



VCISO - SERVICE GUIDE

Last Modification Date: 12/01/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1	Overview	1
1.1	The InterVision vCISO (Virtual Chief Information Security Officer) service starts with executive engagement and a line of business analysis to ensure that risk reduction strategies related to digital assets are in place. Strategies for compliance, IT governance, and security investments are each managed, aligned, and prioritized to serve business needs. The customer is provided with a dedicated cybersecurity consultant team member to guide the maturation of security and risk mitigation for their business. A block of hours is assigned to provide ongoing consultation and engagement with the customer over all aspects of the customer's security practice.....	1
2	Service Description and Details	1
3	Roles and Responsibilities	2

1 OVERVIEW

1.1 THE INTERVISION VCISO (VIRTUAL CHIEF INFORMATION SECURITY OFFICER) SERVICE STARTS WITH EXECUTIVE ENGAGEMENT AND A LINE OF BUSINESS ANALYSIS TO ENSURE THAT RISK REDUCTION STRATEGIES RELATED TO DIGITAL ASSETS ARE IN PLACE. STRATEGIES FOR COMPLIANCE, IT GOVERNANCE, AND SECURITY INVESTMENTS ARE EACH MANAGED, ALIGNED, AND PRIORITIZED TO SERVE BUSINESS NEEDS. THE CUSTOMER IS PROVIDED WITH A DEDICATED CYBERSECURITY CONSULTANT TEAM MEMBER TO GUIDE THE MATURATION OF SECURITY AND RISK MITIGATION FOR THEIR BUSINESS. A BLOCK OF HOURS IS ASSIGNED TO PROVIDE ONGOING CONSULTATION AND ENGAGEMENT WITH THE CUSTOMER OVER ALL ASPECTS OF THE CUSTOMER'S SECURITY PRACTICE.

2 SERVICE DESCRIPTION AND DETAILS

The vCISO service includes recurring sessions with a Cybersecurity Consultant to:

1. Perform discovery and analysis of current people, process, and technologies that support the organization's business objectives.
2. Assess business risk (confidentiality, integrity, and availability) requirements.
3. Determine maturity of security program.
4. Develop roadmaps for improvement.
5. Assist in managing the execution of roadmaps.
6. Re-assess, re-evaluate, and re-prioritize as business environment changes.
7. Assist in strategic activities (i.e., meetings, presentations, budget exercises, policy evaluation and development, IR and DR testing exercises) as needed.

Additionally, stand-alone services may be provided to focus on a specific security maturation objective. Such as:

- Security Risk Assessments
 - Critical Infrastructure Security Review
 - Information Security Policy and Procedure Review
 - Penetration Testing Analysis
 - Risk Assessment
- Gap Assessments for regulatory compliance frameworks
 - HIPAA
 - PCI
 - CMMC



VCISO - SERVICE GUIDE

- Measurement and maturity planning using industry standards such as:
 - NIST Cybersecurity Framework (CSF)
 - CIS Controls
- Cybersecurity Workshops
 - Incident Response Planning Tabletop Exercise (TTX)
 - Ransomware Defense Workshop

Engagement Assumptions

- Customer will provide access to any available schematics, drawings, organization charts and documentation required for completing project activities.
- Customer will provide the necessary workspace for onsite work as well as any face-to-face interviews.
- Any change in resources, timing, scope and/or assumptions, which may impact fees and expenses, will be discussed and approved through a written change order.
- Customer will need to designate a single point of contact (POC) for this project to facilitate communications.

3 ROLES AND RESPONSIBILITIES

	Client	InterVision vCISO	InterVision Extended Services*
Installation and Configuration			
Consult, advise, and assist with developing security practices and roadmaps		X	
Conduct risk assessments and recommend risk mitigation strategies		X	
Implement recommended policies and changes	X		X
Monitoring, Incident Generation, Investigation, Threat Hunting, and Escalation	X		X
Provide Data Forensic Services.			X

*Extended Services can include but are not limited to additional Managed Services, or Professional Services.

