hr | avatar
Illuminating Talent

Test Results and Interview Guide

Candidate: **Elizabeth Wantsajob**
Assessment: Information Security Analysis
Completed: June 30, 2026
Prepared for: Sara Maple
Example Company

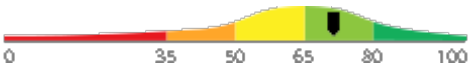
What's Included

- Overall Score
- Competency Summary Table
- Comparison Matrix
- Detailed Competency Results with Interview Guide

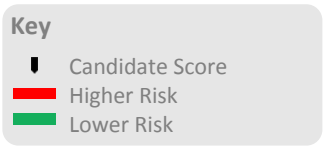
Important Note: The Information Security Analysis assessment measures key factors related to high performance and tenure in this job. Attribute types measured vary by test, but can include cognitive ability, skills, knowledge, personality characteristics, emotional intelligence, and past behavioral history. This report includes a one page summary, followed by detailed results with an embedded interview guide. Note that these results should always be used as a part of a balanced candidate selection process that includes independent evaluation steps, such as interviews and reference checks.

Proprietary and Confidential

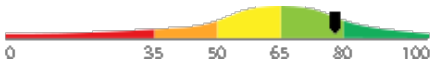
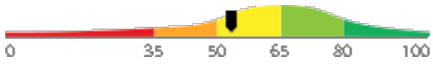
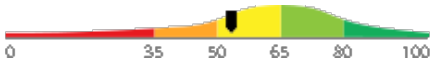
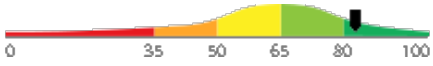
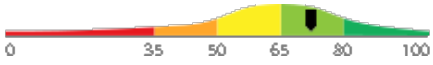
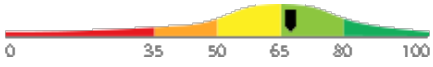
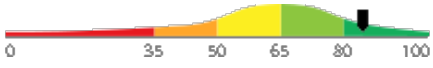
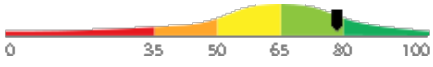
Overall

Candidate	Score	Interpretation
Elizabeth Wantsajob beth.wantsajob@gmail.com Information Security Analysis June 30, 2026	71	

The candidate exhibits a solid and well-rounded understanding of Information Security Analysis principles and practices, reflecting competency across most key domains including risk assessment, cryptography, vulnerability management, and incident response. Minor gaps may exist in select specialized areas, but the candidate demonstrates the knowledge base expected of a capable and contributing practitioner.



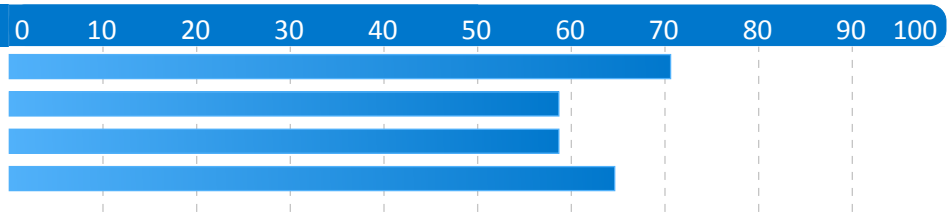
Competency Summary

Competency	Score	Interpretation
Skills/Knowledge (relates to immediate readiness)		
Access Control and Identity Management	78	
Network Security Monitoring and Incident Response (Free Text Responses)	53	
Threat and Vulnerability Assessment (Free Text Responses)	53	
Cryptography and Data Protection	83	
Malware Awareness and Social Engineering Defense	72	
Network Security Monitoring and Incident Response	67	
Security Policies, Compliance, and Risk Management	84	
Threat and Vulnerability Assessment	78	

Comparison

Percentile scores indicate how the candidate compares to other test-takers within various groups. The candidate scored equal to or better than the fraction of test-takers indicated by the percentile.

Test-Taker Group	Percentile
Global	71st
North America	59th
United States	59th
Example Company	65th



Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Artificial Intelligence (AI) Generated Scores

This table includes one or more scores derived from a large language model AI query. AI-derived scores are non-deterministic. That is, they are not precisely repeatable. Therefore, these scores should always be treated as supplementary information and should never be used exclusively or compared to hard cutoff values.

