



# SERVICE DESCRIPTION

---

**Virtual Chief  
Information Security  
Officer (vCISO)**

# Executive Summary

## Thrive vCISO Service Definition

As security grows into a true business function, many organisations require security leadership but are unable to source the function internally. Thrive's vCISO service helps fill the gap between business strategy and security operations. The Thrive offering for vCISO Services scales from an economical, value driven model stressing information security fundamentals for small to mid-sized businesses, to more traditional, full-service vCISO capabilities for more mature organisations with stricter Information Security regulatory or compliance obligations.

The vCISO will work with the Client to develop and maintain an Information Security Program that complements their business strategy and risk tolerance. We help businesses reach balanced conclusions that drive reasonable Information Security decisions and measures while providing clarity and focus to see through the complexities and contradictions of today's Information Security and threat landscape. The service also ensures that the Information Security Program will meet your regulatory, audit and compliance obligations. Lastly, we can provide customised solutions and recommendations for your special Information Security challenges and concerns.

This service offering leverages ISACA's Certified Information Security Manager (CISM) Knowledge Domains (and associated Tasks) and the Center for Internet Security (CIS) framework as a basis for the types of activities to be performed by the Thrive vCISO.

## Services Scope

### The service shall include:

- Information Security Program Management
- Trusted Security Advisor - Coaching and Counsel
- Information Security Governance and Compliance Oversight

### Thrive Scope of Work and Deliverables

- Annual Information Security Program review.
- Review of existing policies, controls, and security toolsets to determine the extent that controls are met and identify areas that require improvements to meet CIS standards.
- Prioritise improvements required and prepare remediation plan for IT Management.
- Center for Internet Security (CIS) framework implementation.
- Incident Response Preparedness and Annual Incident Response Table-Top Exercise.



- If Client subscribes to Thrive's Vulnerability Management Service, a monthly review and reporting of findings will be provided to Management. If Client is performing their own Vulnerability Management, review and reporting available as an additional service.
- Participate in and support Client Information Security audits, up to one (1) per year. Audit project management/leadership available as a separate service.
- Coordination and participation in Client's annual Penetration Test. Penetration Testing is available as a separate service.

## Client Responsibilities

- Make available all Information Security related documentation, diagrams and previous audit findings.
- For annual Incident Response Table-Top exercise, Audit Support and external Penetration Testing, Client to provide Thrive with the appropriate internal resources necessary to conduct these efforts.

## Service Activation Date

Billing of monthly recurring charges will commence at the conclusion of the initial vCISO Service kickoff meeting.

## Service Exclusions

Any service not explicitly included in the vCISO Definition above is considered optional and may be provided under separate agreement for an additional fee.