INFORMATION SECURITY GROUP (ISG)

STRATEGIC MANAGED SECURITY SERVICES

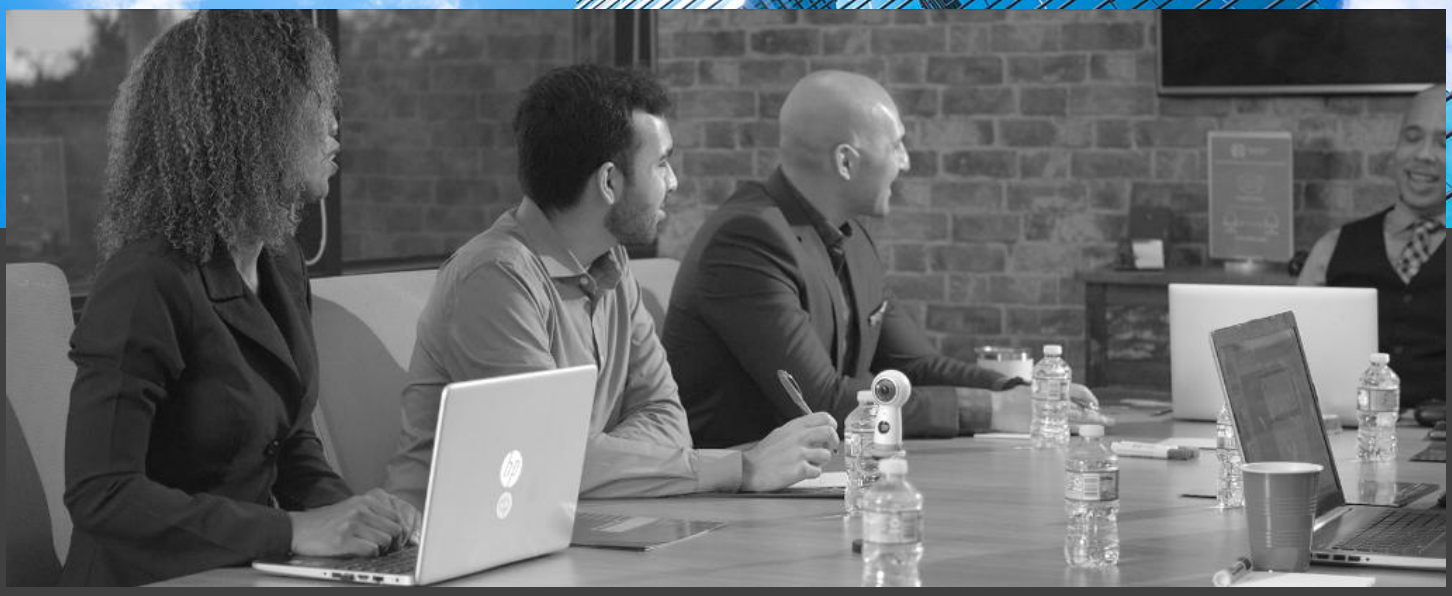


Table of Contents

1 | INTRODUCTION

In today's digital landscape, cybersecurity is a top business priority. Our Information Security Managed Program and Services meet organizations where they are – whether just beginning or maturing an existing security strategy – and provides a tailored path to greater resilience and compliance. With our managed programs and services, organizations can rest assured that they are taking a proactive approach to information security and are well-equipped to mitigate potential threats.

vCISO ISP RMP CIRP VCP SCS OPS

2 | GRC MANAGED SERVICES

Provides structured, ongoing support to help organizations align governance, risk, and compliance with business objectives — continuously driving maturity, reducing risk, and ensuring audit-readiness.

Virtual CISO

Executive Security Leadership or Support

Experienced security executives integrate with your team to shape security strategy, drive decision-making, and oversee compliance initiatives.

- Provides board-facing cybersecurity expertise
- Strengthened trust and confidence among customers and stakeholders.
- Enhances leadership confidence and accountability
- Provides a resource that can capably manage M&A activity

Information Security Program

Build a formal InfoSec program

Build and manage a formal information security program aligned to frameworks like SCF, NIST, or ISO to ensure consistent controls and audit readiness.

- Formalizes policies, roles, and responsibilities
- Drives consistency in security operations and governance
- Supports compliance with popular regulatory standards and contractual obligations
- Scales easily with growing regulatory or customer demands

Risk Management Program

Risk-driven orgs that need continuous assurance

Establishes a risk management function to identify, prioritize, and mitigate security risks while fostering a proactive, risk-informed culture.