Estimated Value	Score	Confidence	Interpretation
Knowledge, Skills, and Abilities Summary	-	-	Summary Points (AI): • (Generic Text for Sample Report) Strong performer in Drag and Drop Files tasks, indicating comfort with file management and basic computer interactions. • Demonstrates solid numerical accuracy in Recognizing and Confirming Numbers, a valuable asset in detail-oriented roles. • Moderate overall performance in Analytical Thinking and Attention to Detail, with adequate grammar skills but room for improvement. • Struggles with Reading and Analyzing Problems, which may limit effectiveness in roles requiring critical reading and complex problem-solving. • Lowest performance in Navigating Between Screens, suggesting difficulty with multi-screen software workflows that could impact productivity in computer-intensive roles. Narrative (AI): Elizabeth Wantsajob demonstrates a mixed profile of knowledge, skills, and abilities across the assessed competencies. Elizabeth shows a strong aptitude in Drag and Drop Files, performing well on this technical task and suggesting she is comfortable with this type of computer interaction. This is a notable strength that would translate well into roles requiring file management and basic computer navigation tasks. In the area of Analytical Thinking and Attention to Detail, Elizabeth performs at a moderate level. She demonstrates solid ability in Recognizing and Confirming Numbers, which suggests she is careful and accurate when working with numerical data — a valuable skill in detail-oriented work environments. Her Grammar performance is adequate but leaves room for improvement, indicating she may occasionally make written communication errors. Her weakest area within this competency is Reading and Analyzing Problems, where she struggled to consistently interpret and work through written problem scenarios. This may impact her effectiveness in roles that require critical reading, written comprehension, or complex problem-solving. Elizabeth's most significant area for development is Navigating Between Screens, where she scored considerably lower than the other competencies. This suggests she may have difficulty efficiently moving through software interfaces or multi-screen workflows, which could slow productivity in roles that rely heavily on navigating computer applications or data entry systems. Overall, Elizabeth brings some useful technical strengths, particularly in file management and numerical accuracy, but would benefit from targeted development in software navigation and analytical problem-solving to be fully effective in roles that demand these skills. Computed on: April 2, 2026, 11:09:49PM EDT

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail

Candidate:	Elizabeth Wantsajob, beth.wantsajob@gmail.com
Assessment:	Information Security Analysis
Authorized:	June 30, 2026, by Sara Maple, Example Company, qamailsaram.mike@hravatar.com
Started:	June 30, 2026, 5:57:17PM EDT
Completed:	June 30, 2026, 5:57:17PM EDT
Overall Score:	71

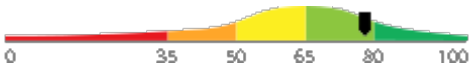
Knowledge and Skills Detail

This section contains a list of job-related knowledge areas and skills that have been evaluated. Low scores in these areas often indicate that additional learning may be required before top performance can be achieved.

Detail | Interview Guide

Access Control and Identity Management

Score: 78



Description:

The principles and practices used to ensure that only authorized users can access systems, data, and resources. This includes authentication methods, authorization models, account lifecycle management, and the principle of least privilege.

Interpretation:

Candidate should achieve above average job performance in this area with little or no training.

The candidate demonstrates a solid and proficient understanding of Access Control and Identity Management, including authentication methods, authorization models, account lifecycle management, and the principle of least privilege. They are likely capable of applying these concepts effectively in most professional information security contexts, with only minor gaps in specialized or advanced areas.

A user in your organization reports they can access files and systems beyond what their job role requires. How would you handle this situation?

1	2	3	4	5
Suggests ignoring it or simply telling the user not to access those resources without any remediation.		Recommends reviewing and adjusting permissions but does not mention auditing, documentation, or policy.		Describes a full review of access rights, remediation, audit logging, and alignment with access control policy.

What does the principle of least privilege mean, and can you give an example of how it would be applied in a workplace setting?

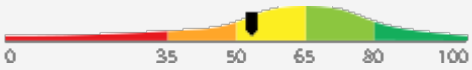
1	2	3	4	5
Cannot define least privilege or provides an inaccurate definition with no practical example.		Correctly defines least privilege but gives only a simple or generic example without depth.		Defines least privilege clearly and provides a specific, realistic example tied to role-based access or account management.

