cynomi

Power PSA CONSULTING

Playbook

Your First 100 Days as a vCISO - 5 Steps to Success

Introduction:

Cyber attacks cast a wide net, and no organization is spared from their potential reach. But not all organizations have the ability to support a full-time in-house CISO with top tier security services.

That's where you come in - the vCISO establishes, develops and builds the organization's cybersecurity infrastructure and strategy, combining both strategic direction and actionable cybersecurity services.

Just like any other organizational leader, vCISOs need to navigate their professional responsibilities, business needs, the various personas in the organizations and leadership requirements, all while fostering trust and positioning themselves as a reliable strategic decision maker.

A 100-day plan serves as an effective framework for achieving significant milestones in a new company. It proposes actions that can help determine clear goals, which steps to take and how to generate stakeholder engagement. This is the groundwork for long-term success.

This guide provides a five-step 100-day action plan designed to help you succeed. It was developed based on the combined professional knowledge and experience of Cynomi and PowerPSA. We have worked with hundreds of vCISOs who have catered to businesses of all sizes, effectively accompanying them throughout their journey to provide top-tier and solid vCISO services.

The guide starts with in-depth research into the company's current security posture and business objectives. This is followed by a comprehensive understanding and gap analysis. Next, it emphasizes prioritizing and strategizing immediate and long-term security needs and executing the remediation plan with clear communication and management buy-in. Finally, the last step details how to report on the strategy's effectiveness and ensure ongoing improvement.

Follow this guide and position yourself as a strategic partner capable of driving security transformation and managing security continuously and dynamically.

