LINQ SEE. SOLVE. SHARE.

LEVERAGING LINQ FOR SOCI ACT COMPLIANCE

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Neil Calvert

7 July 2025

01 INTRODUCTION

Protecting critical infrastructure requires both robust risk management and clear visibility into operations. The Australian *Security of Critical Infrastructure Act 2018* (SOCI Act) mandates that organisations identify and mitigate risks to essential services, from power grids to telecommunications, to strengthen national resilience. LINQ, a business data modelling and visualization platform, can play a pivotal role in meeting these obligations. By creating a "digital twin" of an organisation's people, processes, technology, and information, LINQ helps map out how value and information flow through the business. This comprehensive view enables critical infrastructure operators to pinpoint vulnerabilities, quantify risks, and simulate improvements before implementing changes. The result is evidence-based decision making and streamlined compliance with regulations like the SOCI Act.

Comprehensive Risk Visibility

LINQ's digital twin maps all critical processes and data flows, revealing hidden inefficiencies and vulnerabilities in operations.

Evidence-Based Compliance

Data-driven insights from LINQ support the SOCI Act's requirements by identifying risks and guiding mitigation strategies, providing documentation for compliance reporting.

Accelerated Decision Making

LINQ enables up to **10× faster** analysis of processes and risks compared to traditional methods, allowing quicker implementation of security improvements and controls.

02 SOCI ACT 2018: KEY REQUIREMENTS

The SOCI Act imposes Positive Security Obligations (PSO) on owners and operators of critical infrastructure assets across Australia. In practice, organisations must institute formal risk management and reporting practices to protect assets that are vital to national security, economy, and public safety. *Key requirements under the SOCI Act include:*

- **Critical Infrastructure Risk Management Program (CIRMP):** Entities must develop and maintain a Risk Management Program that identifies "material risks" from potential hazards and minimizes or mitigates those risks as far as practicable. This program should address both cyber threats and physical hazards, ensuring the security and resilience of critical operations. The CIRMP rules (2023) detail hazards to consider, including risks to sensitive data and interdependent systems.
- **Incident Reporting:** Organisations are required to report serious cyber incidents within 12 hours of detection to the Australian Cyber Security Centre (ACSC). Fast, accurate incident reporting helps authorities respond to and contain threats, and it demands that companies have visibility into their systems to know when critical functions are impacted.
- **Annual Board Attestation:** The entity's board (or governing body) must approve and submit an Annual Report on the CIRMP to the regulator. This report needs to demonstrate that all relevant risks have been assessed and addressed according to the SOCI Act's rules. It serves as formal evidence of compliance, requiring organisations to keep detailed records of their risk assessments, mitigation actions, and any incidents.
- **Government Assistance and Directions:** In extreme cases (e.g. during major cyber-attacks), the government may exercise powers under the SOCI Act to direct or assist organisations in responding to threats[1]. While this is a last resort measure, companies must be prepared with up-to-date knowledge of their critical systems and contingency plans.

These obligations span 11 critical infrastructure sectors covering 22 asset types (from electricity and water utilities to banking systems and data centres). Compliance thus entails a comprehensive, ongoing approach to risk identification, mitigation, and documentation.

Critical Sectors Covered

11

industries under SOCI Act oversight

Regulated Asset Types

22

categories of infrastructure deemed critical

Incident Report Time

12 hrs

to report significant cyber incidents

CIRMP Obligations

4

key duties: identify hazards, minimize risk, mitigate impact, comply with rules

03 LINQ CAPABILITIES ALIGNED WITH SOCI OBLIGATIONS

LINQ's platform offers features that align closely with the risk management and oversight needs mandated by the SOCI Act. By using LINQ, organisations can systematically capture their complex operations and turn them into actionable insights for security and compliance. Below, we examine how specific LINQ capabilities support each aspect of SOCI compliance:

3.1 Mapping Critical Processes and Assets (Digital Twin Modelling)

A foundational step in safeguarding critical infrastructure is knowing exactly "what is where" and "who does what." LINQ addresses this through its ability to create a digital twin of the organisation, mapping out people, systems, processes, and information flows. This visual modelling has several compliance benefits:

- **Identify Dependencies and Single Points of Failure:** LINQ diagrams show how data and value move through each step of a process. This reveals critical dependencies. For example, if a particular database or IT system supports multiple essential services, the model will highlight that central role. Such visibility is crucial for the SOCI Act's requirement to identify hazards with material risk to assets. *If a single system outage could have a widespread impact*, LINQ helps flag it as a priority risk to address.
- **Catalogue of Critical Assets:** In LINQ, people and technology assets are first-class elements of the model. The platform's *People and Systems* view allows defining roles (with their capacities and costs) and systems (with their operational costs and attributes). By using this, an organisation can maintain a living inventory of all its critical infrastructure components within the LINQ model. This satisfies the need to know what "critical infrastructure assets" you have, a core part of SOCI compliance, and ensures no important asset is overlooked in risk assessments.
- **Visualisation for Communication:** The digital twin is not just a technical diagram; it's designed to be easily understood by both technical and non-technical stakeholders. This shared visual language helps align teams with a common understanding of how the business operates and where the critical points lie. In practice, this means security, operations, and executive teams can collaboratively identify risks and agree on safeguards, supporting a holistic CIRMP overseen by the board.

Example: *A large water utility could use LINQ to map its treatment and distribution process. The model might reveal that a single SCADA control system is feeding multiple water treatment plants. Recognising this dependency, the utility can designate that SCADA system as a critical asset and ensure redundant controls or enhanced monitoring are in place, directly addressing a material risk to water supply continuity.*

3.2. Risk Identification and Impact Analysis

With a clear map of operations, LINQ enables organisations to identify risks and analyse their potential impacts – a core element of the SOCI Act's Positive Security Obligations. The platform contributes to risk analysis in the following ways:

- **Highlighting Inefficiencies and Bottlenecks:** LINQ automatically surfaces parts of a process where resources are being wasted, or flow is bottlenecked. While an inefficiency might seem like a cost concern, it often correlates with risk. For instance, a bottleneck might be a point of heavy reliance on one person or system, meaning if that element fails, the whole process stalls. LINQ's identification of such choke points is effectively an identification of operational hazards that need mitigation (e.g., cross-training staff or load-balancing systems). This directly supports the CIRMP objective to *"identify each hazard where there is a material risk"* to a critical function.

- **Quantifying the Impact of Changes or Failures:** A standout feature of LINQ is the ability to simulate changes and test scenarios before committing resources. Organisations can use this for *what-if analysis* around risk. For example, "What if this database went offline for 24 hours?" or "How would investing in a backup system improve our risk profile?" LINQ's models can be adjusted to simulate these scenarios, immediately showing how the outputs and value delivery of the business would be affected. This is invaluable for understanding the *"relevant impact of a hazard"*, which the SOCI Act requires to be mitigated. By quantifying impacts, LINQ helps prioritise which risks truly matter by showing the ripple effects across the organisation.
- **Risk Scoring and Visual Dashboards:** LINQ's interface includes dashboards that present data about the model in aggregate. This can include, for instance, the number of processes a system supports, or the total value (monetary or productivity) reliant on a particular team. Such metrics effectively act as risk indicators; a higher value means a bigger impact if disrupted. LINQ makes it possible to assign notional values to information and processes, as seen in real use-cases, which highlights where high-value information is concentrated. This approach was used at Rau Paenga Limited (case study in section 4.1) to pinpoint "high-cost, low-value activities" and areas with multiple handoffs, indicating complexity and higher risk. The insights are presented clearly, allowing decision-makers to grasp risk areas at a glance and back up their intuition with data.

By systematically illuminating risks and their potential business impacts, LINQ supports organisations in fulfilling the SOCI requirement to proactively minimize risk. Instead of managing risk with *"inadequate information – until now"*, as LINQ's insights gives change leaders the evidence needed to address vulnerabilities before they lead to incidents.

