



TraxrGRC

Quick Start Guide

October 2026 · build 244823a

From first sign-in to a working program in an hour.

About this guide

This guide gets you productive in TraxrGRC quickly. It shows you how to sign in and find your way around, how to complete the tasks everyone is asked to do, and, for the person running the program, a short ordered path through the first week. It covers the fast path only: each task ends with a pointer to the User Manual section that describes it in full.

Who this guide is for

- **Everyone with an account:** staff who read and acknowledge policies, complete awareness training or answer questionnaires. Read chapters 1 and 2.
- **GRC leads:** the risk, compliance or security manager setting the program up and running it day to day. Read all four chapters.
- **Record owners and contributors:** risk owners, control owners and anyone assigned reviews, tests or findings. Read chapters 1 and 2, then the parts of chapter 3 that match your work.

Administrators who install the platform, connect sign-in and email, and manage users and roles should start with the Administrator's Guide.

What this guide covers

Chapter	What it covers
First steps	What the platform does, signing in, the layout, your profile and time zone, notifications, and working with lists
Tasks for everyone	Acknowledging a policy, answering a questionnaire, completing awareness training, comments, mentions and attachments
Your first week as a GRC lead	Registering assets and a risk, adding and testing a control, loading a framework, publishing a policy, logging an incident, sending a third-party assessment, running a report and keeping reviews on time
Where to go next	The User Manual chapters by role, the Administrator's Guide and the REST API

Conventions

Convention	Meaning
Bold	A label you see on screen: a menu entry, page title, tab, button, field or status, written exactly as it appears.
Risk Management → Risks	A navigation path: open Risk Management in the sidebar, then Risks .
<code>monospace</code>	Text you type or read literally: addresses, file names, permission names, codes and API values.
<code>module:right</code>	A permission, for example <code>risks:read</code> (Read on the Risks module) or <code>policies:update</code> . Roles grant rights per module.
<i>own</i> and <i>all</i>	The two levels at which a role can hold a right. At <i>own</i> you work only with records that you or one of your groups own; at <i>all</i> you work with every record in the module.
Numbered steps	A procedure to follow in order.

Permission notes. What you see depends on your role. A sidebar entry, button or tab appears only when your role grants the right it needs, so your screens may show fewer options than the figures here. Administrators have every right in every module.

Screenshots. The figures show a demonstration installation populated with fictional data for an invented company, Quillmont Systems. Names, dates and counts on your installation will differ, and the product name and logo follow your organization's branding.

Dates and times are shown in your own time zone once you set one (see Your profile and time zone).

How this guide relates to the other guides

TraxrGRC has three guides:

Guide	Use it for
Quick Start Guide (this guide)	Getting started: the first hour for everyone, the first week for a GRC lead.
User Manual	The complete reference for every screen, field and workflow, one chapter per module.
Administrator's Guide	Installing and operating the platform: deployment, sign-in and SSO, email, users, groups and roles, notifications, backups and the audit log.

Where this guide and the User Manual overlap, the User Manual has the detail: every field, status and permission. This guide names the sections to read next.

Contents

1	First steps	6
1.1	What TraxrGRC does	6
1.2	Signing in	7
1.3	Finding your way around	8
1.4	Your profile and time zone	11
1.5	Notifications	15
1.6	Working with lists	15
2	Tasks for everyone	18
2.1	Acknowledging a policy	18
2.2	Answering a data mapping questionnaire	19
2.3	Completing awareness training	20
2.4	Comments and mentions	21
2.5	Attachments	22
3	Your first week as a GRC lead	24
3.1	Before you start	24
3.2	Register an asset	24
3.3	Record a risk	25
3.4	Add a control and record a test	27
3.5	Load a framework and analyze a requirement	29
3.6	Publish a policy and request acknowledgement	32
3.7	Log an incident	34
3.8	Send a third-party assessment	35
3.9	Run a report	36
3.10	Keep it running: reviews	37
3.11	What you have built	39
4	Where to go next	40
4.1	User Manual chapters by role	40
4.2	The Administrator's Guide	40
4.3	The REST API	41
4.4	Getting help	41
	Index	

First steps

1.1 What TraxrGRC does

TraxrGRC is a self-hosted governance, risk and compliance platform. It gives your organization one place to record what could go wrong, show what you do about it, and prove it to an auditor. Each area of the work has its own module in the sidebar:

Module	What it is for
Risk Management	The risk register with scores, treatments, reviews and exceptions, plus the shared controls, assets and business units
Third Parties	Vendors and partners, their contacts, linked risks and data protection details
Incidents	Security and operational incidents, including personal data breaches
Compliance	Frameworks loaded as packages, the analysis of each requirement, and the gap view
Policies	Policy documents with owners, versions, approvals and reviews
Audits	Audit plans and their findings
Evidence	Access review screenshots, scan review notes and vendors' SOC 2 reports, each linked to the controls and requirements it supports
Assessments	Questionnaires sent to vendors and other outside contacts
Account Reviews	Periodic reviews of who has access to what
Awareness	Training programs with tests, and who has passed them
Projects	Remediation and improvement projects
Data Privacy	Records of processing, transfers, DPIAs and data mapping questionnaires
Reports	The Report Center and reports emailed on a schedule
My Tasks	Everything waiting on you, from every module you can read
Policy Portal	The published policies everyone can read and acknowledge

The modules share one library of records. A control you add once can treat several risks, satisfy several compliance requirements and carry audit findings, and its test results show up wherever it is used.

1.2 Signing in

1. Open TraxrGRC in your browser at the address your administrator gave you. If you are not signed in, the `/login` page shows the **Sign in to GRC Platform** form (with your organization's product name).
2. Enter your **Email** and **Password**.
3. Click **Sign in**.

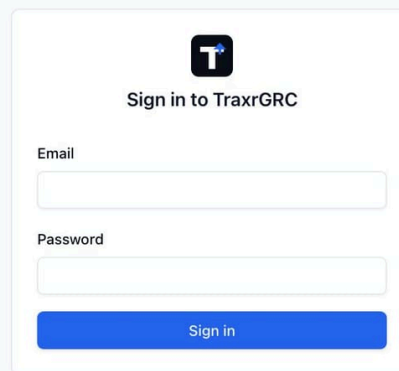
The image shows a sign-in form for TraxrGRC. At the top is a logo consisting of a black square with a white 'T' and a small blue plus sign. Below the logo is the text 'Sign in to TraxrGRC'. There are two input fields: one labeled 'Email' and one labeled 'Password'. Below these fields is a blue button with the text 'Sign in'.

Figure 1.1. The sign-in page with the Email and Password fields and the Sign in button.

You land on the page you originally asked for, or on the Dashboard. If your role has no Dashboard access you land on the **Policy Portal**, or, if you are a Data Liaison, on **My Questionnaires**.

Single sign-on. When your administrator has enabled SAML single sign-on, a **Sign in with SSO** button appears below the password form. Click it and sign in with your organization's identity provider; you return to GRC Platform signed in. When the administrator has made SSO the only way in, the page shows just **Sign in with SSO**. The **Emergency administrator sign-in** link below it is for break-glass administrators only.

Directory (LDAP) sign-in needs no separate button: when it is enabled, your directory email and password work in the normal form.

Two-step verification. If you have set up two-step verification (see Your profile and time zone), the next page asks for the **Code from your authenticator app**: enter the six-digit code and click **Verify**. Without your phone, click **Use a recovery code instead**. If your administrator requires two-step verification and you have not set it up yet, that page asks you to **Set up now** before you can continue. Single sign-on never asks for a code here; your identity provider handles its own verification.

If sign-in fails, the form says why:

Message	What to do
Invalid email or password.	Check both and try again. Repeated failures lock your network address out of that account for 15 minutes.
Your account is inactive. Contact an administrator.	Your account has been deactivated; ask an administrator.
Sign-in is misconfigured. Contact an administrator.	The server's sign-in setup is broken; report it.
Single sign-on failed. Please try again or contact an administrator.	The identity provider's answer was refused; try again, then report it.

Signing out. Open the user menu (your initials and name, top right) and click **Sign out**. **Sign out everywhere** also ends your sessions on every other browser and device within a minute. A session ends on its own after 12 hours, or after 60 minutes without use, unless your administrator changed these limits.

Full details: User Manual, Getting Started, Signing in.

1.3 Finding your way around

Every screen after sign-in shares the same frame: the sidebar on the left, a header across the top, and the page itself.