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail

Network Security Monitoring and Incident Response (Free Text Responses)

Score: 53



Description:

Covers the end-to-end process of planning, building, testing, and deploying AI-enabled applications for both internal staff and external customers. Includes managing iteration cycles, versioning, model monitoring, and coordinating cross-functional teams through each phase of the product lifecycle.

Interpretation:

The candidate exhibits average writing skills, which can hinder high performance in some jobs.

The candidate possesses a moderate understanding of AI product management, demonstrating basic familiarity with lifecycle management, strategic assessment, and process orchestration, though proficiency across these areas is inconsistent. With targeted coaching and hands-on experience, this individual has the potential to develop into a capable contributor in managing AI-enabled application initiatives.

Overall AI Score:	60.0
High words per minute detected while composing one or more essays:	27.3 words per minute. Possible copy/paste or use of AI tools. Average WPM while composing is about 15.
AI Confidence Level:	80
Argument Strength (AI):	70.0
Clarity and Coherence (AI):	80.0
Match with Ideal Response (AI):	60.0
Other Errors per 100 Words:	0.0
Spelling errors per 100 words:	0.0

Please see below to view the essay submitted.

Interview Guide

Describe a time you managed or contributed to an AI product through multiple lifecycle stages. What were the most significant challenges you encountered between phases, and how did you address them?

1	2	3	4	5
Candidate provides a generic or superficial example that lacks detail about AI-specific lifecycle challenges. Does not clearly articulate their personal role or the decisions they made between phases.		Candidate shares a relevant example with reasonable detail, identifying at least one meaningful challenge such as stakeholder alignment or testing delays. However, the response may lack specificity about how AI-related factors (e.g., model performance, data readiness) influenced lifecycle decisions.		Candidate provides a detailed, concrete example that demonstrates ownership across multiple lifecycle phases. Clearly describes AI-specific challenges such as model validation failures, shifting requirements, or deployment infrastructure issues, and articulates the specific actions they took to resolve them and keep the product on track.

Can you walk me through the basic stages you would follow to take an AI-enabled product from an initial idea to a live deployment?

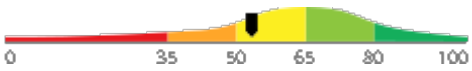
1	2	3	4	5
Candidate provides a vague or incomplete description of the lifecycle, omitting key phases such as testing, validation, or deployment. May conflate AI product development with general software development without acknowledging AI-specific considerations like model training or data pipelines.		Candidate identifies the major phases (discovery, development, testing, deployment) and acknowledges some AI-specific considerations, but struggles to articulate how the phases connect or how cross-functional teams are coordinated throughout.		Candidate clearly outlines a structured lifecycle including discovery, requirements, development, model validation, testing, deployment, and monitoring. Demonstrates awareness of AI-specific challenges such as data quality, model drift, and iterative retraining, and explains how they would coordinate stakeholders across phases.

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail

Threat and Vulnerability Assessment (Free Text Responses)

Score: 53



Description:

Covers the end-to-end process of planning, building, testing, and deploying AI-enabled applications for both internal staff and external customers. Includes managing iteration cycles, versioning, model monitoring, and coordinating cross-functional teams through each phase of the product lifecycle.

Interpretation:

The candidate exhibits average writing skills, which can hinder high performance in some jobs.

The candidate possesses a moderate understanding of AI product management, demonstrating basic familiarity with lifecycle management, strategic assessment, and process orchestration, though proficiency across these areas is inconsistent. With targeted coaching and hands-on experience, this individual has the potential to develop into a capable contributor in managing AI-enabled application initiatives.

Overall AI Score:	60.0
High words per minute detected while composing one or more essays:	27.3 words per minute. Possible copy/paste or use of AI tools. Average WPM while composing is about 15.
AI Confidence Level:	80
Argument Strength (AI):	70.0
Clarity and Coherence (AI):	80.0
Match with Ideal Response (AI):	60.0
Other Errors per 100 Words:	0.0
Spelling errors per 100 words:	0.0

Please see below to view the essay submitted.

Interview Guide

Describe a time you managed or contributed to an AI product through multiple lifecycle stages. What were the most significant challenges you encountered between phases, and how did you address them?