3.3. Mitigation Planning and Change Management

The SOCI Act not only expects identification of risks but also that organisations "as far as reasonably practicable, minimise or eliminate" those risks. LINQ supports the planning and execution of risk mitigations through its change management capabilities:

- **Testing Mitigations Virtually:** Once a risk is identified, such as an over-reliance on a single data centre, LINQ can help model the proposed solution, for example adding a secondary data centre or implementing a new failover process and assessing the consequence of this change. Users can extend or modify the LINQ model to include the mitigation and immediately see how it changes the information flow or process performance. Does it remove the bottleneck? Does it reduce the critical impact of that component's failure? This simulation ability means organisations can iteratively refine their risk treatments *before* investing time and money. In essence, LINQ acts like a sandbox for risk mitigation strategies, ensuring that chosen controls will indeed improve resilience. This aligns with best practices in risk management programs, where you should test the effectiveness of measures in advance.
- **Optimising Processes for Resilience:** Often, improving security and compliance goes hand in hand with improving efficiency. LINQ's modelling can uncover opportunities to streamline operations, which in turn removes unnecessary complexity that could be a source of risk. For example, if a process has six approval steps but LINQ's analysis shows two of those steps add no value, eliminating them not only speeds up the process but also reduces the chances for error or misuse. The case of Rau Paenga highlighted how removing redundancies and automating manual tasks were outcomes of using LINQ. A leaner process is typically more robust, which helps in minimizing material risks as required by SOCI.
- **Change Risk Management:** LINQ enables the management of the risks of change itself. Implementing new security controls or processes (to comply with SOCI) can be disruptive if not managed well. LINQ

provides evidence to support the value of change, helping get leadership buy-in and reducing the chance of "scope creep" or project failure when rolling out improvements. This is important because compliance initiatives often involve significant organisational change (new policies, technologies, training, etc.). LINQ's approach ensures all stakeholders see *why* a change is needed (the risk data supports it) and *what* exactly will change in their day-to-day work. The platform fosters collaboration by allowing teams to share visualisations of future-state processes, which creates a shared understanding of how new measures (e.g., a backup system or revised procedure) will function. Such clarity greatly aids in implementing risk mitigations smoothly and effectively.

Overall, LINQ not only helps design mitigations to address identified risks, but it also ensures those mitigations are integrated into the business with minimal disruption. This fulfils the spirit of the SOCI Act by embedding risk reduction into business-as-usual planning and operations, rather than treating it as a one-off compliance task.

3.4. Compliance Reporting and Audit Support

Given the SOCI Act's emphasis on accountability – particularly the annual reporting of the Risk Management Program's effectiveness – LINQ provides significant support in documentation and communication of compliance efforts:

- **Single Source of Truth:** The LINQ model, once built, becomes a living document of the organisation's processes and controls. It can be kept up to date as processes evolve, serving as a current blueprint of how the organisation manages information and processes. When it comes time to produce the annual CIRMP report for regulators, this blueprint is useful. Instead of starting from scratch to document how risks are being managed, the organisation can extract relevant views and data from the LINQ model: e.g., a list of all identified critical assets and their associated safeguards, or a diagram of contingency workflows for key operations. This ensures consistency in reporting; the data in the report is the same data the teams are actively using to manage the business.

- **Metrics and Evidence for Regulators:** A regulator (or an internal audit) will want to see evidence that the organisation has considered various risks and has plans in place. LINQ's quantification of processes provides exactly that. For example, an annual report might need to include how a company is mitigating the risk of power failure on an essential system. Using LINQ, the company can provide: *a figure of how many processes would be affected by a power failure (before vs. after mitigation), a diagram of the new backup generator process, and the reduction in downtime risk as calculated in the model.* These data-driven illustrations give regulators confidence that the company has a handle on its risk, far more convincing than unquantified statements. LINQ's dashboard and reporting features help extract such metrics, which can be directly incorporated into compliance documents.

- **Demonstrating "Practically Eliminated" Risks:** One of the challenges in compliance is demonstrating that you have *"as far as reasonably practicable"* minimised risks. LINQ can help show this by tracking the status of each identified hazard. For example, if 10 major hazards were identified, the LINQ model and notes can show which have been addressed, how, and which (if any) remain and why. The visual nature of the tool can even allow an auditor to walk through the scenario: *"Here is our primary data centre (hazard: single point of failure), you can see in the model we added a secondary data centre and re-routed certain processes to it. Our LINQ simulation shows that if Data Centre A goes down, 95% of services keep running via Data Centre B, thus we have mitigated the impact."* This level of demonstration goes a long way in satisfying auditors that the company is meeting SOCI obligations diligently.

