# Vendor Risk Assessment Report

Generated on: 2025-06-17 05:17:56

## Vendor Information

**Vendor Name:** abc

**Industry:** other

**Email:** abc@gmail.com

**Assessment Date:** 2025-06-17

## Risk Assessment Summary

### Risk Score: 24
### Risk Classification: Low Risk

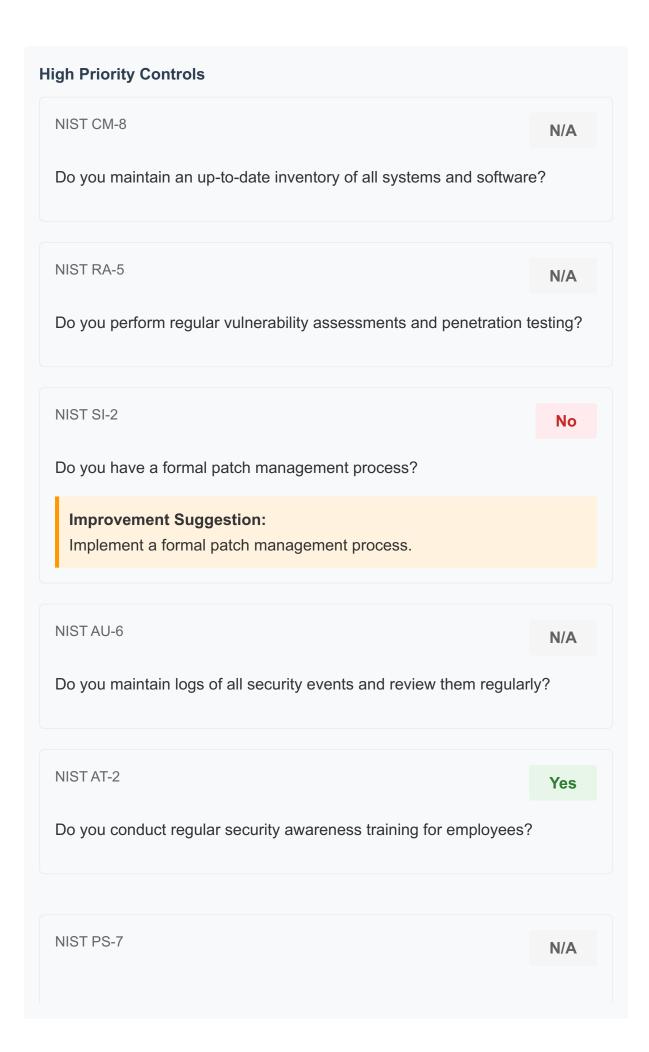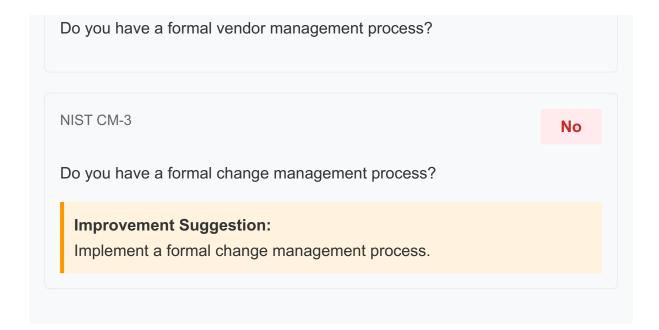| **2** | **6** | **4** |
|---|---|---|
| Controls Implemented | Controls Missing | Not Applicable |

## Detailed Assessment Results

### Critical Controls

NIST AC-2 — **No**

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

> **Improvement Suggestion:**
> Implement MFA for all remote access methods.

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 **Yes**

Do you encrypt sensitive data both 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 **No**

Do you have a formal access control policy?

> **Improvement Suggestion:**
> Develop and implement a formal access control policy.

## High Priority Controls

### NIST CM-8

**N/A**

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

### NIST RA-5

**N/A**

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

**N/A**

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

**N/A**

Do you have a formal vendor management process?

NIST CM-3 **No**

Do you have a formal change management process?

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

## Recommendations

**Key Areas for Improvement:**
• Implement MFA for all remote access methods.
• Develop and test an incident response plan annually.
• Implement a formal patch management process.
• Develop and test a formal backup and recovery process.
• Implement a formal change management process.
• Develop and implement a formal access control policy.