Lexonis

INTERVIEW GUIDE

Information Security Specialist

© Lexonis 2026

Job Reference:	
Candidate Name:	
Date:	
Time:	
Interviewer(s):	

Interview Preparation

- Review screening notes, CV, testimonials and selection testing.
- Note experience relevant to the vacancy; prepare probes for CV gaps.
- Review Key Responsibilities and the competencies to probe.
- Adapt or add questions as required; agree time per section.

During the Interview

- Introduce yourself, your role, and why you're part of the interview.
- Briefly describe the organization and the interview process.
- Confirm all candidates are asked the same core questions.
- Note-take (confirm recording if used); avoid discriminatory questions.
- Leave time for the candidate's own questions.

Information Security Specialist (SE-5SEC)

Develops and implements security standards, procedures, and guidelines for multiple platforms and diverse system environments; facilitates system access, operations, and maintenance.

Key Responsibilities

- Providing resolutions to controlling security risks and threats in IT environments; delivering training to staff on distributed information security administration procedures.
- Investigating and recommending corrective actions for data security incidents to clients and project stakeholders.
- Conducting vulnerability assessments, malware defense assessments and other information security routines, consistently.
- Identifying regulatory changes that will affect information security policies, standards and procedures; recommending appropriate changes.

Job Band: Team Leadership; Technical Professional: Difficult technical tasks; Implementation experience; Self-sufficiency; Small project responsibility; Technical supervision
Job Focus: Technical: Focus on technical activities that require specialized knowledge

#	Rating	Definition
1	**Below Level**	Demonstrates competency inconsistently, even with repeated instruction. Answers are often unclear or off-topic, with few relevant examples and limited understanding of the role.
2	**Meets Level**	Demonstrates basic competency with occasional guidance. Answers are generally clear and relevant, with a moderate number of examples and adequate understanding of the role.
3	**Above Level**	Consistently demonstrates strong competency with minimal guidance. Answers are clear, detailed and directly relevant, with many strong examples and deep understanding of the role.

© Lexonis 2026

Competency Related Questions

1. Information Assurance – Experience with Information Assurance

Purpose: *To understand the candidate's background and level of expertise in information assurance, allowing for a more informed discussion of their skills and experiences.*

Q Tell me about your previous experience or involvement in information assurance.

↳ Follow-up: Can you walk me through a specific example of how you applied information assurance principles to ensure the security of sensitive data?

Notes:

Model answer: A good model answer would be to provide specific examples of projects or initiatives you've worked on that demonstrate your understanding of information assurance principles and best practices. This could include details about the role you played, the challenges you faced, and how you contributed to the overall success of the project.

Rating:

2. Information Security Technologies – Detect Security Breaches

Purpose: *To understand the candidate's experience with detecting and mitigating security breaches, as well as their ability to describe specific technologies used in this process.*

Q What kinds of technologies did you use to detect security breaches?

↳ Follow-up: Can you give an example of a specific technology you used to detect a security breach, and how it helped your team mitigate the impact?

Notes:

Model answer: A good model answer would be a detailed description of various technologies used, such as intrusion detection systems, threat intelligence platforms, or behavioral analytics tools. The candidate should demonstrate an understanding of how these technologies help detect and respond to security breaches.

Rating:

3. Information Security Audits – Problems with Security Audits

Purpose: *To understand the challenges and difficulties faced by candidates while conducting security audits, and to gauge their problem-solving skills.*

Q What kinds of problems did you encounter when conducting information security audits?

↳ Follow-up: Can you walk me through a particular instance where you faced a significant challenge during the security audit? How did you overcome it?

Notes:

Model answer: A good model answer would be one that highlights specific obstacles encountered during the audit process, such as lack of resources or inadequate training, and demonstrates an understanding of how these issues were addressed.

Rating:

© Lexonis 2026

4. Information Security Administration – Control Information Security Risk Factors

Purpose: *To assess the candidate's understanding of information security risk factors and their ability to control them effectively.*

Q How did you control information security risk factors within a prescribed limitation in your previous position(s)?

