

Samuel Woodruff

Risk Assessment - New Artifact

8/17/2026

Dr. Gordon-Phan - IDS 493

Job Posting

Cyber Security Information Assurance Specialist
INPUT TECHNOLOGY SOLUTIONS | SUFFOLK, VA
FULL-TIME

APPLY

Report This Job

Job

Description	Salary	Skills
-------------	--------	--------

JOB DESCRIPTION

Input Technology solutions is seeking multiple Cyber Security & Information Assurance Specialists for an opportunity based out of Suffolk, VA!

Duties:

- Serves as primary security compliance agent.
- Performs vulnerability/risk assessments of computer systems and applications during all phases of the system development life cycle to support the RMF authorization process.

Minimum Experience:

- At least five years' experience in performing Navy Information Assurance and cybersecurity functions to include at least one-year direct experience with RMF and its related components and instructions.

Education:

- Bachelor of Science Degree in IT, Computer Science, Cybersecurity, Information Systems, Computer Engineering, or related discipline.

Certifications or Trainings:

Acceptable certifications for this position are at least one (1) of the following:

- CompTIA Advanced Security Practitioner (CASP), Global Information Assurance Certification (GIAC) – Security Leadership Certification (GSLC), Certified Information system Security Professional (CISSP), or Certified Information Security Manager (CISM).

Clearance:

TS/SCI clearance required (a current SSBI within the five-year scope).

APPLY

This position is open.

For this new artifact, I'm choosing to examine the requirements for a Cybersecurity Analyst position particularly to examine my Risk Assessment skills.

For the role of Cyber Security Information Assurance Specialist, vulnerability/risk assessment is a key requirement in order to be successful. In this new artifact, I will create a simulated risk assessment for a fictional company in order to show my understanding of overall vulnerability/risk assessment.

Lensa. (2026, July 17). *Cyber security information assurance specialist*. Lensa

Fictional Company

Shenandoah Technology Consulting Co.

Overview

Industry:	Information Technology Services
Employees:	50
Location:	Roanoke, VA
Business:	Provides IT support and technology services to businesses local to Roanoke
Systems:	Employee Computers, Email Services, Company Network, Customer Information, Cloud Storage

For this company, it's assumed that the employees use email services frequently. The employees also lack formal cybersecurity training and the company tends to have a relaxed security posture. The company has basic security controls but lacks several important safeguards like MFA, strong passwords, and cybersecurity training. The company is diligent about maintaining uptime and servicing equipment. These factors contribute to a heightened risk for a cybersecurity incident occurring at this business and will be considered in a comprehensive risk assessment.

Assets

For this company, the assets would be the employee computers, employee emails, the company network, stored customer information, and cloud storage.

Risks

<u>Risk</u>	<u>Likelihood</u> 1-5	<u>Impact</u> 1-5	<u>Rating</u> (Likelihood x Impact)
Phishing	3	4	12
Weak Passwords	4	4	16
Ransomware Malware	3	4	12
Social Engineering Attacks	3	4	9
Hardware Failure	1	2	2

Phishing: Employees could fall for malicious email phishing attacks due to their heavy use of email and lack of cybersecurity training. Potential impacts could be unauthorized access to company systems and information. A recommendation to lower the risk of these attacks would be to establish regular, formal cybersecurity training that includes phishing attack simulations.

Weak Passwords: Since this company has a relaxed cybersecurity posture and no strong password requirements, weak passwords present a great risk. Potential impacts could include hackers accessing employee accounts and systems. A recommendation would be to increase the length and complexity requirements for employee passwords.

Ransomware/Malware: Ransomware and Malware present a great risk to this company due to its lack of cybersecurity training and overall security controls. Employees might download ransomware/malware from emails or from the internet. Potential impacts could include the ransoming of customer, business, and employee information as well as the compromise of company systems. I would recommend performing routine system monitoring, installing a strong anti-malware software, implementing a strong firewall, and increasing employee awareness.

Social Engineering Attacks: Social Engineering attacks come in many forms such as identity theft/fraud, tailgating, and deepfakes. Employees might let other employees into parts of the building without scanning their keycard first. Employees may also fall for deepfakes of an executive requesting sensitive access without providing proper credentials. A recommendation would be to establish a cybersecurity-focused culture, implement keycard use across the site, and increase employee awareness.

Hardware Failure: Hardware failure represents the least risk to this company. The employees maintain their equipment and physical systems regularly. A recommendation would be to continue focusing on physical security and maintenance.

Conclusion

Shenandoah Technology Consulting Co. is a small sized company that has several different kinds of security risks. Most risks stem from the fact that there is no cybersecurity awareness training and an overall relaxed security posture. Implementing the security recommendations in this risk assessment would lower the overall vulnerabilities and risks for this specific company.