarity about the form and type of information about

[4] Including the Wellington Region Lifelines Group 2022-23 pilot of Planning Emergency Management Levels of Service

dependencies that will be expected, and how this information will be moderated and managed to provide benefit without undue costs.

Measure 2: Establish a voluntary information exchange

The intent for Measure 2 to create a cross-sectoral mechanism for engagement is sound. There are interdependencies and connections between critical infrastructure entities and sectors, and information sharing will assist in managing risk or responding to events.

We participate in the Control Systems Secure information Exchange. This has proved useful for some information sharing, however it is evident that some entities are cautious about what information is shared in this type of exchange. Powerco is concerned that increased sectors and entities in an exchange will discourage openness and increase risk of disclosure outside of the intended audience. Specific threat and risk information being disseminated does support Powerco to apply appropriate risk mitigations, however having this validated and endorsed by an authoritative party (NCSC) adds to its effectiveness. We particularly see value in an improved approach to DPMC and NSCC sharing information, for example about national threats.

In our view the creation and administration of a new information exchange platform for sharing information is not a priority. Mechanisms for sharing sensitive information between infrastructure providers and government are already available. If infrastructure providers supply details of major security incidents, the government can de-sensitise and share this information for the broader industry without needing a new secure platform. Improving the sharing of cyber security information is about the approach of people and the culture for sharing information and learning from it, not about having a platform to do so. Rather than developing another portal, we encourage the government to focus on the portals existing (or in development for other aspects of hazard/risk data sharing).

We do support forums to encourage information sharing including strategies and capabilities in cybersecurity threat identification and responses.

Measure 3: Require critical infrastructure entities to share certain information with each other

A requirement for critical infrastructure entities to share commercially sensitive information carries considerable risk, even if there may be benefits in that exchange. There is not enough information in the consultation document to understand when or why such a requirement might be needed. As a minimum, this requirement should only apply to critical infrastructure of national significance.

We appreciate that the government intends that information shared be held in strict confidence as set out on page 13 of the consultation document. In our view, the self-imposed 'constraints' are reasonably open and do not provide the reassurance required. For example using and sharing sensitive information 'consistent with the purpose of enhancing critical infrastructure security' provides a very broad scope.

Our preference is that this measure not be included at this stage. Measure 2 should be adequate at least until the new system is tested.

Measure 4: Require critical infrastructure entities to report cyber incidents

We acknowledge the value of reporting cyber incidents to the National Cyber Security Centre. Reporting requirements should be as streamlined and simple as possible. The purpose and use of the reports must be clearly articulated and reporting protected.

Any measure for cyber incident reporting requires a clear and appropriate impact scale that defines the level and type of incident to be reported. The likelihood for an incident to have 'likely impact on confidentiality, integrity or availability of information' is high with this very broad definition. Without an appropriate severity scale and the qualification of its relevance to performing our critical service, it could encompass a large range of incidents with little value (but potentially significant cost) in reporting.

If the New Zealand Information Security Manual (NZISM) categorisation is to be used, a 'critical incident' would be the category threshold better aligned with the government's objective, rather than 'serious incident'. In particular, the first half of the definition "Critical: Incident affecting critical systems or information with potential to impact operations ". While reference to NZISM and entities applying a reasonable person test to its application is useful, some aspects of the definitions are not relevant to cyber security specifically, and inconsistency is still likely in the application of definitions. There is likely to be confusion in entities understanding reporting requirements. As a minimum, this is a matter where guidance will be important.

3.2 Minimum cyber risk management

We agree that good risk management is key to enhancing the cyber security of our critical infrastructure system. Powerco follows comprehensive enterprise risk management procedures, with cyber security risk part of that framework. We also agree that it is the critical infrastructure providers that best know the risks and responses to those risks.

Measure 5: Require critical infrastructure entities to develop, implement and maintain a risk management programme aligned with an internationally recognised cyber security framework

Individual infrastructure providers are best placed to understand their customers, their networks, and what good cyber risk management looks like in their situation. Care will be needed that regulations do not undermine this, or force action or investment when not actually needed or wanted by customers, or where more efficient options are available to an entity.

