

Sample of Interactive, Web-based Assessment Application

Security Readiness Self-Assessment

[Home](#) / [Solutions](#) / [Security](#) / [FREE Assessment](#)

SECURITY: FREE ASSESSMENT

Solutions

FREE Security Assessment!

Fill out our questionnaire for a free assessment of your security needs.

SCREEN 1 Contact Information:

Name:

Joe Customer

Title:

Village Crier

Company Name:

The Village

E-mail Address:

Joe@village.com

Business Type and Size:

My industry is best described as:

Service/Telecommunication/Technology

How many end-users does your company have on the network?

1,000 - 10,000

As a percentage, how much company revenue relies on Internet connectivity either through electronic commerce, B2B transactions, EDI, etc.?

75%

Security Assessment Questionnaire:

SCREEN 2 - Network Architecture

1. Does your organization allow remote network connectivity to Internal network?

Yes No

2. Does your organization have a perimeter firewall installed?

Yes No

3. Does your organization utilize VPN technology for all remote network connectivity?

Yes No

4. Does your organization utilize enterprise virus protection software?

Yes No

5. Is your customer vital on-line transaction encrypted?

Yes No

6. Does your organization utilize two-factor authentication for remote connectivity?

Yes No

Security Assessment Questionnaire:

SCREEN 3 - Internal Environment

7. Does your organization require ID and password for desktop PCs?

Yes No

8. Does your organization require session inactivity time out with password on servers and PCs?

Yes No

9. Does your organization maintain mobile device virus protection software?

Yes No

10. Do you use web content filtering and restriction?

Yes No

11. Does your organization restrict use of wireless networking?

Yes No

Security Assessment Questionnaire:

Screen 4 - Intrusion Detection and Response

12. Does your organization have an incident response procedure?

Yes No

13. Does your organization monitor the network and systems for intrusions?

Yes No

14. Is an intrusion detection system deployed?

Yes No

15. If so, is the intrusion detection system monitored 24x7?

Yes No

Security Assessment Questionnaire:

Screen 5 - Policy and Procedure

16. Does your organization have a dedicated information information security staff?

Yes No

17. Does your organization have an information security policy in place?

Yes No

18. Has the security policy document been distributed to the users?

Yes No

19. Does your organization perform periodic security assessments?

Yes No

20. Does your organization have a formal security awareness program?

Yes No

Your Security Assessment Questionnaire results:

OVERALL RESULTS

Network Architecture: High potential vulnerability. [Read More](#)

Internal Environment: High potential vulnerability. [Read More](#)

Intrusion Detection and Response: Moderate potential vulnerability. [Read More](#)

Security Policy and Procedure Concerns: Moderate potential vulnerability. [Read More](#)

Your overall security posture is estimated to be: **High Risk** [Read More](#)

- I'd like to discuss the results with a Security Consultant
- Send me a printer-friendly version of these results via email.

DETAILED SELF-ASSESSMENT RESULTS

Network Architecture	Internal Environment
<p>SECURITY: ASSESSMENT RATING</p> <p>Network Architecture:</p> <p>You showed a High overall potential vulnerability relative to your network security architecture because the industry you are in may not be regulated, and you use the Internet for business transactions.</p> <p>This is based on your current Internet security implementation without the following:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Security assessment <input checked="" type="checkbox"/> Encryption <p>Since remote access is used, you are at high risk to unauthorized access to your network. You should consider using following to reduce this risk:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Two-factor authentication <input checked="" type="checkbox"/> VPN for remote access 	<p>SECURITY: ASSESSMENT RATING</p> <p>Internal Environment:</p> <p>You showed a High overall potential vulnerability relative to your internal environment.</p> <p>Ratings Explanation:</p> <p>High: You are at risk to malicious attack from internal network. You are susceptible to loss of business information from internal misuse or abuse.</p> <p>Moderate: You have some internal controls in place to protect you from internal misuse or abuses. You could benefit from other security measures. A security assessment could give you a better picture on the posture of your internal security.</p> <p>Minimal: Congratulations, you have many good security implementations in place. We recommend that you continue with your diligence in managing your internal security risk.</p>
Intrusion Detection	Policy and Procedure
<p>SECURITY: ASSESSMENT RATING</p> <p>Intrusion Detection and Response:</p> <p>You showed a Moderate overall potential vulnerability relative to your intrusion detection and response process.</p> <p>Ratings Explanation:</p> <p>High: You are at risk to theft of business or other proprietary information and not knowing about it because you lack a comprehensive intrusion detection and monitoring mechanism.</p> <p>Moderate: You have some intrusion detection and or monitoring mechanism in place. You may benefit from diligent continuous intrusion monitoring or a quick intrusion response process.</p> <p>Minimal: You have minimal risk in this area due to your relentless effort in intrusion detection and monitoring effort. You should consider using real time intrusion monitoring, if you are not already.</p>	<p>SECURITY: ASSESSMENT RATING</p> <p>Security Policy and Procedure Concerns:</p> <p>You showed a Moderate overall potential vulnerability relative to your information security policy and procedures.</p> <p>Ratings Explanation:</p> <p>High: The type of industry you are in may not be regulated, you may not have performed all the necessary requirements to ensure proper information security policy and process is in place.</p> <p>Moderate: You have some information security policy and procedures in place but could benefit from additional components to complement what you have in place.</p> <p>Minimal: You have necessary policy and procedure in place to ensure a robust information security program. You should consider periodic security assessment to continually evaluate and monitor enforcement.</p>