- **Continuous Improvement and Record-Keeping:** Compliance is not a one-time event; regulators expect continual review and improvement. LINQ's ease of updating models encourages organisations to continuously refine their "risk picture." Each time a process change is made, or a new system comes online, it can be added to LINQ. Over a year, this provides a clear record of how the risk profile has changed and what has been done to improve it. When the next annual report is due, the organisation can highlight improvements since last year *with concrete data* (e.g., "reduced average recovery time for critical systems from 4 hours to 1 hour after investing in new failover technology, as seen in our model updates”). This directly supports the reporting requirement and showcases a proactive compliance posture.

In summary, LINQ acts as a powerful ally in compliance reporting, turning the complex web of enterprise operations into clear visuals and hard data. It helps bridge the gap between technical risk management activities and the high-level documentation that boards and regulators require, ensuring nothing gets lost in translation.

04 REAL-WORLD APPLICATION EXAMPLES

While LINQ's application to SOCI Act compliance is emerging, its core strengths have been proven in similar contexts where organisations needed to understand and transform their operations under tight constraints. Below are examples and scenarios illustrating how LINQ has been used – or could be used – in critical infrastructure and regulated industries:

4.1 Case Study: Rau Paenga – Streamlining a Critical Infrastructure Agency

Rau Paenga Limited (formerly Ōtākaro Ltd) and now Crown Infrastructure Delivery is a New Zealand Crown agency responsible for major infrastructure and reconstruction projects (formed after the Canterbury earthquakes). As the agency's role expanded from earthquake recovery to broader national infrastructure delivery, it faced the challenge of re-evaluating internal processes and data governance to meet new government directives. Essentially, Rau Paenga needed to ensure its operations were robust, efficient, and could scale – goals very much in line with what an Australian critical infrastructure operator under SOCI might face when reevaluating processes for risk management.

Rau Paenga engaged LINQ to create a comprehensive model of its information flows and processes. Over 95% of the organisation's team were interviewed to capture an accurate current-state model, showing how every project and function was executed. The results were impressive and offer insight into what LINQ can achieve:

- **Enhanced Visibility:** By visualising the entire "information ecosystem," LINQ uncovered critical handoffs and iterative loops in processes that had previously been obscured. For example, the model might reveal that a report was being compiled in one department, then re-processed in another, indicating a redundant effort. Identifying such points is akin to discovering latent risks (e.g., delays, errors) hidden in complexity. Rau Paenga's team described this enterprise-wide visibility as *"transformative,"* giving them clarity on bottlenecks that they *"hadn't imagined possible before"*. For a SOCI-regulated entity, this level of clarity means no part of a critical service is left in the dark, every dependency and process is accounted for.

- **Risk and Cost Efficiency:** LINQ allowed Rau Paenga to assign nominal dollar values to each process and piece of information, essentially performing a value stream analysis. This quickly highlighted high-cost, low-value activities that were draining resources without commensurate benefit. In compliance terms, those are often the areas where risk hides because money and effort wasted on redundant tasks could be reallocated to important security improvements. By pinpointing these, Rau Paenga could cut out waste and redirect efforts. The organisation discovered multiple manual processes and hand-offs that weren't necessary, what one executive called *"real gold"* in terms of insight. Eliminating such inefficiencies not only saved cost but also reduced the complexity that security teams must manage (fewer unnecessary moving parts means fewer potential failure points).

- **Strategic Re-engineering:** With LINQ's model in hand, Rau Paenga was able to plan a targeted transformation of their processes. They focused on automation opportunities and better data governance, for example, establishing a proper data stewardship framework where none existed. The changes were prioritised based on LINQ's insights (tackling biggest pain points first) and implemented faster than would have been possible without a clear plan. As Ken Forrest, a director at Rau Paenga, noted, seeing the high-value information streams and all the manual intervention needed was eye-opening and allowed them to quickly seize opportunities to automate. For a SOCI context, this experience shows how LINQ can pave the way for fast-tracked risk mitigation projects; when you know exactly what to fix, you can fix it much more rapidly. In a regime where timelines for compliance are often strict, that speed is invaluable.