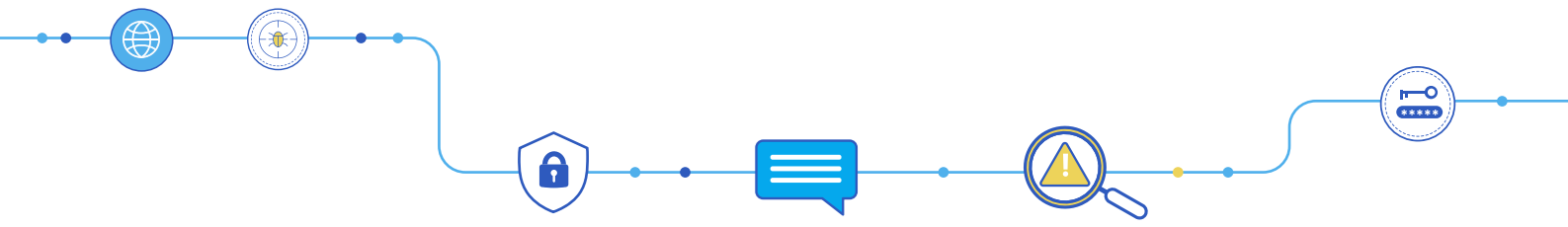
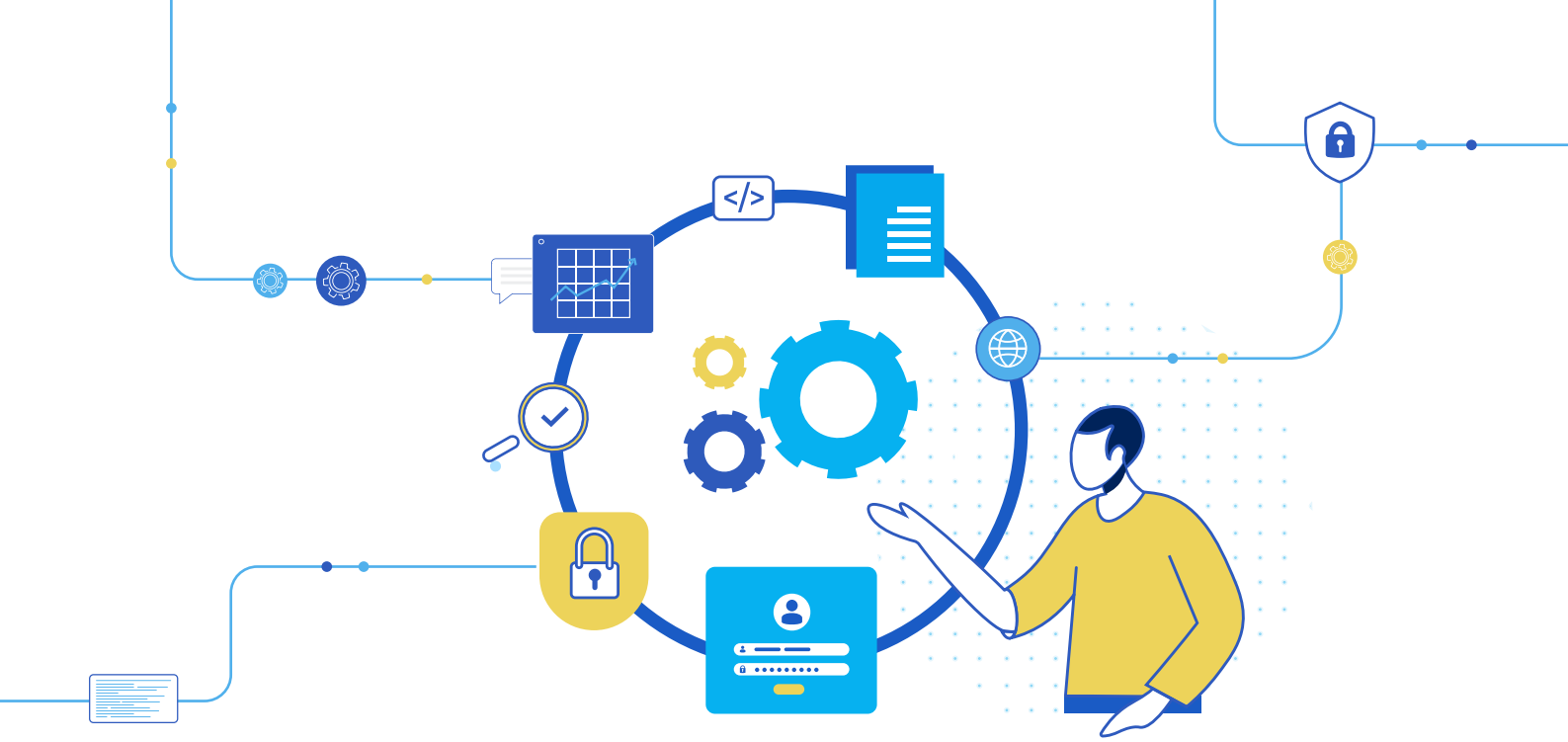


Table of Contents



Spotlight: What is a vCISO

A vCISO (Virtual Chief Information Security Officer) is an external executive-level professional who offers both strategic guidance and practical cybersecurity services to companies. Acting in a capacity similar to a traditional CISO, a vCISO brings organizations the flexibility of working part-time, remotely, or on a project basis. This is particularly advantageous for small to mid-sized enterprises that require top-tier cybersecurity services but may not have the resources for a dedicated full-time position.

The responsibilities of a vCISO include the development and management of a cybersecurity strategy, risk and vulnerability management, incident response planning, security training, compliance ownership, budget and vendor management, and more.

To learn more about the vCISO's roles & responsibilities, download the eBook: What does it take to be a full-fledged virtual CISO?

Download the eBook

As a vCISO, we recommend steering clear of stretching your services too thin across multiple industries. Clearly define your ICP (Ideal Customer Profile) to ensure a focused and specialized approach that leverages your experience and knowledge and emphasizes your value.

vCISO Goals

Before we dive into the practical steps, let’s take a look at the overarching goals of the vCISO throughout the first 100 days and beyond. These goals should guide us when executing the detailed steps.

1.

Establish, Oversee and Manage Organizational Security

As a vCISO, your primary and most important goal is to establish and maintain the organization's security posture in the dynamic threat landscape. The role requires an understanding of technological security requirements, the organization’s business objectives and the balance between them. A vCISO is a key player in establishing a robust, yet flexible, security strategy.

2.