1	2	3	4	5
Candidate provides a generic or superficial example that lacks detail about AI-specific lifecycle challenges. Does not clearly articulate their personal role or the decisions they made between phases.		Candidate shares a relevant example with reasonable detail, identifying at least one meaningful challenge such as stakeholder alignment or testing delays. However, the response may lack specificity about how AI-related factors (e.g., model performance, data readiness) influenced lifecycle decisions.		Candidate provides a detailed, concrete example that demonstrates ownership across multiple lifecycle phases. Clearly describes AI-specific challenges such as model validation failures, shifting requirements, or deployment infrastructure issues, and articulates the specific actions they took to resolve them and keep the product on track.

Can you walk me through the basic stages you would follow to take an AI-enabled product from an initial idea to a live deployment?

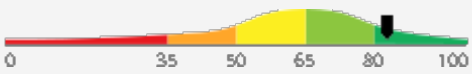
1	2	3	4	5
Candidate provides a vague or incomplete description of the lifecycle, omitting key phases such as testing, validation, or deployment. May conflate AI product development with general software development without acknowledging AI-specific considerations like model training or data pipelines.		Candidate identifies the major phases (discovery, development, testing, deployment) and acknowledges some AI-specific considerations, but struggles to articulate how the phases connect or how cross-functional teams are coordinated throughout.		Candidate clearly outlines a structured lifecycle including discovery, requirements, development, model validation, testing, deployment, and monitoring. Demonstrates awareness of AI-specific challenges such as data quality, model drift, and iterative retraining, and explains how they would coordinate stakeholders across phases.

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail

Cryptography and Data Protection

Score: 83



Description:

Understanding of how cryptographic methods such as hashing, symmetric encryption, and asymmetric encryption are used to protect data in storage and in transit. Includes practical knowledge of when and how to apply encryption, certificate management, and data classification to ensure sensitive information is handled appropriately.

Interpretation:

Candidate should achieve superior job performance in this area with little or no training.

The candidate demonstrates an advanced and comprehensive understanding of cryptography and data protection, reflecting strong proficiency in applying hashing, symmetric and asymmetric encryption, certificate management, and data classification to protect sensitive information. They are well-equipped to independently address complex information security challenges in this domain at a high level of expertise.

Interview Guide

Your organization needs to ensure that sensitive customer data stored in a database is protected. What cryptographic or data protection measures would you recommend and why?

1	2	3	4	5
Cannot recommend any specific measures or suggests only basic controls like passwords without cryptographic reasoning.		Recommends encryption at rest but does not address key management, data classification, or access controls.		Recommends encryption at rest and in transit, key management practices, data classification, and role-based access controls.

Can you explain the difference between encryption and hashing, and give an example of when each would be used?

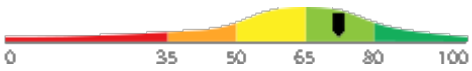
1	2	3	4	5
Cannot distinguish between encryption and hashing or uses the terms interchangeably with no examples.		Correctly distinguishes the two concepts but provides only basic or textbook examples without practical context.		Clearly explains both concepts and gives practical, accurate examples such as hashing passwords and encrypting files in transit.

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail

Malware Awareness and Social Engineering Defense

Score: 72



Description:

Knowledge of common malware types, how they spread, and how to defend against them. Also includes understanding social engineering tactics such as phishing, pretexting, and baiting, and the controls and user awareness strategies used to reduce their effectiveness.

Interpretation:

Candidate should achieve above average job performance in this area with little or no training.

The candidate demonstrates a solid working knowledge of malware behavior, propagation vectors, and social engineering tactics, along with the controls used to counter them. They are likely capable of applying this knowledge effectively in most practical information security contexts, with some room for deeper expertise.

Interview Guide

An employee contacts you saying they received a suspicious email asking them to click a link and verify their login credentials. How do you respond, and what steps do you take?

1	2	3	4	5
Tells the employee to just delete it with no further action, investigation, or awareness follow-up.		Identifies it as a phishing attempt and advises the employee but does not describe investigation or escalation.		Guides the employee, investigates the email headers and links, escalates, checks for clicks, and uses it as a training opportunity.

Can you name two or three common types of malware and explain how each one typically affects a system or network?

