ATECH IOMART

Service Definition Document

vCISO

Contents

Solution Overview

Aim and Objectives

Overview

The Virtual Chief Information Security Officer (vCISO) service provides organisations with expert-level cybersecurity leadership and strategic guidance without the need for a full-time, in-house CISO. This service is designed to help businesses manage risk, ensure compliance, and strengthen their security posture through a flexible and cost-effective delivery model.

Benefits Summary

- Cost-effective access to CISO-level expertise.
- Improved security posture and risk visibility.
- Enhanced compliance readiness.
- Scalable and adaptable to organisational needs.

Key Objectives

- These objectives collectively aim to help organisations manage risk, ensure compliance, and enhance their security capabilities through a flexible and cost-effective service model strategically aligned with the organisation's goals.
- Strategic Security Leadership: Align cybersecurity initiatives with business objectives and strategic initiatives.
- Risk Management: Identify, assess, prioritise and mitigate security risks.
- Compliance Support: Ensure adherence to regulatory and industry standards (e.g., ISO 27001, GDPR, NIST, PCI DSS).
- Incident Response Readiness: Develop and maintain incident response plans.
- Security Program Development: Build and mature security policies, procedures, and frameworks.

Engagement Model

The engagement profile is designed to accommodate different organisational sizes, maturity levels, and security requirements, ensuring that every customer receives a tailored experience.

Engagement Profile Options

- **Flexible Subscription:** Organisations can choose between monthly, quarterly or annual engagement models, allowing them to scale the service up or down as their needs evolve.
- **On-Demand Expertise:** Customers can request access to senior security professionals providing expert guidance for planned initiatives and unexpected challenges. Delivery of expert services falls outside of the vCISO service and additional charges will be incurred and follows the standard professional services sales process.
- **Virtual Delivery:** The service is primarily delivered remotely, with the option for onsite visits when deeper collaboration or hands-on support is needed.

Tailored Approach

- The vCISO engagement is not a one-size-fits-all solution. Each customer receives a bespoke plan, developed in collaboration with their leadership and technical teams, to address specific risks, compliance obligations, and strategic objectives.
- Service components can be selected and prioritised based on the organisation's current security posture, regulatory environment, and business goals.
- The vCISO service is designed to support the customer, whilst service components have been listed that fall within the remit of a CISO role, bespoke outputs can be included as key deliverables.

Typical Engagement Profiles

- **Start-ups and SMEs:** Benefit from foundational security leadership and rapid policy development without the overhead of a full-time CISO.
- **Growing Enterprises:** Leverage the vCISO's expertise to mature their security programmes, prepare for audits, and respond to evolving threats.
- **Established Organisations:** Use the service to supplement in-house teams, provide independent oversight, or drive strategic initiatives such as certification or incident response improvements.

Scope & Exclusions

The vCISO service provides executive cybersecurity leadership and advisory support. Unless explicitly contracted, the service excludes hands-on engineering/administration, 24×7 monitoring/SOC, penetration testing, legal counsel, and breach notification services. Where needed, these capabilities can be provided via add-on work packages or partner services subject to a separate statement of work.

Statement of Work (SoW) Reference

This overview document provides a summary of the vCISO service offering, including typical engagement models, deliverables, and service components. Please note that all vCISO engagements are tailored to the specific needs of each customer.

A detailed Statement of Work (SoW) will be produced at the sales order stage for every engagement. The SoW will define:

- The specific deliverables and outputs to be provided
- Roles and responsibilities (including a RACI matrix, where appropriate)
- Engagement cadence and communication protocols
- Service level agreements (SLAs) and key performance indicators (KPIs)
- Commercial terms, pricing, and any agreed exclusions or limitations

The SoW ensures that all parties have a clear, shared understanding of the scope, objectives, and commercial arrangements for the vCISO service. This approach provides both flexibility and assurance, allowing each engagement to be fully aligned with the customers requirements and expectations.

Deliverables

Custom Delivery Plan

Creation of a customer centric plan including defined outputs and timescales. As the plan is bespoke to each customer the plan can include some or all of the service components listed in section 5.

- Delivery plan detailing outputs and timescales
- RACI matrix and agreed delivery components
- Agreed engagement profile e.g. working sessions, update reports and executive briefings

Operating Cadence & Service Levels

The vCISO engagement operates to the following cadence and targets:

- Weekly working sessions with key stakeholders.
- Monthly status reports and risk register updates.
- Quarterly executive briefings and roadmap reviews.

Decision Rights & RACI

Decision rights remain with the Customer's executive team. The vCISO recommends and advises. A RACI matrix defines accountability for policy approval, risk acceptance, vendor exceptions, and audit remediation.

