cynomi

How vCISOs can extend their services from security into compliance readiness without increasing cost



Introduction

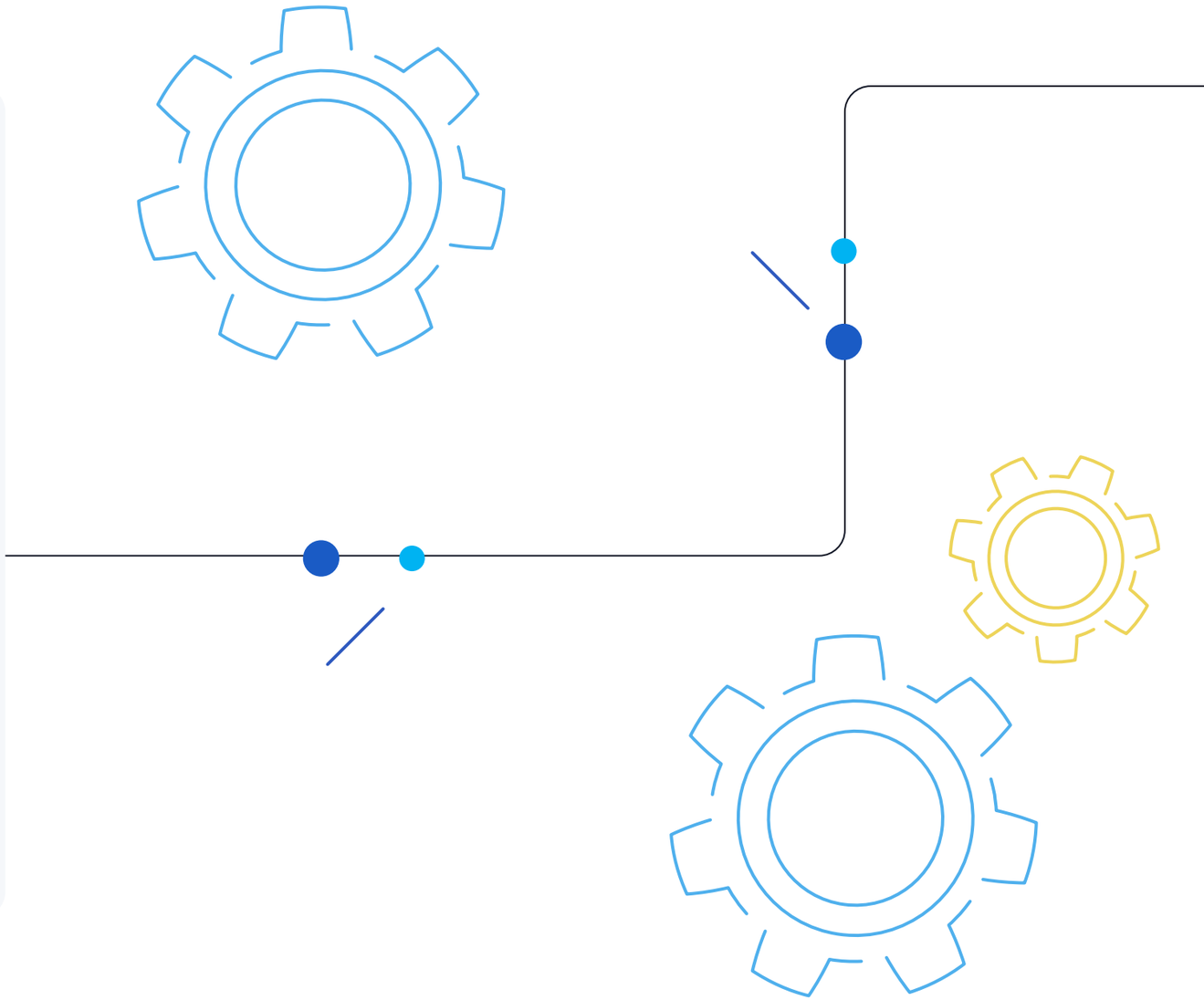
A growing number of security and IT service providers offer Virtual Chief Information Security Officer (vCISO) services. Instead of hiring a full-time CISO, businesses pay a subscription or retainer to gain access to expert C-level cyber-assistance in devising and implementing strategies to prevent breaches, reduce risk, and mitigate the consequences of attacks. These virtual security executives perform a vital role in building a comprehensive cybersecurity program. They 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.