- Prioritizes security investments based on actual risk
- Builds proactive culture of risk-informed decision-making
- Supports risk registers, assessments, and remediation tracking
- Improves readiness for regulatory reviews or partner due diligence to security incidents

ESTIMATED EFFORT FOR PLANNED ENGAGEMENTS

Virtual CISO		ISP Managed Program		RMP Managed Program	
[1] Annual Commit	68-164 hours	[1] Annual Commit	96-244 hours	[1] Annual Commit	60-472 hours
[2] SOC 2 Commit	90 *	[2] SOC 2 Commit	120	[2] SOC 2 Commit	144

[1] We plan your managed program operating workloads in 12-month sprints and estimate the effort of each workload based on our operating framework. Based on your regulatory requirements and risk appetite, we provide a plan with ample hours for all required activities.

[2] The estimated effort for annual maintenance of SOC 2 compliance that meets Trust Service Principles for Security, Confidentiality and Availability.

* Represent estimated effort for CISO support procurement option of our vCISO services. We offer fractional CISO as a staff augmentation resource.

CIRP

Cyber-Incident Response Program

Efficient and Effective Response to Incidents

Delivers structured response planning and incident command services to ensure organizations are prepared for cyber events with coordinated containment and recovery operations.

- Accelerated readiness for high-severity incidents
- Clear roles and escalation paths for crisis scenarios
- Rapid, coordinated containment and recovery

VCP

Vendor Compliance Program

Continuous Vendor Security Posture Validation

Manages third-party risk by aligning vendor practices with organizational risk tolerance, contractual controls, and regulatory expectations.

- Improved visibility and control over third-party risks
- Audit-ready documentation of vendor assurance
- Reduced exposure through proactive vendor oversight

SCS

Security Compliance Services

Maintain Continuous Audit-Readiness

Delivers sustained audit support and regulatory alignment using change monitoring and continuous policy compliance tracking.

- Sustained audit support and regulatory alignment
- Regulatory risk reduction using continuous change detection technology
- Audit stakeholder preparedness for third-party audit confidence and efficiency

ESTIMATED EFFORT FOR PLANNED ENGAGEMENTS

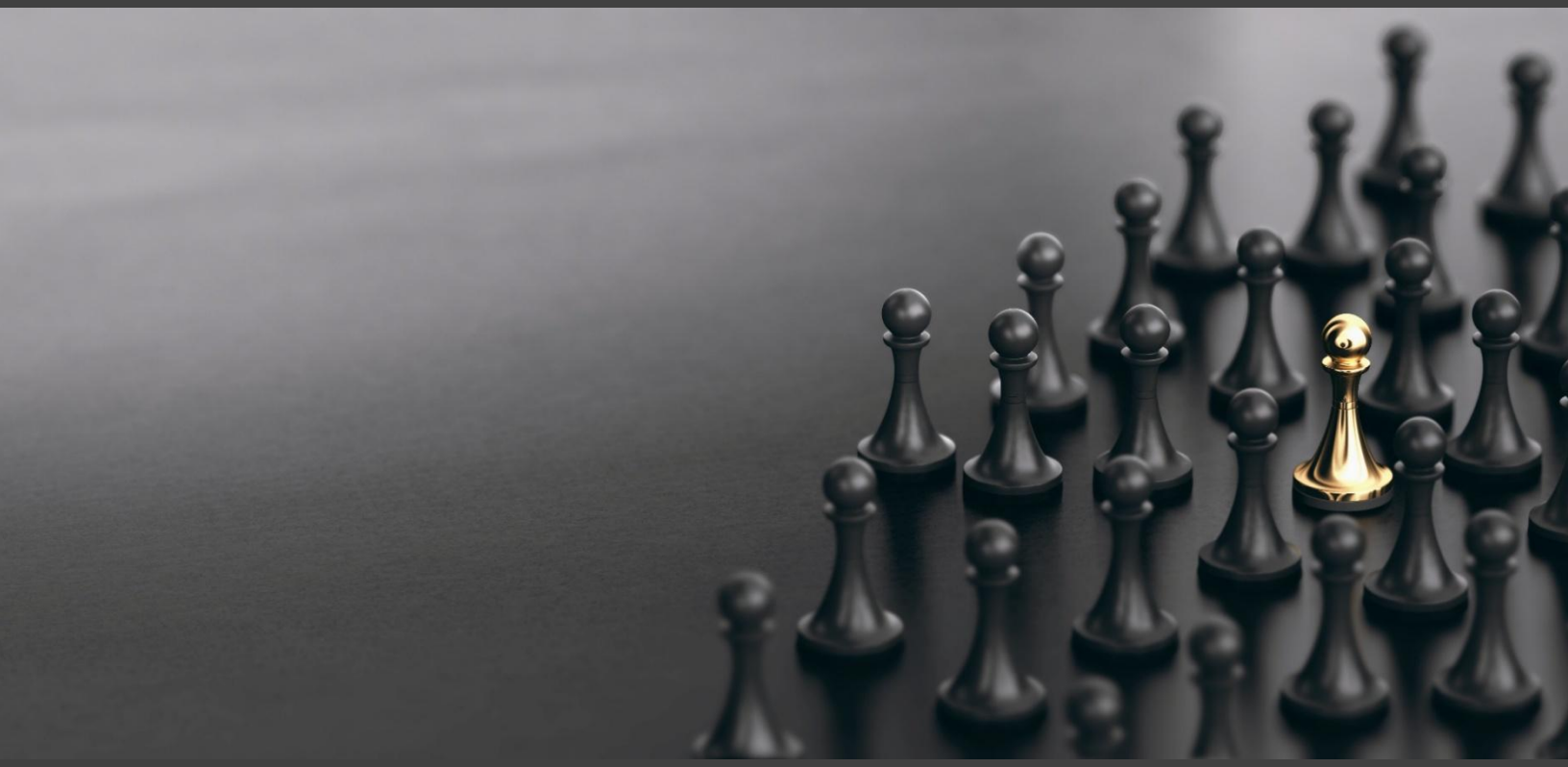
CIRP Managed Program		VCP Managed Program		SCS Managed Program	
[1] Annual Commit	70-120 hours	[1] Annual Commit	120-365 hours	[1] Annual Commit	60-120 hours
[2] SOC 2 Commit	100	[2] SOC 2 Commit	240	[2] SOC 2 Commit	60