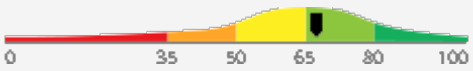
1	2	3	4	5
Cannot name or accurately describe any malware types; conflates malware with general hacking.		Names common types like viruses or ransomware but provides only surface-level descriptions of their effects.		Names and accurately describes multiple malware types, their behaviors, propagation methods, and potential impact.

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail

Network Security Monitoring and Incident Response

Score: 67



Description:

The ability to monitor network traffic and system logs to detect suspicious activity, and to follow a structured process to respond to security incidents. This includes using tools like firewalls, intrusion detection systems, and SIEM platforms, as well as executing containment, eradication, and recovery steps.

Interpretation:

Candidate should achieve above average job performance in this area with little or no training.

The candidate demonstrates a solid and competent understanding of network security monitoring and incident response, including the use of firewalls, intrusion detection systems, and SIEM platforms. They are likely capable of identifying suspicious activity and executing containment, eradication, and recovery steps with moderate independence.

Interview Guide

Describe a time or scenario where you used log analysis to identify a potential security incident. What indicators did you look for?

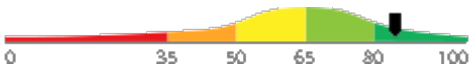
1	2	3	4	5
Cannot name specific log types or indicators of compromise; response is vague or generic.		Mentions reviewing event logs and looking for failed logins but does not discuss correlation or context.		Discusses correlating multiple log sources, specific IOCs, and using tools like SIEM to build a timeline.

If you noticed unusual outbound traffic from a workstation on your network, what would you do first and why?

1	2	3	4	5
Suggests only rebooting the machine or ignoring it; shows no awareness of incident response steps.		Mentions isolating the machine and notifying a supervisor but cannot describe further response steps.		Describes isolation, evidence preservation, investigation, escalation, and documentation in a logical sequence.

Security Policies, Compliance, and Risk Management

Score: 84



Description:

The ability to interpret and apply organizational security policies, and to understand compliance frameworks and regulations that govern how data must be protected. This includes assessing risk, applying controls, and ensuring that security practices align with standards such as NIST, ISO 27001, or regulatory requirements like HIPAA or PCI-DSS.

Interpretation:

Candidate should achieve superior job performance in this area with little or no training.

The candidate exhibits a strong and comprehensive understanding of security policies, compliance frameworks, and risk management, demonstrating the ability to confidently interpret, apply, and align security practices with established standards and regulatory requirements. They are well-equipped to operate at an advanced level in this domain with minimal oversight.

Your organization is preparing for a compliance audit under a framework like NIST or PCI-DSS. What steps would you take to help ensure the organization is ready?

1	2	3	4	5
Cannot name any compliance framework requirements or describe any preparation steps.		Mentions reviewing controls and gathering documentation but lacks a structured or complete approach.		Describes a gap analysis, control mapping, evidence collection, remediation of gaps, and coordination with stakeholders.

What is the purpose of a security policy, and how would you use one in your day-to-day work as a security analyst?

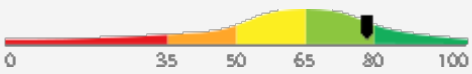
1	2	3	4	5
Cannot explain what a security policy is or describes it only as a document with no practical use.		Explains that policies set rules for behavior but cannot connect them to specific analyst tasks or decisions.		Explains policies as guides for decision-making and gives concrete examples of applying them in daily security tasks.

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Detail	Interview Guide

Threat and Vulnerability Assessment

Score: 78



Description:

The process of identifying, analyzing, and prioritizing weaknesses in systems and networks that could be exploited by threats. This includes vulnerability scanning, risk scoring, and recommending remediation steps. It is a core daily activity for information security analysts.

Interpretation:

Candidate should achieve above average job performance in this area with little or no training.

The candidate demonstrates a solid and proficient understanding of Information Security Analysis principles and practices, including risk assessment, incident response, compliance frameworks, cryptography, and security architecture. Minor gaps may exist in certain specialized areas, but overall performance at this level indicates the candidate is well-prepared to function effectively as an Information Security Analyst with minimal supervision.

You have just received a vulnerability scan report showing 200 findings across several systems. How do you decide which vulnerabilities to address first?

