



Risk Assessment Template

# NIST CSF

# Need a better way to **scale** your risk assessments?

This template is a helpful tool, but UpGuard Vendor Risk offers a more efficient and automated risk assessment process.

## Streamlined Workflows for Faster Risk Reviews

Save hours by automating risk assessments. UpGuard combines scanned data, vendor evidence, and questionnaire responses into a unified workflow, giving you a comprehensive view and enabling faster, more-informed decisions.

## Centralized Remediation & Audit Trail

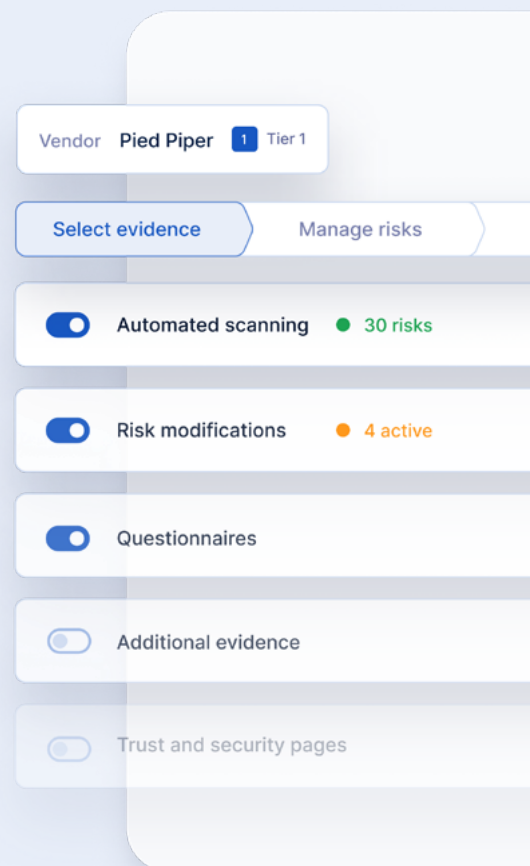
Manage remediation workflows from a single location. Track actions taken, ensure accountability, and maintain a comprehensive audit trail

## Real-time Risk Visibility & Actionable Insights

Proactively manage risks with automated alerts UpGuard generates high-quality reports, providing a clear, actionable view of your vendor cybersecurity posture.

## Industry Leading Expertise

Looking for additional support? UpGuard's Managed Vendor Assessment offering allows you to outsource critical vendor risk assessments. Our expert team delivers high-quality reviews, ensuring thorough risk evaluations without overburdening your resources.



Helping 12,000+ security professionals work smarter.

[See UpGuard in Action →](#)

Escape the limitations of manual assessments and scale your risk management process with ease. Learn how UpGuard can transform your organisation.

Risk Assessment

# NIST CSF

Issued By:

*Your Organization*

Vendor Being Assessed:

*Vendor Name*

Date Published:

*Date*

## Overview

*Overview of the objectives of this risk assessment. For example: This report provides a detailed overview of the key factors contributing to the security posture and level of NIST CSF compliance of [name of vendor].*

# Evidence Used to Generate this Report

The list of data sources referenced to create this risk assessment report.

Date Published:

Author:

## Questionnaires

The list of data sources referenced to create this risk assessment report.