Powerco has defined 'cyber critical assets' for the purpose of our risk management approach. While we have a robust enterprise risk management framework, we have additional work underway to improve our cyber risk identification.

Risk management process standards could assist to align regulated sectors and unregulated sectors in consistent approach, for example adopting the ISO risk management process. Providing a common framework or approach could provide improvements and transparency while enabling individual sectors or infrastructure providers to apply the approach at an individual level.

We support an approach where infrastructure providers are managing cyber risks alongside, rather than separately to, all risks. Should there be a requirement to adopt a cyber-specific risk standard, this would add a higher level of assessment and reporting for that one aspect of our enterprise risk management programme, which could add significant costs to our business. We do encourage an uplift in performance in cyber security across critical infrastructure and would support a measure for critical infrastructure providers to 'align with' rather than 'comply with' an internationally recognised cyber security framework. The consultation document uses both terms. Compliance with formal standards would add significant administration and compliance costs, and there is no evidence that it is necessary for this to be mandated. Aligning with a recognised standard would provide scope to adapt our existing frameworks suitable for our business.

We would caution against referencing just one recognised standard, as there are a number of standards that are relevant, some more sector specific which is useful, such as the Australian Energy Sector Cyber Security Framework which a number of EDBs use for self-assessment.

Any standard used across critical infrastructure, must only be a tool for investigation purposes and not impose where or how infrastructure providers focus their investment in response. Directing specific action linked to the risk assessment could force overspend in assets that all customers have to pay for, when there are likely to be alternative options. We do not support regulation enabling the Minister to prescribe actions to manage specific risks, even where the actions relate to critical infrastructure of national significance.

Rather, Powerco would support increased information sharing of currently restricted risk and threat information relating to specific threats that would inform our risk assessment and support voluntary actions that support the objective of this requirement.

We do not think it appropriate or justified to require entities that are not critical infrastructure entities, such as suppliers or contractors, to meet regulated risk management obligations. It should be for the critical infrastructure entity to understand and manage these risks. Imposing regulatory requirements on suppliers and contractors would be difficult, as many are located overseas. It is also unclear who would be responsible for managing and enforcing requirements on these other entities.

Making directors of critical infrastructure entities responsible for ensuring compliance with minimum requirements for cyber security would be consistent with similar regulatory requirements. We would accept this form of compliance while noting that a detailed director focus on compliance does not necessarily promote improved performance (which is the real objective) and does add significant cost, for example in audit expectations alongside a director responsibility. The cost/benefit of a range of options should be investigated to ensure this is the most appropriate option.

Powerco, like many critical infrastructure providers, is subject to significant regulatory reporting requirements. We agree that new reporting requirements related to cyber security must align with, and not duplicate, existing requirements. The document notes that "for entities subject to price-quality regulation by the Commerce Commission, any investments required to comply with minimum requirements could be able to be offset with additional revenue". This is factually correct, but underplays the significant process, cost and uncertainty that could be involved in a reopener application to seek additional revenue allowance, and the outcome of this being

additional costs for energy customers. The objective should be to minimise reporting requirements and costs to avoid, as far as possible, the need for additional revenue to address the new regulatory requirements. For the same reason, we also do not support, or think necessary, to require third-party audit to demonstrate the entity's compliance.

We would like to see analysis of an option to enhance existing frameworks for risk management programmes so entities and regulators can build on existing systems, rather than creating an entirely new risk management regulatory framework just for cyber risk. For example, building on the Civil Defence and Emergency Management Act / Emergency Management Bill systems and processes, noting many of the measures are already enabled in the Bill.

3.3 National security risks

Measure 6: A power to direct the management of cyber threats for national security reasons

There may be a case for government being able to intervene only when there is clear evidence of repeated under-performance causing a national security threat, for example if there was repeated failures of a critical infrastructure entity's risk management system and a major cyber national security incident occurs.

The power should only be exercised as a last resort when evidence demonstrates there is a significant threat to national security, and following consultation with the relevant critical infrastructure entity.

3.4 Compliance with requirements

We agree that compliance measures are an important part of lifting performance in cyber security. However, there are many factors that may contribute to a cyber security incident, and the compliance regime must require regulators to assess responsibility and reasonable action fairly, for example the regulation could require regulators to take into account the matters listed on page 19. We support an emphasis on voluntary compliance, particularly in the short term, and a range of tools and mechanisms being made available for regulators.

