

RiskAuto: Third-Party Risk Assessment Automation

- A web-based SaaS solution for Third-Party Risk Assessment with Cloud security capability.

Note for: Visitors & Contributors:

This is a learning-focused weekend project to help the broader community of Cybersecurity professionals, and newbies learn and identify mistakes in design, code, or overall approach. That's intentional to some extent — I'm using this space to experiment, try new ideas, and improve over time.

This project is a work in progress. If you notice something that could be better, I'd genuinely appreciate your help:

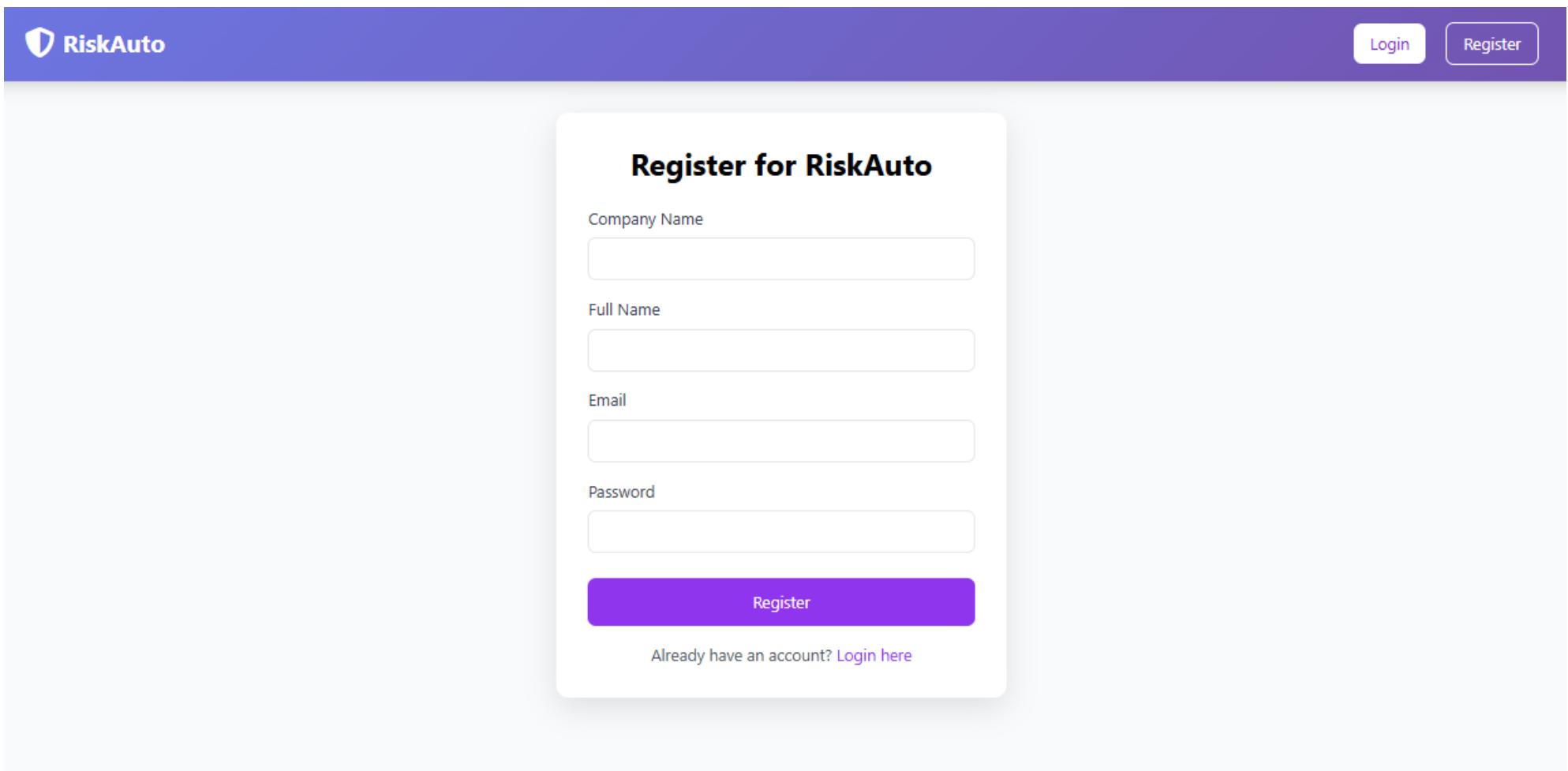
- Please feel free to open an issue to share suggestions or ask questions.
- Submit a pull request with improvements.
- Share best practices, alternative designs, or helpful resources.