↳ Follow-up: Can you walk me through a specific situation where you had to balance the need for information security with other business priorities?

Notes:

Model answer: A good model answer would demonstrate a clear understanding of information security risk factors, such as data breaches or unauthorized access, and provide specific examples of steps taken to mitigate these risks within prescribed limitations.

Rating:

5. Information Security Operation Center (ISOC) – Experience with ISOC

Purpose: *To understand the candidate's hands-on experience and skills acquired while working with ISOC, which will help assess their ability to work with similar systems in this role.*

Q Tell me about your working experience with ISOC in your previous job.

↳ Follow-up: Can you walk me through the specifics of how you implemented this system, and what were some of the key challenges you faced during that process?

Notes:

Model answer: A good model answer would be a concise description of the specific tasks, responsibilities, and technologies involved in your previous role, highlighting any notable achievements or challenges you overcame. For example: 'In my previous role, I worked with ISOC to develop an automated reporting system, which improved data accuracy by 20%. I was responsible for designing and implementing the system architecture, working closely with the development team to ensure seamless integration.'

Rating:

6. Penetration Testing – Difference with Vulnerability Assessment

Purpose: *To assess the candidate's understanding of the concepts and their ability to differentiate between penetration testing and vulnerability assessment.*

Q What is the difference between penetration testing and vulnerability assessment?

↳ Follow-up: Can you provide an example of when penetration testing would be more effective than vulnerability assessment?

Notes:

Model answer: A good model answer would be one that explains the differences between the two, such as 'Penetration testing is a simulated attack on an organization's computer system to identify vulnerabilities, whereas vulnerability assessment is the process of identifying and prioritizing vulnerabilities before they can be exploited.'

Rating:

© Lexonis 2026

7. Vulnerabilities Assessment – Experience with Vulnerability Assessment

Purpose: *To understand the candidate's practical application of vulnerability assessment skills and their ability to articulate their thought process*

Q Describe your working experience with vulnerability assessment in your previous job.

↳ Follow-up: Can you give an example of a particularly challenging vulnerability assessment you conducted and how you overcame any obstacles?

Notes:

Model answer: A good model answer would provide a clear overview of the vulnerability assessment process, highlighting specific tools or methodologies used, and demonstrating an understanding of the importance of vulnerability assessments in a previous role.

Rating:

8. Information Security Management – Problems with Handling Incidents

Purpose: *To understand the candidate's experience and skills in dealing with security incidents and vulnerabilities, and to assess their ability to provide effective solutions.*

Q What kinds of problems did you encounter in handling security incidents and vulnerabilities?

↳ Follow-up: Can you give an example of a particularly challenging security incident you handled in the past, and how did you resolve it?

Notes:

Model answer: A good model answer would be one that highlights specific challenges faced by the candidate, such as lack of resources or inadequate training, and how they overcame these obstacles. The answer should also demonstrate a deep understanding of incident handling best practices and a commitment to continuous learning.

Rating:

9. Encryption Technologies – Security and Efficiency

Purpose: *To understand the candidate's approach to balancing competing priorities in a complex system*

Q What did you do to achieve a balance between the level of security and decryption efficiency?

↳ Follow-up: Can you provide an example of how you implemented one of these strategies, and what were the results?

Notes:

Model answer: A good model answer would demonstrate an understanding of the importance of finding a balance between security and efficiency, highlighting specific techniques or strategies used to achieve this balance.

Rating:

© Lexonis 2026

10. Security Information and Event Management (SIEM) – Problems in SIEM Deployment

Purpose: *To assess the candidate's experience with solving common issues during SIEM deployment and their problem-solving approach.*

Q What kinds of problems have you met in the SIEM deployment processes, and how did you solve them?

↳ Follow-up: Can you elaborate on what kind of data integration challenges you faced during the SIEM deployment process?

Notes:

Model answer: A good model answer would highlight specific challenges they've faced, such as data integration or configuration issues, and describe the steps they took to resolve them, including any collaboration or research involved.