1	2	3	4	5
Cannot explain a prioritization method; suggests fixing all issues equally or at random.		References severity scores like CVSS but does not factor in asset criticality or exploitability.		Combines CVSS scores, asset criticality, exploitability, and business impact to drive prioritization decisions.

Can you walk me through the steps you would take to assess the vulnerabilities of a system you are responsible for protecting?

1	2	3	4	5
Cannot describe a structured process; confuses vulnerabilities with threats or incidents.		Describes basic steps like scanning and patching but lacks detail on prioritization or risk scoring.		Clearly outlines scanning, risk scoring, prioritization, and remediation planning with real examples.

Free Text Responses

During the assessment, the candidate was asked to answer one or more questions using text, audio, video, or an uploaded text file. Their responses are included below for review.

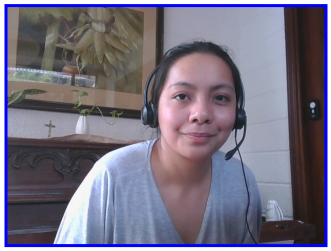
Question or Task	Response
After an AI product is deployed, what is model monitoring and why is it a necessary part of the product lifecycle?	Model monitoring is a technique for ensuring that the model does not wander or become overtrained after an extended period of repeated queries that have the same or similar prompts. This is very important for preventing hallucinization. It's also a key aspect of any guardrails strategy. **Comments (AI):** The answer is clear and coherent but lacks depth in explaining the importance of model monitoring. The phrase 'hallucinization' is not commonly used in this context and may confuse readers. The answer could be improved by providing more specific examples of model performance metrics and how they are tracked. The argument strength is moderate as it does not fully explain why model monitoring is necessary in the product lifecycle. **Misspelled Words:** guardrails (1), hallucinization (1)

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Identity Confirmation Photos

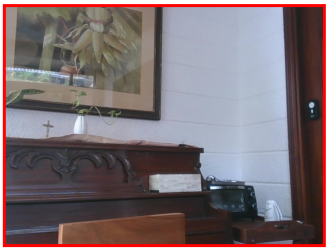
The following photos of the candidate and any identification were uploaded during the assessment session.

Photo Analysis Results	
- Risk:	Medium risk of cheating based on image inconsistencies
- Percent match among processed faces	100%
- Total images processed	17
- Total images with valid faces	14 (82%)
- Total pairs of faces compared	13
- Pairs in which faces matched	13 (100%)

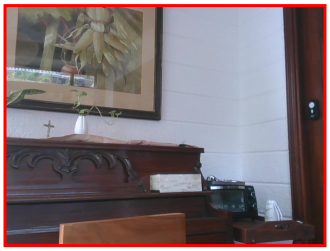


Pre/Post-Test Photo

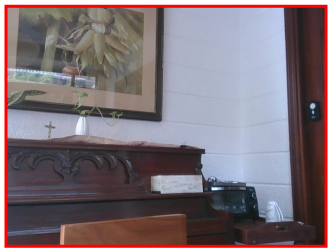
ID Photo



In-Test Error Detected (No Face Detected)

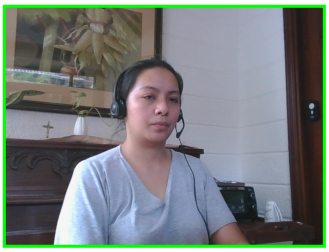


In-Test Error Detected (No Face Detected)

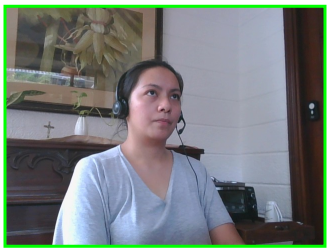


In-Test Error Detected (No Face Detected)

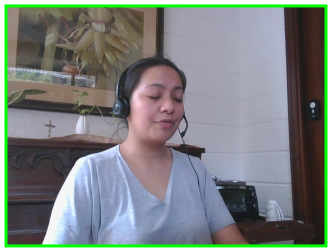
In-Test Photo



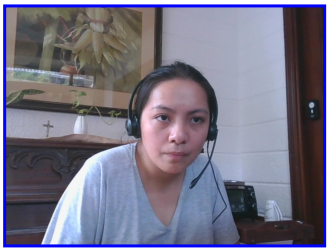
In-Test Photo



In-Test Photo



In-Test Photo



Pre/Post-Test Photo

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Resume or CV

Summary Updated on

Motivated career professional with extensive experience in office administration and management. Proven track record of improving efficiency, reducing costs, and enhancing office operations through strategic initiatives and technology implementation.