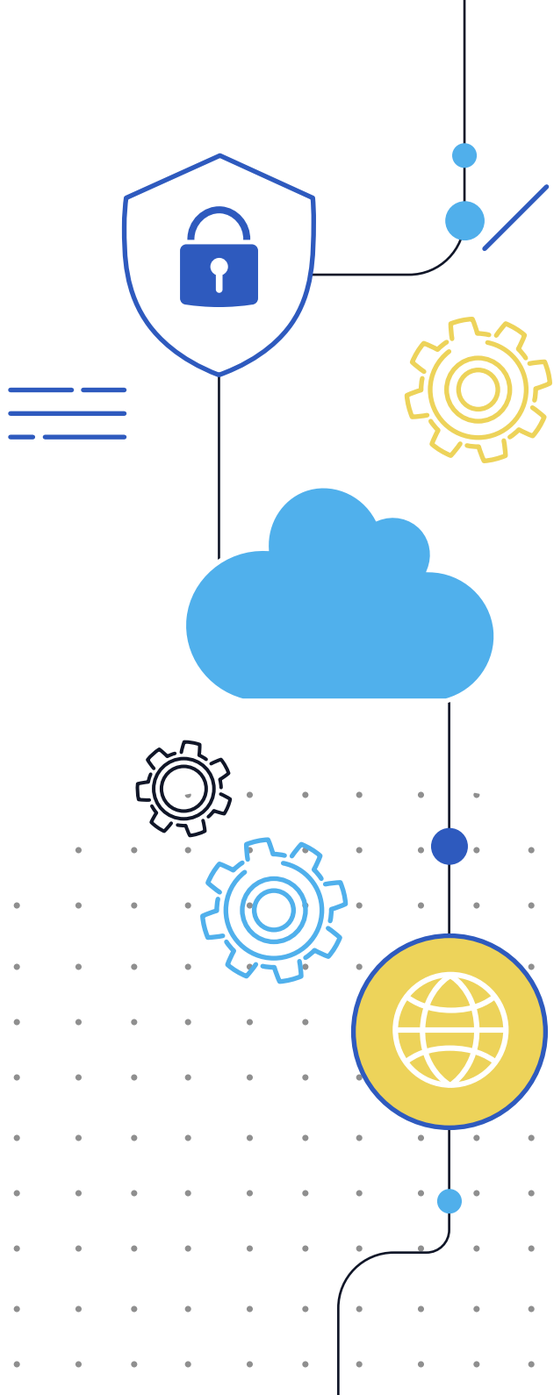
To receive compliance and audit preparedness services, businesses contract with consultants and compliance service firms to help them comply with applicable regulations, implement different security frameworks, and prepare for audits. Thus, compliance represents a ripe area for vCISO provider expansion. Those delivering vCISO services can add value and extend their service portfolio by adding compliance-related services. While there may be a learning curve and some adjustments to be made, compliance is a natural extension of the security function. It is a transition that vCISO providers should be able to make far more easily than attempting to extend into other zones of security.



In this guide we explain:

- What compliance services are
- How vCISO providers can add value to the compliance sector
- What the different compliance frameworks are and how they fit in with the CISO role
- The upsell potential of compliance services
- How compliance services tie into audit preparedness
- How vCISOs in possession of detailed security assessments are well-positioned to provide compliance services
- The platforms that can help vCISO providers automate security and compliance

