Job Description: Consultant - IT Security Auditor
Location: Remote
Department: Service Delivery
Employee Type: Full Time

Purpose of Position:
The Lead Internal Auditor will own the internal audit lifecycle for the Information Security Management System (ISMS) and supporting controls environment, ensuring readiness for external certifications/attestations (ISO 27001, SOC 2, and where applicable PCI/NIST-based programs). This role combines hands-on control testing with program leadership, stakeholder coaching, and continuous improvement of security and compliance processes.

Accountability
The IT Security Auditor is directly accountable to the Director of Service Delivery and will undergo a yearly performance review.

Duties and Responsibilities

- Lead the annual and ongoing internal audit program for ISO 27001, including audit planning, fieldwork, reporting, and recommendations.
- Coordinate and perform internal readiness assessments for SOC 2 (Type I/II), testing control design and operating effectiveness against the Trust Services Criteria.
- Support or lead internal assessments against PCI DSS requirements (e.g., evidence review, control walkthroughs, remediation tracking).
- Perform gap analyses against ISO 27001, SOC 2, and applicable NIST frameworks to identify control weaknesses, process gaps, and improvement opportunities.
- Review and test security, availability, confidentiality, and related controls (e.g., access management, logging/monitoring, change management, backup/recovery, vendor management).
- Conduct document reviews of policies, standards, procedures, ISMS manuals, and records to verify compliance with ISO 27001 and SOC 2 expectations.
- Lead stakeholder interviews and process walkthroughs with IT, Security, Engineering, HR, Legal, and Operations to understand control design and implementation.
- Prepare clear audit reports that summarize scope, approach, findings, and prioritized recommendations, including suggested corrective actions.
- Serve as internal subject matter expert for ISO 27001, SOC 2, and related frameworks (e.g., NIST CSF, PCI DSS), advising teams on control requirements and evidence expectations.
- Champion continuous improvement of the ISMS and broader security/compliance program, recommending enhancements to controls, metrics, and governance.
- Ensure internal audit independence and objectivity by avoiding conflicts of interest with control design or day-to-day ownership.
- Contribute to training and awareness efforts on audit readiness, evidence quality, and control operation for technical and non-technical staff

Qualifications

- Bachelor's degree in information security, computer science, accounting, or a related field (or equivalent experience).
- Proven experience (typically 5–8+ years) in internal audit, IT audit, or security/compliance roles with direct responsibility for ISO 27001 and/or SOC 2 programs.
- Strong knowledge of ISO/IEC 27001 requirements and ISMS concepts, including risk assessment, Statement of Applicability, and continual improvement.
- Hands-on experience testing controls against SOC 2 Trust Services Criteria.
- Familiarity with PCI DSS and NIST Cybersecurity Framework (or NIST 800-53/171) and their typical control expectations.
- One or more relevant professional certifications such as ISO 27001 Lead Auditor/Lead Implementer, CISA, CISSP, CISM, or SOC-related credentials.
- Demonstrated ability to perform control design assessment, sampling, and evidence evaluation in complex technical environments (e.g., cloud, SaaS).
- Excellent written and verbal communication skills, including the ability to explain audit results and security concepts to both technical and executive audiences.
- Strong attention to detail, analytical mindset, and ability to maintain objectivity under pressure while upholding audit ethics.
- You will need to be organized, efficient and able to work unsupervised under your own initiative.

Preferred Qualifications

- Experience in technology, SaaS, financial services, healthcare, or other regulated industries with mature security/compliance requirements.
- Prior involvement in achieving or maintaining ISO 27001 certification and SOC 2 Type II reports, including remediation program leadership.
  Exposure to additional frameworks or regulations (e.g., HIPAA, GDPR, HITRUST, CIS Controls).
- Experience with GRC or audit management tools for issue tracking, evidence collection, and workflow management.

Why SemperSec?

This role offers employees the opportunity to work with a diverse range of industries from clients that create state of the art robotics that perform complicated surgeries, drone manufacturers delivering the next generation of unmanned aircraft, to startups building the next generation of agentic artificial intelligence tools. Each engagement is unique with distinct challenges and opportunities and will give skilled individuals a broad base of experience to further their career as information security specialists, managers, and developers.

Compensation And Benefits

Salary: $80000-$120,000

The actual salary offer will carefully consider a wide range of factors, including your skills, qualifications, experience and is based on a 40-hour work week.
Benefits:

- Health and dental insurance
- Vision insurance
- Flexible Time Off
- 401(k) plan