Foster Trust with Security Goals

Security cannot operate in a silo. Therefore, the vCISO needs to ensure the entire organization is aligned with the security goals and what can be expected from security activities. Alignment is necessary for getting leadership and stakeholder buy-in, which ensures cross-department collaboration and teamwork and the ability to promote and execute security decisions and processes.

3.

Make Security a Business Enabler

The vCISO needs to ensure the technicalities of cybersecurity contribute to the goals of the business: compliance, operational efficiency, a competitive advantage, financial responsibility, and more. This not only helps build trust in security, it also ensures the right security decisions are being made for this specific business.

Pitfalls to Avoid

Being a vCISO is a high-demanding and strategic job. That's why it's important to always keep your eye on the ball (the goals listed above). Here are some pitfalls that might take you off track, so be sure to avoid them as much as possible.

→ Putting out fires

As a vCISO, your goal is to be strategic. However, you might find yourself in reactionary mode, rather than planning. Stay strategic, otherwise, you won't be able to effectively meet your goals. This will impact the organization's security posture, as well as how your customers perceive your capabilities.

→ Getting caught up in organizational politics

Maintain your objectivity and focus on security outcomes. Your outsider stance lets you avoid getting tangled in internal disputes that can impact your ability to deliver.

→ Using manual processes instead of automation

Automation is a necessity in cybersecurity. Manual processes are time-consuming, error-prone, and inefficient compared to automated systems that keep you on track and ensure standardization.

→ Forgetting about compliance

Being compliant ensures the organization aligns with relevant laws, regulations, and industry standards. This is important for avoiding grave legal and reputational consequences. Compliance is also a prerequisite from some clients.

→ Doing everything yourself

As mentioned above, the role of the vCISO is strategic, not tactical. Therefore, doing everything yourself instead of delegating and building infrastructure is counterproductive. Technical vCISOs are especially at risk of falling into this pitfall.

→ Forgetting to set expectations with the client

Set expectations as early as the sales process to maintain a clear division of roles and responsibilities. Clients may sometimes have unrealistic expectations, believing the vCISO will engage in both the strategy and hands-on cyber engineering.

→ Being too dogmatic

Security measures should facilitate business objectives, not stifle them. Keep a flexible, open-minded approach that adapts to the needs of each business unit.

→ Avoiding challenging paradigms and decisions

Being flexible does not mean shying away from challenging established norms or practices, if they present security risks. This could involve difficult conversations with stakeholders to articulate and manage risk effectively.

→ Juggling too many industries

Having an Ideal Customer Profile (ICP) is vital to ensure that your vCISO services are tuned to the specific needs and risk profiles of your clients. Spreading services across too many diverse industries can lead to diluted expertise and increased risk of errors. By concentrating on specific industries, you can replicate success and minimize risk through familiarity and targeted expertise.

→ Forgetting to integrate data from other parts of the business

Make the most of your industry-wide expertise and experience. Efficient integration facilitates quicker, more informed decision-making processes and enables faster response times to security incidents, such as patch management, blocking suspicious IP addresses, disabling affected user accounts, and more.

The 5 Phases: Your 100 Day Action Plan

Research (Days 0-30)

The vCISO security strategy and plan begins with researching current state of the organization's security posture and business objectives.

Key Activities:

Meet stakeholders and management to understand their expectations and learn about the organization.

Meet the IT/security team to build relationships, evaluate the team's skills, understand current workflows, and identify any gaps in expertise or resources.

Get access to tools, data and all relevant systems so you can review configurations, management practices, and security controls.

Analyze existing infrastructure, tools, frameworks, policies and reports to gain insights into potential vulnerabilities and the effectiveness of existing security controls and procedures.

Obtain and understand network and data flow diagrams to recognize critical data flows and potential points of exposure.

Review past security incidents and responses to evaluate the organization's ability to respond and recover from such incidents.

Conduct threat intelligence research of the threat landscape, including CVEs, zero-days, regulations and key players. Take note of which threat actors are targeting these types of clients, how they get access, and preferred methods of persistence.

Understand the existing vendor management process to reveal third-party risks and compliance with security policies.