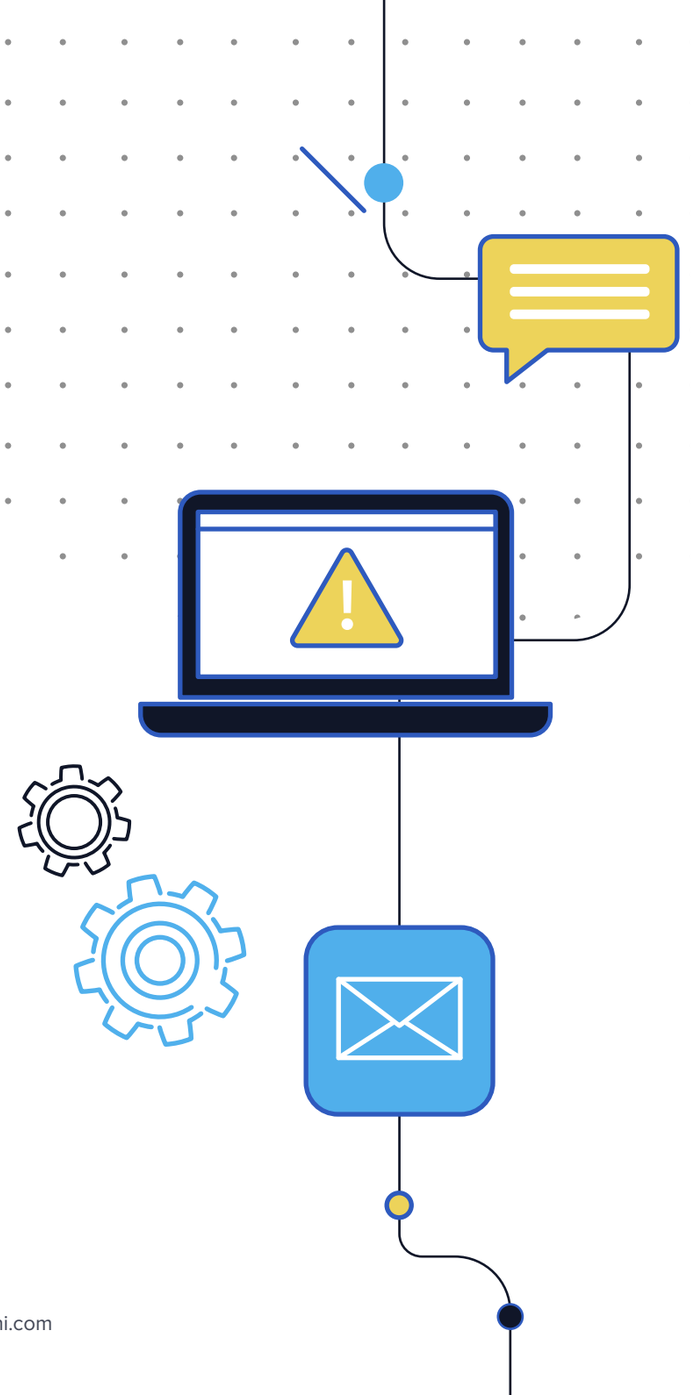




Compliance Services are Booming

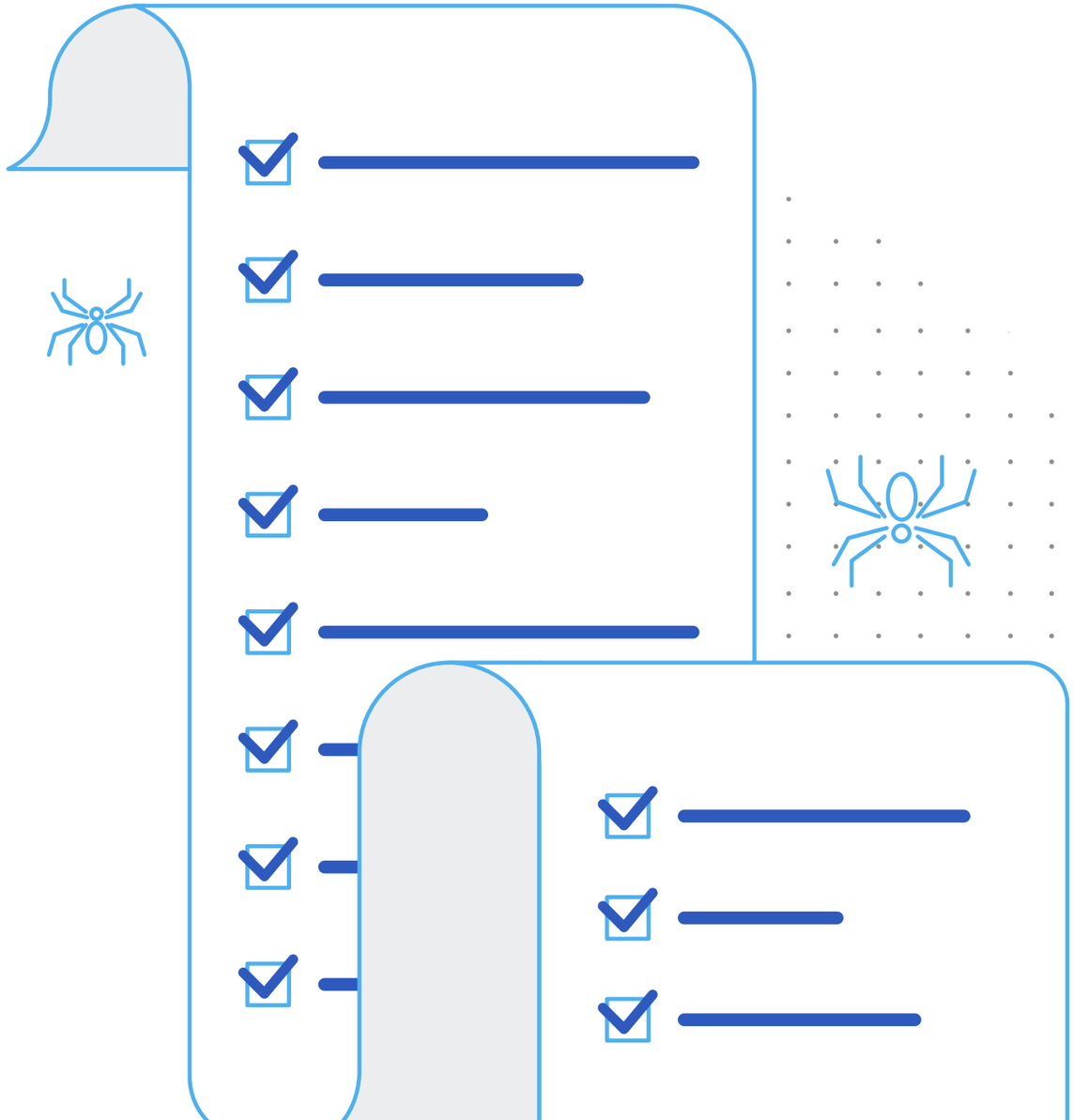
Compliance services are emerging as one of the hottest areas of cybersecurity. According to McKinsey, the governance, risk and compliance sector currently only has about a 30% software/service penetration yet it represents a $100 billion addressable market. This is a major opportunity for vCISO providers if they can broaden their offerings to encompass compliance.

Compliance services cover a wide range of different security frameworks and regulations. This includes PCI-DSS, HIPAA, HITECH, GDPR, ISO 27001, NIST, SEC, SoC 1, and SOC 2. Some services only determine which areas that are in compliance with a certain standard and where the organization is out of compliance. Others extend further to remediation of all points necessary for compliance. There are services, too, that prepare organizations in advance of an audit. A few also provide certification of compliance.



Which companies need it? Compliance used to mainly be the province of large enterprises. But demand is steadily making its way down the food chain and all across the supply chain. 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 similar standards and demands on their suppliers. In turn, large suppliers pass on compliance needs to smaller partners. Many businesses now require that prospective vendors show evidence that they have achieved minimum compliance and cybersecurity standards. Requests for Proposals (RFPs) often falter due to lack of adherence to a specific framework. Additional factors include regulatory pressures specific to certain industries and cyber-insurers demanding that policy holders adhere to certain security frameworks. This shift in the market is driving a rising need for compliance services.

