cynomi

What does it take to be a

FULL-FLEDGED VIRTUAL CISO?



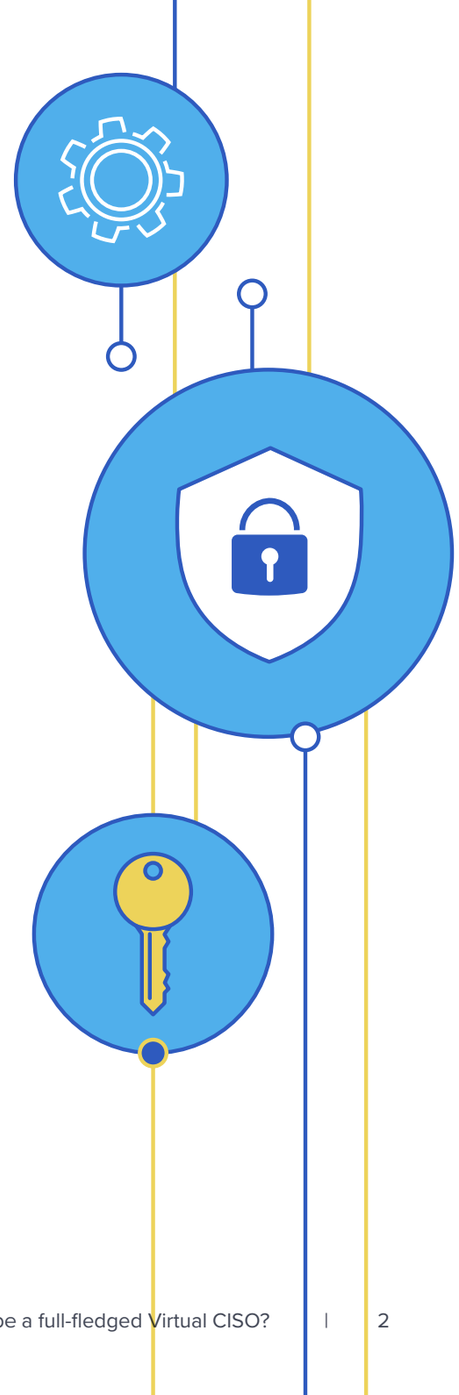
Introduction

The delivery of Virtual Chief Information Security Officer (vCISO) services has grown markedly in popularity in recent years. Many MSPs and MSSPs have added them to their repertoire as they recognize the potential for high margins. What is delivered, though, varies from provider to provider. Some take the compliance part of vCISO duties and help organizations with compliance preparedness. Others perform risk assessments to assist IT in identifying, managing, and addressing potential risks. There are other areas, too, where MSPs provide portions of the vCISO role for clients. These include reporting and communication with management, cybersecurity audit preparation, continuity planning, cybersecurity strategy, the setting of policy, financial management of cybersecurity, and the supervision of security technology evaluation and implementation.

vCISOs that provide services in one or two of these areas will reap the rewards. However, those that span the entire range of vCISO responsibilities can achieve much higher margins as they are highly valued by their customers. Standing in the way are challenges such as finding qualified and experienced personnel and being able to scale those services without having to add yet more resources.

In this guide we explain:

- The essential functions of the vCISO
- What it takes to move from partial delivery of vCISO duties to comprehensive delivery
- The upsell potential of delivering comprehensive vCISO services
- How vCISOs already providing security risk assessments or compliance services can expand those offerings effortlessly
- The platforms that can help vCISO providers add sufficient automation to be able to broaden their offerings and scale without adding more personnel resources



What is a CISO and why are they in such high demand?

CISOs ensure that organizations put basic security measures in place to reduce the risk of a cyberattack as well as adequate safeguards to protect sensitive information. They coordinate all security technologies, tactics, strategies, and processes to ensure the organization is protected now and in the future. In addition, they develop, implement, and enforce policy to protect critical systems, identities, and data while forwarding the overall goals of the business.



The CISO is typically involved in:

- **Risk management** – Identifying the gaps, monitoring, evaluating, and managing overall cybersecurity and technology risk in coordination with business leaders.
- Setting an all-encompassing **cybersecurity strategy** that guides technology investment.
- **Actual protection** - Development and implementation of processes and systems used to prevent, detect, and mitigate cyberattacks.
- Overseeing cyber **governance and compliance** processes.
- **Communication** - Reporting to top management and the board of directors, and ensuring cybersecurity awareness among employees.
- Overseeing **incident response** and its planning.
- Managing relationships with **vendors**.

