INCRUITER
TECH DRIVEN HIRING SOLUTION

IN0095386

Sagar Shah | Chief Information Security Officer | 13.0 years
Company: Paysquare Consultancy Ltd

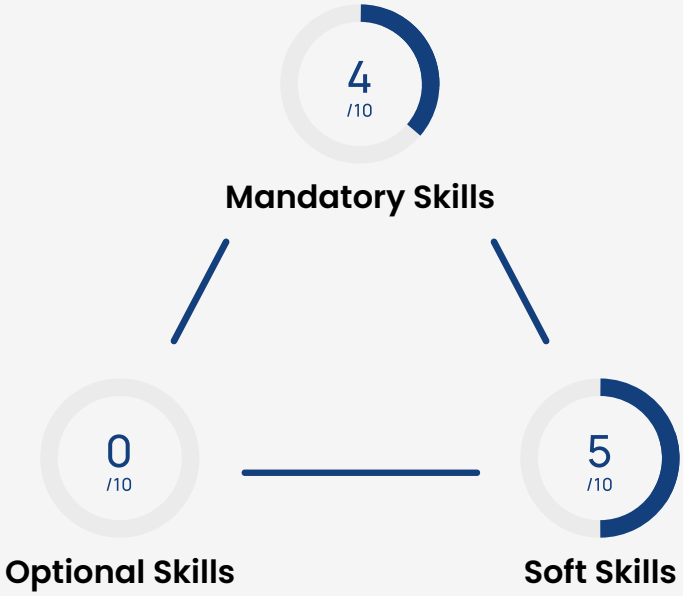
link2sagar@gmail.com | +919653662759

Date of Interview: Sat, Jun 1, 2024 11:00 AM

Resume Summary

- - 13+ years in information security, risk management, and cybersecurity technology. - Expertise in pre-sales solution architecture, cybersecurity services, and consultancy. - Hands-on experience with Azure and AWS native security controls. - Skilled in bid response, cost modeling, and developing competitive proposals. - Knowledgeable in disaster recovery planning, auditing, risk analysis, and contingency planning. - Managed security operations centers (SOC) and compliance with standards like NIST, ISO 27001. - Led large teams, managed multi-crore budgets, and provided project/program management leadership. - Experience in infrastructure management, cloud security, data protection, and vulnerability management. - Developed strategic visions for cybersecurity practices aligned with business objectives. - Built partnerships, designed solutions, and responded to RFPs in line with client requirements.

Overall skills



Soft Skills

- **Confidence** — Low Self-Assurance
- **Communication** — Avg. Communication
- **Pressure Handling** — Vulnerable

Analytical Skills

- **Approach & Attitude** — Poor
- **Problem Solving** — Moderate
- **Result Oriented** — Passable

Leadership Skills

- **Decision Making** — Moderate
- **Team Management** — Poor Admin. & Control
- **Accountability** — Low Accountability

Mandatory Skills

CISM

Poor

Optional Skills

CISSP

Very Poor

CCISO

Very Poor

Detailed Feedback

Final Remarks

Strengths:
- Exhibits knowledge of regulatory compliance, including RBI, SEBI, and ISO standards
- Shows understanding of security policies, standards, and the importance of aligning them with business objectives

Weaknesses:
- Lacks direct experience with law enforcement communication in cybersecurity contexts
- Unclear on the specifics of handling data breaches and the associated steps post-breach
- Admits to not having completed certifications like CISM or CISSP, indicating a potential gap in formal qualification
- Has not developed an SDLC policy from scratch, suggesting a limitation in policy development experience
- Shows uncertainty when discussing the details of RTO and RPO in business continuity
- Lacks direct experience in performing comprehensive risk assessments for an entire information security program
- Admits to weakness in handling management, particularly in convincing non-technical stakeholders
- Uncertain about the selection criteria and process for vendor management

Areas of Improvement:
- Gain experience in liaising with law enforcement agencies to enhance incident response capabilities
- Develop a clearer understanding and methodology for handling data breaches, including post-breach actions
- Pursue and complete relevant certifications to solidify formal knowledge in cybersecurity
- Enhance skills in policy development, particularly in creating SDLC policies from the ground up
- Improve understanding of business continuity concepts, specifically RTO and RPO definitions and applications
- Acquire comprehensive risk assessment skills to evaluate and improve the security posture of an entire organization
- Strengthen management skills, focusing on effective communication with non-technical leadership
- Learn the intricacies of vendor selection processes to better manage third-party risks

Conclusion:
The candidate knows ISMS but has not worked on many implementation projects which are very essential for a CISO role. Like as risk assessment, GDPR, ISMS awareness, Senior Management, Policies, Standards, Business continuity etc.
He doesn't have any certification as well, Like CISA, CISM, ISO etc which is mandatory.

Screening Questions

1. What Actions Should Be Carried to Investigate the Data Breach

No experience, in data breach investigation. Technical information on Root cause analysis is poor.