This poses a problem for small and mid-sized businesses. When SMBs are asked to demonstrate compliance to frameworks such as the Center for Internet Security Controls (CIS) or the National Institute of Standards and Technology (NIST), they face significant disruption in terms of time, money, and key personnel. They are hard pressed to do it alone. Some are forced to let lucrative contracts go due to the burden of compliance requirements. Forward-thinking vCISO providers, therefore, are poised to capitalize on a supply/demand imbalance in compliance services.



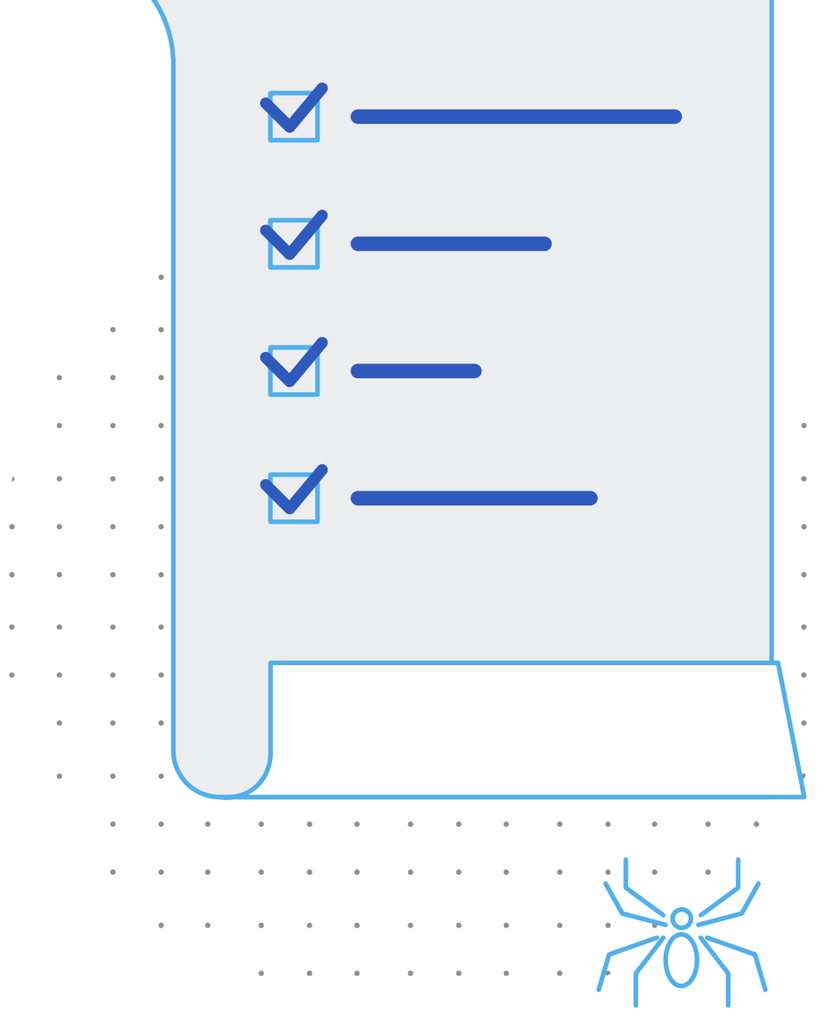
How vCISOs Add Value to Compliance

Compliance alone can be a dry and dreary subject. Too often, it becomes a case of endless ticking of boxes and engaging in laborious documentation. One reason for this is the chasm that sometimes exists between security and compliance. Those working on compliance can sometimes carry out their actions in a way that is largely divorced from the needs of cybersecurity. Yes, these actions ultimately help make the organization more secure. But their efforts can sometimes place so much emphasis on arriving at 100% compliance that urgent threats in today's hostile cyber environment may not receive sufficient priority. The reality of the hostility of current-day cyber-environments can sometimes be lost by those checking boxes on a lengthy compliance checklist.

On the other side of the coin, those in security focus may not pay enough attention to compliance. Their attention is on where the biggest risks are, how to minimize them, remediation of threats, and finding ways to further safeguard the organization. Compliance is often an afterthought. Although the organization may believe it is generally following a certain security framework or standard, it may not have any real idea how well or poorly it is doing on the compliance front. Outside compliance specialists are brought in to bridge the gap.

This is where the vCISO has an advantage. Instead of compliance being thought of as a separate function, the vCISO provider has the potential to unify both fields. Rather than receiving a report showing which boxes have been ticked and which are out of compliance, vCISOs can help their clients to significantly improve their cybersecurity posture, and minimize the level of risk while enhancing compliance. Compliance is often a by-product of security.

The end-to-end cybersecurity knowledge of the vCISO can be harnessed to simplify processes that take the enterprise far along its journey toward full compliance and prepare the organization for a scheduled audit.



What are Compliance Frameworks?

Compliance falls into two camps – regulatory and framework-based. This guide focuses primarily on the latter category as a great many compliance initiatives are standardized around compliance frameworks.