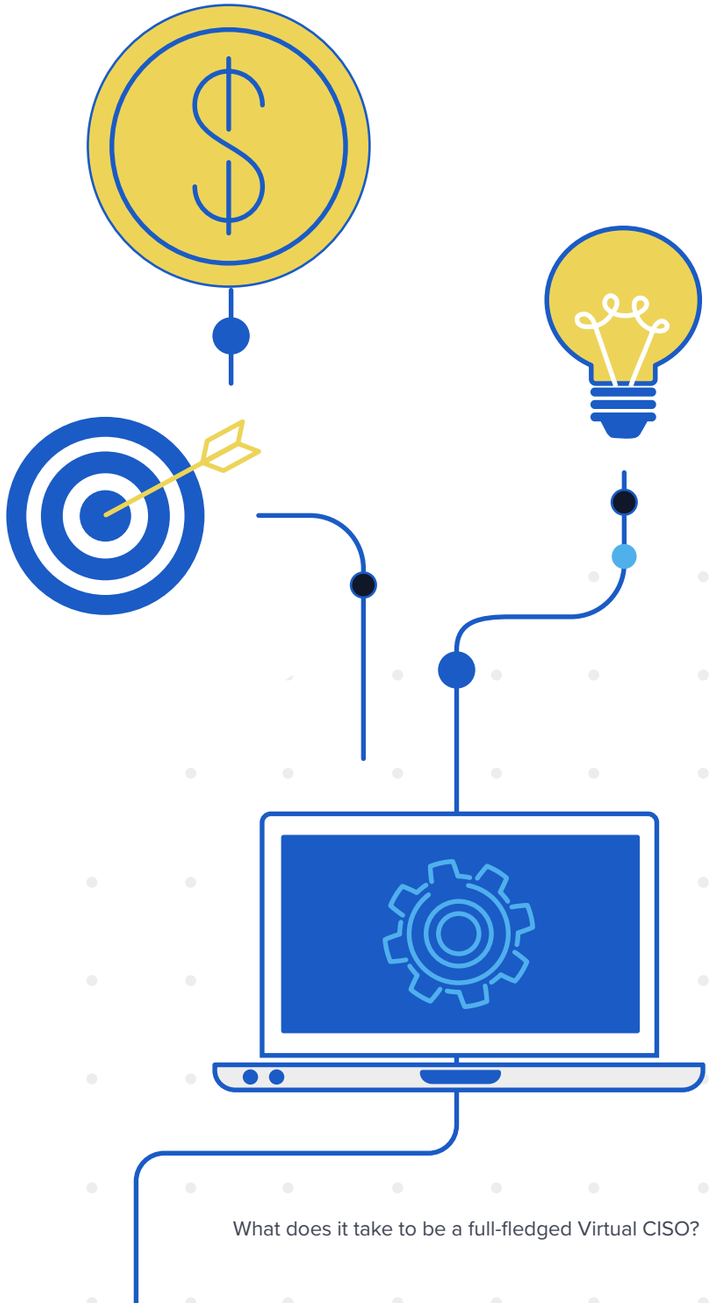
As cyberattacks, phishing scams, and ransomware outbreaks have ramped up in recent years, the role of the CISO had become even more critical. And with a large portion of the workforce operating remotely, the risk posture of organizations has shifted markedly. CISOs must constantly reassess risk and revise plans and policies to maintain compliance. This requires solid knowledge of all applicable standards such as the National Institute of Standards and Technology (NIST) and ISO, as well as a firm grip on regulations such as HIPAA, and GDPR.

It goes without saying that a CISO must be highly experienced in the world of security. Many have advanced degrees in IT and cybersecurity as well as certifications such as the Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), or Certified Information Security Manager (CISM). To operate successfully at a C-level and understand the interplay between IT and the business, a knowledge of business is essential – some possess an MBA.

Unfortunately, skilled CISOs are in very short supply. Those that can afford them pay top dollar. CISOs typically command in excess of $150,000. Few SMBs can afford that amount. Yet states such as New York and others mandate that the CISO position must be filled in certain regulated markets such as financial services.