[1] We plan your managed program operating workloads in 12-month sprints and estimate the effort of each workload based on our operating framework. Based on your regulatory requirements and risk appetite, we provide a plan with ample hours for all required activities.

[2] The estimated effort for annual maintenance of SOC 2 compliance that meets Trust Service Principles for Security, Confidentiality and Availability.

3 | BENEFITS OF OUR METHODOLOGY

In today's dynamic digital landscape, safeguarding information is essential. Our modular Information Security Managed Programs meet organizations at any maturity level—providing an integrated approach to establish or enhance your security posture at every stage.



1

Enterprise-grade security scaled to midmarket needs

We deliver enterprise-grade security programs tailored to midmarket needs through a top-down framework, expert guidance, and pre-built tools for fast deployment and consistent service delivery.

2

Increased Efficiency for Compliance Readiness

Put routine compliance tasks on autopilot using our streamlined workflows and a rich set of artifacts customized by senior analyst for fast, continuous audit readiness.

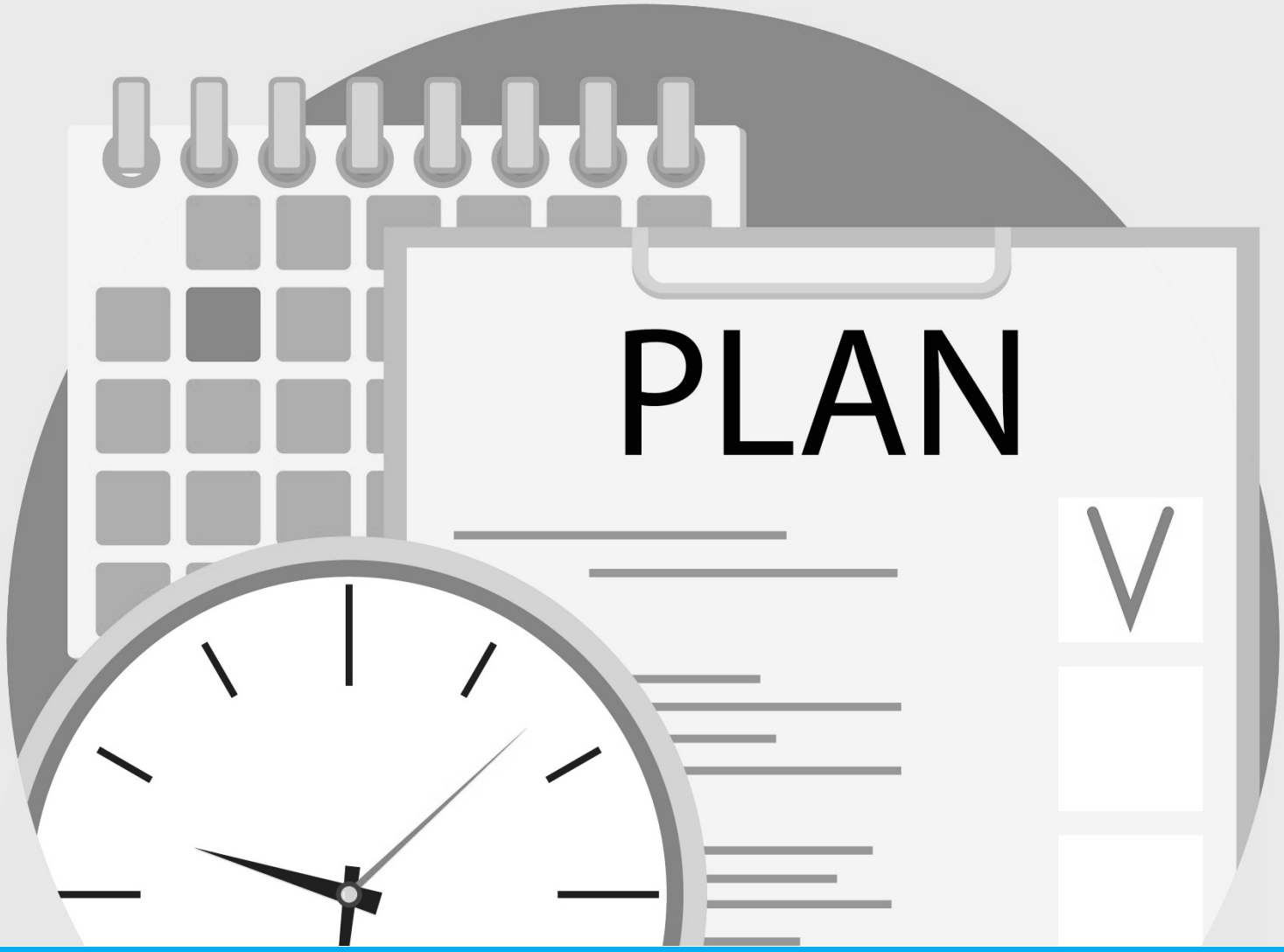
3

Optimized, Flexible Spend for Top-Tier Security

Maximize your information security management ROI using our scalable GRC and cybersecurity services — no added headcount or costly tech licenses required.

4 | How we Deliver our Services

This section provides an overview of how we plan, deliver and report on our Strategic Managed Security Services



Our Three-Step Engagement Process

1

Govern & Plan
The operating plan(s) and runbooks required to deliver the services

2

GRC Operations
Managed & hosted on your M365 tenancy or Enterprise GRC system

3

Managed SOC