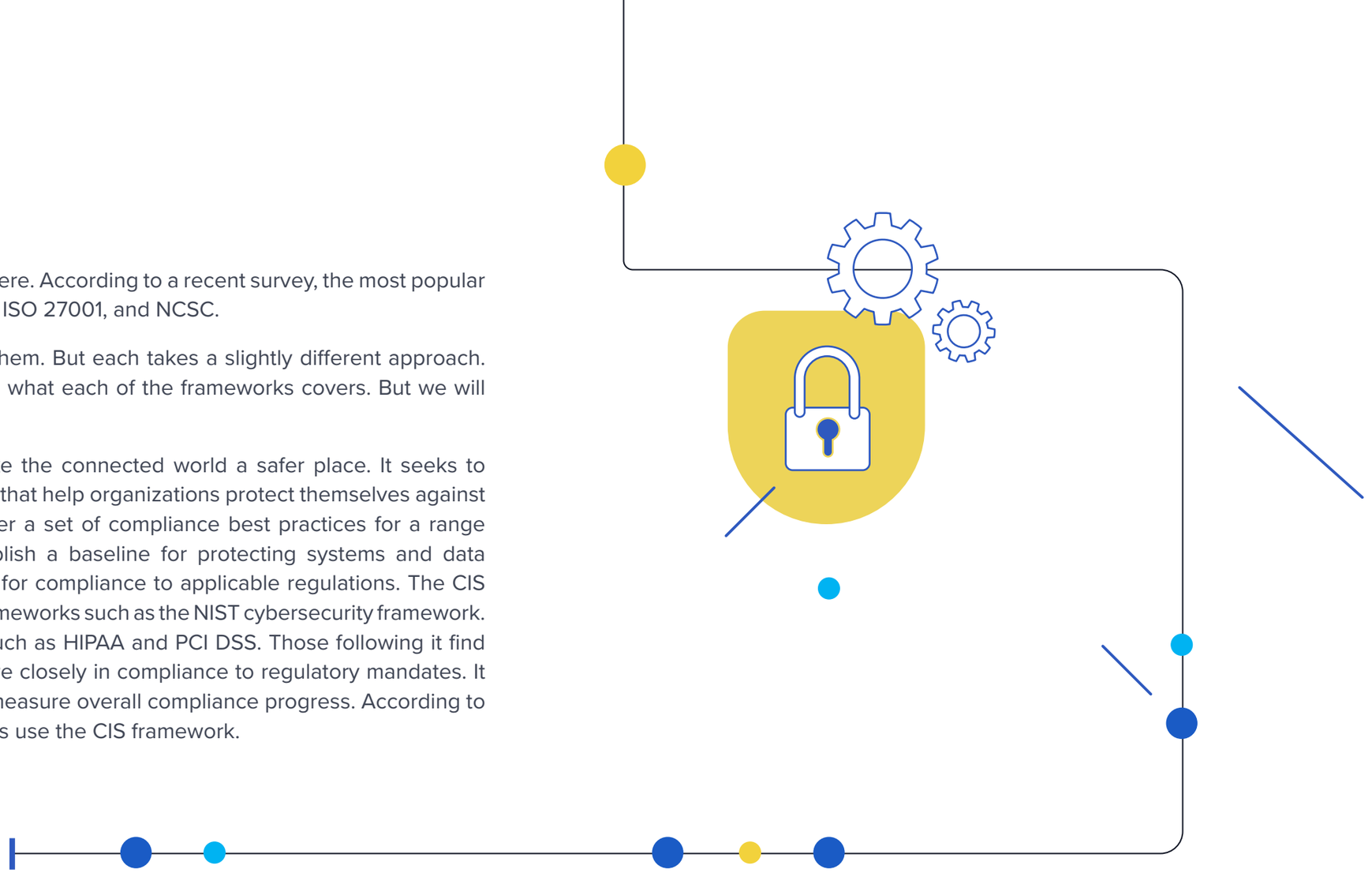
A compliance framework is a highly structured group of guidelines detailing an organization's processes for maintaining a certain standard in cybersecurity, implementing best practices in security, and adhering to regulations, specifications, or legislation. A framework helps the organization to achieve a more coherent picture of the existing compliance posture and serves to highlight the steps that must be implemented to achieve an improved cybersecurity posture. In addition, a framework serves as a tool to assist in managing and minimizing compliance risk, and in implementing any needed changes to align with new or existing regulations. In essence, it provides a standard against which the organization's compliance posture can be judged. By mapping compliance efforts to the requirements of a cybersecurity framework, organizations can demonstrate their commitment to certain standards, and gauge how much progress they have made.



There are a great many frameworks out there. According to a recent survey, the most popular frameworks are CIS, CMMC, COBIT, NIST, ISO 27001, and NCSC.

There is a great deal of overlap among them. But each takes a slightly different approach. The purpose of this guide is not to detail what each of the frameworks covers. But we will summarize one as an example.

CIS is a nonprofit with a mission to make the connected world a safer place. It seeks to achieve this by developing best practices that help organizations protect themselves against cyber threats. CIS benchmarks, then, offer a set of compliance best practices for a range of IT systems and products. They establish a baseline for protecting systems and data from cyberattack and help pave the way for compliance to applicable regulations. The CIS framework is aligned closely with other frameworks such as the NIST cybersecurity framework. It is also aligned to various regulations such as HIPAA and PCI DSS. Those following it find their business both more secure and more closely in compliance to regulatory mandates. It is arranged so that the organization can measure overall compliance progress. According to surveys, more than a third of organizations use the CIS framework.