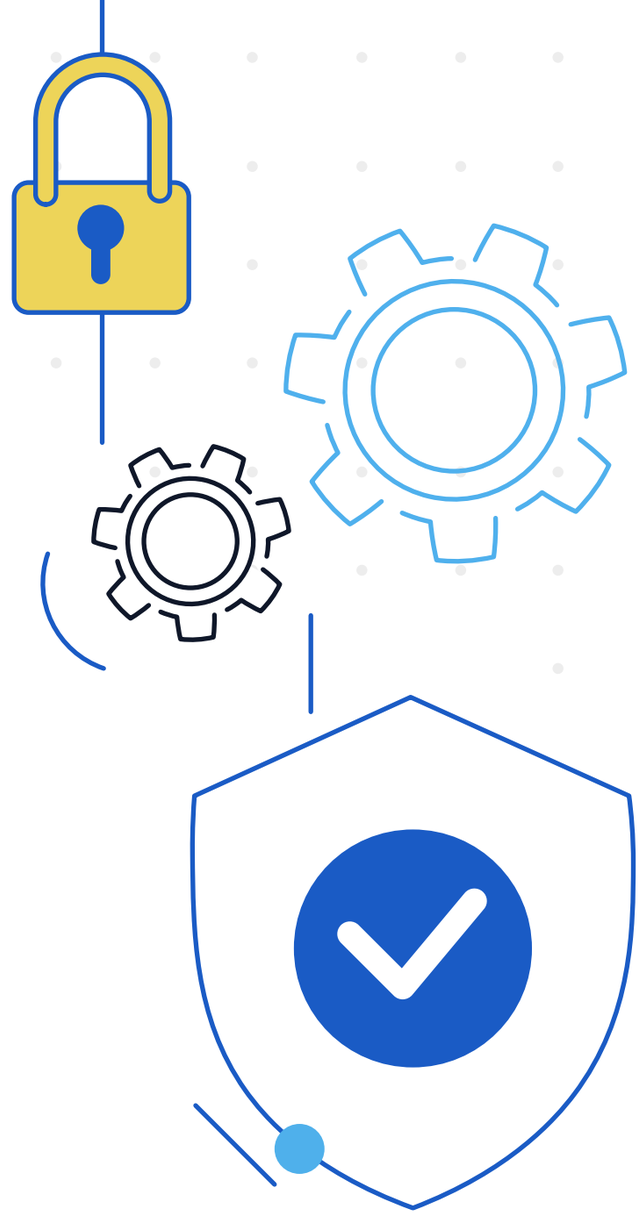
Why are vCISO services so attractive to MSPs?

Studies show that a significant portion of MSP clients fell victim to a cyberattack within the last 12 months. The danger inherent in the virtual world is forcing them to spend more than ever on cybersecurity. However, only 50% of SMBs have a dedicated internal IT person who manages their cybersecurity. That is where the vCISO role comes into play. Instead of hiring a full-time CISO, businesses pay a subscription or retainer to gain access to expert C-level cyber-assistance in devising and implementing strategies to prevent breaches, reduce risk, and mitigate the consequences of attacks. These virtual security executives perform a vital role in building a comprehensive cybersecurity program. vCISOs ensure that organizations put basic security measures in place to reduce the risk of a cyberattack as well as adequate safeguards to protect sensitive information. They coordinate all security technologies, tactics, strategies, and processes to ensure the organization is protected now and in the future. In addition, vCISOs develop, implement, and enforce policy to protect critical systems, identities, and data while forwarding the overall goals of the business.



vCISO services are especially attractive to MSPs and MSSPs as:

- They enable service providers to address a growing need from their SMB clients for proactive cyber resilience
- They offer the potential to grow recurring revenues - expand into a new customer base or sell a new service to existing customers
- They help service providers differentiate themselves
- They are an excellent vehicle from which to upsell additional cybersecurity services to existing customers
- Those offering the complete range of vCISO services can charge a lot more while delivering highly valued services that earn word of mouth



Minimum requirements for full vCISO services

> As MSPs and MSSPs add more and more vCISO duties to their roster, they extend their reach deeper and deeper into customers' operations. They gain the ability to enhance their reputation directly with senior management. No longer are they dealing with the IT manager, the systems administrator, or the backup manager. They are interfacing directly with C-level executives and boards of directors. With their duties well fulfilled, the MSP/MSSP moves into a trusted position of strength. Smart service providers, therefore, seek to extend their existing offerings to be able to provide the entire vCISO service range and become true partners of their clients.

We spoke to our community of experienced vCISOs to determine what service providers need to consider if they wish to embrace the full scope of vCISO services. Based on these conversations, here are the essential parts.