Review customer contracts to ensure that customer-imposed security requirements are met, as these can influence the prioritization of security tasks.

Understand the Software Development Life Cycle (SDLC) program to see how security is integrated into application development (when applicable).

Sample Questions to Ask Stakeholders:

1. Can you list the mission-critical applications your department uses daily?
2. What data types are most commonly processed within these applications?
3. Could you walk me through the business workflow using these systems?
4. What types of payment methods are processed, and through what systems?
5. What are your primary concerns about your current systems and data security?
6. What ongoing projects are being conducted?
7. What are your specific expectations from the vCISO service and this engagement?

Understand (Days 0-45)

Now, it’s time to consolidate your findings into a comprehensive view of the organization's security maturity and posture.

Key Activities:

Conduct a security risk assessment. Taking all the info you've gathered, you'll want to begin to collate and synthesize it in a formal risk assessment to baseline the environment. Use a standard onboarding questionnaire and scanning tool to provide objective assessment of current risks.

Create a clear picture of security maturity and the security posture. Compile the data from your initial assessments into clear, executive-friendly reports that include technical metrics and an evaluation of the processes, people, and technology in place. Use established cybersecurity frameworks like NIST to measure the organization's security practices against industry benchmarks.

Show the current security posture and gaps to the management. Present a gap analysis to management that clearly delineates where the organization stands versus where it needs to be. This should be done in the context of the organization's risk appetite, regulatory requirements and business goals.

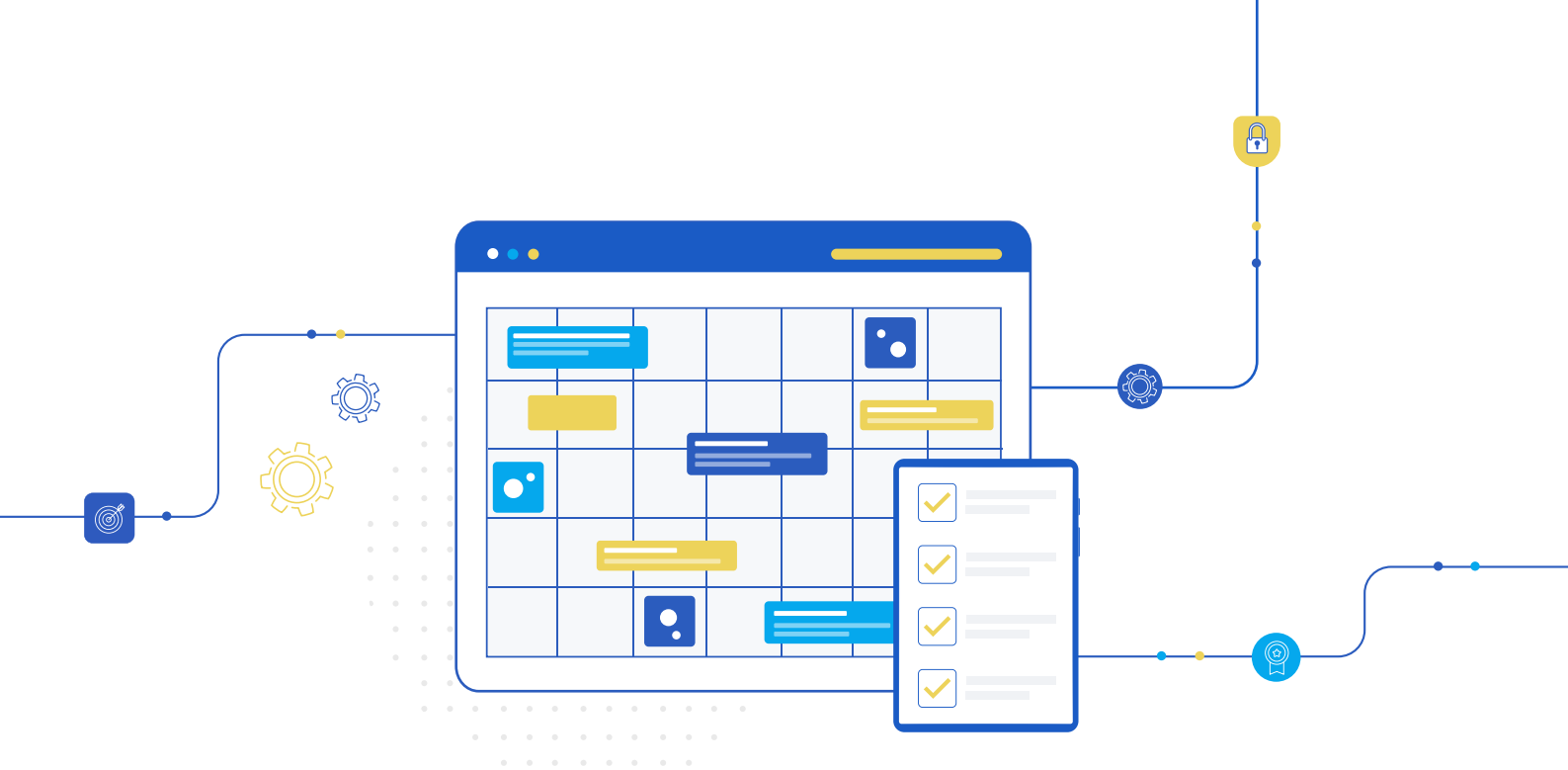
Identify short-term and long-term needs. Based on the gap analysis, develop a prioritized list of risks and associated remediation steps that align with business objectives, distinguishing between immediate (short-term) and strategic (long-term) needs.