The Upsell Potential of Compliance Services

As noted above, the governance, risk, and compliance sector has massive market potential – as much as $100 billion. It is far from saturated. It currently only has a 30% software/service penetration. Further, McKinsey noted that the MSSP/outsourcing space only has a 5% to 10% penetration rate and represents a colossal $400-$500 billion opportunity.

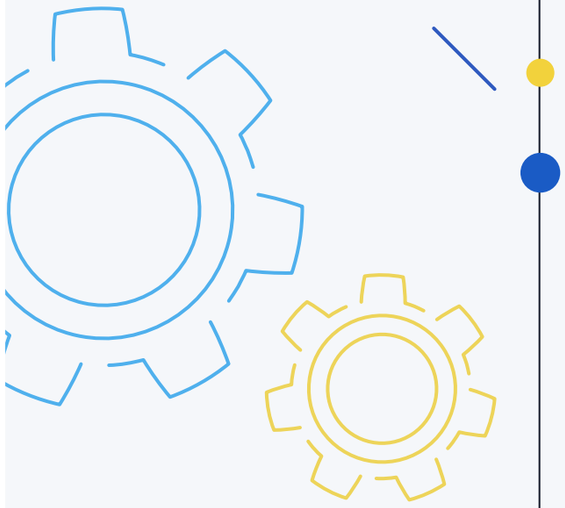
Cybersecurity, after all, affects every facet of an organization. Compliance is often a by-product of ongoing security initiatives.

Those offering vCISO services, therefore, are in a strong position to capitalize on opportunities in both the security and compliance spaces.



Here are just a few factors to highlight the upsell potential of compliance services for vCISO providers:

- The combination of security and compliance is unusual and one that will prove popular in the marketplace – many compliance firms don't offer cybersecurity protection.
- Adherence to a rich cybersecurity framework that includes a great many requirements and best practices is lucrative business for a service provider as there are so many more tasks to implement.
- When the vCISO sees the need to add additional remediation services, the compliance element gives an extra lever to help with the upsell.
- By integrating a security plan with a cybersecurity framework such as NIST or CIS, the recommendations of the vCISO carry more weight in the board room.
- As many vendors that provide vCISO services also provide other security products and services, working on compliance and exposing the gaps/flaws offers an opportunity to sell additional products and services.
- Reporting against compliance progress is a good way for vCISOs to highlight steady improvement over time as evidence of the value of existing services as an aid to contract renewal.