- **Data-Driven Decision Making:** The LINQ engagement gave Rau Paenga leadership confidence in their decisions because those decisions were grounded in data. When debating investments in new tools or systems, they could refer to the LINQ model to justify why it was necessary and what benefit it would bring. This replaced gut feel with evidence. A direct quote from Rau Paenga's Head of IT underscored that *"LINQ wasn't just a tool for us; it was a revelation"*, allowing them to map out their entire process landscape at a *"super-speedy pace"*. This kind of buy-in and clarity is exactly what board members (who sign off on SOCI annual reports) need. They can be presented with a LINQ-driven analysis showing, for example, how an investment in cybersecurity technology will concretely reduce risk in the business model, making it far easier to approve and support.

Takeaway: Rau Paenga's success with LINQ demonstrates its ability to handle the complexity of a critical infrastructure organisation and drive significant improvements in efficiency and governance. While this case was not explicitly about SOCI compliance, the parallels are clear: By cleaning up and understanding their operations deeply, an organisation inherently becomes more compliant and secure. The same approach can be applied to Australian critical infrastructure providers looking to strengthen their risk management programs, LINQ helps ensure no stone is left unturned and that enhancements deliver tangible value (and risk reduction).

4.2 Potential Use in a SOCI Context

Consider some hypothetical applications of LINQ for different SOCI-regulated entities:

- An electricity distribution company must comply with SOCI, meaning it needs a CIRMP covering everything from physical security of substations to cybersecurity of its control systems. It uses LINQ to model its end-to-end operations, generation, transmission, distribution, billing, customer service, etc. This model immediately highlights, for example, that the billing system is fed by a single data centre which also supports operational control systems. Recognising this, the company marks that data centre as housing "business critical data" (as the 2024 amendment to SOCI now demands consideration of data storage systems) and a hazard because if it fails, both billing and grid monitoring are at risk. Using LINQ, they simulate adding a secondary data replication site and show that it would isolate billing from grid operations. They implement this change; LINQ's updated model now shows that a failure in one site would not collapse both processes, thus mitigating a systemic risk. When reporting to regulators, the company can visually demonstrate this improvement via the LINQ model excerpt, satisfying them that the risk has been addressed.

- A major port authority uses LINQ to map its cargo handling and vessel movement processes. The model reveals that the port's operations rely heavily on a single external logistics system for shipping schedules and container data – a critical dependency. Recognising this interdependency hazard (which the SOCI Act explicitly requires to be addressed), the port tests mitigations by introducing additional safeguards. For example, they add an independent, on-site container weight verification step to catch mis-declared weights. (In one real incident, a mis-declared container caused a crane failure, halting operations for 72 hours, underscoring the need for such a control.) By simulating this new step in LINQ, the port saw that it would prevent similar incidents without significantly slowing operations. They implemented these changes, and LINQ's simulation provided evidence of improved resilience, showing that even if the main logistics system fails, cargo flow can continue via backups. Because port authorities must justify major investments to government boards, the digital twin's data helped demonstrate the ROI of these risk mitigations in terms of safety and throughput. This made it easier to secure approval and clearly documented their compliance measures for SOCI regulators.

- An oil and gas pipeline operator can similarly use LINQ to map its emergency shutdown and incident response processes. By visualising the flow of information during a pipeline emergency (from sensors detecting a pressure drop, to control room alerts, to valve shut-off commands), the company might discover that a particular communication node is handling an overload of signals. In the model, this appears as a single control system receiving too many inputs, a potential bottleneck if the system were under cyber-attack or had to process multiple simultaneous alarms. Using LINQ, they simulate adding a redundant communication path and additional fail-safe procedures. The updated model shows that alerts would still reach operators even if the primary system is compromised, thereby reducing the risk of an uncontrolled incident. The company implements these improvements and uses the LINQ model to train staff on the new process flow (since the visualisation makes it clear who needs to do what in an emergency). When a serious incident later occurs, they respond swiftly and effectively, and the post-incident report to the ACSC notes that thanks to the new redundancies, the impact was contained to a small segment of the pipeline. This not only meets the SOCI Act's incident management expectations but also provides a strong story of resilience in their annual board attestation report.