24/7 cybersecurity protection, incident response & continuous red team testing

GOVERN & PLAN

STEP 1: ALIGN ON DELIVERABLES

Clearly defined and documented delivarables to govern GRC-Ops and SecOps

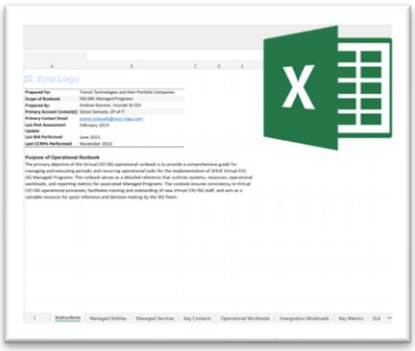
Client Operating Plans

Memorializes a customized operating plan for each Client deployment and assures the delivery of services is understood and authorized by the primary account owner.

- **Define & Authorize Service Delivery.** We use standard client operating plan templates to comprehensively define program deliverables.
- **Establish Operational Workload Retainers.** Defines the frequency and estimated effort required for planned GRC workstreams.
- **Performance Reporting.** Defines program performance metrics and measures for periodic reporting.
- **Define Shared Responsibility.** Clearly delineated Shared Responsibility Matrix to assign security responsibility across program objectives and initiatives.

Operation runbooks defines schedule of workloads, risk escalations and more

- **Establish Operating Project Plan.** Used by ISG service delivery admins to operationalize your strategic managed security services
- **Define Escalations and Service Levels**. Defines indicators or compromise, attack and exposure with associated escalation paths
- **Schedule of Operational Workloads.** Defines and includes a calendar schedule of planned GRC operational workloads



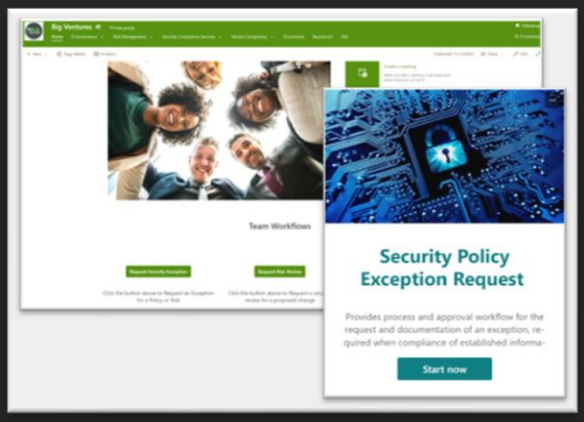
ISG-GRC Operational Runbooks

Customized configuration for managed processes and services across Client deployments.

GRC OPERATIONS

STEP 2: DEPLOY GRC OPERATIONAL SYSTEMS

GRC Operations hosted using M365 or your Enterprise GRC system



M365 GRC Management System or your own Enterprise GRC System

An optional service component for organizations managing no more than 5000 information assets.