Consider these as the minimum requirements:





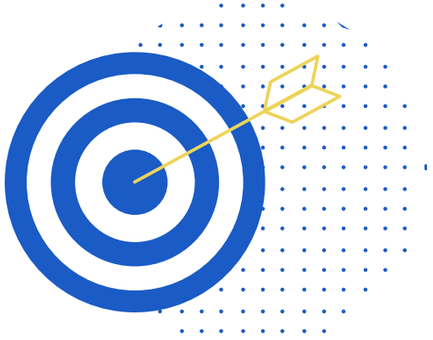
Risk assessment & management

Most vCISO engagements start with a risk assessment. This is the very first step that is required for the vCISO to understand the current posture of the organization.

Cybersecurity risk assessments vary from provider to provider. The basic elements include identifying any risks and vulnerabilities that could affect organizational assets, as well as analyzing, evaluating, and prioritizing those risks based on the risk appetite of the board. This helps them to implement appropriate cybersecurity controls to address risks and eliminate security flaws. Some MSPs and MSSPs offer assessments and turn over the results to IT. Others manage risk for their clients over time and provide remediation actions.

Risk assessment and management must always be done in accordance with business goals. They must encompass general risk such as ransomware, data leakage and other cyber threats. Risk assessment can't be done unless comprehensive asset management is in place that can discover any and all systems, endpoints, applications, and users running within or connecting to the network. Risk management can then utilize this knowledge to discover a multitude of potential threats such as unpatched systems, passwords that don't follow policy, misconfigurations, open ports, and other vulnerabilities.

> "We start our client engagements with a risk assessment. From there, it is clear to both sides what needs to be done to close the security gaps. It also enables us to sell them solutions that will have the most impact in terms of reduced risk."
>
> **Carlos Becerra**, CCISO
> Co-Founder, CISO, CEO / Cyber Security Speed



Setting strategy

A good risk assessment opens the door to the creation of sensible strategies that can thwart existing attack vectors and proof the organization against future risk.

Cybersecurity strategy should always be done in full alignment with business priorities. It sets a roadmap that prioritizes short-term, mid-term, and long-term actions. It takes into account budget and financial management realities.

The strategy and roadmap can then be used to guide the creation of policy to cover all areas of cybersecurity (both for IT and cybersecurity professionals, as well as all employees). Armed with the right strategy and applicable policies, the vCISO can guide the organization to remediate the most potent threats as well as address any low-hanging cybersecurity fruit.

> “The vCISO has the disadvantage of not being an employee, yet we have the advantage of being an unbiased third-party voice. This allows the vCISO to help the business to continue to operate at a secure level, while at the same time support the security program by coming beside the security team to implement solutions across the organization.”
>
> **Brent Forrest**, CCISO
> Field CISO / Flair Data Systems



Actual protection

vCISOs must be more than planners, observers, and supervisors of the actions of others. They must be hands-on in remediating immediate threats and taking direct action to shore up the organization against further attacks. This begins with the implementation of controls such as multi-factor authentication (MFA), strong password policy, firewall configuration, and anti-virus installation.

Protecting assets such as endpoints, data, network, email, and websites is an important responsibility of the vCISO. This is done by deploying technological tools such as endpoint detection and response (EDR) and email protection, or by implementing best practices for actions such as vulnerability scanning, access and identity management, security configuration and patch management.



Continuity planning

Disaster Recovery (DR) encompasses backup but takes it a stage further by including factors such as alternative data centers, standby colocation infrastructure, and other features designed to help an entire business recovery swiftly from a natural disaster, cyberattack, or grid failure. Business Continuity (BC) adds organizational, documentation, and human aspects to DR such as drills to verify the workability of the plan, lists of phone numbers and addresses where personnel go if the office is unreachable, and more. The vCISO should offer guidance on BC and DR, as well as data protection, data retention, archiving, and disposal.



Training & security awareness

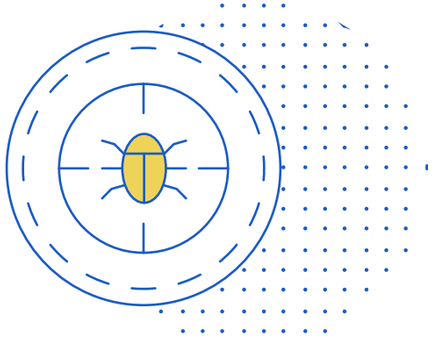
The strategy should lay out the various aspects of cybersecurity training that are required. At a minimum this must include employee and executive security awareness training, as well as training of technical personnel on more advanced aspects of cybersecurity. Security awareness training is best arranged by partnering with a vendor specializing in this area. It should include phishing simulation tests to assess the propensity of people to click on malicious URLs and attachments. The success of this training can be demonstrated by a steady reduction in the number of employees failing these simulations. Existing IT and security personnel should be rotated through training and certification programs to continually improve their skills in areas such as threat detection and response, access and identity management, and vulnerability management.