Rating:

11. Firewall Management – Describe a Major Challenge

Purpose: *To understand how the candidate handles obstacles and adapts to change, as well as their problem-solving skills and ability to reflect on past experiences.*

Q Describe a major challenge you've experienced with this process or area. How did you deal with it? What was the resolution?

↳ Follow-up: Can you elaborate on what you mean by 'resolution' in this context? How did you measure its effectiveness?

Notes:

Model answer: A good model answer would be one that provides a specific example of a challenge they faced, describes the steps they took to address it, and highlights any key takeaways or lessons learned from the experience.

Rating:

12. Crisis Management – Describe Crisis and Response

Purpose: *To assess the candidate's ability to think critically about crisis situations and develop a thoughtful response.*

Q Describe a crisis scenario and an effective and appropriate response.

↳ Follow-up: Can you walk me through your thought process when developing this response? How did you prioritize the different stakeholders involved?

Notes:

Model answer: A good model answer would describe a clear and concise scenario, highlighting key stakeholders, potential risks, and a well-considered response plan that addresses the crisis.

Rating:

© Lexonis 2026

13. Effectiveness Measurement – Measurement Driven Improvements

Purpose: *Understand how the candidate uses data-driven insights to inform decision-making and drive positive change.*

Q Tell me about a time that a measurement prompted you to implement process or policy changes. What improvements were seen?

↳ Follow-up: Can you walk me through the steps taken to implement these changes and what role did stakeholder engagement play in the process?

Notes:

Model answer: A good model answer would demonstrate self-awareness of the impact of measurements on organizational improvements, highlighting specific numbers and metrics that led to meaningful changes.

Rating:

14. Standard Operating Procedures – SOP Implementation

Purpose: *To assess the candidate's understanding of Standard Operating Procedure (SOP) implementation and their ability to share specific experiences.*

Q Describe your experience with SOP implementation within a department.

↳ Follow-up: Can you elaborate on how you addressed any resistance or concerns from team members during the SOP implementation process?

Notes:

Model answer: A good model answer would provide a clear example of an SOP they implemented, including the steps taken, challenges faced, and outcomes achieved.

Rating:

15. Problem Solving – Conflicting Solutions

Purpose: *To assess the candidate's ability to handle conflicting opinions, evaluate different solutions, and resolve issues collaboratively.*

Q Tell me about a time that two or more colleagues had conflicting ideas on the best way to solve a problem. How were the ideas evaluated and the issue resolved?

↳ Follow-up: Can you explain why you think your approach helped resolve the issue successfully?

Notes:

Model answer: A good model answer would be one where the candidate describes a situation where colleagues had differing opinions, how they addressed the conflict, and the outcome. For example: 'In my previous role, I was part of a team tasked with implementing a new project management tool. Two of my colleagues, John and Sarah, had different ideas on which tool to use. John believed that Tool A was more efficient, while Sarah thought Tool B was more user-friendly. To address the conflict, we decided to create a pros-and-cons list for each tool and then voted on which one to implement. We ultimately chose Tool B because it received the most votes.'

Rating:

© Lexonis 2026

16. Confidentiality – Demonstrate Breach of Confidentiality Process

Purpose: *To assess the candidate's understanding and adherence to confidentially policies, as well as their ability to handle a sensitive situation.*

Q What would you do if you heard a co-worker had breached the organization's policies on confidentiality?

↳ Follow-up: Can you give me a specific example of how you would handle this situation?

Notes:

Model answer: A good model answer would involve reporting the incident to the appropriate authority, such as HR or management, while also ensuring the integrity of any confidential information that may have been compromised. The candidate should demonstrate an understanding of the importance of maintaining confidentiality and the procedures in place for handling breaches.

Rating:

After the Interview

1. Thank the candidate for coming to the interview.
2. Check on their availability and their current notice period.
3. Discuss the candidate's remuneration expectations.
4. Explain where you are in the interview process.
5. Indicate when the candidate should expect to hear from you.
6. Inform the candidate that they may be asked to attend a second interview (if appropriate).
7. Allow the candidate to ask any additional questions.
8. Close the meeting.

