

VIRTUAL INFORMATION SECURITY OFFICER (vISO)

305-828-1003

info@infosightinc.com

Our vISO Program

- ✓ Keeps executive, operations and IT management informed and up to date on technology security related best practices and regulations.
- ✓ Works with executive management to develop, evaluate, recommend, select and implement technology security solutions
- ✓ Works with executive management to develop long-term IT security strategy and align IT strategy with business goals
- ✓ Lowers costs by maximizing IT budget and strategic planning.
- ✓ Provides ISO's who are advanced security experts with high level certifications

The Challenge

With the current and future landscape of cyber threats, the need for an ISO is critical. Many organizations don't have a dedicated ISO on staff due to budget constraints. If there is an ISO, they may be stretched thin due to limited resource, juggling multiple areas of responsibility, and may not have the knowledge needed to handle cyber threats or a crisis properly. When a crisis hits, the lack of a full time or fully qualified ISO can lead to the loss of valuable response time and wasted efforts figuring out how to properly respond, leaving an organization at risk. Cyber attacks aren't going to wait and with ISO's being in such high demand and salaries on the rise, an organization may feel paralyzed in getting the ISO help that may be desperately needed.

How We Solve It

InfoSight provides organizations with a contracted Virtual ISO (vISO) who serves as an extension of your team through a choice of two service level offerings, Tactical or Strategic, custom fit to achieve your information security business goals. Not entirely sure what those goals are? We can help you make that determination based on your senior management's vision, the industry you are in, and any regulations or frameworks you choose or that you may be required to follow.

Our Tactical & Strategic vISO Programs include options for organizational oversight, risk assessments, security tools monitoring and reporting, policy writing, vulnerability management, controls reviews and assessments, and audit preparation, all utilizing our GRC Platforms. To top it off, the vISO helps your organization to determine and pinpoint strategic long term goals.



A Deeper Dive into InfoSight's vISO Programs

InfoSight offers TWO unique programs to fulfill the needs of your organization: Tactical vISO and Strategic vISO.

▶ TACTICAL vISO

Our Tactical vISO Program offers an ISO in an advisory role to review organizational security policies, processes, monitoring, and reporting.

Our Tactical vISO Platform:

- ▶ Focuses on specific regulatory frameworks, departmental responsibilities, and cross functional regulatory requirements as it relates to corporate security oversight.
- ▶ Provides guidance and recommendations toward information security program improvement
- ▶ Drives standard program deliverables

▶ STRATEGIC vISO

Our Strategic vISO Program is based on the Tactical vISO Program deliverables with the addition of strategic components tailored to fit your organization. The Strategic platform offers enhanced value with the inclusion of our GRC (Governance, Risk, and Compliance) platforms to help your organization streamline information security program initiatives and provides the following platform benefits.

Our Strategic GRC vISO Platform:

- ▶ Provides regular reviews of security monitoring tools and reporting
- ▶ Assesses risks and identifies overlapping controls, control weaknesses, and recommendations on risk management strategies
- ▶ Assesses and assists in IT and IT Security policy and Program creation, change management, and approval processes
- ▶ Assists with security awareness training and testing, including vulnerability management
- ▶ Provides management of multiple organizational frameworks and hybrid regulatory oversight plans
- ▶ Participation in Monthly, Quarterly, and Annual meetings where an information presence is beneficial or required

Other Assessments



Vulnerability & Penetration Testing

Consists of a multi-disciplinary, multi-faceted review of the organization's systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.



Red Team/Blue Team Testing

Designed to test an organization's readiness to detect, withstand and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches.



Web & Mobile Security & API

Involves the security testing of web, mobile and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