> “Security awareness training is a crucial investment in the employees, empowering them to protect themselves and the organization from cyber threats. A specific area to focus on is the education of executive and leadership teams on why and how they should be engaged in cybersecurity governance and risk management. This is because without their support your cybersecurity program will fail. We also advise that you let everyone know what their role in cybersecurity is and to make sure that they know what your policies are, how to locate them and how to comply with them. Make it easy for everyone to understand and fulfill management’s expectations when it comes to cybersecurity.”
>
> **Carlos Rodriguez,** CISSP, CISM, CDPSE
> CEO & vCISO / CA2Security



Compliance & governance

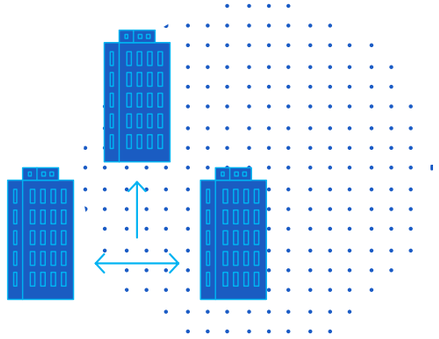
Compliance addresses two areas: applicable regulations and reputable security frameworks such as PCI-DSS, HIPAA, GDPR, ISO, NIST, and SOC 2. It is important to understand that compliance services are no longer the province of large organizations or those in heavily regulated markets. As large businesses adopt cybersecurity and compliance frameworks and agree to certain standards (or are required by law to comply to various regulations), they are imposing these requirements on their suppliers. In turn, those suppliers pass on compliance needs to smaller partners. Therefore, many small businesses are being asked to show evidence that they have fulfilled compliance and cybersecurity standards. Requests for Proposals (RFPs) often falter due to lack of adherence to a specific framework. When SMBs are asked to demonstrate compliance to frameworks such as the Center for Internet Security Controls (CIS) or NIST, they face significant disruption in terms of time, money, and key personnel. Some are forced to let lucrative contracts go due to the burden of these requirements. Forward-thinking vCISO providers, therefore, are poised to capitalize on a supply/demand imbalance in compliance services. According to McKinsey, the governance, risk and compliance sector currently only has about 30% software/service penetration yet it represents a $100 billion addressable market. This is a major opportunity for vCISO providers that can broaden their offerings to encompass compliance.



Incident response

vCISO are responsible for the response in the first 24-48 of an attack. After taking care of immediate threats, the vCISO needs to take the time to prepare the organization to minimize the impact of future threats. This entails the development of a cybersecurity incident response plan, the assigning of roles and responsibilities throughout the IT and cybersecurity teams on who does what in case of a cyber incident, and engaging with third parties to support remediation and recovery. Personnel should also be drilled on incident response using table-top exercises. Make sure, too, that company data is accessible as part of attack containment. That requires an updated asset inventory and network diagram, as well as adequate logging and monitoring capabilities of sensitive assets.

> “The vCISO is not necessarily the one who handles incidents in real-time when they happen, but it’s the vCISO’s responsibility to oversee these activities and ensure the organization is prepared for such a scenario and that everyone knows their role in this situation.”
>
> **Brent Forrest**, CCISO
> Field CISO / Flair Data Systems



Third party management

Another important duty of the vCISO is to manage any security risk posed by third parties. Most businesses have a variety of third parties they interact with such as supply chain partners, software provides, Software-as-a-Service (SaaS) vendors, cloud providers, and other service providers. The vCISO must ensure they take adequate precautions to prevent their connectivity to the enterprise from becoming a conduit for a breach. Their privileges should be narrowly defined and they should be required to log in via multi-factor authentication.

> “Considering the growing supply chain threats and incidents from past years, I believe vendor security is a paramount challenge that organizations are scrambling to address. Helping to manage this risk with vCISO services is a unique way providers can position themselves as indispensable to their clients.”
>
> **Jesse Miller**
> Principal Consultant, Helping MSPs build and scale security services / PowerPSA



Communication

The vCISO is a leader who manages, oversees, and sets the strategic direction. This encompasses strategic planning for cybersecurity, execution of plans, monitoring the implementation of cybersecurity technologies, and the setting of cybersecurity policy.

Central to this is security-to-IT mapping. The vCISO ensures alignment between security and enterprise architectures, verifies that security and IT teams are fully coordinated, and that the various MSPs, MSSPs, and SaaS services in play within the enterprise are working smoothly together.