These scenarios illustrate how LINQ helps transform SOCI compliance from a theoretical checklist into practical action. By identifying concrete weaknesses and testing solutions virtually, organisations can avoid "learning the hard way" through outages or crises. Instead, they shore up defences proactively and can show stakeholders, from frontline staff to Boards and regulators, tangible proof of their improved security posture.

4.3 Broader Industry Use and Feedback

Outside of direct critical infrastructure use-cases, LINQ has been applied in various industries for process optimisation, and the feedback underscores its suitability for complex, regulated environments:

- **Public Sector & Government IT:** LINQ's cloud-based solution is trusted even by public sector clients with high security demands. In fact, LINQ itself, as a company, *"was able to demonstrate [its] security credentials to the most demanding of customers in the public sector"* when moving to a new cloud infrastructure. This proved that LINQ's platform meets stringent security standards for data handling, an important consideration for any critical infrastructure operator worried about the confidentiality and integrity of their operational data.

- **Business Transformation Projects:** Users have praised LINQ for dramatically reducing the time required to understand and improve a business. One strategy analyst noted that *"without LINQ, the process of understanding the value of the opportunity to transform our business would take up to 10 times longer"*. This speed is crucial when compliance deadlines loom or when rapid response is needed to emerging threats. Quicker analysis means faster remediation of risks.

- **Usability and Collaboration:** LINQ emphasises engaging the people in the process of change. Its approach of capturing knowledge from those who run the processes (often through workshops or interviews) ensures buy-in. According to LINQ, *"your people say they no longer feel that change is being done to them"* when they are involved in modelling future ways of working. This is a soft benefit but a meaningful one: building a strong security culture is a big part of compliance, and a tool that encourages collaboration can foster a culture where everyone takes ownership of managing risks.

Clients across different sectors consistently highlight clarity, speed, and confidence in decision-making as key benefits of using LINQ. These are exactly the qualities needed to navigate the complexities of regulatory compliance like the SOCI Act.

4.4 Data Security and Integration Considerations

Given that SOCI compliance deals with highly sensitive operations, it's essential that the tools used to manage compliance are secure and fit into the broader IT ecosystem. Here's how LINQ addresses these aspects:

- **Secure SaaS Platform:** LINQ is a cloud-native application, which has been built with security in mind from day one. Utilising Microsoft Azure best-practice has ensured that LINQ is suitable for use across a range of industries, including New Zealand Defence and other government agencies. This is important for SOCI entities because any model of critical infrastructure likely contains sensitive information (like network schematics or contingency plans). LINQ's ability to operate securely in the cloud means organisations can use it without increasing their exposure. It also simplifies compliance with any data sovereignty requirements, as cloud deployments can be region-specific if needed (e.g., ensuring Australian data stays in Australia).

- **Data Integrity and Accuracy:** The usefulness of LINQ for compliance rests on the accuracy of the model. LINQ's structured approach to modelling ensures that every piece of data (process step, information object, system, person) is an explicit object that can be reviewed and validated. The platform encourages completeness; it becomes evident if a process has missing steps or undefined inputs in the model, prompting users to fill those gaps. Moreover, LINQ allows capturing notes and assumptions for each element, making it easier to review by subject matter experts for correctness. This means the digital twin can be trusted as an authoritative reference. When auditors come knocking, an organisation can walk them through the LINQ model as a faithful representation of their operations. Any claims in compliance reports can be cross-checked against this model, lending credibility and traceability to the compliance process.

- **Integration with Other Tools:** Organisations may wonder how LINQ fits with their existing risk management and monitoring tools. While LINQ primarily focuses on business process modelling and analysis, it can complement other systems. For instance, outputs from LINQ (like identified critical assets or process maps) can feed into risk registers or GRC (Governance, Risk, Compliance) software used by the company. Conversely, data from asset management inventories or monitoring systems could be imported into LINQ to ensure the model reflects real system states. LINQ can serve as a bridge between technical data and business context. For example, a vulnerability scanning tool might flag a weakness in a SCADA system; that information can be annotated in the LINQ model at the SCADA system node, instantly contextualising the risk in terms of business impact. This integration of technical risk data with business modelling is where many compliance efforts struggle, and LINQ offers a solution by being the canvas that unifies these perspectives.