Questionnaire Name	Sent	Submitted	# of Risks

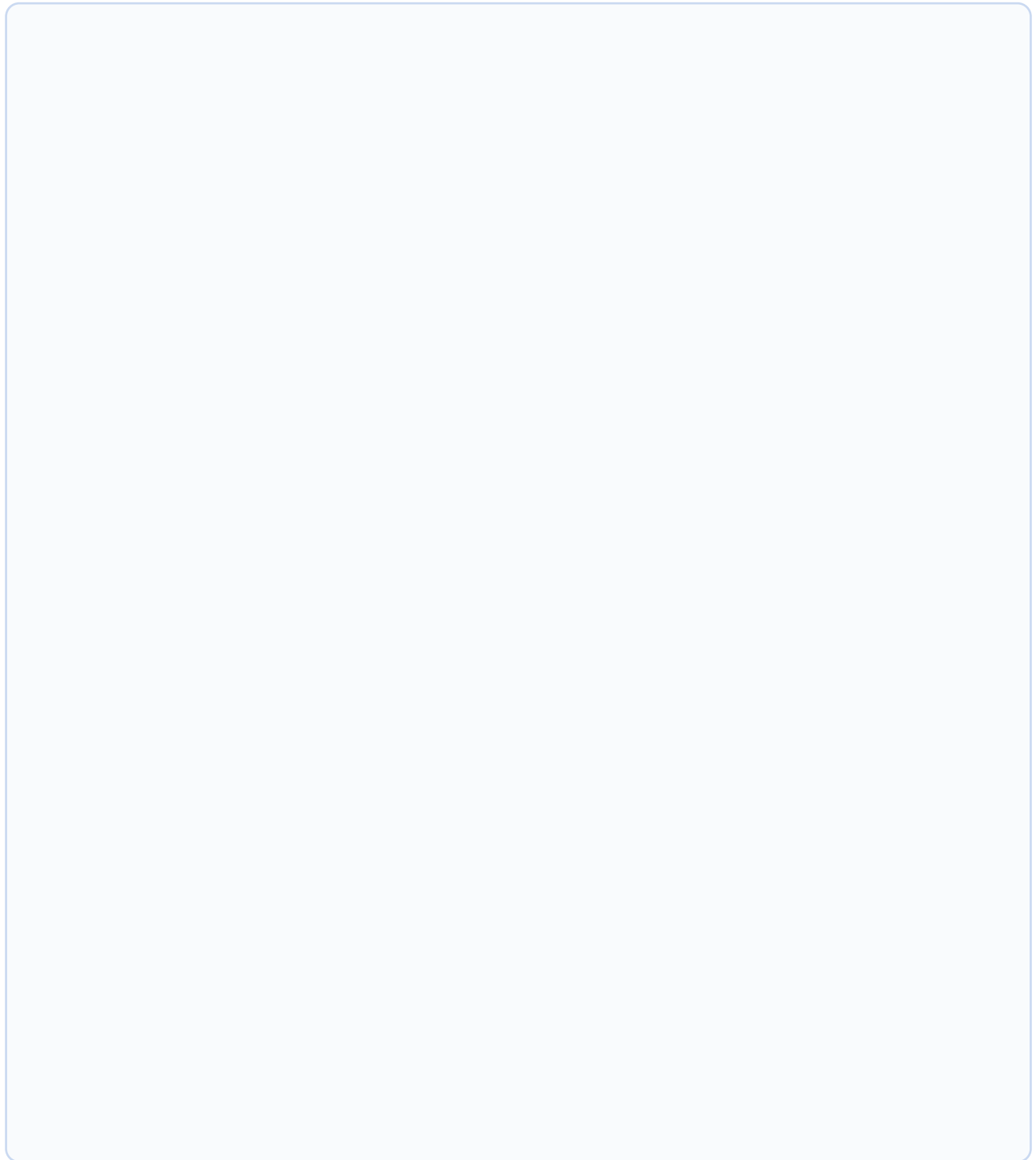
## Additional Evidence

List any additional sources used to gather insights about the vendor's security posture and NIST CSF compliance efforts.