What sets a full-fledged vCISO apart is understanding of the business. Therefore, the following factors should impact most vCISO decisions:

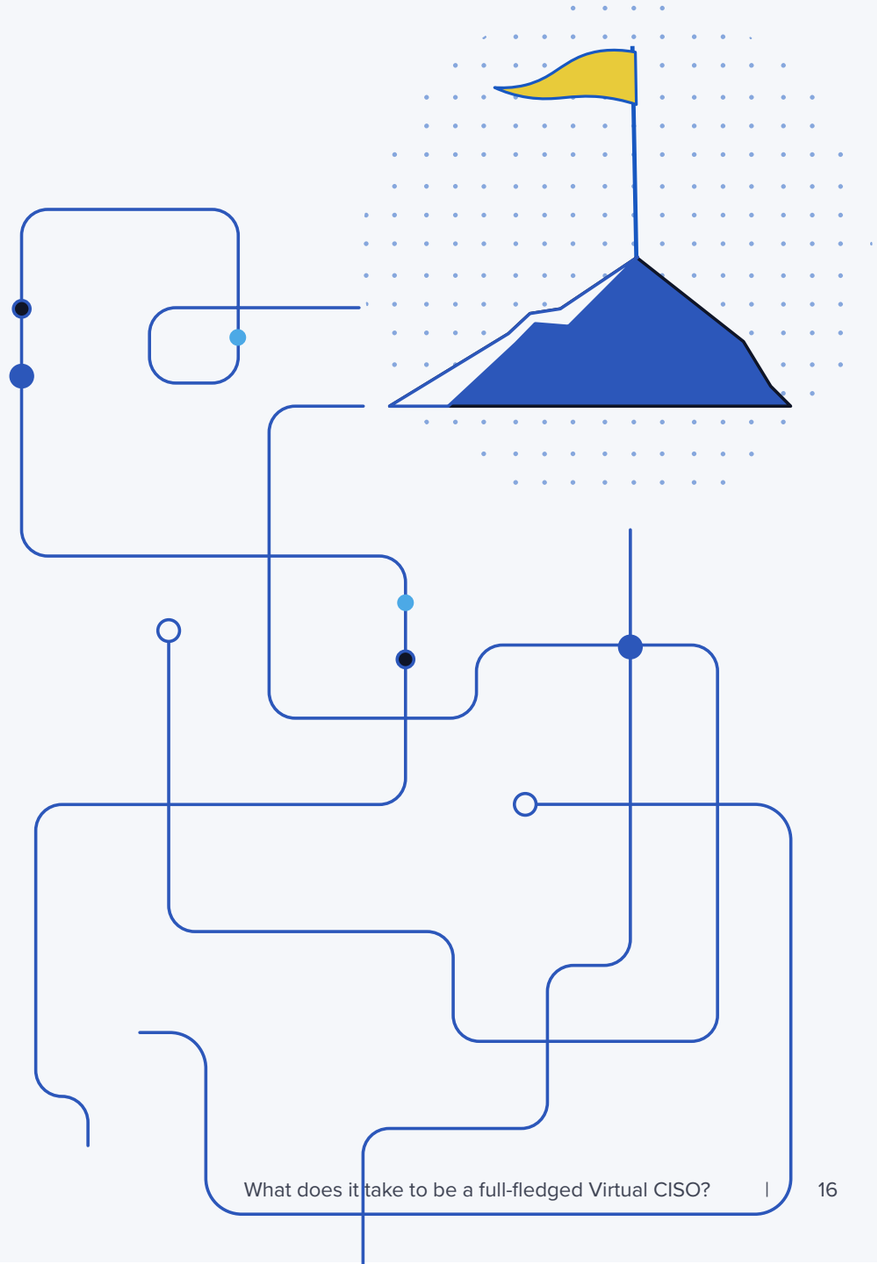
- Understanding mission and objectives of the business
- Understanding risk appetite of the customer
- Reporting and liaising with top management and the board of directors
- Communicating effectively with management
- Guiding management on how best to communicate cyber-guidance to employees

The vCISO can also use reports on the state of risk to highlight steady improvement over time. This provides tangible evidence of the value of existing services as an aid to contract renewal.

The challenges in providing holistic vCISO services

Each of the above elements provides value to customers. Those that offer the entirety of these functions can achieve the highest margins. But that is easier said than done.

