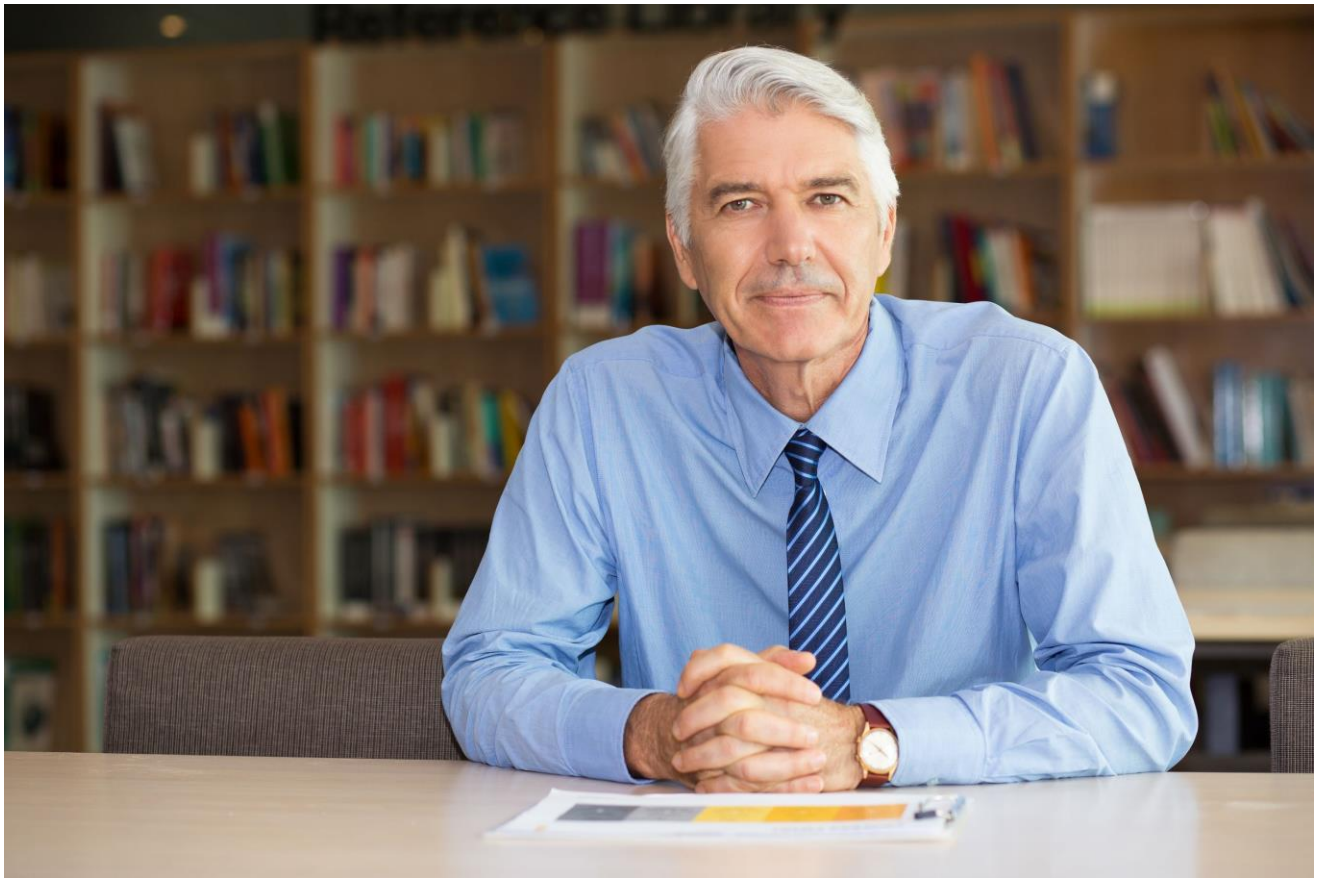
AIS
ALVIN INTEGRATED SERVICES

Hire a Virtual CISO (vCISO)

Ensure your business' growth with holistic solutions.



+91 88025 05619 | +91 82875 09289 | consulting@alvinintegrated.com

Virtual CISO (vCISO) Service

72% of organisations, according to ISACA's State of Cyber Security 2019, have a chief information security officer (CISO). Only 55% of the organisations in that research have a budget for increased security. Budgets are often already tight for small and midsized businesses, so hiring a full-time CISO could seem like a luxury.

How can a company ensure that its top leadership is information security-focused when it either lacks security budgets or is reducing them? Hiring a virtual CISO (vCISO), usually referred to as an on-demand CISO, is one option.

Executive Level Virtual Outsourcing Cybersecurity Management

A virtual chief information security officer, or vCISO, is a service created to offer organisations part-time access to outsourced executive-level professional cyber and information security experience.

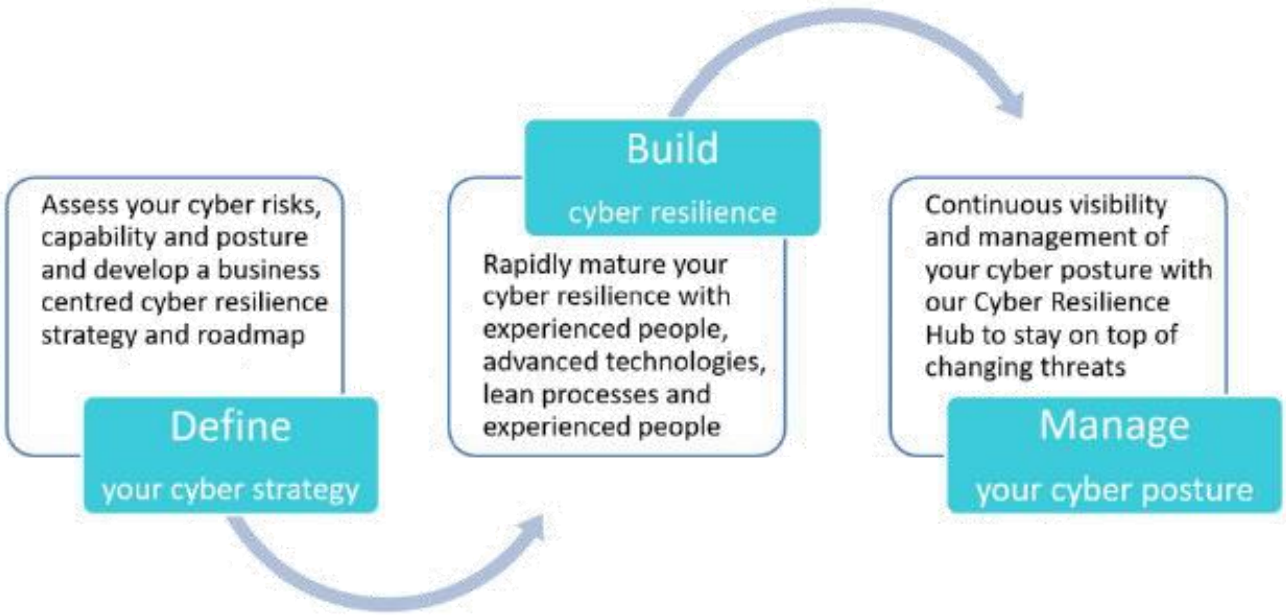
A vCISO service is customised to meet the unique cyber and information security maturity, capacity, and demands of your organisation. Your own virtual CISO, who can offer executive-level guidance and direct your cyber and information security strategy, may be accessible both on-site and remotely.

From a few hours per month to a fully outsourced information security function, the vCISO service can be provided. In order to adapt to your evolving information security requirements and maturity over time, the services can easily be scaled up or down.

What is a vCISO?

The only difference between a vCISO and a full-time chief information security officer is that a vCISO is an outsourced senior-level security executive who is in charge of developing and implementing information security programmes strategically. A supporting group of information security experts who assist in putting the vCISO cybersecurity vision into practise is a part of the services provided by vCISO. Our team of specialists has years of expertise creating information security programmes that support corporate goals and demonstrate quantifiable security posture improvements.

The task of establishing policies and processes in accordance with corporate culture, risk tolerance, and compliance standards falls to the vCISO team. An successful security programme must be created using a customised strategy. An IT risk assessment, which identifies areas for improvement and aids in setting priorities for the security programme, is the typical first step in a vCISO engagement. A remediation plan is created after problems are found to start closing security holes. We reevaluate when remediation is finished, assist executive leadership in understanding the results, and then repeat the process.



Why does the Virtual CISO (vCISO) service exist?

- Over the past few years, there has been a sharp increase in demand for vCISO services. The need for security experts will expand as threats to information security grow and corporations continue to be the main targets. The job gap between the need and supply of security experts is growing. Because of this, there is intense competition in the market for security experts, which makes it extremely difficult for businesses to find qualified candidates.

- A virtual CISO can add value in this situation. With the help of virtual CISO services, organisations that would otherwise be unable to acquire a suitable security candidate may collaborate with a seasoned CISO and security team without having to add more employees to their staff. Many organisations don't require a full-time CISO; instead, they require an independent security expert to guide their business by analysing cybersecurity problems, developing a cybersecurity programme, and ensuring that the right security milestones are met.

What types of businesses are using vCISO?

- Businesses of all sizes and in a variety of sectors are taking use of vCISO services. For instance, at AIS, we collaborate with companies in the financial, insurance, retail, manufacturing, healthcare, and technology sectors. Technology is crucial to running a business, regardless of the industry, but it also poses a security risk.

- Every company is different, and every organisation approaches risk in a different way. But every organisation uses the same strategy. A vCISO assists organisations in two ways: first, by helping them identify their risk, and second, by assisting them in aligning their security decisions with their business goals.

Virtual CISOs Bring Experience, Expertise, Leadership:

A valuable combination of technical, executive, and organisational knowledge is provided by AIS vCISO Advisory Services, which draws on the expertise of previous CISOs from a range of industries, including professional services organisations and multinational conglomerates. They are among of the most skilled technical practitioners working today, with unique knowledge of developing risks and solutions from their experience working at the forefront of cyber security. Our multinational, multidisciplinary team, which comprises former IT and security executives, digital forensic experts, intelligence analysts, and regulatory specialists from a wide range of industries, supports AIS vCISOs. This elite group will help your overall information security programme mature more quickly.

In today's competitive information security job market, it can be difficult, time-consuming, and expensive to find an experienced, well-qualified CISO. This is the ideal time to take into account AIS Virtual CISO Advisory Services if you currently require a CISO.

Why Hire a vCISO?

Expertise across Industries: Because virtual CISOs engage with a variety of clients in distinctive industries, they have access to opportunities that isolated vertical CISOs do not. The security expertise a virtual CISO gains from each distinct client environment provides ongoing development and enhanced proficiency for the security leader, which benefits each client the vCISO leads.

Flexibility in Diverse Business Environments: Virtual CISOs can easily adapt to any environment and are ready to start working right away with little onboarding time. By definition, vCISOs are able to enter a new environment and quickly adapt to meet business and security expectations. The vCISO must first have a solid awareness of the goals, risk tolerance, company culture, and business model of each organisation. From there, they are able to comprehend the organization's security risks. The vCISO will share the findings with clients to assist in making the best security decisions for their environment after having a complete understanding of the security landscape.

Why Hire a vCISO?

- Efficiency with Core Competencies: Where organisations need it most, a virtual CISO fills in the security gaps. Internal teams are relieved of this enormous burden by vCISOs, who concentrate on cybersecurity strategy and implementation. This makes it possible for both internal workers and cybersecurity experts to continue to focus on their respective areas of expertise.
- vCISOs are objectively independent and are not influenced by office politics or individual career aspirations. The mission of vCISO, an impartial third party, is to assist clients in choosing the appropriate security measures for their company.
- Economical: In general, AIS vCISO programmes are much less expensive than hiring a full-time CISO and supporting security staff. The average CISO compensation is $223,000 per year, according to a report published in May 2016 by Silver Bull. The costs associated with hiring more employees are not even included in the base compensation. Clients of AIS vCISO often pay a small portion of what hiring an internal CISO would cost. Additionally, vCISO clients have access to the collective knowledge of a full team, eliminating the inherent skills gap that exists with a single person.

	vCISO	CISO
Resources	Security Leader + Security Resources	Security Leader
No. of Resources	Team	Single
Roles	Strategic + Operational	Strategic
Scalability	Yes	No
Project Start	Immediate	3-6 Months
Turnover	0	1.5 Years
Team Integration	Full	Full
Value of Services	*****	***
Total Cost	$$	$$$

Why our vCISO?

- Through our virtual CISO service, businesses have access to a pool of experts and seasoned cyber security practitioners who assume the position of Chief Information Security Officer in your company. Our reasonably priced V-CISO service brings expertise and management to identify, design, and carry out a special procedure particular to your company.
- Our compliance and governance group members work with our V-CISOs to support them in meeting the diverse needs of your organisation.
- In addition to bolstering your current staff, setting strategic goals to support business-critical technology demands, balancing IT administration, and establishing clear communication with the board of directors, investors, and government agencies are all skills that the team of experts at AIS has to offer.
- The leadership you require, when you need it, is provided by AIS Virtual CISO Advisory Services, whether you're seeking for an interim CISO, a resource to support your CISO, or a longer-term agreement.
- You can rely on a vCISO from AIS to have the technical expertise, business acumen, and communication skills to make an immediate difference. Our experts have served in a broad range of industries for companies of various sizes and will know how to align information security strategies with your company's unique needs and challenges.

Services and offerings include:

- establishing or directing privacy and security standards, guidelines, and processes
- taking charge of and leading information security teams
- interacting with the executive branch
- carrying out risk analyses for operational security
- supplying danger information and overseeing corporate security
- crisis intervention

How Do We Do It?

- We use industry norms, laws, and best practices to analyse the threats to your information security assets in an unbiased manner. You are fully aware of your most vulnerable areas as a consequence, and you have a strategy to reduce the risk. Plainly put:

- We evaluate current information security programmes (administrative, physical, and technical security controls) and create, execute, and monitor information security plans that are specialised to the security requirements of each customer.

Proactive Security
(Prepare & Detect)

1. Security Governance
- Organisation & Awareness
- Risk Management
- Security Policy

2. Operations
- Asset Management
- Vulnerability Assessment & Penetration Testing
- Asset Protection

Reactive Security
(Respond & Restore

3. Technology
- Identity & Access Management
- Security Monitoring
- Incident Response

4. Matrics
- Operations Efficiency
- Board Reporting

You can Prepare, Protect, and Strengthen your Defenses with the aid of Virtual CISO advisory services.

Our virtual CISO advice services are customised to meet your unique demands and information security requirements. There are four areas where most organisations gain from the expertise of a virtual CISO, albeit you have a variety of options when it comes to the scope and duration of services:

Definition of Strategy: The AIS vCISO serves as a resource for executives in business operations and IT, helping to identify business threats, establish a baseline for your present security programme, and develop security strategy in line with corporate goals and technological plans.

Our staged approach makes sure that our plan is effective and efficient, makes use of NIST 800-53, and can be linked to various cyber regulations (e.g., PCI, HIPAA, GDPR, FINRA, and NYDFS).

Assessment: The AIS vCISO creates prioritised actions to assist you manage your information security strategy and programme successfully after assessing culture, processes, and technology from a security governance viewpoint. Assessments may consist of:

robust reviews of a number of areas, such as information asset management, acceptable use policies, data classification, threat and vulnerability management, and third-party management, as well as interviews with stakeholders from the technical, business, and executive teams and the collection of supporting documentation

Monitoring: In accordance with the results of the evaluation, the AIS vCISO can offer a range of continuous assistance options, such as:

- Creating policies and processes to fill documentation shortages
- Creating a corrective action plan with prioritised, concrete recommendations

Implementing the remediation plan and providing ongoing, less intensive strategic direction that helps the organisation stay on track with its long-term objectives

Training is crucial to maintaining a strong programme because security awareness. Every level of user group within your business can benefit from training that your vCISO can suggest and assist with implementing. To combat business email compromise, this might range from the highly technical (such secure coding methods) to general data handling instruction. The vCISO can also supervise carefully monitored phishing attempts run by AIS to gauge the level of security awareness among employees.

IT Environment Security Design: For organisations looking to build from the ground up, AIS vCISO can provide your team with necessary system hardening configuration guides and network designs. This will also include multiple security protections and incident monitoring controls.

Virtual CISO Services and Responsibilities:

Like a standard CISO, the vCISO services and offerings are remarkably similar. However, what a vCISO will be responsible for will vary and depend on the specific needs of the organization. Generally, some of a vCISO responsibilities will include, but are not limited to the following:

- establishing the information security and compliance governance program's vision, strategy, direction, and implementation.
- Inform the organization's board of directors about your security objectives.
- Identifying the appropriate security framework(s) that the firm must adhere to

- Architecting security solutions with the team while recognising industry trends
- Identify the most suitable and affordable security solutions, as well as security budgets.
- Provide direction and assistance in order to meet any compliance needs the organisation may have
- In charge of the information security team
- Establishing, organising, creating, examining, and approving guidelines, standards, and procedures
- Either assisting or in charge of the incident response team
- Determining the appropriate degree of risk and controlling the risk faced by the organisation
- Examine the internal security measures in place.
- To help with training and planning for yearly security

Define	Manage	Optimize
Policies & Standards	Review & Update	Operationalize Governance
Tech Security Controls	Expand Control Set	Regular Control Audits
Develop Risk Register	Appy Threat & Impacts	Risk Reporting
Define Scope of Vendors	Foster Vendor Remediation	Contractual Risk
Define Remediation Timelines	Fulfil Remediation Times	Report Remediation Metrics
Establish Exception Guidelines	Ensure Proper Cadence	Reduce Exceptions
General Security Awareness	Apply Targeted	Enterprise Modular Training
Understand Compliance Landscape	Training	Audit Scope Reduction
	Operationalize Compliance	

Compliance Assurance / Project Management Methodology

Before the kickoff of the engagement

- Clearly defined goals and objectives
- Critical Success Factors Identified
- Identified Critical Risk Areas
- Roles and responsibilities defined
- agreed-upon deliverables
- The change management procedure has been established.

During the engagement

- Regular progress updates through agreed-upon channels, viz., email or in the form of reports
- Expectations Management
- Any change must be managed as per the defined Change Management Process.
- Dashboard-based reports for executive management and technical/implementation teams with recommendations

After the engagement

- Project Indicator of
- Project final report with all the findings and recommendations
- Roadmap for next steps
- Continuous improvement demonstrated by matrices and dashboards

Contact us:

Call us at +91 88025 05619 or +91 82875 09289, send an email to consulting@alvinintegrated.com, or visit our website for additional information.