I'm always keen to learn from others, so if you're interested in collaborating or giving feedback, you're very welcome here.

GitHub Link: [RiskAuto](#)

RiskAuto Processes	Description
User Registration	New user registration.
Dashboard	User dashboard showing third-party risk assessment automation options.
Passive Scanning	Non-intrusive scanning to collect information about internet-facing assets including open ports, SSL/TLS certificates, and DNS records.
Questionnaires	Create customizable security questionnaires to share with third parties for risk assessment.
Risk Assessments	View completed questionnaires by third-party and the risk ratings.
Reports	Auto-generated risk assessment reports with detailed analysis based on risk assessment questionnaires.

User Registration



The image shows a user registration form titled "Register for RiskAuto". The form is contained within a white rectangular box with rounded corners, set against a light gray background. At the top left of the form is the RiskAuto logo, which consists of a shield icon with a checkmark inside and the word "RiskAuto" in a sans-serif font. At the top right are two buttons: "Login" and "Register", both in a white rounded rectangle with black text. The main body of the form contains four input fields: "Company Name", "Full Name", "Email", and "Password", each with a corresponding text input box below it. Below these fields is a large purple button with the word "Register" in white. At the bottom of the form is a link "Already have an account? [Login here](#)".

Register for RiskAuto

Company Name

Full Name

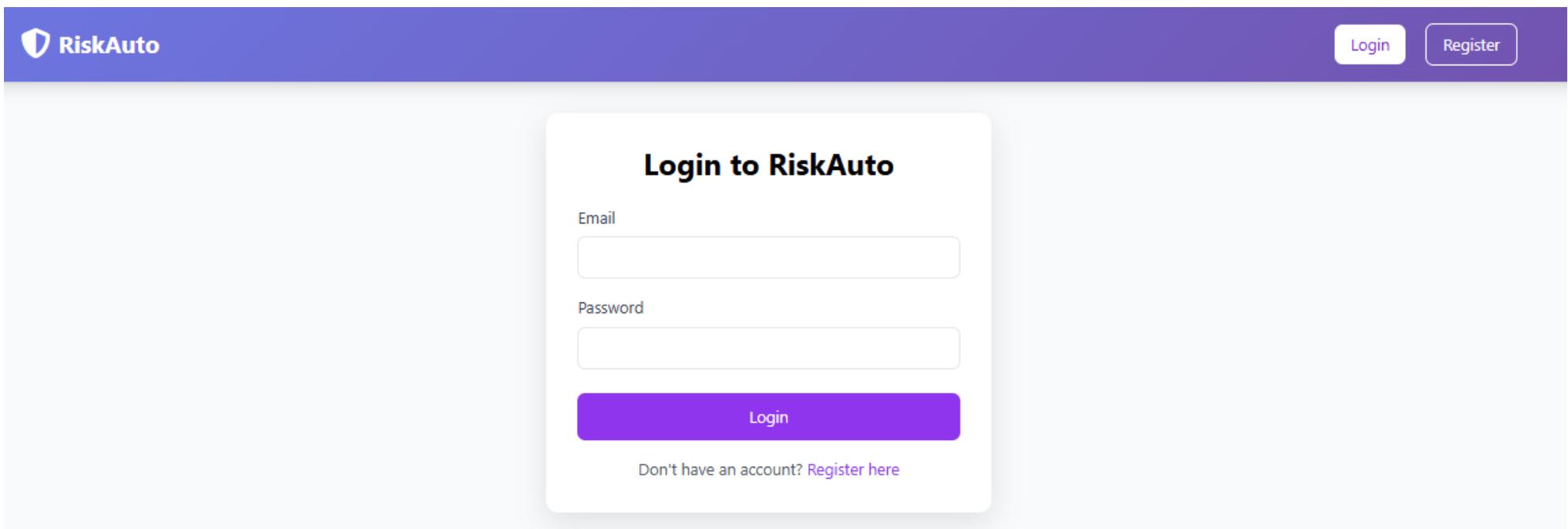
Email

Password

Register

Already have an account? [Login here](#)

User Login



The image shows the RiskAuto user login interface. At the top left is the RiskAuto logo, which consists of a shield icon with a checkmark inside. To the right of the logo are two buttons: "Login" and "Register", both in white text on purple rounded rectangles. The main area is a white card with a shadow. It features a title "Login to RiskAuto" in bold black font at the top center. Below the title are two input fields: "Email" and "Password", each with a placeholder text box. At the bottom of the card is a large purple "Login" button with white text. Below the button, a link "Don't have an account? [Register here](#)" is displayed in purple text.

Login to RiskAuto

Email

Password

Login

Don't have an account? [Register here](#)

RiskAuto has 3 options.

- (1) **Passive Scanning**.
- (2) **Security Questionnaires** for third-party risk assessment.
- (3) **Automated Reports** for risk assessment.