Identify business needs. Perform an analysis of how security investments translate into business value, considering factors like reduced downtime, compliance fines avoided, and reputational benefits.

Examine the use of automation. Identify areas where security processes can be automated for efficiency, like risk and compliance assessments, gap analysis, tailored policies, creation of strategic remediation plans with prioritized tasks, use of tools for ongoing task management, progress tracking and customer-facing reports.

How Cynomi's Platform Supports This Phase - Automation, Risk Assessment and Compliance Readiness

- Cynomi tailors intuitive concise and visual onboarding questionnaires for each client.
- Cynomi performs expedited external scans to uncover critical vulnerabilities in externally visible IPs and URLs, including ports, protocols, encryption, websites, and more. These scans are available for Office365, Active Directory and endpoint security configuration.
- Following a quick risk assessment process, Cynomi automatically builds a unique cyber profile for each client and reflects its cybersecurity posture and gaps.
- Cynomi immediately provides compliance readiness reports.
- An easy to understand dashboard and exportable customer-facing reports ensure clients understand their posture.
- Cynomi automates many of the vCISO’s manual tasks including risk assessment, creation of tailored security policies, generating customer-facing reports, and remediation plan creation.



Prioritize (Days 15-60)

The third phase includes taking the foundational understanding of the organization's security landscape and shaping actionable plans.

Key Activities:

Define short, mid and long-term goals. Draft specific, measurable, achievable, relevant, and time-bound (SMART) goals for the current 100 days, the end of the year, and the following year. These goals should focus on mitigating the most significant risks first.

Create a remediation/work plan based on those goals that lays out the steps necessary to achieve each goal. This should include timelines, responsible parties and expected outcomes.

Identify 2-3 quick wins that can improve security posture with minimal effort or investment. For example, enabling MFA or optimizing existing security tool configurations for better coverage.