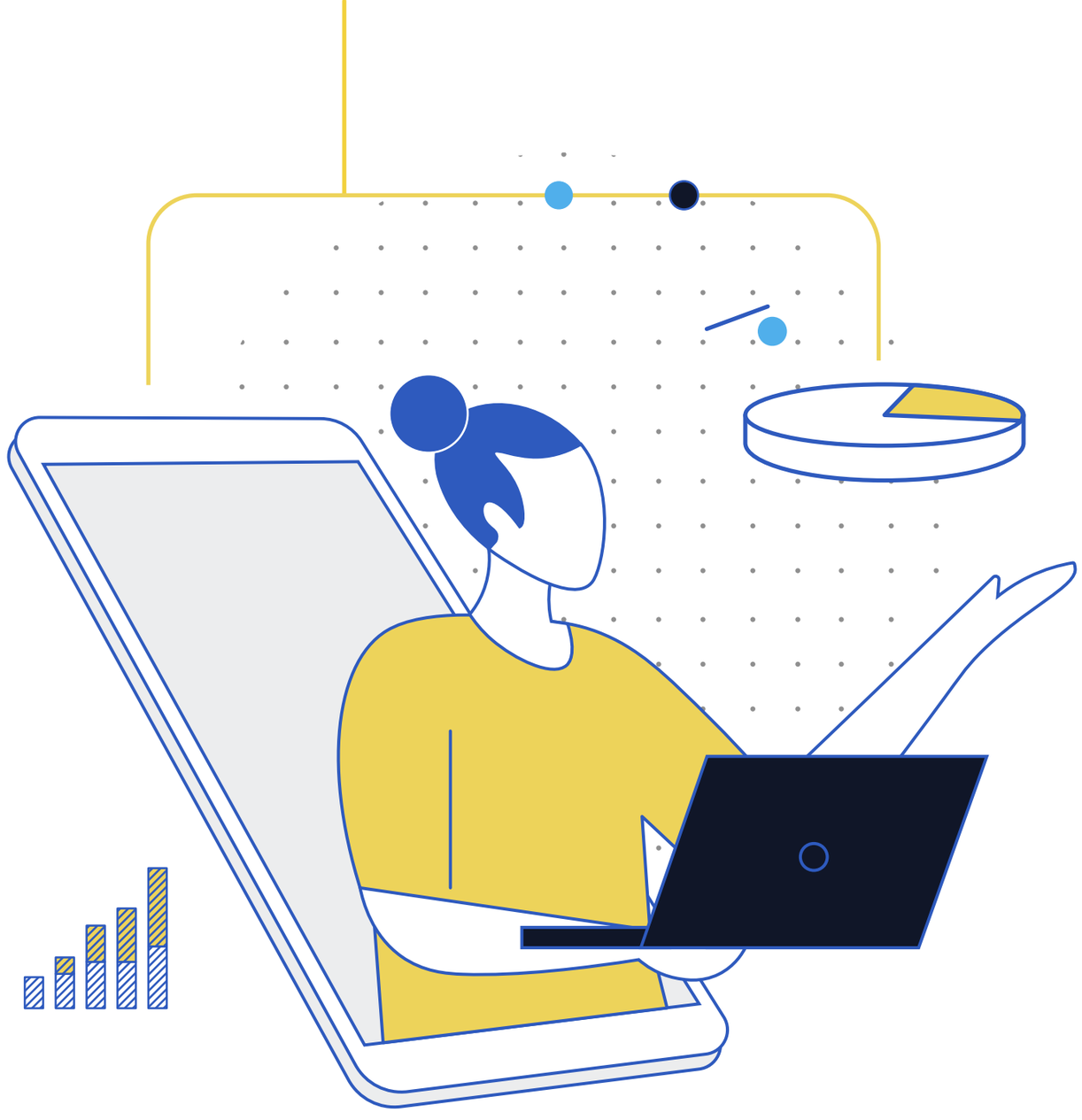


Here are a few factors to highlight the importance of compliance services for vCISO customers:

- Regulatory bodies and many potential clients (especially larger accounts) often insist that their vendors' level of cybersecurity matches theirs across the supply chain. They are demanding that vendors achieve minimum compliance to cybersecurity standards.
- The compliance burden has risen as one vendor may be required to comply with framework X by one customer and framework Y by another. Thus, companies of all sizes face the prospect of demonstrating maintain compliance across a range of frameworks and standards.
- Most SMBs lack the skills and manpower to address compliance requirements.
- To gain a major order, SMBs may be in a hurry to achieve compliance.
- Those businesses following a well-known framework have an easy way to demonstrate to potential customers that they can be trusted to handle cyber security.

vCISOs, therefore, have it in their power to make life much easier for small and midsized businesses, and existing clients, by helping them to understand where they are in their compliance journeys and how they can achieve the next level. By working with the vCISO, these organizations can be given a strategic roadmap that takes them step by step towards full compliance without losing sight of the need to address urgent cybersecurity matters.

By mapping security functions to compliance frameworks, the vCISO can show how compliant an organization is, what else it needs to be fixed to be compliant, and can provide compliance reports based on whatever framework a client demands. This kind of flexibility makes it easier for the vCISO to deliver compliance services without having to add personnel.