The screenshot shows the homepage of the RiskAuto platform. At the top, there is a purple header bar with the RiskAuto logo on the left and 'Login' and 'Register' buttons on the right. Below the header, the title 'Third-Party Risk Assessment Platform' is displayed in large, bold, dark blue text. A subtitle 'Comprehensive cloud security and vendor risk management solution' follows. The page is divided into three main sections, each represented by a white box with rounded corners and a shadow:

- Passive Scanning**: Represented by a shield icon. Description: Non-intrusive scanning of internet-facing assets, ports, SSL/TLS certificates, and DNS records. Number: (1).
- Security Questionnaires**: Represented by a checkmark icon. Description: Customizable questionnaires to assess third-party security posture and compliance. Number: (2).
- Automated Reports**: Represented by a document icon. Description: Auto-generated risk assessment reports with actionable insights and risk ratings. Number: (3).

Dash Board:

There are 4 sections.

1. **Passive scanning.**
2. **Questionnaires.**
3. **Assessment.**
4. **Report.**

The screenshot shows the RiskAuto dashboard interface. At the top, there is a purple header bar with the RiskAuto logo, a 'Welcome, Khon' message, and a 'Logout' button. Below the header, the word 'Dashboard' is displayed in large, bold letters. Underneath 'Dashboard', it says 'Manage your third-party risk assessments and security scans'. There are four tabs labeled (1) Passive Scanning, (2) Questionnaires, (3) Assessments, and (4) Reports. The (1) Passive Scanning tab is currently selected and highlighted in purple. In the 'Passive Security Scanning' section, there is a sub-section titled 'Scan Type' with a dropdown menu set to 'Comprehensive Scan'. Below this, there is a 'Target Domain/IP' input field containing 'example.com or 192.168.1.1' and a 'Start Scan' button. In the 'Scan History' section, it says 'No scan history available'. The overall layout is clean and modern, using a white background with blue and purple accents for branding.

1. Passive Scanning:

The screenshot shows the RiskAuto dashboard with the following interface elements:

- Header:** RiskAuto logo, Welcome, Khon, Logout.
- Navigation:** Dashboard, Passive Scanning (selected), Questionnaires, Assessments, Reports.
- Section Header:** Passive Security Scanning.
- Target Domain/IP:** https://cybersolution.au/
- Scan Type:** A dropdown menu with the following options:
 - Comprehensive Scan (selected)
 - Comprehensive Scan
 - Port Scan Only
 - SSL/TLS Only
 - DNS Records Only
- Buttons:** Start Scan (purple button).
- Section:** Scan Results.