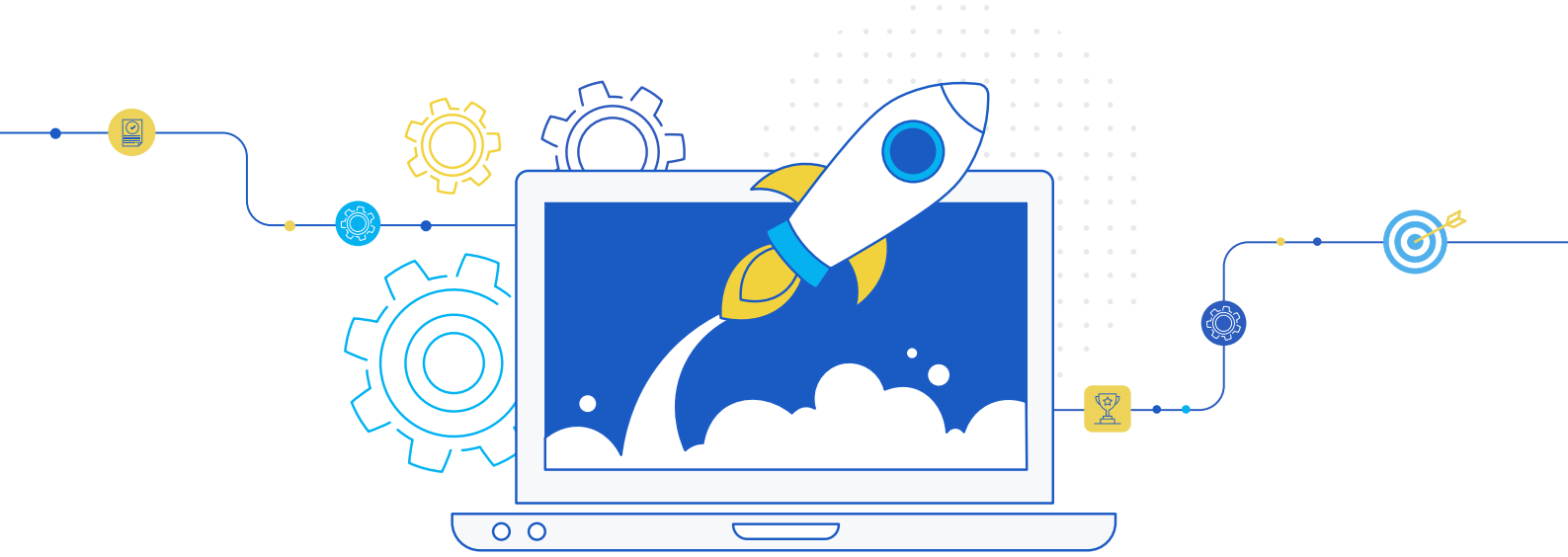
How Cynomi's Platform Supports This Phase - AI-based Remediation Plan

- Cynomi automatically creates customized remediation tasks, analyzes the relevancy and impact of each task in security and compliance, and generates a CISO-like, prioritized and easy-to-implement task list.
- Cynomi supports remediation planning and management, assigning tasks to relevant plans and team members.

Plan budgets and resources for security initiatives, ensuring cost-effectiveness and alignment with broader financial planning. Assess where automation can reduce the need for additional resources and streamline existing operations, to save costs and improve efficiency.

Create a risk register that documents all identified risks along with their likelihood and impact and prioritizes them.

Share the goals and high level plan with the management, ensuring transparency and setting the stage for ongoing support and engagement from the top down.



Execute (Days 30-80)

During the "Execute" phase, your goal is to execute your strategic plan. This phase establishes your vCISO credibility and sets the tone for ongoing security management.

Key Activities:

Get stakeholder and management buy-in by explaining the strategic plan, its benefits, and its impact on the organization. Ensure that the value of your proposed security measures is clearly understood.

Communicate the plan to all stakeholders - vertical and horizontal. Ensure that all departments feel included and responsible for its success.

Implement automated systems that can deliver low hanging fruit. Here are some examples, but the right automated system will depend on the vertical and company type.

- Automated password reset platforms
- Automated report generation
- Accounting systems that require dual approval for money transfers
- A vCISO platform
- Orchestration platforms that can automate cog deployments to prevent misconfigurations
- RPA (Robotic Process Automation) providers for enforcing JIT (Just-in-Time) admin access
- Automated code scanning or static testing tools

Focus on the quick, impactful wins that you identified, like policy updates or turning on unused but available security features. This helps build momentum and demonstrates early successes.

Start with high priority policy creation, such as those governing incident response, data protection, and access control.

Recommend purchasing products or tools if needed.

Set a cadence for external scanning and reporting, demonstrating improvement and risk reduction over time.

Continuously manage and adjust remediation plans to ensure they remain effective and responsive.

