# Virtual Chief Information Security Officer (vCISO) Job Description

### **Role Overview:**

The vCISO serves as our clients' primary cybersecurity advisor. This role ensures the alignment of cybersecurity efforts with business goals, drives risk management, maintains regulatory compliance, and provides leadership in the development and execution of security strategies.

### **Key Responsibilities:**

1. Risk Management

* Identify, assess, and prioritize cybersecurity risks and vulnerabilities
* Develop risk mitigation strategies to protect business-critical assets
* Guide remediation efforts and track risk reduction progress

2. Regulatory Compliance

* Interpret and apply applicable laws, regulations, and industry frameworks (e.g., HIPAA, GDPR, CMMC, NIST, CIS)
* Develop and enforce cybersecurity policies and procedures
* Support audits and assist with third-party assessments

3. Strategic Security Planning

* Create and maintain a cybersecurity strategy and roadmap aligned with business priorities
* Set tactical and strategic security goals in collaboration with client leadership
* Define security KPIs and reporting mechanisms

4. Incident Response and Policy Management

* Lead the design and testing of incident response plans
* Oversee security policy development, review, and enforcement
* Guide incident handling, root cause analysis, and lessons learned

5. Security Awareness and Executive Reporting

* Build a culture of security through awareness training and leadership engagement
* Deliver clear, executive-level security reporting and briefings
* Translate technical risk into business impact for non-technical stakeholders

6. Additional Cross-functional Duties

* **Liaise with Technical Teams**: Work closely with internal MSP engineers and third-party vendors to ensure the timely implementation of security initiatives. Translate high-level risk assessments into actionable technical tasks and oversee execution to ensure alignment with strategic security goals.
* **Performance Management**: Monitor and evaluate the effectiveness of existing security services and tools provided by the MSP. Define and track performance metrics related to risk reduction, incident response readiness, and policy compliance. Recommend service improvements based on performance data and threat landscape changes.
* **Security Protocol Improvement**: Continuously review and enhance security protocols embedded across the MSP’s service offerings—such as patch management, endpoint protection, identity and access management, and backup. Ensure protocols align with current security standards and adapt to evolving client needs and regulatory requirements.

### **Core Skills and Traits**

* **Risk Assessment & Management:** Identifying, quantifying, and prioritizing risks to drive decision-making and client action.
* **Security Framework Proficiency:** Fluent in applying NIST, CIS, ISO 27001, and industry-specific standards like HIPAA, CMMC, etc.
* **Strategic Planning:** Skilled at creating security roadmaps that align with client business objectives, budgets, and growth plans.
* **Regulatory Knowledge:** Understands the nuances of data protection laws and compliance requirements across various sectors.
* **Incident Response Leadership:** Experience designing, leading, and improving incident response playbooks and post-incident reviews.
* **Policy Development:** Able to draft and update security policies and procedures that are practical, enforceable, and client-appropriate.
* **Executive Reporting & Presentation:** Can communicate security priorities to CEOs, boards, and non-technical decision-makers in plain language.
* **Technical Acumen:** Understands security controls across common MSP toolsets (EDR, patching, MFA, IAM, backup, etc.).
* **Performance Monitoring:** Capable of defining KPIs and tracking the effectiveness of security services with data-backed insights.
* **Client-Facing Presence**: Confident and professional demeanor with the ability to build trust and credibility with clients.
* **Business-Oriented Thinking**: Prioritizes security initiatives that align with business risk, continuity, and operational goals.
* **Adaptability**: Can tailor approach for clients at different stages of maturity, in varied industries, or with unique constraints.
* **Leadership Without Authority**: Influences internal and external teams without direct control—especially across MSP functions.
* **Critical Thinking & Judgment**: Applies sound judgment in ambiguous scenarios and balances ideal solutions with real-world constraints.
* **Proactive Communication**: Keeps clients informed with clarity, urgency, and context—avoids surprises or reactive posture.
* **Continuous Learner**: Keeps up with emerging threats, compliance trends, and evolving best practices in the cybersecurity field.
* **Process Discipline**: Comfortable using structured methods for documentation, reviews, and planning (e.g., ITIL, CSF, PDCA).

### **Preferred Experience, Skills, and Certifications:**

* Prior experience as a CISO or senior security leader (in-house or virtual)
* Strong knowledge of cybersecurity frameworks, standards, and risk management practices
* Experience working with SMBs or mid-market clients in regulated industries
* Ability to communicate clearly with both technical teams and executive stakeholders
* Familiarity with the MSP model and service delivery frameworks (ITIL, CSF, etc.)
* Have (or achieve within 6 months):
  + CompTIA Sec+
  + CompTIA CySA+
  + CompTIA CASP
  + CISM / CISSP
  + Carnegie Mellon CISO Program
  + CRISC

### **Engagement Model:**

* Virtual/remote role with structured monthly or quarterly client interactions
* This may include onsite meetings, security program reviews, and participation in board or leadership sessions
* Supported by technical teams for tactical execution (e.g., MDR, EDR, compliance automation)