As noted above, our preference would be for regulatory cyber measures, and associated compliance tools/liabilities, to be part of an existing system. For example the Emergency Management Bill provides a range of compliance measures.

4. Responses to consultation questions

Question		Powerco response
General		
1.	Is your entity, based on the draft thresholds set out on pages 10 and 11, likely to be a critical infrastructure entity?	Yes, information about Powerco is attached. For RY25, we have around 363,000 electricity ICPs and our gas pipelines convey around 7,820,000 GJ per annum. Powerco has entered into an agreement to purchase Firstlight Network and if the transaction proceeds as planned, the Firstlight connections will become part of Powerco in 2026. Firstlight currently has just over 25,000 electricity ICPs.
2.	What one-off capital costs do you expect to incur to comply with each measure, if any (e.g. the cost of developing new reporting systems)? Please provide a range between expected costs and highest possible costs.	There is insufficient detail in the proposals to respond to this question however we anticipate some administrative set up costs.
3.	What ongoing capital costs do you expect to incur to comply with each measure, if any (e.g. the cost of additional investments in resilience to meet the requirements of the risk management programme)? Please provide a range between expected costs and highest possible costs.	There is insufficient detail in the proposals to respond to this question.
4.	What ongoing operational costs do you expect to incur to comply with each measure, if any (e.g. the cost of undertaking a risk assessment, as required by the risk management programme)? Please provide a range between expected costs and highest possible costs.	There is insufficient detail in the proposals to respond to this question, however we anticipate there would be significant ongoing costs which would be charged on to energy customers.
5.	What assumptions have underpinned these cost estimates?	
Defining critical infrastructure		
6.	Would you support the proposed approach to defining critical infrastructure and critical infrastructure of national significance, and if not, what changes would you recommend?	We are concerned about confusion between essential infrastructure providers and critical infrastructure providers. For example, the schedule of essential infrastructure providers in the Emergency Management Bill is a smaller list than the critical infrastructure providers in this proposal, yet critical infrastructure is intended to be a subset of essential infrastructure.

Question		Powerco response
		The components likely to become critical infrastructure of national significance are unclear based on the description provided. It will be important that a decision on those components to fall in this definition fully accounts for the views and information provided by the infrastructure provider.
7.	Do you consider any essential services have been included or excluded that should not be? If so, what services are they and why should they be added or removed?	In our submission on the Emergency Management Bill, we recommended that scientific hazard warning systems be included as essential infrastructure. We have commented in section 2.1 above, about the importance of aligning definitions across regulations. We see discrepancies in this current proposal.
8.	Do you think the example thresholds for defining critical infrastructure have been set appropriately and provide sufficient clarity as to what level of service provision constitutes critical infrastructure? If not, what alternative thresholds would you support, and why?	All electricity distribution services should be included in the definition of critical infrastructure. The thresholds are arbitrary, meaningless and do not achieve the objective for these reforms. Thresholds may be appropriate in some other sectors. Gas distribution services should not be included in the definition of critical infrastructure for the purpose of cyber security. Refer section 2.2 above.
9.	In addition to interdependencies and consequences of a disruption, are there other factors you think should be considered in assessing whether an asset should be declared critical infrastructure of national significance?	The difference between critical infrastructure and critical infrastructure of national significance is not clear. All critical infrastructure has interdependencies and consequences of disruption. It is unclear what the scale of consequence would determine national significance.
10.	Do you agree that the Minister responsible should have the ability to designate or exempt critical infrastructure entities? In not, what alternative approach would you support, and why?	We do not agree. We are concerned that this approach creates ambiguity in which entities would be subject to the requirements. If thresholds are to be used, all entities should have confidence in those thresholds without the possibility of arbitrary decisions to include or exclude entities notwithstanding the thresholds.
Improving information sharing and collection		
11.	Do you agree with the proposed approach to protecting the data shared? If not, what alternative provisions would you suggest and why?	The protections relate to government use of the data and appear appropriate. However, these protections do not support or protect cross-entity sharing of information.
12.	If you are likely to be deemed a critical infrastructure owner or operator, what effect would having all essential infrastructure providers participating in the formal information exchange, rather	The more entities involved, the more cautious all entities will be.