How Cynomi's Platform Supports This Phase - Tailored Security Policies

- Cynomi automatically generates easy-to-follow, actionable policies, based on common security frameworks and adjusted based on the client's cyber profile, relevant regulatory requirements and industry benchmarks.
- Cynomi specifies the level of task completion associated with each policy to help identify quick wins and prioritize tasks.

Policies include:

Access | Awareness | Workstations | Servers | Domain and DNS | Email and Messages | Risk Management | Incident Response | Logging and Monitoring | Network | Remote Access | Office365 | Active Directory | Compliance and Auditing | Data Protection | HR | Password | SaaS | Physical Infrastructure | Website | Secure Software Development | Vulnerability Management | Workstations and Mobile | Generative AI

Report (Days 45-100)

The final phase of a vCISO's first 100 days validates the strategy's effectiveness and ensures ongoing support from management and stakeholders.

Key Activities:

Measure Success by collecting and analyzing data that reflects the success of the executed plan. This could include metrics such as:

- Reduced incident response times
- Fewer successful phishing attempts
- Improvement in security and compliance postures
- Reduced risk levels for malicious activities like data leaks, ransomware, fraud and website defacement
- Higher scores for domains like access management, threat intelligence, passwords, website and data protection
- Advancement in task progress

Craft detailed reports for management that articulate successes, challenges, and areas requiring attention. Reports should translate technical operations into business impacts, making it easy for executives to understand the return on their security investments.

Communicate progress at least once a month, ensuring transparency and maintaining the urgency of cybersecurity initiatives. Pro tip: Use the same standard reports to make reporting easier to create and to consume.

Integrate reporting into your overall plan, reflecting on how the security measures contribute to the overall business strategy and risk management framework.

Conduct an additional full assessment after 3-4 months to demonstrate progress and identify any new or unresolved vulnerabilities.

How Cynomi's Platform Supports This Phase - Measuring and Reporting

- Cynomi highlights vulnerabilities clients are exposed to and prioritizes simple and clear remediation steps.
- Cynomi calculates a cyber protection score for each client's specific risks, including ransomware, data leaks, fraud and website defacement. Scores enable tracking client's risk.
- Cynomi includes a built-in customer-facing reporting suite. This enables vCISOs to deliver branded, real-time, exportable status and progress reports for customer stakeholders – operations and management alike. These reports show security level, improvement trends, compliance gaps and comparison with industry benchmarks – helping easily show the progress you helped them make.

Reassess and readjust

- Use the findings from continuous assessments to realign the security strategy with the organization's evolving needs and threat landscape.
- Prioritize new initiatives or scale back on those that are less effective.
- Work closely with the executive team to interpret report findings and plan for the coming quarters.
- Continuously adapt and improve your processes and controls to keep security measures effective and relevant.

Your Next Steps as a vCISO

In your first 100 days, you have laid down substantial groundwork. You built relationships with key stakeholders, aligned security goals with business objectives, delivered a number of quick wins and leveraged automation for efficiency.

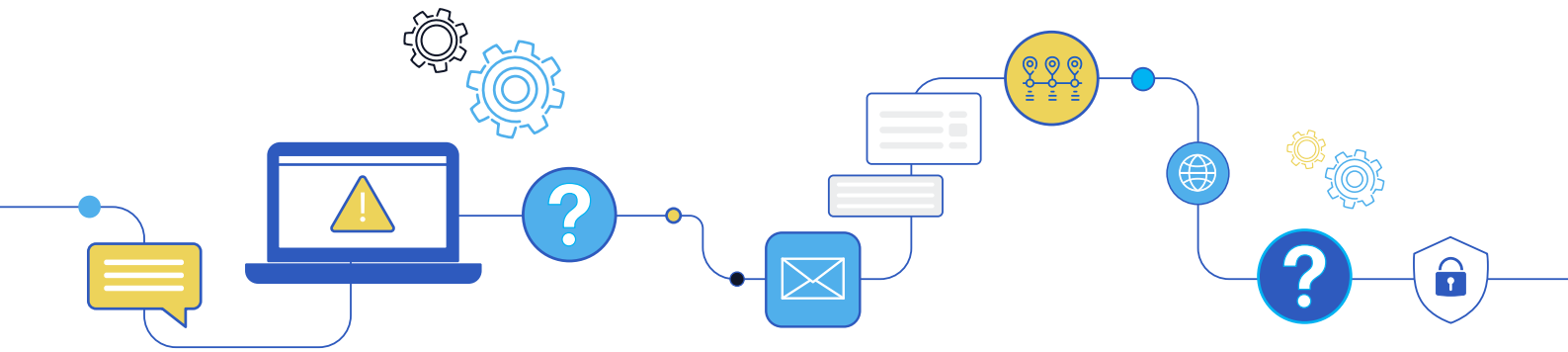
Now, your efforts should focus on setting your long-term security plan in motion. On top of carrying out your tasks and activities, be sure to regularly review and revise your security practices, policies and technologies.