- **Deploy & Configure GRC Systems.** Deployed and operationalized on your organizations M365 tenant or your enterprise GRC system.
- **Define Control Baseline.** Establish the baseline of controls and tailor controls for risk and regulatory environment.
- **Operationalize Managed Programs.** Deployment and configuration of secure share, request workflows, client portal, risk register, vendor profiles, action plans, BI tools and a lot more.

Continous Change detection across system with actionable Indicators of Risk

- **Real-time Change Detection.** Continuous monitoring of system changes for detection of unauthorized changes and misconfigurations.
- **Risk Posture Change Notifications.** Actionable alerts for Indicators of Risk (IoR) defined in GRC runbooks.
- **Multi-platform support.** Inspectors for MS Azure, AWS, M365 and other popular cloud and SaaS platforms.

Continuous Change Detection

Multi-platform Endpoint Agents and Cloud API Inspectors for Continuous Change Monitoring across on-premises and cloud.

SECURITY OPERATIONS

STEP 3: DEPLOY MANAGED SOC SERVICES

24/7 Managed Security Operations

ISG-OPS Managed SOC Services

Our GRC Integrated Security Operations service provides a complete security stack for cybersecurity operations with continuous oversight by your vCISO and GRC Team.

- **Managed Detection & Response (MDR).** We use leading commercial and open source technologies for rapid detection and investigation of anomalies and security events.
- **Internet Threat Protection.** Real-time phishing email, and digital masquerading detection, and threat intelligence integration.
- **Managed Zero-Trust Network Access.** Implement Zero Trust to improve secure remote access and data protection.
- **Threat Hunting & Red Team Testing.** The Whitedog SOC uses threat intel with automated and manual techniques to proactively hunt for threats and continuously test defenses.

GRC INTEGRATIONS

RISKOPS INTEGRATED. Improved contextual understanding and mitigation of security incidents.

OPTIMZIED INCIDENT RESPONSE. Broader risk response and mitigation strategies beyond containment and eradication.

AUDIT READINESS. Monitors system changes to ensure incident response activities does not result in non-compliance.

SERVICE LEVEL PROMISE

24/7 REAL-TIME MONITORING. Always on detection & analysis of anomalies and security events.

FAST INCIDENT RESPONSE. From detection, initial analysis to client notification within 15-minutes.

COMPOSABLE PROTECTION. We continuously refine our tools using rigorous threat simulation and MITRE-style evaluations to ensure we evolve with emerging threats.

PLATFORMS SUPPORTED

Operating Systems

Windows Mac kubernetes redhat ubuntu docker

Cloud Platforms

amazon web services Microsoft Azure Google Cloud

Other Linux distributions include CentOS, Scientific, Debian and other legacy platforms.