Objective

I am seeking a role where I can use my many skills and my exceptional judgment and empathy for customers to make a difference to a growing company.

Education

- Associate of Applied Science in Office Administration, Portland Community College, 2020

Experience

- General Office Clerk, Paramount Office Management, 09/2023 – Present
- Administrative Assistant, Global Enterprises Inc., 04/2021 – 08/2023
- Administrative Assistant, Innovative Business Solutions Ltd., 07/2019 – 03/2021

Other Qualifications

- Microsoft Office Specialist (MOS) Certification
- Certified Administrative Professional (CAP)
- International Association of Administrative Professionals (IAAP) Certification

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Report Preparation Notes

- Hiring decisions should never be based on a single source of information. The most effective use of this assessment report is as a part of a multi-faceted program of candidate evaluation that includes resume review, interviews, and reference checks.
- Overall vs Percentiles Scores: The overall score reflects the success in the test, based on the mean (average) and standard deviation of the test scores. The percentile score reflects the percentage of test-takers who scored equal or below this overall score. We recommend you use the Overall Score as your primary evaluation criteria. However, percentile scores can often be useful in comparing specific candidates against one another and with a group, such as for test takers in a certain organization or within a certain account.
- Note that comparison information is calculated based on completed instances of this assessment at that time the assessment is scored. As additional instances are completed, the comparative data may change. You can always update a report to the current values by clicking on 'Recalculate Percentiles' within the online results viewing pages at www.hravatar.com.
- Most competency scores are norm-based, which means that they can be interpreted in terms of their distance from the average or mean score. For all scales, a score equal to the mean receives a score of 65 and scores above and below this value are set so that a score change of 15 equals one standard deviation.
- For linear competencies, higher is better across the entire scale. For these scales a score between 65 and 80 (light green) represents 0 to 1 standard deviation above the mean and a score above 80 (dark green) represents more than one standard deviation above the mean. Similarly, a score of 50 - 65 (yellow) represents 0 to 1 standard deviation below the mean, while a score of 35 - 50 (orange) equates to 1 to 2 standard deviations below the mean, and a score below 35 represents more than 2 standard deviations below the mean.
- Sim ID: 20836-1, Key: 0-0, Rpt: 68, Prd: 9659, Created: 2026-06-30 17:57 EDT
- UA: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; Touch; rv:11.0) like Gecko

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Score Calculation Detail

The following table provides a summary of how the overall score was calculated from each of the individual competency scores. First, all competency scores are calculated on a scale of 0-100. Note that some competencies use their color category rather than their actual numeric score in the overall calculation. For these, a standard score associated with the assigned color category is used in the overall score calculation rather than the actual numeric score. This is reflected in the ''Score Value Used'' column. Next, a weighted average of scores is computed using individual competency weights, typically set using job analysis data provided by the US Government Occupational Information Network (O*Net).

Competency	Score	How applied to overall	Score Value Used	Weight (%)
Access Control and Identity Management	78.3259	Numeric Score	78.3259	12.5000
Cryptography and Data Protection	83.1432	Numeric Score	83.1432	12.5000
Malware Awareness and Social Engineering Defense	72.6790	Numeric Score	72.6790	12.5000
Network Security Monitoring and Incident Response	67.8639	Numeric Score	67.8639	12.5000
Network Security Monitoring and Incident Response (Free Text Responses)	53.8624	Numeric Score	53.8624	12.5000
Security Policies, Compliance, and Risk Management	84.8944	Numeric Score	84.8944	12.5000
Threat and Vulnerability Assessment	78.7761	Numeric Score	78.7761	12.5000
Threat and Vulnerability Assessment (Free Text Responses)	53.8624	Numeric Score	53.8624	12.5000
Weighted Average:				71.6759
Final Overall Score:				71

Copyright 2026, HR Avatar, Inc. All Rights Reserved.

Notes

(This area is intentionally blank - it's reserved as space for your notes.)

Copyright 2026, HR Avatar, Inc. All Rights Reserved.