- **Scalability and Collaboration:** LINQ is designed to handle large models (entire enterprises) and multiple collaborators. This means an organisation can have its security team, operations team, and compliance team all working within one LINQ organisation concurrently or in a coordinated fashion, each enriching the models with their perspective. For instance, operations might map the process, security might annotate threats, and compliance officers might check controls and reporting links. With role-based access, sensitive parts of the model can be restricted. This collaborative, scalable approach ensures that compliance is not siloed, it becomes a shared responsibility documented in one place.

In terms of limitations, users should note that LINQ is not a direct cybersecurity tool, in that it won't perform network intrusion detection or log analysis. It should be used alongside traditional security tools (firewalls, SIEMs, etc.). LINQ's role is to inform where those tools and controls need to be strongest by providing the business context of risk. Additionally, building a detailed LINQ model requires an upfront investment of time and effort (capturing information from many stakeholders, as seen with Rau Paenga's broad interviews). However, this process has its own benefit: it forces an organisation to have the important conversations about "what if" scenarios and "who is responsible for what," which are exactly the conversations the SOCI Act is trying to ensure happen regularly.

4.5 Benefits of Using LINQ for SOCI Compliance

Bringing the discussion together, leveraging LINQ to support SOCI Act compliance offers multiple compelling benefits:

1. **Holistic Risk Visibility:** LINQ provides a *bird's-eye view* of an organisation's critical infrastructure, processes, and information. This comprehensive perspective ensures that all potential hazards, whether cyber, physical, or process-related, are identified and can be addressed in the CIRMP. Nothing important falls through the cracks.

2. **Proactive Risk Reduction:** Through simulation and analysis, LINQ helps organisations move from reactive to proactive. Instead of learning about a critical dependency during a crisis, you learn it in advance via the model and fix it on your own terms. This means fewer incidents to report and manage, aligning with the SOCI Act's emphasis on minimizing risks before they materialise.

3. **Efficiency and Cost Savings:** Compliance efforts can be expensive and time-consuming, but LINQ's ability to fast-track analysis (up to 10× faster modelling) translates into saved time and money. Moreover, by pinpointing low-value activities to trim, LINQ frees up resources that can be reallocated to critical security improvements, making compliance not just a cost centre but an opportunity to optimise operations.

4. **Better Decision Making and Governance:** Decisions about how to protect infrastructure (e.g., which cybersecurity project to fund first) are better when backed by data. LINQ offers quantifiable evidence of where a vulnerability would hurt the most, so organisations can prioritise intelligently. This data-driven approach resonates well with boards and regulators. Boards can see clearly why certain investments are needed, which fosters a culture of support for security initiatives. And when regulators ask tough questions, companies can answer with specifics rather than generalities.

5. **Streamlined Reporting and Audits: Preparing** for audits or writing annual reports becomes less dreaded. With LINQ, much of the heavy lifting (documenting processes, controls, impacts) is already done in the model. Compliance officers can extract diagrams, lists of controls, and metrics directly from LINQ, ensuring reports are accurate and comprehensive. Auditors, in turn, can be walked through a live model for clarification, which often satisfies their inquiries quickly. This level of transparency can even build trust with regulators over time.

6. **Cultural and Organisational Alignment:** Using LINQ tends to break down silos, because it involves multiple parts of the business in contributing to the model. In doing so, it helps create a shared responsibility for critical infrastructure protection. When employees see their role in the LINQ model and how it connects to others, they understand the importance of their actions in the bigger picture (for example, why following a security protocol is crucial not just in IT's eyes but for keeping a whole business process running). This kind of alignment and awareness is an intangible but powerful benefit – it nurtures a risk-aware culture which is the best defence against negligence or oversight.

7. **Futureproofing and Adaptability:** The regulatory landscape is evolving (SOCI was amended in 2020, 2021, 2022, and new rules commenced in 2023 and 2025). LINQ's flexible modelling ensures that as requirements change, the organisation can adapt its model accordingly. For instance, if new legislation requires tracking of a different kind of risk, the LINQ model can incorporate that (just as LINQ added a feature to track carbon emissions associated with systems, it shows the platform's adaptability to new types of data). This means investments in building a LINQ model continue to pay off as compliance obligations grow, you simply enrich the model instead of starting over.