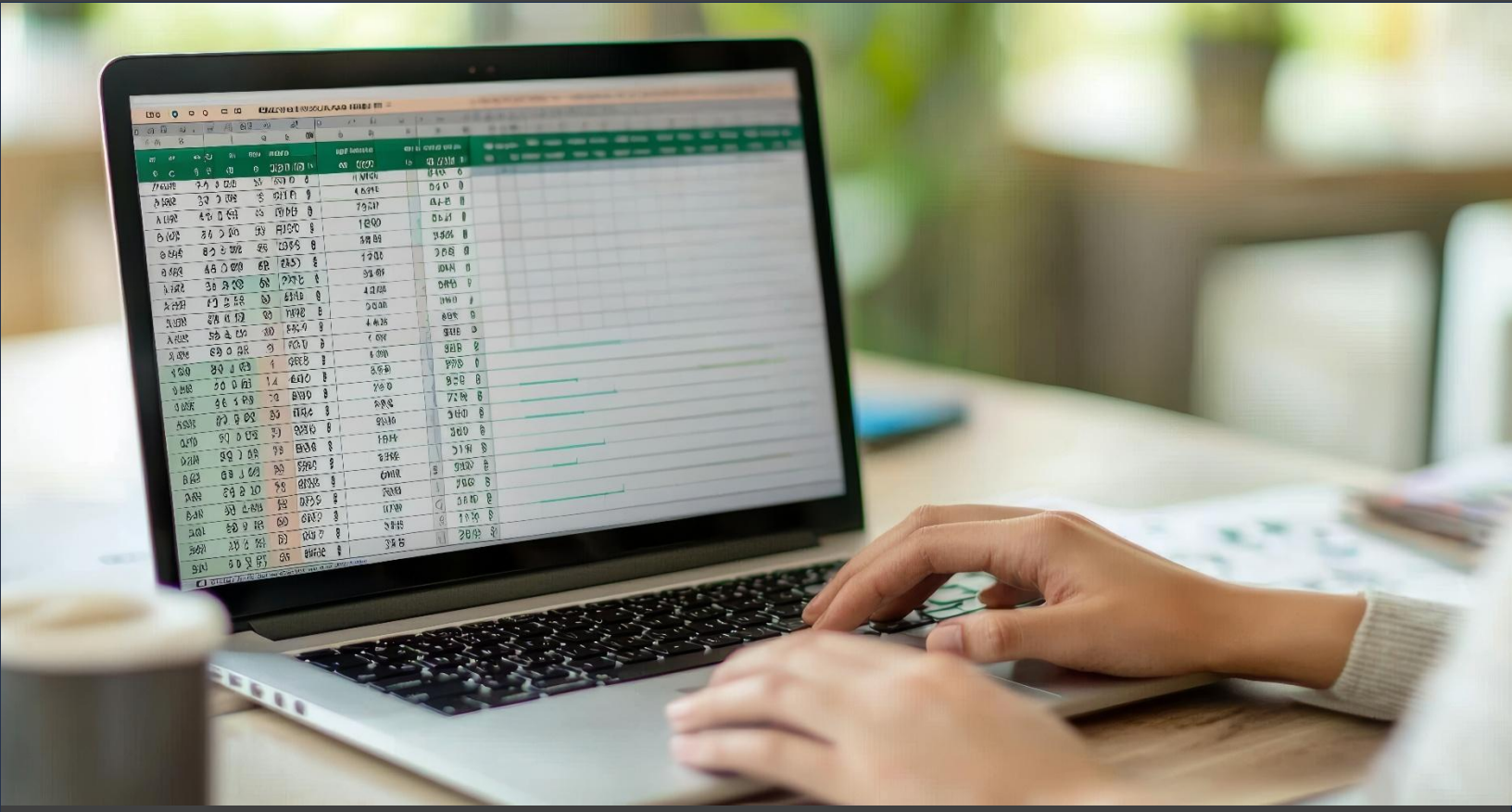
Key Solutions Used

SentinelOne ATTACKIQ ALIEN VAULT

Powered by

WHITE DOG

The Whitedog Cyber SOC partner leverages a mixture of over 50+ commercial and open-source tools across security operations offerings.



5 | SCOPING AND PRICING

The guidance in this section provides an overview of how we scope and bill for our services to provide a basis for budget planning.

STEP 01: Select your Leadership Option

OPTION 1	OPTION 2	OPTION 3
No Virtual CISO Best for organizations with a full-time CISO or experienced Information Security Leader	**CISO Support** Best for organizations that want to build an internal CISO capability	**Fractional CISO** Best for organizations seeking staff augmentation for their CISO role.

STEP 02: Select your GRC Managed Programs

ISG-ISP	ISG-RMP	ISG-CIRP	ISG-VCP	ISG-SCS
Information Security Program	Risk Management Program	Cyber-incident Response Program	Vendor Compliance Program	Security Compliance Services
Pricing determined by scope and commitment	Pricing determined by scope and commitment	Pricing determined by scope and commitment	Pricing determined by scope and commitment	Pricing determined by scope and commitment

* For customers requiring reduced costs, and don't have a need for US-based resources only, we offer offshore and nearshore options at greatly reduced rates, often times as low as 50% of the standard rate

STEP 03: Select your Core Managed Security Services

MDR	M-ZTNA	M-IP
Managed Detection & Response	Managed Zero-Trust Network Access	Managed Internet Protection and Distributed DNS Defense
Detection and response to cybersecurity threats in real time.	Continuous, identity-aware, and context-based access control.	Real-time protection against advanced phishing, spoofing, and network-based manipulation
Quantity level discounts provided at higher licensing thresholds.	Quantity level discounts provided at higher licensing thresholds.	Quantity level discounts provided at higher licensing thresholds.

[1] Endpoints can be desktops, laptops, virtual/physical servers and cloud workloads

6 | BUDGET JUSTIFICATION

This section serves as a strategic guide for information security budget holders to effectively communicate cybersecurity investment value to executive leadership. Use these justification points when building budget approval worksheets or delivering business case presentations.

Use these justification points when building budget approval worksheets or delivering business case presentations to the CEO.

Key Interests

- Enhancing customer trust, perceptions, and loyalty.
- Safeguarding brand and market position.
- Ensuring business continuity and resilience.

Key Outcomes

- Strengthen customer trust and brand loyalty.
- Enable revenue growth through secure innovation.
- Avoid high-impact security incidents that stall strategic initiatives.

Justification Statements

Virtual CISO	Delivers board-level cybersecurity leadership that connects risk, innovation, and strategic growth. Enables better decision-making and preparedness at the executive level.
Managed GRC Programs	Integrates governance, risk, and compliance into daily operations to reduce regulatory exposure and ensure strategic agility in fast-changing markets.
Managed SOC Services	Delivers real-time threat detection and rapid incident response that protects uptime, customer trust, and digital assets across all platforms.