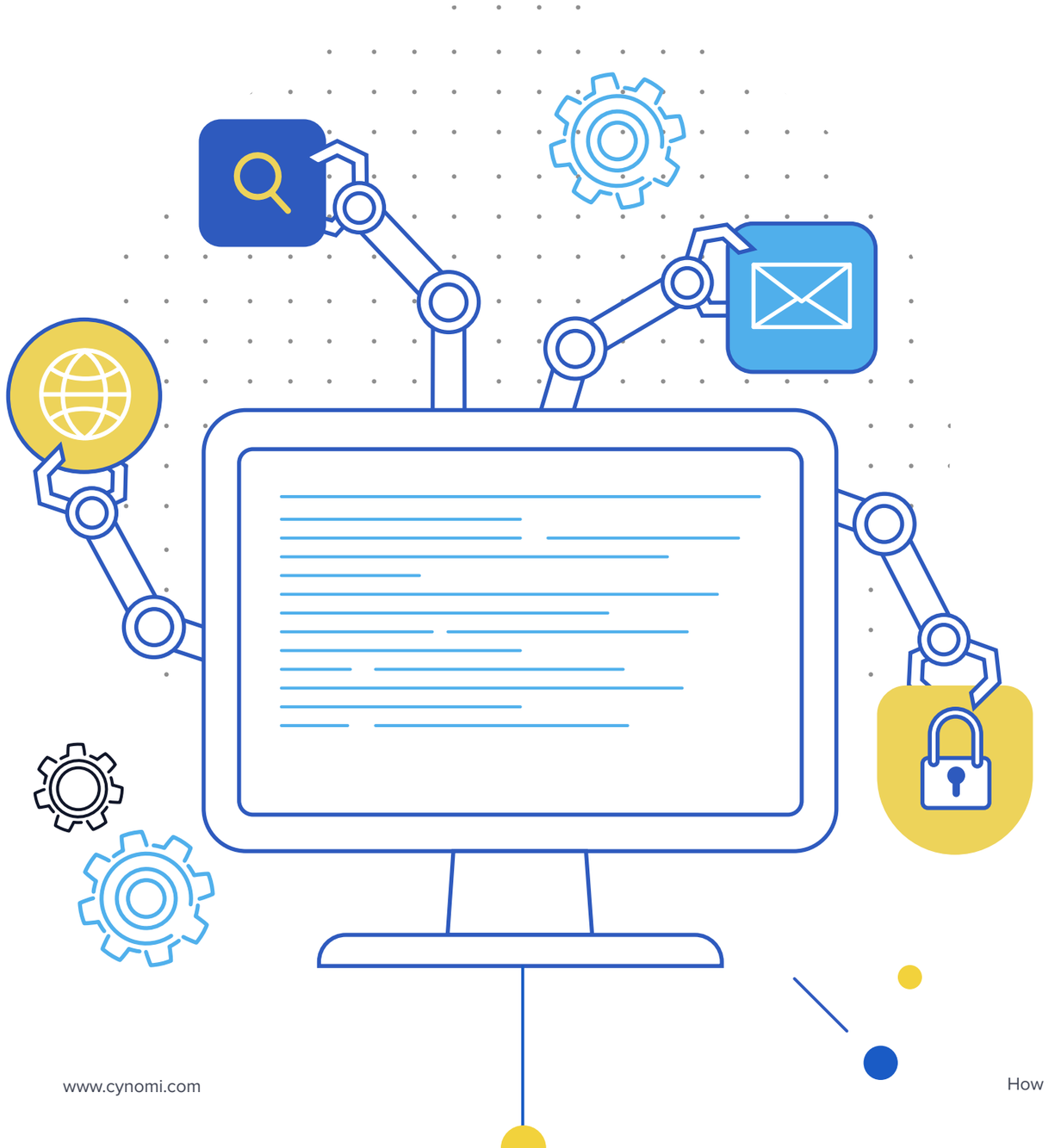


Audit Preparation

Compliance isn't the only market the vCISO can invade. A related area – audit preparation – has similar needs to those of cybersecurity framework compliance. Companies preparing for an audit spend a tremendous amount of time and money getting ready, conducting compliance assessments, and addressing issues that need to be fixed before the audit occurs. This growing niche of cybersecurity and regulatory audit preparedness is currently served by software tools and consultant services that help the company get ready for an upcoming audit.

vCISOs can take care of much of the audit preparation function by mapping ongoing security actions to applicable compliance frameworks, highlighting exactly where there are missing compliance elements, and drawing up plans to get these points in.

Additionally, reports can be automatically generated based on the framework to be used in the audit. This can bring big savings by eliminating the need to buy compliance and audit preparation software or hire expensive consultants, as well as on audit fees. As the organization is better prepared for the audit, it will go much faster and therefore cost less.



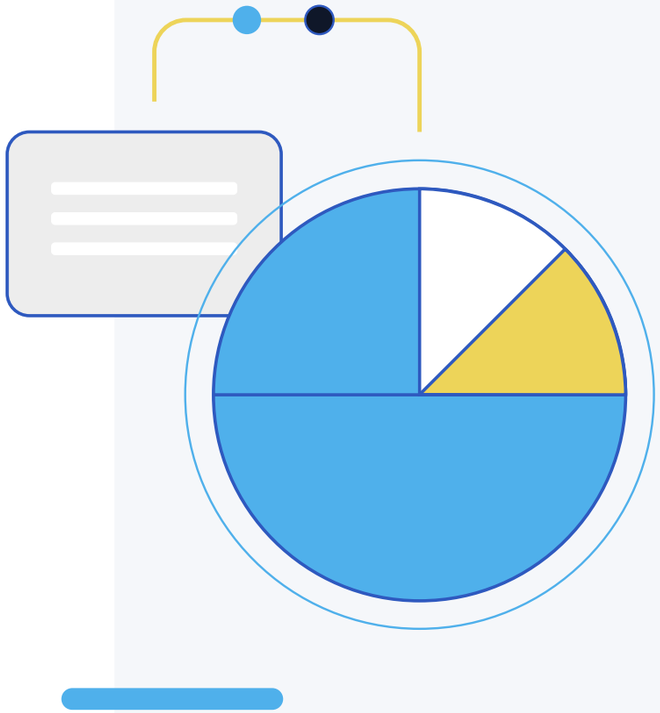
Automated Cybersecurity and Compliance Platforms Emerge

Some vCISOs may initially feel overwhelmed by the idea of adding compliance and audit preparedness services to their existing repertoire. The obvious worry would be the skill level required to know all relevant compliance frameworks and cybersecurity regulations, as well as the time involved in reviewing hundreds of points within each framework and the endless clauses and subclauses listed out in different regulations.

Fortunately, vCISO platforms are emerging that integrate the compliance function and automate much of the work.

- They follow a wide range of official cybersecurity frameworks.
- They automatically map the security plans of vCISOs directly into official frameworks.
- They create plans based on whatever framework the customer prefers, or a different framework demanded by one of their customers.
- They show improvement over time.
- They help prepare customers for an audit.
- They enable vCISOs to increase the number of accounts by expanding the customer base.
- They eliminate excel sheets and manual processes.
- They bridge the gap between security and compliance.
- They 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 and audit preparedness services without the need to add personnel or increase costs.



Cynomi's vCISO Platform

Cynomi's vCISO Platform streamlines the security and compliance work of vCISOs, allowing MSSPs, MSPs and consultancies to offer vCISO services to their clients at scale without adding extra resources. This automated platform enables vCISOs to extend their security services into compliance assessment and audit preparation while requiring nominal effort. It aligns with a wide range of official cybersecurity frameworks including CISV8, ISO 27001, NIST-CSF, NIST-SSDF and SOC 2. By following these frameworks, customer trust is enhanced. Cynomi automatically maps vCISO security plans to official frameworks and can be used to provide reports aligned to any framework demanded by a potential customer. Based on the assessment process, the system automatically classifies the controls into those that are not relevant to the company, those that have already been implemented, and those that need to be implemented. In this way, the user focuses on the open tasks only, without the need to fill in Excel sheets. Dashboards in the Cynomi platform show a compliance overview of multiple frameworks, including maturity level (if relevant). While users work on their security plan, they can check if the plan is related to one or more frameworks, and create a framework-based plan.

For more information, visit www.cynomi.com

