Certane Information Security Overview

Purpose

The following is an overview of Certane's approach to security and compliance within our internal corporate environment, and our public products and services. A key focus is on organisational and technical controls regarding how Certane protects customer and partner information assets.

All Certane's subsidiaries and its customers utilising provided products and services is the targeted audience of this paper to provide assurance and transparency of security posture in mitigating associated risk.

Roles and Responsibilities

The Certane Board has ultimate responsibility for the information security management of the Certane group and understands the group's information security risks and regulatory implications. They oversee the following:

- delegation of information security management responsibilities to the Chief Technology Officer (CTO), Chief Operating Officer (COO), Chief Risk Officer (CRO) and the relevant sub-committees are being executed as per Board directive.
- implementation of the information security policy, including appropriate procedures, controls, and monitoring, as well as ensuring appropriate integration and alignment with the group's Risk Management Framework and Incidents policies and procedures.
- information security vulnerabilities and risks both internally and associated with Certane third and related parties are addressed in a timely and appropriate manner.

Dedicated information security and technology team

Certane employs security and privacy subject matter experts to embed a security culture and manage information security risks across the group. A three lines of defence model is implemented as part of the Risk Management Framework to provide appropriate oversight and assurance of security risks.

Information Security Framework

Certane has adopted the NIST Cyber Security Framework and ISO 27001 ISMS to develop and implement our own Information Security Framework, which provides a methodology, structure and process to help manage security risks in supporting business objectives.

The Framework ensures that our security capability has a level to baseline and measure against with the goal to mature by continuing to build, test and review all security functions and services.

Framework Components

The Framework consists of the following components to manage security risk:

- Framework Core - consists of security functions, capabilities, controls, and services that allows Certane to achieve its cyber security and business outcomes.
- Policy Framework - collection of security policies, standards, procedures, and guidelines to govern security requirements enterprise wide and employee security responsibilities.
- Implementation Tiers and Profile - assessment of current security capabilities and maturity with a desire to reach a targeted security and business outcome by remediating identified gaps.

Certane's security culture

At Certane, we believe that security is a responsibility that all employees must maintain and support to ensure ongoing protection of our information assets. To ensure this security culture, we have in place a robust hiring process, mandatory training for onboarding and continued education and awareness.

Security awareness and training

All Certane employees undergo cyber security, privacy, and fraud training as part of the orientation process and receive ongoing training throughout their Certane careers. In compliance with relevant company policies, new employees agree to a Code of Conduct, which highlights Certane's commitment to keep member and customer information safe and secure. In addition to specific job roles, tailored and specialist security training is provided where required.

The security awareness program at Certane involves partaking in community cyber safety education events and forums, provision of education material and learning workshops to ensure that employees are safe at work and at home.

Community collaboration

Certane is partnered with government and industry security groups and forums such as ACSC, AIST, ASFA, SIT Group and various major security consultancies and vendors. We continue to expand and build upon our security network to ensure that we support the greater community in combating cyber security within the financial industry.

Operational Security

Security is an integral part of our operations and the controls and services we provide are all based on the Information Security Framework. Control implementation requirements are governed by the Certane Information Security Policies and Standards.

Since Certane adopts a cloud-first strategy, we base our architecture upon modern approaches such as zero-trust model, cloud-based infrastructure and networks, and Software-as-a-Service (SaaS) where appropriate.

Data protection

Data encryption and data disposal controls are implemented to ensure Certane data and information is secure and protected based on industry best standards.

Data Backup

Certane's cloud-based solutions maintain ongoing data backup as per service agreement requirements at reasonable interviews. This ensures the appropriate DR redundancy to business critical applications and data can be effectively performed.

Cyber Resilience – Incident Management

Incidents are managed in accordance with the group Incident Management Policy and Process. The Policy sets out the minimum standards based on regulatory requirements to

effectively manage incidents and provides guidance on components of incidents such as identifying, actions, roles and responsibilities, training requirements, monitoring and reporting.

More specifically to security, security incidents are directly guided by our Security Incident Management Response Plan and underpinning playbooks. Testing and reviewing the security incident management program formally occurs annually and as part of managing real world incidents during the post incident review phase to ensure continuous improvement happens dynamically.

Compliance with Industry Standards

To ensure Certane meets industry standard in managing information security risk the following globally recognised standards are adopted and adhered to:

- ISO/IEC 27001:2013 ISMS
- NIST Special Publication 800-53
- CIS Security Benchmarks
- OWASP standards and guides

It is important to note that Certane and its subsidiaries currently hold ISO/IEC 27001:2013 ISMS certification from an external and independent auditor.