Documentation & Presentations

- Translate security initiatives into business value: growth, resilience, and competitive advantage.
- Quantify avoided costs (e.g., breach recovery, lost deals, delayed M&A) to support budget queries.
- Use peer examples and breach case studies to frame risk and opportunity in familiar terms.

Use these justification points when building budget approval worksheets or delivering business case presentations to the CFO.

Key Interests

- Protecting financial performance and shareholder value.
- Controlling compliance costs and reducing audit fatigue.
- Enabling secure scalability and risk-aligned growth.

Key Outcomes

- Reduced financial and reputational risk exposure.
- Lower total cost of maintaining compliance.
- Predictable security spend aligned to business goals.

Justification Statements

Virtual CISO	Aligns cybersecurity with enterprise risk to improve cost control and financial protection.
Managed GRC Programs	Reduces compliance costs and audit effort by embedding controls into daily operations and reducing audit prep.
Managed SOC Services	Provides 24/7 threat response at predictable cost without increasing internal headcount.

Documentation & Presentations

- Frame cybersecurity as financial risk management by emphasizing cost avoidance and protection of shareholder value.
- Translate spend into ROI by connecting security investments to reduced breach costs, audit savings, and regulatory readiness.
- Use real-world financial impacts highlighting breach-driven fines, lost deals, or delays in strategic initiatives like M&A.
- Show cost predictability illustrating how managed services control budget volatility and reduce unplanned expenses.

Use these justification points when building budget approval worksheets or delivering business case presentations to the CIO.

Key Interests

- Modernizing IT through secure-by-design transformation.
- Executing the IT roadmap on time and within scope .
- Maintaining uptime and operational continuity.

Key Outcomes

- Accelerated delivery of digital initiatives with reduced risk.
- Security-aligned IT execution that scale with business priorities.
- Resilience and reliability with reduced disruptions from cyber incidents.

Justification Statements

Virtual CISO	Integrates cybersecurity strategy into IT planning, architecture, and governance, ensuring modernization efforts are risk-aligned.
Managed GRC Programs	Streamlines compliance and embeds risk controls into delivery pipelines, improving roadmap velocity and audit readiness.
Managed SOC Services	Monitors infrastructure and workloads 24/7, enabling immediate response to threats while reducing load on internal teams.

Documentation & Presentations

- Show security as a delivery enabler and not just protection, but acceleration of IT programs.
- Map cyber investments to KPIs such as faster deployment, fewer audit findings, improved SLA compliance.
- Highlight architectural synergy that support and align security initiatives with observability, identity, DevOps, and cloud-native goals.

Use these justification points when building budget approval worksheets or delivering business case presentations to the Board of Directors.

Key Interests

- Preserving enterprise value and brand reputation
- Enabling secure innovation and digital growth
- Strengthening governance, resilience, and oversight

Key Outcomes

- Improved stakeholder confidence through governance transparency
- Faster time-to-market through trusted transformation
- Reduced exposure to regulatory and reputational events

Justification Statements

Virtual CISO	Aligns cybersecurity with business strategy and board risk oversight—enabling secure execution of growth, M&A, and innovation.
Managed GRC Programs	Reinforces enterprise governance with embedded controls that lower audit risk and improve board reporting posture.
Managed SOC Services	Reduces operational and brand risk through 24/7 visibility, improving resilience and board assurance on incident response.

Documentation & Presentations

- Translate risk into enterprise value terms by quantifying impact on revenue protection, brand equity, and investor trust.
- Connect security to strategic plans by showing how controls enable transformation, M&A readiness, and geographic expansion.
- Use board-relevant peer benchmarks to demonstrate where similar companies invest to stay compliant and competitive.
- Tell fiduciary-aligned stories such as case studies on governance lapses, disclosure risks, and recovery leadership.

7 | HOW TO GET STARTED

To start your journey with 3HUE Virtual CIO Services choose from the practical engagement paths aligned to your organization's current cybersecurity posture.

Your Current State	Recommended Next Steps	Expected Outcome
Scenario 1: No Program in place. No security program or recent enterprise-wide security & controls evaluation	• Schedule meeting with Client Success to schedule deep-dice overview and facilitate initial discovery using the contact information below. • For clients that have not performed a risk posture assessment for more than 18 months we strongly recommend inquiring about our Holistic Risk & Control Posture Assessment as a first step.	• Formal Risk Assessment Report • NIST CSF 2.0 Maturity Scorecard • Security Architecture Remediation Plan • Plan of Actions & Milestones • Cyber-Risk Advisory Retainer
Scenario 2: Partial Program in place. Security Program exists, but needs strategic review	• Schedule meeting with Client Success to schedule deep-dice overview and facilitate initial discovery using the contact information below. • A second meeting will be scheduled with appropriate stakeholders for an overview of recommendations.	• Review existing plans, policies, and controls for modernization opportunities
Scenario 3: Need for Urgent Program Review. Facing urgent audit deadlines or compliance gaps	• Schedule meeting with Client Success to schedule deep-dice overview and facilitate initial discovery using the contact information below. • A second meeting will be scheduled with appropriate stakeholders for an overview of recommendations.	• Controls Gap Assessment aligned to framework. (e.g., SOC 2, HIPAA, CMMC) • Gap Reports, Remediation plans and engineering resources