Document Type	Name	Last Updated	# of Risks

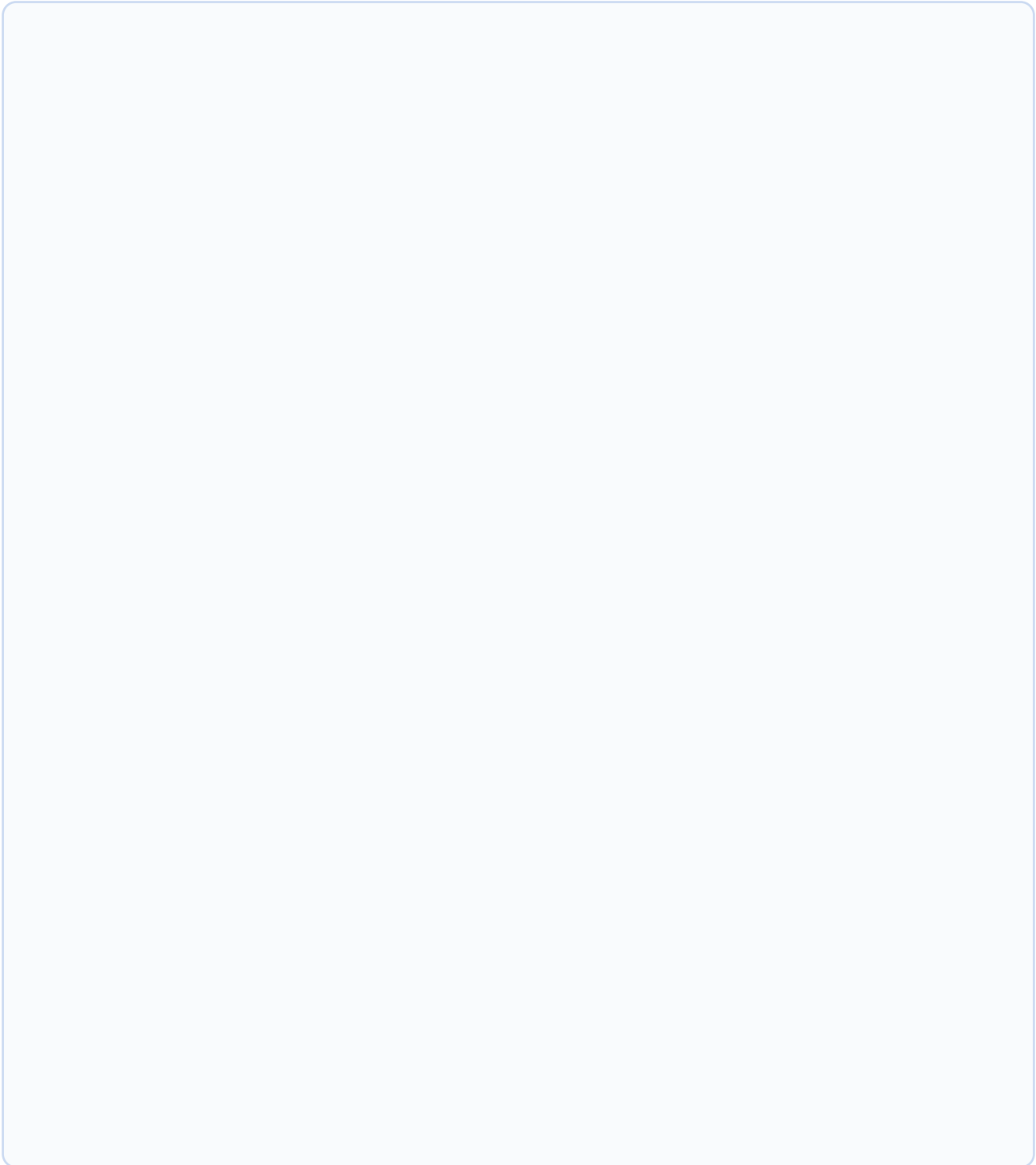
# Executive Summary

An overview of the vendor's security posture, NIST CSF compliance risks, and follow-up risk treatment plans based on key findings from this risk assessment.