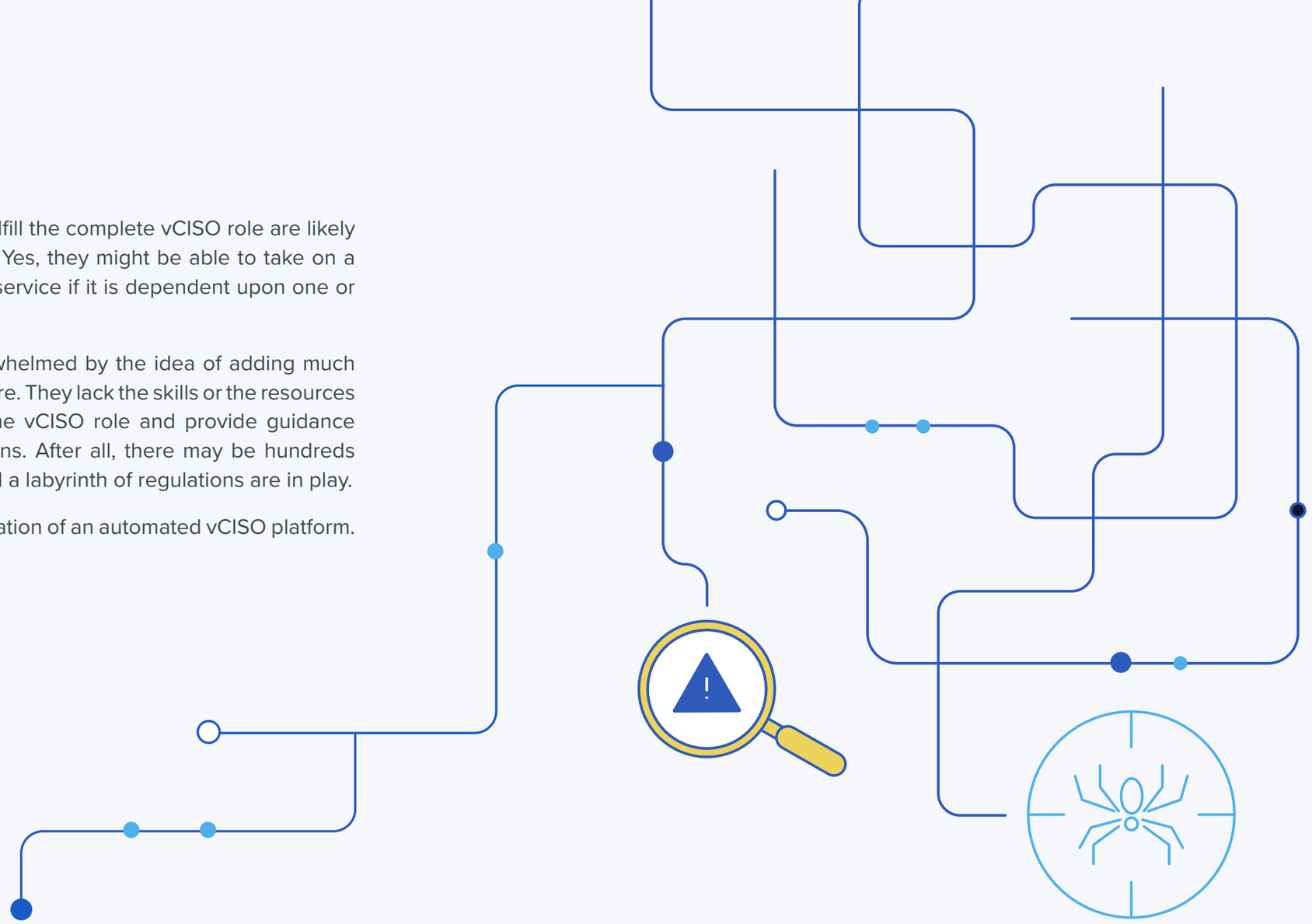
Some service providers are comfortable with what they are currently providing and may be reluctant to expand. They are unsure where to start from and how to structure additional vCISO services. In any case, many lack the cybersecurity, executive, and project management skills to be able to function competently as an end-to-end vCISO, and significant upfront investment may be needed to launch a full-fledged vCISO practice.



But even those that have personnel that can fulfill the complete vCISO role are likely to hold back due to scalability considerations. Yes, they might be able to take on a couple of clients. But how can they scale that service if it is dependent upon one or two highly trained resources?

No wonder some MSPs and MSSPs feel overwhelmed by the idea of adding much broader vCISO services to their existing repertoire. They lack the skills or the resources to be able to confidently span all facets of the vCISO role and provide guidance concerning relevant frameworks and regulations. After all, there may be hundreds of points to address within each framework and a labyrinth of regulations are in play.