4.6 Challenges and Recommendations

Implementing LINQ to support SOCI compliance is highly beneficial, but organisations should be mindful of a few challenges and best practices:

- **Initial Setup Effort:** Building a complete digital twin can be labour-intensive. It requires gathering information from many domains (IT, operations, security, HR, etc.). As seen, Rau Paenga had to interview 95% of staff to get the full picture. ***Recommendation:*** Treat the LINQ modelling exercise as a project with executive sponsorship. Break it into phases (perhaps start with the most critical service or department first). Use workshops to capture information efficiently and consider enlisting LINQ's own consultants or partners who are experienced in quickly translating business knowledge into the tool.

- **Keeping the Model Updated:** A model can become outdated as soon as things change. If not maintained, it loses value for compliance. ***Recommendation:*** Integrate model updates into change management processes. For any significant change (new system, process change, etc.), require an update to the LINQ model as a step in the change's rollout. Assign clear ownership for the model, e.g. a business analyst or an enterprise architect, who champions its accuracy. LINQ's collaborative features mean multiple people can update it, so leverage that by having each department update their part under oversight.

- **Integration with Risk Frameworks:** Some organisations might already follow standards like NIST CSF or ISO 27001 for cybersecurity. LINQ is not a 1-to-1 mapping to those frameworks (it doesn't output a control compliance checklist, for example). ***Recommendation:*** Use LINQ alongside these frameworks by mapping LINQ findings to framework controls. For instance, if LINQ identifies a critical system without redundancy, that maps to a need for an ISO 27001 Annex A 17.2.1 (availability redundancy) control, which you then document as implemented. LINQ tells you *what* to fix and *where*; the frameworks tell you *how* it should be fixed best practice-wise. Together, they cover both bases.

- **Not a Real-Time Monitoring Tool:** LINQ provides a static or design-time model of your business, not real-time alerts. ***Recommendation:*** Ensure you have complementary monitoring and incident response tools in place as required by SOCI's operational aspects. Use LINQ to decide what should be monitored closely. For example, if LINQ shows System X is critical, ensure your security operations centre has an alert on System X for any anomaly. LINQ will strengthen the focus of your live defences.

- **Training and Skill:** Users will need to learn how to use LINQ effectively. However, LINQ provides onboarding support, and the interface is designed for business users (not just IT). ***Recommendation:*** Take advantage of LINQ's training sessions and support. Start with a small pilot model to get familiar with the tool. Encourage cross-functional teams to participate early so they become comfortable with it and can champion it to others. Given LINQ's visual nature, many users find it intuitive once they see their own work represented in it.

05 CONCLUSION

In an era where critical infrastructure faces unprecedented threats, from cyber-attacks to natural disasters, complying with frameworks like the SOCI Act is both a challenge and an imperative. LINQ offers a modern, intelligent approach to tackle this challenge. By building a dynamic digital twin of an organisation, LINQ empowers critical infrastructure operators to see their entire operational landscape, illuminate the risks, and take decisive action to strengthen resilience. It aligns perfectly with SOCI Act requirements: from identifying and minimizing risks, to enabling thorough reporting and continuous improvement, LINQ embeds compliance into the DNA of daily operations.

With LINQ, companies can move beyond viewing compliance as a checkbox exercise. Instead, they gain a powerful decision-support system that improves their efficiency and agility while keeping them safe and compliant. They can confidently answer the question at the heart of SOCI: *"Do we truly understand our critical assets and are we doing everything reasonably practicable to protect them?"* With LINQ, the answer will be a data backed "Yes". The platform's proven ability to deliver clarity and speed in complex environments means that even as the regulatory landscape evolves, organisations will be well-equipped to adapt and stay ahead.

In two sentences: LINQ supports SOCI Act compliance by providing a clear, data-driven map of an organisation's critical processes and assets, allowing it to identify vulnerabilities and model risk mitigations before issues arise. This digital-twin approach helps meet key SOCI obligations – from robust risk management programs to informed board reporting – faster and with greater confidence, ensuring critical infrastructure remains secure and resilient.