Annotations in red text:

- (1) Provide vendor web site and press Start Scan button.
- (2) You can select type of scan from the drop down list.

- (1) Select third-party's business web-site for passive scan. This is non-intrusive scanning to collect information about internet facing assets including open ports, SSL/TLS certificates and DNS records.
- (2) Scan type: User can select various scanning process depends on the business requirements.
 - a. Comprehensive Scan.
 - b. Port Scan.
 - c. SSL/TLS Scan.
 - d. DNS Records.

Scan Result

 Welcome, Khon Logout

Dashboard

Manage your third-party risk assessments and security scans

Passive Scanning Questionnaires Assessments Reports

Passive Security Scanning

Non-intrusive scanning to collect information about internet-facing assets including open ports, SSL/TLS certificates, and DNS records.

Target Domain/IP: Scan Type:

▶ Start Scan

Scan Results Showing the passive scan result 

Scan Summary

Target: https://cybersolution.au/
Scan Type: comprehensive
Completed: 29/11/2025, 10:35:46

Open Ports Medium

Details: Ports 80, 443, 22 are open
Recommendation: Ensure only necessary ports are exposed. Consider closing port 22 or restricting access.

SSL/TLS Certificate Low

Details: Valid SSL certificate found. TLS 1.2 and 1.3 supported
Recommendation: Certificate is valid. Ensure automatic renewal is configured.

DNS Records Low

Details: DNSSEC not configured, SPF and DMARC records found
Recommendation: Consider implementing DNSSEC for additional security.

Security Headers High

Details: Missing security headers: X-Frame-Options, Content-Security-Policy
Recommendation: Implement recommended security headers to prevent clickjacking and XSS attacks.

Scan history

Scan History

<https://cybersolution.au/>

comprehensive - 29/11/2025, 10:35:46

[View Report](#)

<https://www.telstra.com.au/>

comprehensive - 29/11/2025, 10:34:42

[View Report](#)

2. Questionnaires

- User can complete all the necessary information as shown in the screenshot.
- Questionnaire Template: User can select questionnaires type according to the business need and scope of the risk assessment.
 - a) Standard Security Assessment.
 - b) Cloud Security Assessment.
 - c) GDPR Compliance.
 - d) Custom Questions.

(1) Select Questionnaires tab

(2) You can select different categories of security questionnaires.

Dashboard
Manage your third-party risk assessments and security scans

Welcome, Khan Logout

Passive Scanning Questionnaires Assessments Reports

Create Security Questionnaire
Create customizable security questionnaires to share with third parties for risk assessment.

Questionnaire Name:

Third-Party Company Name:

Third-Party Email:

Questionnaire Template: **Standard Security Assessment**

Standard Security Assessment

Cloud Security Assessment
GDPR Compliance
Custom Questions

Do you perform regular security awareness training for employees?
Training: **MEDIUM**

Are security patches applied within 30 days of release?
Patch Management: **HIGH**

Do you encrypt data at rest and in transit?
Data Protection: **Critical**

Do you have an incident response plan?
Incident Management: **HIGH**

Are regular security audits conducted?
Compliance: **MEDIUM**

Do you maintain data backups with tested recovery procedures?
Business Continuity: **HIGH**

+ Add Question Create & Send Questionnaire

Sent Questionnaires
No questionnaires sent yet

Custom Questions

 RiskAuto

Welcome, Khon [Logout](#)

Dashboard

Manage your third-party risk assessments and security scans

Passive Scanning [Questionnaires](#) [Assessments](#) [Reports](#)

Create Security Questionnaire

Create customizable security questionnaires to share with third parties for risk assessment.