CONTACT US

855-374-7129

info.3hue.net/start-now

success@3hue.net

8 | FREQUENTLY ASKED QUESTIONS

1. What if we already have a CISO or CIO?	Our programs are operated by senior information security analysts and architects, and we offer Virtual CIO or Virtual CISO as a component of our managed programs.
2. What is the role of a Virtual CISO (vCISO) resource, and how can it benefit my organization?	Our Virtual CISO's are offered in several engagement models, including the option to go with senior analyst lead service delivery. Our Virtual CIOs and CISOs are former CISO and CIO professionals that augment the expertise of small to medium-sized enterprises (SMEs) on a flexible basis. This allows businesses to access top-tier security expertise without the cost and commitment of a full-time executive hire.
3. What is the difference between your Virtual CIO and Virtual CISO services?	The Virtual CIO (vCIO) focuses on aligning your IT strategy with business goals and ensuring that your technological infrastructure supports organizational growth. The Virtual CISO (vCISO) is specifically focused on cybersecurity, managing risk, shaping security strategies, and ensuring regulatory compliance. You can select either or both services depending on your needs.
4. How does your Governance, Risk, and Compliance (GRC) Managed Service support our organization?	Our GRC Managed Service helps align your organization's governance, risk, and compliance strategies with your business objectives. It ensures ongoing risk mitigation, audit-readiness, and supports continuous improvement. We operate in 12-month sprints, providing tailored support that helps you mature your security posture and ensure compliance with relevant standards like NIST, ISO, and SOC 2.
5. How do you integrate with existing Managed Service Providers (MSPs) or security teams	We offer a seamless integration model for clients who already have MSPs or internal security teams. Our Managed Programs are designed to complement and enhance your current operations, filling gaps in compliance, incident response, and strategic security management, ensuring that your organization's needs are met without disruption
6. What is your approach to cybersecurity incident response and how can it help us mitigate risks	Our Cyber-Incident Response Program (CIRP) ensures that your organization is prepared for high-severity incidents. We provide structured response planning, containment, and recovery services, reducing exposure and ensuring rapid, coordinated responses during a cyber event. This program improves visibility and control over potential risks and enhances preparedness for security incidents.

7. Can your services help with compliance readiness for frameworks like SOC 2, HIPAA, or NIST?	Yes, our Managed GRC Programs are designed to support continuous audit-readiness, helping you stay compliant with various regulatory frameworks, including SOC 2, HIPAA, and NIST. Our services include ongoing policy compliance tracking, risk assessments, and change detection to ensure that your organization always remains compliant.
8. How are operational workloads determined and what does the Get-Well methodology entail?	Operational workloads are determined based on your organization's specific needs and regulatory requirements. Our Get-Well methodology is a structured approach to GRC management, offering three levels of service: Essentials for regulatory compliance, Enhanced for high-risk environments, and Data-Driven for continuous security improvement. This framework integrates with leading standards like SCF, NIST, and CIS.
9. What if our organization doesn't need a full-time Virtual CIO or Virtual CISO?	If your organization does not require a full-time Virtual CIO or Virtual CISO, you can still access these services on a flexible, as-needed basis to handle work overflow or mentor your incumbent CISO. Our experienced professionals can provide strategic guidance, leadership development, and knowledge transfer to empower your security leaders, ensuring they have the tools and insights needed to drive your organization's security strategy effectively. Whether it's managing specific compliance initiatives, improving security processes, or providing an additional layer of expertise during critical incidents, we work alongside your team to deliver greater resilience, operational efficiency, and audit-readiness.
10. What are the benefits of your Managed Security Operations Center (SOC) services?	Our Managed SOC services provide 24/7 monitoring, detection, and incident response, ensuring rapid identification and mitigation of security threats. These services also include threat hunting, red team testing, and the integration of zero-trust network access, which enhances secure remote access and data protection.
11. How do you determine the pricing for your GRC services?	Pricing is determined based on the selected services, including leadership options like Virtual CIO or Virtual CISO, and the scope of managed programs such as GRC, incident response, and security compliance services. We offer discounted rates for international clients and flexible service packages to suit your organization's needs, without the added costs of internal headcount or tech licenses.