The answer to these concerns is the implementation of an automated vCISO platform.



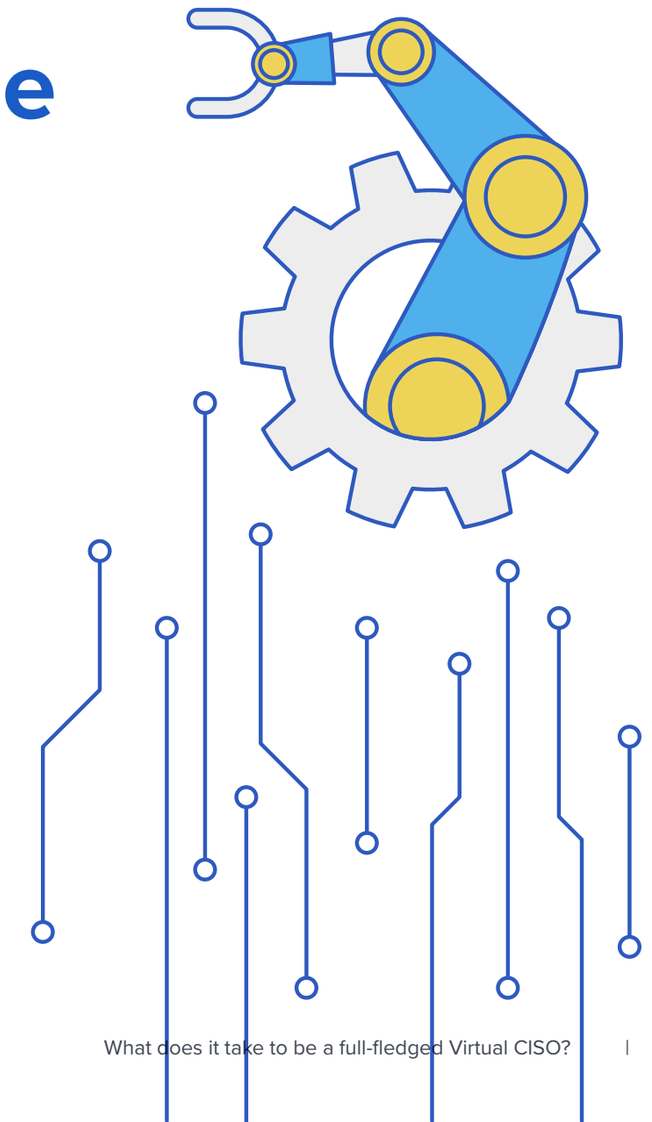
Automated cybersecurity and compliance platforms emerge

vCISO platforms now exist that can take the MSPs and MSSPs from where they currently to being able to cover all aspects of vCISO services. vCISO platforms:

- Encompass automating the knowledge and knowhow of experienced CISOs
- Automate the manual time-consuming tasks of the vCISO and streamline the work processes
- Follow a wide range of official cybersecurity frameworks
- Automatically create remediation plans and map tasks to official frameworks
- Show improvement over time
- Help prepare customers for an audit
- Enable vCISO service providers to expand their customer base
- Bridge the gap between security and compliance
- Do all that in a multi-tenant manner as they were designed for vCISOs

These platforms provide the secret of how vCISOs can add compliance, risk management, audit preparedness, technology evaluation, business continuity, financial management, and governance services without the need to add personnel or increase costs.

This represents an area with major upsell potential. Those already providing security risk assessments, compliance services, or other aspects of the vCISO role can use these platforms to expand their offerings effortlessly into the delivery of comprehensive vCISO services.



Cynomi’s vCISO Platform

Cynomi’s vCISO platform streamlines the work of vCISOs. It enables MSSPs, MSPs and consultancies to offer more efficient vCISO services to their clients at scale, growing their revenue and reducing operational costs.

By combining proprietary AI algorithms with CISO-level knowledge, it provides proactive cyber resilience, without the need to add extra resources. Automation eliminates up to 70% of manual, time-consuming tasks such as risk assessment, compliance readiness, cyber posture reporting, creation of tailored security policies and remediation plans, and task management optimization.

The Cynomi platform sets standards for vCISO service processes and deliverables, ensuring consistency and enabling service providers to bridge the skill gap. Through easy-to-digest reporting, it helps vendors show progress over time, supports upselling and enhances their differentiation.

Built exclusively for service providers and consultancies, Cynomi’s multitenant vCISO platform helps vendors expand into offering vCISO services or scale those services without the need for additional headcount.

For more information, visit www.cynomi.com

