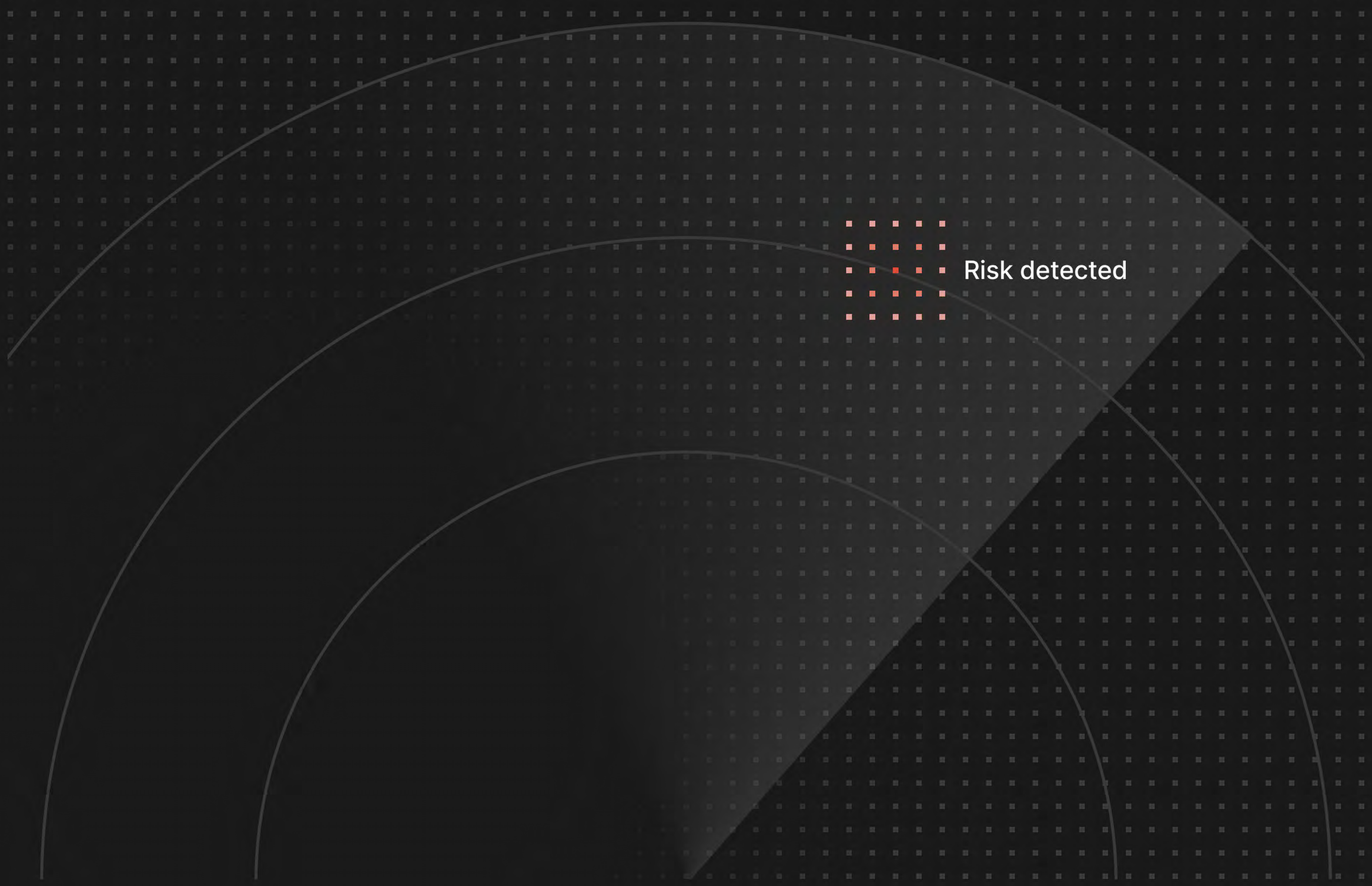
Vendor Risk Powered by UpGuard

Risk Assessment Template
ISO 27001



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.

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.

Centralized Remediation & Audit Trail

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

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.

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

See UpGuard in action

PagerDuty NYSE hopin iag ICE TDK

Risk Assessment
ISO 27001

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 ISO 27001 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

Additional Evidence

List any additional sources used to gather insights about the vendor's security posture and ISO 27001 compliance efforts.

Questionnaire name	Sent	Submitted	# of Risks

Additional Evidence

List any additional sources used to gather insights about the vendor's security posture and ISO 27001 compliance efforts.

Document Type	Name	Last Updated	# of Risks

Executive summary

An overview of the vendor's security posture, ISO 27001 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 four domains of Annex A, which defines a vendor's risk treatment alignment with ISO 27001:2022.

Organizational controls

Overview

Current risks by severity

!!!! Critical: !!! High: !! Medium: ! Low:

Risks identified

People controls

Overview

Current risks by severity

!!!! Critical: !!! High: !! Medium: ! Low:

Risks identified

Physical controls

Overview

Current risks by severity

!!!! Critical: !!! High: !! Medium: ! Low:

Risks identified

Technological controls

Overview

Current risks by severity

!!!! Critical: !!! High: !! Medium: ! Low:

Risks identified

Key risks

A list of security and ISO 27001 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

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 →

Questions? Email us at sales@upguard.com or find out more at www.upguard.com