Vendor Risk Assessment Report

Generated on: 2025-06-17 05:49:31

Vendor Information

Vendor Name: vansh

Industry: tech

Email: spidervr300@gmail.com

Assessment Date: 2025-06-17

Risk Assessment Summary

Risk Score: 37
Risk Classification: Medium Risk

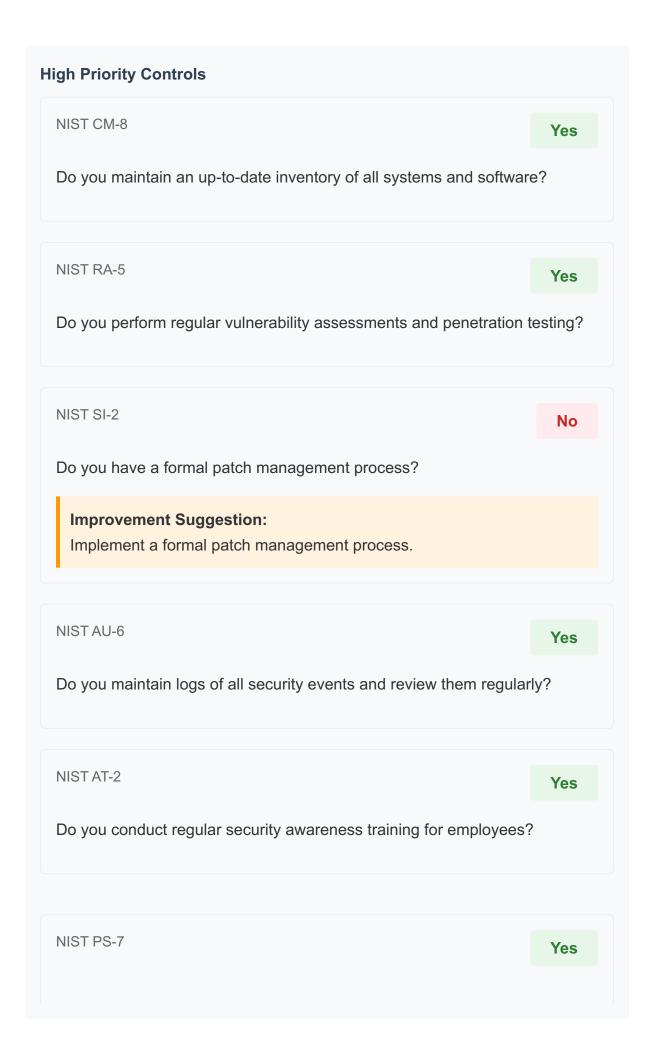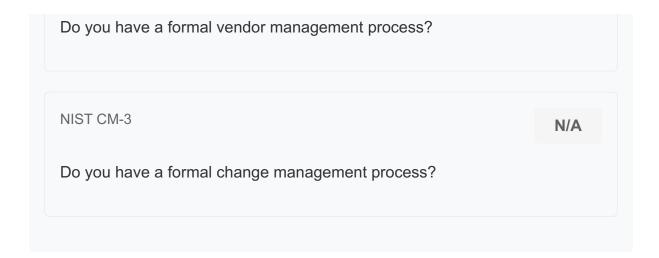| **6**	**4**	**2**
Controls Implemented	Controls Missing	Not Applicable

Detailed Assessment Results

Critical Controls

NIST AC-2   Yes

Does your organization implement Multi-Factor Authentication (MFA) for all remote access?

NIST IR-1   No

Do you have a formal incident response plan that is tested annually?

Improvement Suggestion:
Develop and test an incident response plan annually.

NIST SC-28   No

Do you encrypt sensitive data both in transit and at rest?

Improvement Suggestion:
Implement encryption for sensitive data in transit and at rest.

NIST CP-9   No

Do you have a formal backup and recovery process?

Improvement Suggestion:
Develop and test a formal backup and recovery process.

NIST AC-1   N/A

Do you have a formal access control policy?

High Priority Controls

NIST CM-8 — **Yes**

Do you maintain an up-to-date inventory of all systems and software?

NIST RA-5 — **Yes**

Do you perform regular vulnerability assessments and penetration testing?

NIST SI-2 — **No**

Do you have a formal patch management process?

> **Improvement Suggestion:**
> Implement a formal patch management process.

NIST AU-6 — **Yes**

Do you maintain logs of all security events and review them regularly?

NIST AT-2 — **Yes**

Do you conduct regular security awareness training for employees?

NIST PS-7 — **Yes**

Do you have a formal vendor management process?

NIST CM-3

N/A

Do you have a formal change management process?

Recommendations

Key Areas for Improvement:

• Develop and test an incident response plan annually.

• Implement encryption for sensitive data in transit and at rest.

• Implement a formal patch management process.

• Develop and test a formal backup and recovery process.

This report was automatically generated by the Vendor Risk Assessment System.