Measurement & Reporting

Each engagement includes baseline KPIs/KRIs. These metrics are tracked and presented in the Quarterly Executive Security Report.

Onboarding & Transition

Whilst every engagement is customer specific the following provides an overview of the standard delivery profile.
Days 0–30: Discovery & baseline assessment.

Days 31–60: Strategy draft & priorities.

Days 61–90: Program roadmap approval & first initiatives.

On exit, all artifacts and knowledge are handed over with a continuity plan.

Core Service Components

The vCISO service is built around a set of core components, each designed to address a critical aspect of organisational cybersecurity. These components are modular and can be tailored to meet the specific needs, priorities, and maturity level of each customer. The following areas can be delivered as part of your bespoke vCISO engagement:

a. Security Strategy & Governance

- Develop and maintain an Information Security Strategy aligned with business objectives.
- Establish governance frameworks and reporting structures to ensure accountability.
- Define roles and responsibilities for security stakeholders.

  Typical deliverables: Security Strategy Document, Governance Framework.

b. Risk Assessment & Management

- Conduct regular risk assessments to identify and prioritise threats.
- Implement risk treatment plans and provide executive-level risk reporting.

  Typical deliverables: Risk Register, Risk Treatment Plan, Executive Risk Reports.

c. Compliance & Regulatory Alignment

- Map organisational controls to relevant compliance requirements (e.g., ISO 27001, GDPR, NIST, PCI DSS).
- Support audits and certification processes, maintain compliance documentation, and oversee corrective action plans.

  Typical deliverables: Compliance Gap Analysis, Audit Support Materials, Remediation Plans.

d. Policy & Procedure Development

- Create and update security policies and standards.
- Develop operational procedures for critical security functions.

  Typical deliverables: Policy & Procedure Library, Operational Playbooks.

e. Security Awareness & Training

- Develop and deliver organisation-wide security awareness programmes.
- Provide executive-level briefings and workshops to foster a security-conscious culture.

  Typical deliverables: Training Materials, Awareness Campaigns, Workshop Agendas.

f. Incident Response & Crisis Management

- Develop incident response plans and playbooks.
- Coordinate tabletop exercises and advise during security incidents, focusing on root-cause analysis and continuous improvement.

  Typical deliverables: Incident Response Plan, Tabletop Exercise Reports, Post-Incident Reviews.

g. Vendor Management

- Oversee the security assessment of third-party vendors.
- Advise on remediation where vendors do not meet security requirements, using the risk management framework.

  Typical deliverables: Vendor Risk Assessments, Remediation Recommendations.

h. Security Architecture and Design Review

- Provide insight and guidance during the design and implementation of new systems and infrastructure.
- Advise on security best practices and promote adherence throughout technological initiatives.

  Typical deliverables: Architecture Review Reports, Design Recommendations.

i. Cybersecurity Programme Evaluation

- Regularly evaluate the effectiveness of the cybersecurity programme.
- Recommend and implement improvements as necessary, assisting in meeting compliance requirements.

  Typical deliverables: Programme Evaluation Reports, Improvement Roadmaps.

j. Security Certifications or Accreditations Assistance

- Support the achievement and management of security certifications, both new and existing.

  Typical deliverables: Certification Readiness Assessments, Accreditation Support Materials.

k. Horizon Scanning

- Provide expert advice on emerging trends, technologies, processes, and best practices to keep your organisation ahead of evolving threats.

  Typical deliverables: Horizon Scanning Reports, Strategic Recommendations.

Optional Add-Ons and Partner Services

Where required, additional services such as penetration testing, 24×7 monitoring, or hands-on engineering support can be provided via add-on work packages or partner arrangements, subject to a separate Statement of Work.

Assumptions & Prerequisites

Assumptions

No.	Assumption
1.	All relevant staff are available for calls, meetings, document reviews and workshops (if applicable).
2.	Access to relevant systems is available upon commencement of any work.
3.	Any standards, documentation templates, security policies etc. to be provided to Iomart in advance of the engagement commencing.

Pre-requisites & Engagement Activities

No.	Prerequisite
1.	It will be necessary for to provide the following in advance of any testing: Contact details of personnel to provide support and to resolve any issues with the system(s) under test, should any arise. IP addresses and hostnames of the targets Any documents, network Architecture or design details if available. User credentials for testing the application at each level of authority. Two users at each level per tester. URLs and other details necessary to reach the targeted application(s). Whitelisting or similar mechanism to facilitate remote testing of attack IPs.

Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

Why Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** - a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications

Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure

Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified, Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.


ATECH IOMART
6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD