Virtual CISO Service

From "What Now!" To "What's Next?"

The Virtual CISO (VCISO) service, otherwise known as CISO as a Service or Fractional CISO, provides our clients with high level strategic advice, cost management, and risk & compliance supervision. All delivered by executives with compelling experienced leadership that is committed to success and available on an as-needed basis. This consultant provides direction and oversees the implementation of your security initiatives, engages with key players in your business regularly, and advocates on your behalf with services providers and vendors.

This VCISO ensures that your spending aligns with your risk profile, while enabling IT systems and teams to keep pace with advancements in technology and everchanging cybersecurity threats and compliance requirements

This service is extremely flexible and can be tailored to fit the areas of focus and level of engagement required. It is actively adjusted throughout the engagement.

This gives our clients a relatable partner to work with and ultimately allows them to focus on their business with confidence in their technology and cybersecurity.

We employ **a one of a kind "Office of the CISO"** approach to VISO engagements, providing a primary resource with industry expertise to lead the team and provide continuity and consistency, along with subject matter experts that are engaged throughout the life of the partnership. This provides a "complete" CISO with business, risk, and technological depth so that we can meet any challenge or request with the best quality response as well as coverage and scheduling flexibility.

Our team holds many certifications including CISSP and CMMC. We specialize in highly regulated industries and verticals such as Financial Services, Health Care and Department of Defense contractors, with an acute focused on cloud and shared security models over the past several years.

We have assessed, designed, implemented, managed and/or tested security plans and technical solutions for requirement and compliance related to PCI-DSS, HIPAA, NY DFS, NIST 800-171, ITAR and DFAR, CMMC, and ISO 27001.

Why a Virtual CISO

- Many businesses don't need a full time CISO
- Avoid the time and expense trying to identify, attract, afford, or retain a qualified person full time.
- Work with a qualified and experienced security executive at a fraction of the cost for that caliber talent
- Get an unbiased perspective of your IT and information security environment
- You get a team of technical resources behind the VCIO

Value of a Virtual CISO

- Investing strategically in IT will create the right level of protection, cost efficiencies, and economies of scale
- Reduced cybersecurity risk and peace of mind that you are protected
- Proactively receive education on ever changing threats
- Assurance that your service providers are protecting your information appropriately
- Having an expert when something goes wrong can keep you in business

Virtual CISO Service

From "What Now!" To "What's Next?"

Services and activities may include:

DEVELOP SECURITY STRATEGY

- Advise executives on security strategy for technical and non-technical components
- Assess existing Security team and systems and propose adjustments
- Apply industry experience and best practices to develop a documented strategy
- Socialize the strategy with your leadership and key stakeholders
- Quantify and prioritize initiatives and provide regular reporting on progress

LEAD CYBERSECURITY

- Address security gaps and 3rd party requirements
- Oversee security incidents
- Provide education to your organization's leadership team and employees on security threats
- Provide, manage, and review a summary of cybersecurity risks
- Provide recommendations to improve business continuity
- Assess existing systems, identify gaps in security and configuration
- Develop policies and procedures
- Update security plans
- Coordinate annual security testing and remediation

OVERSEE OPERATIONS

- Provide direction to IT staff and managed service providers
- Ensure all security services are provided effectively
- Develop and socialize a plan for upgrades, including timetable and cost
- Maintain a list of current and future projects
- Track project status and associated risks
- Review existing spending and identify cost savings/avoidance opportunities
- Manage Security Vendors
- Advocate on behalf of clients in relationships and negotiations

Real Business Results

- **Law Firm -** Performed IT Risk Assessment, implemented policies, procedures, and controls. Respond to client Cybersecurity questionnaires and inquires. Manage all of IT day to day reporting to Managing Partner.
- **Financial Services Firm –** Managed an active security breach, performing containment, remediation, and forensics. Interfaced with law enforcement and quickly getting them back to business. Overhauled cloud security configuration and implemented security plan.
- **DOD Contractor –** Architected, implemented, and managed a security plan and 100% self-contained cloud-based solution to meet NIST 800-171 and ITAR requirements, including security training and user onboarding, in under 4 months.

Contact Next Phase Consulting at info@gotonextphase.com or 201-822-5453