© Lexonis 2026

Notes

© Lexonis 2026

Rating Summary

	Rating
Information Assurance - Experience with Information Assurance	
Information Assurance - Mitigation Techniques	
Information Assurance - Problems in Certification Programs	
Information Assurance - Problems with Strategy Implementation	
Information Assurance - Assess Vulnerability	
Information Security Technologies - Detect Security Breaches	
Information Security Technologies - Dissolve Information Dangers	
Information Security Technologies - Integrate Security Systems	
Information Security Technologies - Problems with Package Implementation	
Information Security Technologies - Upgrade Anti-Virus System	
Information Security Audits - Experience with Information Security Audit	
Information Security Audits - Information Security Audit Key Areas	
Information Security Audits - Perform Multiple Security Evaluations	
Information Security Audits - Problems with Security Audits	
Information Security Audits - Review Plan Implementation	
Information Security Administration - Control Information Security Risk Factors	
Information Security Administration - Experience with Information Security Administration	
Information Security Administration - Improve Procedural Effectiveness	
Information Security Administration - Benefits of Information Security Programs	
Information Security Administration - Problems with Program Administration	
Information Security Operation Center (ISOC) - Differences Between Host and Network Monitoring	
Information Security Operation Center (ISOC) - Experience with ISOC	
Information Security Operation Center (ISOC) - Operating Processes of ISOC	
Penetration Testing - Difference with Vulnerability Assessment	
Penetration Testing - Ethical Issues as a Penetration Tester	
Penetration Testing - Experience with Penetration Testing	
Vulnerabilities Assessment - Comparing Different Vulnerability Assessment Tools	
Vulnerabilities Assessment - Experience with Vulnerability Assessment	
Vulnerabilities Assessment - Problems on using Fault Tree Method	
Information Security Management - Enhance Security Architecture	
Information Security Management - Detect Security Breaches	
Information Security Management - Problems with Handling Incidents	
Information Security Management - Problems with Defining Standards	

© Lexonis 2026

Information Security Management - Use of Information Platforms	
Encryption Technologies - Comparing Encryption Techniques	
Encryption Technologies - Bridging Multiple Technologies	
Encryption Technologies - Security and Efficiency	
Encryption Technologies - Width of Professional Knowledge	
Security Information and Event Management (SIEM) - Compliance Issues in SIEM	
Security Information and Event Management (SIEM) - Experience with SIEM	
Security Information and Event Management (SIEM) - Problems in SIEM Deployment	
Firewall Management - Describe a Major Challenge	
Firewall Management - How Best Can You Contribute?	
Firewall Management - Technical Problem Resolution	
Firewall Management - Toolkit Development	
Crisis Management - Describe Crisis and Response	
Crisis Management - Describe Disaster Recovery Plan Success	
Crisis Management - Past Experience Crisis Management Process	
Effectiveness Measurement - Explaining the Need for Measures	
Effectiveness Measurement - Measurement Comparisons	
Effectiveness Measurement - Measurement Driven Improvements	
Effectiveness Measurement - Measurement Tool Selection	
Effectiveness Measurement - Selecting Appropriate Measures	
Standard Operating Procedures - Problems in SOP Design	
Standard Operating Procedures - SOP Evaluation	
Standard Operating Procedures - SOP Implementation	
Standard Operating Procedures - SOPs and Performance Improvement	
Problem Solving - Conflicting Solutions	
Problem Solving - Failed Solutions	
Problem Solving - Problem Impacts and Work-arounds	
Problem Solving - Use Market Research to Solve Problems	
Problem Solving - Solving Long-term Problems	
Confidentiality - Demonstrate Breach of Confidentiality Process	
Confidentiality - Past Confidentiality Tools Experience	
Confidentiality - Past Experience Inappropriate Information Disclosure	
Candidate Rating / Total Rating	/

© Lexonis 2026