Question		Powerco response
	than just other critical infrastructure entities, have on your willingness to participate?	
13.	If the government required regular reporting of all cyber incidents, how frequently do you think this information should be required (e.g. every quarter, every six months)?	Reporting should be annual to align with other regulatory reporting requirements. More frequent reporting may be justified for certain types of significant incidents.
14.	Do you consider the proposed definition of a cyber incident can be given effect within your existing approach to enterprise risk management? If not, what alternative definition would you recommend?	The "confidentiality, integrity or availability of information," requires a severity threshold, and to be more targeted to an impact on the critical service. Refer section 3.1 (Measure 4) above.
15.	Would a requirement to report significant cyber incidents make you less willing to report other cyber incidents voluntarily?	No, assuming the thresholds are appropriate, and consistency supported through guidance.
16.	Do you consider using the criteria of serious and above for cyber incidents that should be reported within 72 hours are appropriate. If not, what criteria for reporting would you recommend?	A large scale cyber incident may run for an extended period. The requirement of a full report is more appropriate to be associated with the incident closure, not a timeframe from first detection. We agree that an early warning could be provided to NCSC/regulators within 24 hours, but after that time, any additional reporting should be determined between NCSC and the entity on a case by case basis depending on the type and severity of incident. As noted in section 3.1, 'critical' incident is a more appropriate threshold, but would still require clarification for application to cyber security specifically.
17.	What impact do you think the requirement to report significant cyber incidents could have on your incident response process? For example, would you need to involve lawyers to determine what incidents to report and when?	A requirement for mandatory reporting (beyond limited notification) would likely reduce focus on incident response and recovery processes. To reduce impact, reporting requirements must be streamlined and post-event unless agreed on a case-by-case basis.
Cyber risk management requirements		
18.	Are any of the specific words proposed to set the requirements of the risk management programme on page 15 likely to conflict with your existing approach to risk management in a way that requires you to make significant changes to these processes, rather than build on what already exists?	If there is a requirement to "comply with" a cyber security framework endorsed by NCSC or internationally this will require significant change to our processes. Refer section 3.2 above

Question		Powerco response
19.	Do you agree that critical components should be defined in a way that aligns with the scope of the requirements in the emergency management system? If not, what alternative scope would you recommend, and why?	Yes, we support alignment of definitions between these two regimes.
20.	Do you consider that the concept of a risk that is material can be given effect to within your existing approach to enterprise risk management? If not, what alternative approach to defining the level of risk that must be treated would you recommend, and why?	"Material" as a description of risk is not utilised within Powerco's risk management framework. Powerco would be required to adjust our framework to align. This would introduce complexity for Powerco's business context.
21.	Do you consider that the threshold for treating risks should be set at so far as reasonably practicable? If not, what alternative language to set the scope of risks to be treated would you recommend, and why?	We acknowledge that the concept of "so far as reasonably practicable" applies in some disciplines and in some jurisdictions, but is not currently universally applied to treat all risks, nor is it applied in the Powerco risk framework. Importantly, this concept does not recognise that every organisation has their own agreed risk appetite. In our view risks should be treated *to the extent necessary to reduce residual risk to an acceptable level as defined in the organisations approved risk appetite or formally accepted by the risk owner*.
22.	Do you support the risk management programme complying with a cyber security framework that is endorsed by the NCSC or recognised internationally?	No. This would add significant process, rework and cost to require compliance with a topic-specific framework for one part of our risk framework. While it would not achieve the same degree of consistency, *aligning* with recognised cyber security frameworks would be appropriate to life performance. Refer section 3.2 above
23.	Do you agree that government should not prescribe the international internationally recognised cyber security frameworks that are acceptable if compliance with an international cyber security framework were required? If not, what framework(s) would you suggest should be included on such a list, and why?	A list of options is a pragmatic way to respect prior investment of organisations into selected framework alignment. It does however reduce the effectiveness of a standardised measure across the industry.
24.	Do you consider that a requirement for third-party vendors that have operational control over critical components, to support responsible entities to comply to the extent reasonably practicable, is important to the effective implementation of the risk management programme? Do see any unintended consequences? If so, what do you consider those to be?	This is not reasonably practicable. We do not see that this has been justified or an approach provided for how this would be managed. Refer section 3.2

