XINJA
HOW MONEY SHOULD BE

Chief Information Security Officer (CISO)

About Us

Xinja is building the first, Australian, independent 100% digital bank designed entirely for mobile. We are building a bank with our customers and designed in their interests. Neobanking will disrupt the existing banking model and create a whole new generation of experiences.

Developing the first neobank in the country is an exciting and challenging task. Our ethos is based on a win-win with our customers; if they do well, so do we. We believe it’s time Australians had access to the kind of technology that just allows them to get a lot more out of their money, with less angst.

We extend that attitude to our people and our partners. We look after our staff, and trust them with significant responsibility, but support them well. This is a great opportunity to be part of building a great company, and a fabulous brand.

Our 10 golden rules

To be successful at Xinja you are going to need to be happy working with our 10 golden rules

1. No dickheads… however good they may be. No dress code. No power trips because of a hierarchy. Intellect and implementation is all that matters.□
2. Everything is in the cloud.
3. We use real time data to evaluate our business and we reward staff on a quarterly basis with an entirely discretionary bonus. No one gets a bonus if our investors aren't making money and our customers aren't happy.□
4. We are here to make money, that's why we exist, and we don’t screw people over to do it. We don’t lie to our clients in person or in marketing. We don’t engage in immoral lending, if our grandmother would think it was wrong, then it is. We aim to make lots of money ethically and we are proud of it.□
5. No one is entitled to work at Xinja. It a huge honour to represent people’s hopes of a new bank and we earn that honour every day.
6. We look after our people bloody well. We stand by them if they are in genuine need.□

7. We are truthful and direct with each other. Everyone says what they think in a robust, challenging, edgy environment. That means we won't be the right place for everyone to work, and that's ok.▯
8. We only hire people better than us. We never, ever settle because we need a body. We do psychometric testing to get the best people, every time.▯
9. About half our team, executive and board will be female, if they aren't we aren't recruiting the best people.▯ We actively seek all types of diversity combined with brilliance.
10. If you discriminate against someone because of who they love/sleep with, you're a dickhead...please see rule 1.

The Role

Secure access to information assets is critical to achieve business objectives. The CISO is responsible for establishing and maintaining the information security program to ensure that Xinja's information assets and associated technologies are adequately protected.

The CISO is responsible for identifying, evaluating and reporting on legal and regulatory, IT, and cybersecurity risks, while supporting and advancing business objectives.

The CISO position requires a strategic leader with sound knowledge of business management and a exceptional knowledge of cybersecurity technologies.

Responsibilities

Establish Governance and Build Knowledge

- Facilitate an information security governance structure including the formation of an information security steering committee or advisory board.
- Provide regular reporting on the current status of the information security program to risk teams, ExCo and the Xinja Board as part of a strategic enterprise risk management.
- Work with IT Operations vendor management to ensure that information security requirements are included in contracts upfront.
- Create and manage a targeted information security awareness training program.
- Ensure the consistent application of policies and standards.
- Provide clear risk mitigating directives.

Lead the Organization

- Lead the information security function across Xinja to ensure consistent and high-quality delivery to achieve strategic objectives.
- Determine the information security approach and operating model.
- Manage the budget for the information security function, monitoring and reporting discrepancies.
- Manage the security team, including Security Architects, SecOps, Consultants and others.

Set the Strategy

- Develop an information security vision and strategy that is aligned to organizational priorities and enables and facilitates the organization's business objectives, and ensure stakeholder buy-in and mandate.
- Develop, implement and monitor a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, safety, privacy and recovery of information assets owned, controlled or/and processed by the organization.
- Work effectively with business units to facilitate information security risk assessment and risk management processes, and empower them to own and accept the level of risk they deem appropriate for their specific risk appetite.
- Develop and enhance an up-to-date information security management framework/s e.g ISO 2700x, ITIL, COBIT etc.
- Create and manage a unified and flexible control framework to integrate and normalize the wide variety and ever-changing requirements resulting from global laws, standards and regulation.
- Develop and maintain a document framework of continuously up-to-date information security policies, standards and guidelines. Oversee the approval and publication of these information security policies and practices.
- Create a framework for roles and responsibilities with regard to information ownership, classification, accountability and protection of information assets.
- Facilitate a metrics and reporting framework to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation, and increase the maturity of the information security, and review it with stakeholders at the executive and board levels.

Build the Network and Communicate the Vision

- Liaise with external agencies, such as law enforcement and other advisory bodies, as necessary, to ensure that the organization maintains a strong security posture and is kept well-abreast of the relevant threats identified by these agencies.
- Liaise with the architecture team to build alignment between the security and enterprise (reference) architectures, thus ensuring that information security requirements are implicit in these architectures and security is built in by design.

Operate the Function

- Work with the compliance staff to ensure that all information owned, collected or controlled by or on behalf of the company is processed and stored in accordance with applicable laws and other global regulatory requirements, such as data privacy.
- Define and facilitate the processes for information security risk and for legal and regulatory assessments, including the reporting and oversight of treatment efforts to address negative findings.
- Ensure that security is embedded in the project delivery process by providing the appropriate information security policies, practices and guidelines.
- Manage and contain information security incidents and events to protect corporate IT assets, intellectual property, regulated data and the company's reputation.
- Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action.
- Develop and oversee effective disaster recovery policies and standards to align with the enterprise business continuity management (BCM) program goals, with the realization that components supporting primary business processes may be outside the corporate perimeter.
- Coordinate the development of implementation of incident response plans and procedures to ensure that business-critical services are recovered in the event of a security event; provide direction, support and in-house consulting in these areas.
- Facilitate and support the development of asset inventories, including information assets in cloud services and in other parties in the organization's ecosystem.

Requirements and Qualifications

- Minimum of seven to 10 years of experience in a combination of risk management, information security and IT (at least five must be in a senior leadership role).
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate information security and risk-related concepts to technical and nontechnical audiences at various hierarchical levels, ranging from board members to technical specialists.

- Strategic leader and builder of both vision and bridges, and able to energize the appropriate teams in the organization.
- Sound knowledge of business management and a working knowledge of information security risk management and cybersecurity technologies.
- Up-to-date knowledge of methodologies and trends in both business and IT.
- Proven track record and experience in developing information security policies and procedures, as well as successfully executing programs that meet the objectives of excellence in a dynamic business environment.
- Poise and ability to act calmly and competently in high-pressure, high-stress situations
- Must be a critical thinker, with strong problem-solving skills.
- Knowledge and understanding of relevant legal and regulatory requirements· Excellent analytical skills, the ability to manage multiple projects under strict timelines, as well as the ability to work well in a demanding, dynamic environment and meet overall objectives.
- Project management skills: financial/budget management, scheduling and resource management.
- Ability to lead and motivate the information security team to achieve tactical and strategic goals, even when only "dotted line" reporting lines exist.
- A master of influencing entities and decisions in situations where no formal reporting structures exist, but achieving the desirable outcome is vital.
- Degree in business or a technology-related field.·
- Professional security management certification is desirable, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials.
- Knowledge of common information security management frameworks, such as ISO/IEC 27001, ITIL, COBIT as well as those from NIST, including 800-53 and Cybersecurity Framework.
- Experience with contract and vendor negotiations.
- Excellent stakeholder management skills.
- High level of personal integrity, as well as the ability to professionally handle confidential matters and show an appropriate level of judgment and maturity.
- High degree of initiative, dependability and ability to work with little supervision while being resilient to change.