2. What Techniques do You Apply to Stay Updated About the Latest Cybersecurity News, Tools, and Threats?

By joining forums, and tools within the organization for current updates.

3. Can You Highlight Your Biggest Weakness and one failure in your career?

weakness handling of management. does not have people convincing.

4. What is Your Experience in Dealing with Law Enforcement Organizations?

No experience. haven't worked with any of the law enforcement agency

5. How would You Help us Strengthen Our Organization's Cybersecurity Efforts?

Do not have a clear vision about how cybersecurity is strengthened. moreover a process-driven candidate.

6. Do You Have Any Experience in Building Information Security Policies?

Candidate do not have experience in drafting from the scratch

7. Which Strategies Do You Use to Ensure Security in the Remote Work Environment?

Basic knowledge of authentication, authorization, VPN connectivity

8. How Do You Prioritize Security Projects Within an Organization?

good knowledge to priotize the project based of regulatory and client criticality

9. How Do You Handle Conflicts Between Security Needs and Business Objectives?

good knowledge presented with good examples of customer data.

10. Could You Recount an Instance Where You Were Required to Manage a Significant Security Incident?

incident management process with good knowledge. but lacks the communication towards client

11. What Are Your Strategies for Ensuring Compliance with Various Security Regulations?

SEbi. RBI guideline, ISO27001, SOC2, NIST partially HIPAA, PCI DSS

12. How Do You Cultivate a Security-Conscious Culture Within an Organization?

No clear vision for how to implement ISMS culture in the organization

13. How Do You Assess and Implement Advanced Threat Protection Systems?

Yes, Checkpoint is been implemented but this is with a team efforts

14. Describe Your Experience with Cloud Security Management. AWS or Azure

Yes, AWS and Azure. monitoring controls and access controls.

15. What Approaches Do You Utilize to Ensure Security in the Software Development Life Cycle (SDLC)?

only knowledge on the change management. documents are revied

16. How Do You Approach Data Encryption and Key Management in a Large Enterprise?

HP encryption tools are used. masking is also used. Key management does not experience.

17. How Do You Evaluate and Manage Vendor Security Risks?

Yes. Onboarding to offboarding. but do not Indepth knowledge

18. Describe Your Method for Implementing Security Information and Event Management (SIEM) Solutions.

monitoring and transition. qradar, mccafe, fortysiem

19. How Do You Manage Insider Threats in an Organization?

Basic knowledge. explained well about insider threat as per ISMS but not as per financial organization.

20. How Extensive is Your Experience With Cybersecurity Standards Like NIST and ISO and other Audits

Do not have good audit process knowledge and has not driven any project alone.

21. How Do You Approach Cybersecurity Training and Awareness Programs?

do not have good knowledge only basic understanding of trainings. has implemented any project on this.

22. Describe Your Experience With Security Audits and Compliance Assessments.

have managed ISO27001 SOC and regulatory audit as a team member but not driven solely

23. What is Your Strategy for Incident Response and Disaster Recovery?

have not defined BC/DR project, was only involved in Testing.

24. Please share your experience in risk management.

No experience with risk management, treatment or assement

25. What strategies would you employ in a dynamic legal environment to ensure continuous compliance with international data protection laws, such as GDPR and CCPA?

No experience GDPR, CCPA or any other data privacy

26. How would you assess the cybersecurity maturity of an organization and identify key areas for improvement?

No experience. basic knowledge of it. have not done any cybersecurity maturity assessment project

Soft Skills

Confidence (Low Self-Assurance)
Unlikely to have knowledge, skills, and abilities more than 10-20%.

Communication (Avg. Communication)
Somewhat likely to be able to structure one's thoughts and communicate in a clear, concise, and accurate manner. Moderately likely to be a good listener.

Pressure Handling (Vulnerable)
Unlikely to exhibit more than 20-30% capabilities to accomplish work during a critical phase.

Analytical Skills

Approach & Attitude (Poor)
Unlikely to be approachable and this attitude negatively impacts the morale of the team. Occasionally delivers work using a strategic approach. Easily gets frustrated.

Problem Solving (Moderate)
Somewhat likely to identify potential problems or investigate them in greater depth and choose the best solution. Identifies risks and takes appropriate actions.

Result Oriented (Passable)
Somewhat likely to be able to achieve results on time. Moderately enthusiastic while working on challenging tasks.

Leadership Skills

Decision Making (Moderate)
Somewhat likely to take inputs before making important decisions. May occasionally weigh the possible consequences of decisions.

Team Management (Poor Admin. & Control)
Unlikely to take an interest in the work of team members or coach them on how to execute tasks effectively. Less likely to provide constructive feedback and improve the performance of the team.

Accountability (Low Accountability)
Unlikely to take responsibility for one's own actions or decisions. Unlikely to take one's duties and responsibilities seriously. Less likely to be a self-starter.

Screenshots

INCRUITER®
TECH DRIVEN HIRING SOLUTION

Very Poor : <=2 Poor : 3 to 4 Average : 5 Above Average : 6 Good : 7 Very Good : 8 Excellent >= 9