Questionnaire Name

Third-Party Company Name

Third-Party Email

Questionnaire Template

Custom Questions  (1)

Click "Add Question" to create custom questions

[+ Add Question](#) [Create & Send Questionnaire](#)

(2) (3)

1. Select Custom Questions options.
2. Add Question according to business & risk assessment scope.
3. Create & Send Questionnaire.

Questionnaires Sent Notification:

- Questionnaires can be sent to the vendor's email.
- A sharable link also generated.

The screenshot shows the RiskAuto dashboard with the following interface elements:

- Header:** Welcome, Khan | Logout
- Navigation:** Passive Scanning, Questionnaires (highlighted), Assessments, Reports
- Section:** Create Security Questionnaire
- Form Fields:**
 - Questionnaire Name: [Input field]
 - Third-Party Company Name: [Input field]
 - Third-Party Email: [Input field]
 - Questionnaire Template: Standard Security Assessment (dropdown)
 - Do you have a documented information security policy? (checkboxes: Governance, HIGH)
 - Is multi-factor authentication (MFA) enforced for all users? (checkboxes: Access Control, CRITICAL)
 - Do you perform regular security awareness training for employees? (checkboxes: Training, MEDIUM)
 - Are security patches applied within 30 days of release? (checkboxes: Patch Management, HIGH)
 - Do you encrypt data at rest and in transit? (checkboxes: Data Protection, CRITICAL)
 - Do you have an incident response plan? (checkboxes: Incident Management, HIGH)
 - Are regular security audits conducted? (checkboxes: Compliance, MEDIUM)
 - Do you maintain data backups with tested recovery procedures? (checkboxes: Business Continuity, HIGH)
- Success Modal:** A central modal window displays a green checkmark icon, the word "Success!", and the message "Questionnaire created and sent to xyz@cybersolution.au!". It also shows the sharable link: <https://019a8557-3633-7b55-82ab-19791e4ae2a4>. A yellow arrow points from the text "Security Questionnaires send the third-party and created a sharable link." to this modal.
- Buttons:** + Add Question, Create & Send Questionnaire
- Sent Questionnaires:** A section showing a recent questionnaire entry for "Third Party Security Questionnaires" sent to "CyberSolution (xyz@cybersolution.au)" on "20/11/2023, 18:52:09".

3. Assessments

- Select Assessments tab for the risk assessment.

The screenshot shows the RiskAuto dashboard interface. At the top, there is a purple header bar with the RiskAuto logo on the left, a "Welcome, Khon" message, and a "Logout" button on the right. Below the header, the word "Dashboard" is prominently displayed in large black font. Underneath "Dashboard", a sub-header reads "Manage your third-party risk assessments and security scans". A red notification bubble in the center indicates "(3) Automated third-party risk assessment". Below this, there are four navigation tabs: "Passive Scanning", "Questionnaires", "Assessments" (which is highlighted in purple), and "Reports". In the main content area, there is a section titled "Risk Assessments" with the sub-instruction "View completed questionnaires and their risk ratings.". A message below states "No completed assessments yet".

4. Reports

- Based on the security answers from third-party, the risk assessment report will be generated.

The screenshot shows the RiskAuto dashboard interface. At the top, there is a purple header bar with the RiskAuto logo, a "Welcome, Khon" message, and a "Logout" button. Below the header, the word "Dashboard" is prominently displayed in large, bold, dark blue text. Underneath "Dashboard", the subtext "Manage your third-party risk assessments and security scans" is visible. In the center of the page, a red call-to-action button labeled "(4) Generate third-party risk assessment report" is centered above a horizontal navigation bar. This bar contains four items: "Passive Scanning", "Questionnaires", "Assessments", and "Reports". The "Reports" item is highlighted with a blue background and white text. Below this navigation bar, a large, rounded rectangular container is titled "Generated Reports" in bold black text. Inside this container, the subtext "Auto-generated risk assessment reports with detailed analysis." is displayed, followed by the message "No reports generated yet".