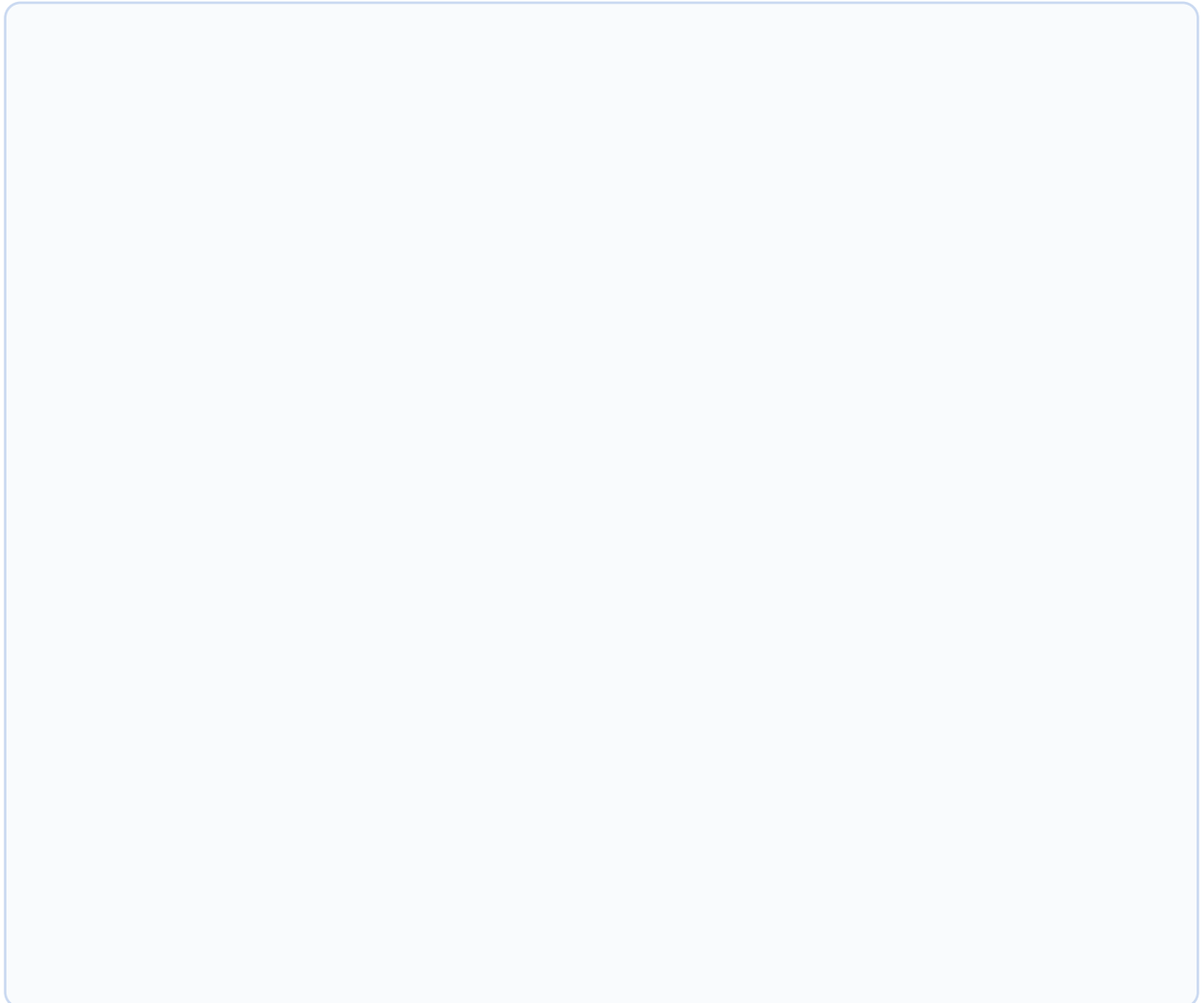
# Vendor Background

An overview of the vendor being assessed and their primary service offerings.



# Assessment Summary

An overview of insights gathered across the six primary security risk categories defining a vendor's security posture and required risk treatment plan.









# Security Policies and Processes

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:





---

RISKS IDENTIFIED

# Infrastructure and Asset Management

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:





---

RISKS IDENTIFIED

# Data Classification and Handling

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:





---

RISKS IDENTIFIED

# Application Security

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:





---

RISKS IDENTIFIED

# Application Security

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:





---

RISKS IDENTIFIED

# Risk Management

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:





---

RISKS IDENTIFIED

# Recovery and Response

OVERVIEW

CURRENT RISKS BY SEVERITY

-  Critical:
-  High:
-  Medium:
-  Low:

---

RISKS IDENTIFIED

# Key Risks

A list of security and NIST CSF compliance risks identified in the questionnaire component of this risk assessment.

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan



Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan

**Risk Finding:**

**Risk Severity**

**Risk Category**

**Risk Details:**

**Compensating Control Information**

**Risk Treatment Plan**

**Risk Finding:**

**Risk Severity**

**Risk Category**

**Risk Details:**

**Compensating Control Information**

**Risk Treatment Plan**

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan

**Risk Finding:**

**Risk Severity**

**Risk Category**

**Risk Details:**

**Compensating Control Information**

**Risk Treatment Plan**

**Risk Finding:**

**Risk Severity**

**Risk Category**

**Risk Details:**

**Compensating Control Information**

**Risk Treatment Plan**

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan

Risk Finding:

Risk Severity

Risk Category

Risk Details:

Compensating Control Information

Risk Treatment Plan



# Explore the Benefits for Your Organization

Third-Party Cyber Risk Management (TPCRM) is an essential component of any organization's cybersecurity strategy, regardless of size. Dispelling common myths about TPCRM software reveals the true value and necessity of these solutions. By adopting TPCRM solutions, such as UpGuard, organizations can effectively manage third-party risks, protect sensitive data, and maintain their competitive edge in an increasingly interconnected digital landscape. Investing in TPCRM is not just a prudent decision—but a vital step towards a secure and resilient future.

Prospective customers can explore the UpGuard platform with a free 14-day trial. Contact UpGuard to get started and learn how TPCRM software can help your organization.

[Free Trial →](#)

Trusted by hundreds of companies worldwide



www.upguard.com +1 888-882-3223	650 Castro Street, Suite 120-387, Mountain View CA 94041 United States
	© 2024 UpGuard, Inc. All rights reserved. UpGuard and the UpGuard logo are registered trademarks of UpGuard, Inc. All other products or services mentioned herein are trademarks of their respective companies. Information subject to change without notice.