Iterate and optimize continuously to ensure your plan remains effective, that your security infrastructure remains up-to-date with technological advancements and evolving threats and that you meet all compliance requirements. As you move forward, a vCISO platform will keep you on top of the organization's security status and roadmap as well as external changes in the threat and regulatory landscapes.

Staying ahead of the curve also requires developing a culture of security within the organization. This includes regular training, proactive threat hunting, incident response drills and being on the constant lookout for automated solutions. These will ensure the team is well-equipped to manage and mitigate incidents effectively.

We hope that our suggestions will help you on your first 100 days and beyond. Making meaningful choices, measuring your impact and maintaining a flexible mindset will set you up for success on your vCISO journey.

To learn how Cynomi can support you on your vCISO journey, make it easy and effective, **schedule a demo** to see Cynomi's vCISO platform in action.

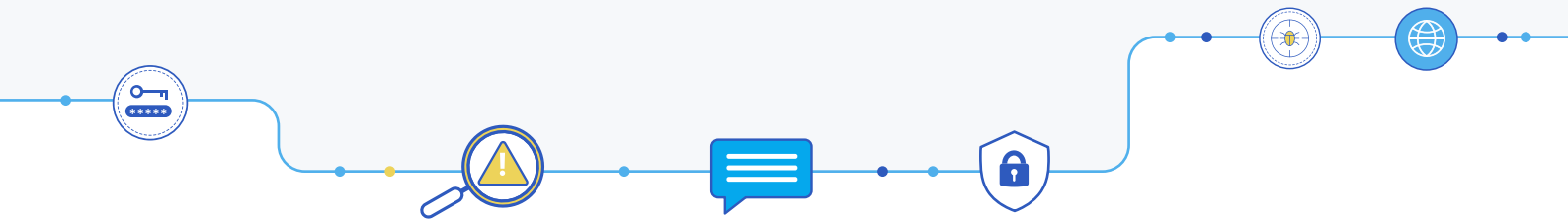


About Cynomi

Cynomi's AI-driven vCISO platform empowers MSSPs, MSPs and consultancies to offer structured cybersecurity services to SMEs at scale and provide them with proactive cyber resilience.

Combining proprietary AI algorithms with CISO-level knowledge and knowhow, Cynomi's platform streamlines the vCISO's work while automating manual time-consuming tasks including risk assessment, compliance readiness, cyber posture reporting, creation of tailored security policies and remediation plans, as well as task management optimization.

Cynomi helps partners overcome the cybersecurity skill gap and scale their business, allowing them to offer new services, upsell and increase revenues while reducing operational costs. To learn more about Cynomi, visit http://www.cynomi.com.



About PowerPSA

At PowerPSA, we delight in equipping MSPs to deliver top-tier vCISO services.

Our strength lies in helping you demystify risk analysis, refine service delivery with business process acumen, and foster robust, profitable cyber service offerings.

Through a meticulous operational design and cross-functional execution, you'll enable seamless collaboration within your organization, enhancing efficiency, reducing burnout, and propelling growth.

Our approach is simple: elevate your processes, empower your team, and exceed your business goals.

Want to learn more about how to revolutionize your service catalog and unleash the power of your MSP? Explore our methods and success stories at PowerPSA.com.