Question		Powerco response
25.	Do you consider that there are alternative ways for the government to recognise that compliance with other regulation is equivalent to the minimum requirements for cyber risk management? If so, what do you propose?	Powerco is regulated under the Commerce Act and is subject to established reporting and disclosures. This includes our Asset Management Plans for electricity and gas which report on our secondary assets and critical systems investment. We also provide an annual integrated report[5] which sets out our risks and opportunities and incorporates our climate disclosures. We also have regulatory requirements as a lifeline under the civil defence and emergency management regime. Compliance with our ID and other regulatory requirements is public and not equivalent to the level of detail likely expected for demonstrating compliance with minimum requirements for cyber risk management. A separate reporting and compliance system should be avoided if possible. To minimise compliance costs, these existing tools should be supplemented rather than duplicated.
26.	Do you consider there is a more effective way to ensure compliance than to attach responsibility for minimum requirements for cyber risk management to individual directors? If so, what would you propose?	We would accept a form of director compliance while noting that a detailed director focus on compliance does not necessarily promote improved performance (which is the real objective) and comes with significant cost due to the assurance regime directors will expect to accompany this responsibility.
27.	Do you have a preference on how responsible entities should demonstrate compliance with minimum requirements for cyber risk management?	See our response to question 25 above
Cyber threats affecting national security		
28.	When responding to a cyber incident for national security reasons, what support from government is most helpful to aid the restoration of essential services?	We do not have a view on this matter.
29.	Do you think the thresholds for the use of the last-resort power are appropriate? If not, what changes would you propose?	We do not have a view on this matter.
30.	Do you think that the protections and rights for entities subject to the last-resort power are appropriate? If not, what changes would you propose?	We do not have a view on this matter.
Compliance		
31.	Do you consider that the breaches are appropriately mapped to compliance and enforcement tools? If not, what changes would you propose?	We do not have a view on this matter. As set out in section 3.4, our view is that breaches, liabilities and tools should be part of an existing system (such as emergency management) rather than an entirely new system.
32.	Do you support the proposed approach to compliance and enforcement where	Yes

[5] Powerco's integrated-report 2025

Question		Powerco response
	an entity breaches requirements across two or more regulatory regimes? If not, what alternative would you propose?	
33.	Do you agree that penalties in respect of compliance with minimum cyber security requirements should apply to the entity's directors as well as to the organisation as a whole? Why or why not?	We do not have a view on this matter. As noted in question 26, there are ongoing administrative costs with director liability.
34.	Do you perceive any perverse outcomes as a result of directors being individually liable for the most serious breaches of the regime?	As noted in question 26, a director responsibility/liability does not necessarily promote improved performance (which is the real objective), and does involve ongoing administrative costs.

5. Information about Powerco and our network

Providing an essential service

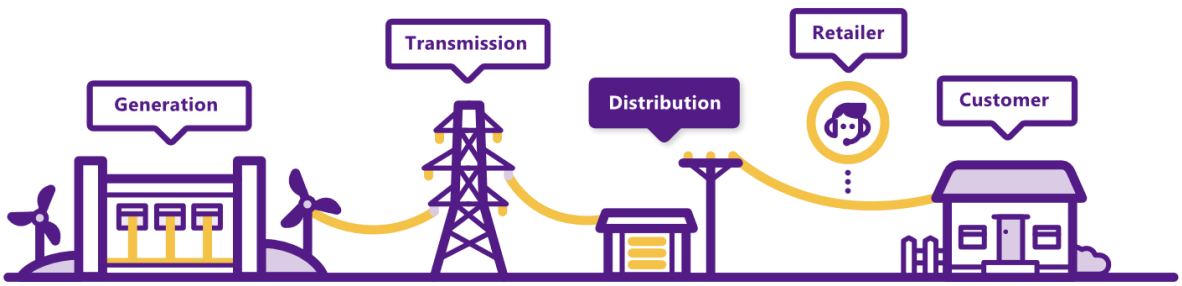
We bring electricity and gas to over 1 million kiwis across the North Island. We're one part of the energy supply chain. We own and maintain the local lines, cables and pipes that deliver energy to the people and businesses who use it. Our networks extend across the North Island, serving urban and rural homes, businesses, and major industrial and commercial sites. We are also a lifeline utility. This means that we have a duty to maintain operations 24/7, including in the case of a major event like an earthquake or a flood.

The cost of operating our business is not dependent on the amount of gas or electricity we distribute in our networks. These costs reflect the need to maintain the safe operation of the network and are mostly driven by compliance with safety regulations. This includes replacing assets when they reach their end of life. Additional costs to grow the size or the capacity of the network are often met by customers requiring the upgrade or new connection.

Under Part 4 of the Commerce Act, Powerco's revenue and expenditure are set by the Commerce Commission as part of monopoly regulation. We are also subject to significant information disclosure requirements, publicly publishing our investment plans, technical and financial performance, and prices. The regulatory regime allows us to recover the value of our asset base using a regulated cost of capital (WACC) set by the Commission, and a forecast of our expenditure. Every five years, the Commission reviews its forecasts and resets our allowable revenue. This process is designed to ensure the costs paid by customers for us to manage and operate our network is efficient given we are a monopoly and an essential service.

Our electricity customers

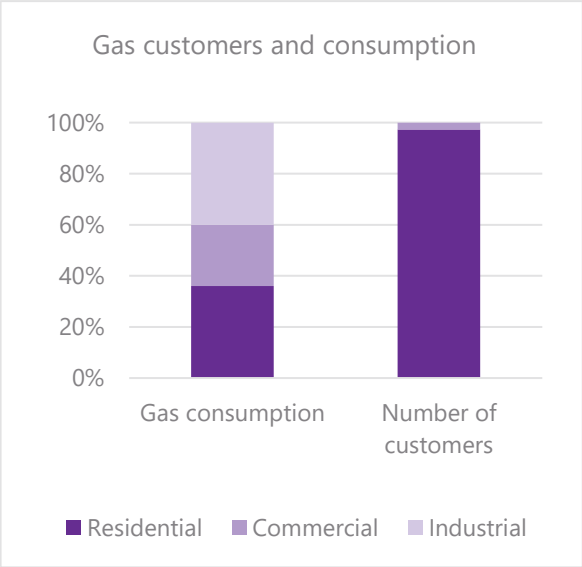
Powerco is New Zealand's largest electricity utility by the area we serve. Our electricity networks are in Western Bay of Plenty, Thames, Coromandel, Eastern and Southern Waikato, Taranaki, Whanganui, Rangitikei, Manawatu and Wairarapa. We have over 29,300 km of electricity lines and cables connecting around 363,000 homes and businesses. Our place in the electricity sector is illustrated below.



Our network contains a range of urban and rural areas, although is predominantly rural. Geographic, demographic, and load characteristics vary significantly across our supply area. Our development as a utility included several mergers and acquisitions that have led to a wide range of legacy asset types and architecture across the network. Powerco is one of 29 electricity distribution companies. Our customers represent around 13% of electricity consumption (similar in magnitude to the Tiwai aluminium smelter) and around 14% of system demand. Powerco's

network is almost three times the size of Transpower's in terms of circuit length. The peak demand on our combined networks (2025) was 940 MW, with an energy throughput of 5,297 GWh.

Our gas customers



Powerco is New Zealand's largest gas distribution utility. Our gas pipeline networks are in Taranaki, Hutt Valley, Porirua, Wellington, Horowhenua, Manawatu and Hawke's Bay. We have over 6,200 km of gas pipes connecting to around 113,300 homes and businesses. Our customers consume around 7.8 PJ of gas per year.

Our industrial customers are less than 1% of our customer base and consumer approx. 40% of gas on our network. Our residential customers are 97% of our customer base and consume approx. 35% of gas on our network. The remaining 25% of gas is consumed by our commercial customers.

Around 30% of our larger customers are in the food processing sector, around 20% in the manufacturing sector and around 10% in the healthcare sector.

Our network footprint

Our network represents 46% of the gas connections and 16% of the electricity connections in New Zealand. We operate assets within six regions and across 29 district or city council areas.