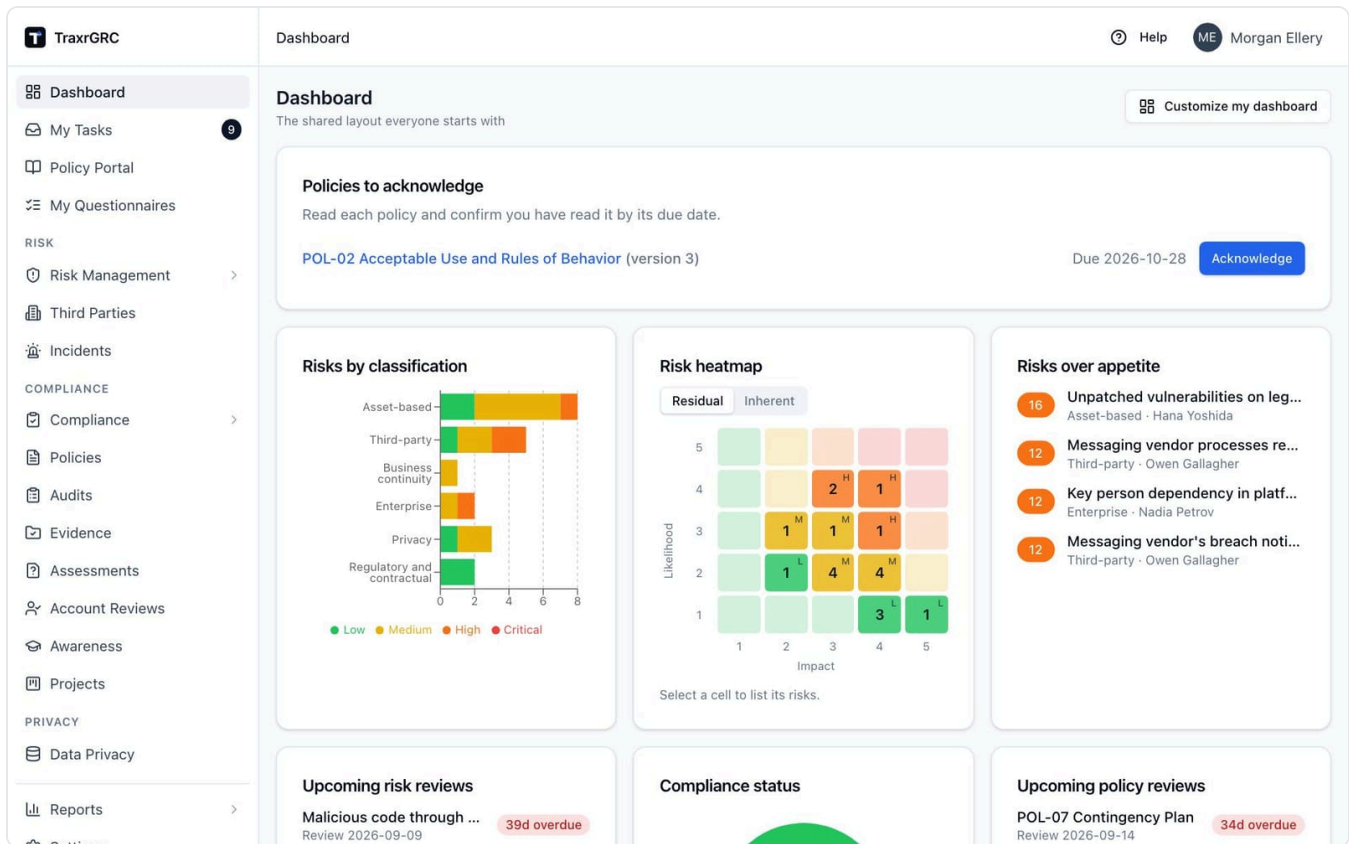


Figure 1.2. The application frame: the sidebar on the left with its Risk, Compliance and Privacy sections, the header with the user menu, and the Dashboard.

1.3.1 The sidebar

Section	Entries
(top)	Dashboard ; My Tasks (every signed-in user); Policy Portal (every signed-in user); My Questionnaires (Data Liaisons)
Risk	Risk Management (with Risks , Controls , Assets , Business Units and Risk Settings); Third Parties ; Incidents
Compliance	Compliance (with Analyses , Packages , Gaps , POA&M and Catalog); Policies ; Audits (with an Open findings button for findings across all plans); Evidence ; Assessments ; Account Reviews ; Awareness ; Projects
Privacy	Data Privacy
(bottom)	Reports (with Report Center and Scheduled); Settings

An entry with sub-pages opens while you are on one of them; click its name to open or close it.

Collapse at the bottom of the sidebar shrinks it to icons; click the button again to expand it.

You see only the modules your role can read. Roles are attached to groups, and you receive the roles of every group you belong to. If a module you need is missing, ask your administrator to add you to the right group.

1.3.2 The header and user menu

The header shows where you are on the left, as a trail such as **Risk Management > Risks > UNP-01**, each step linking back to its list, and **Help** and your user menu on the right. **Help** opens the User Manual section for the page you are on in a panel beside it, with a link to the whole manual. Click your initials and name to open the menu:

Item	What it does
My profile	Your time zone, your policies and your notification choices.
Sign out	Ends this session.
Sign out everywhere	Ends this session and every other session you have, within a minute.

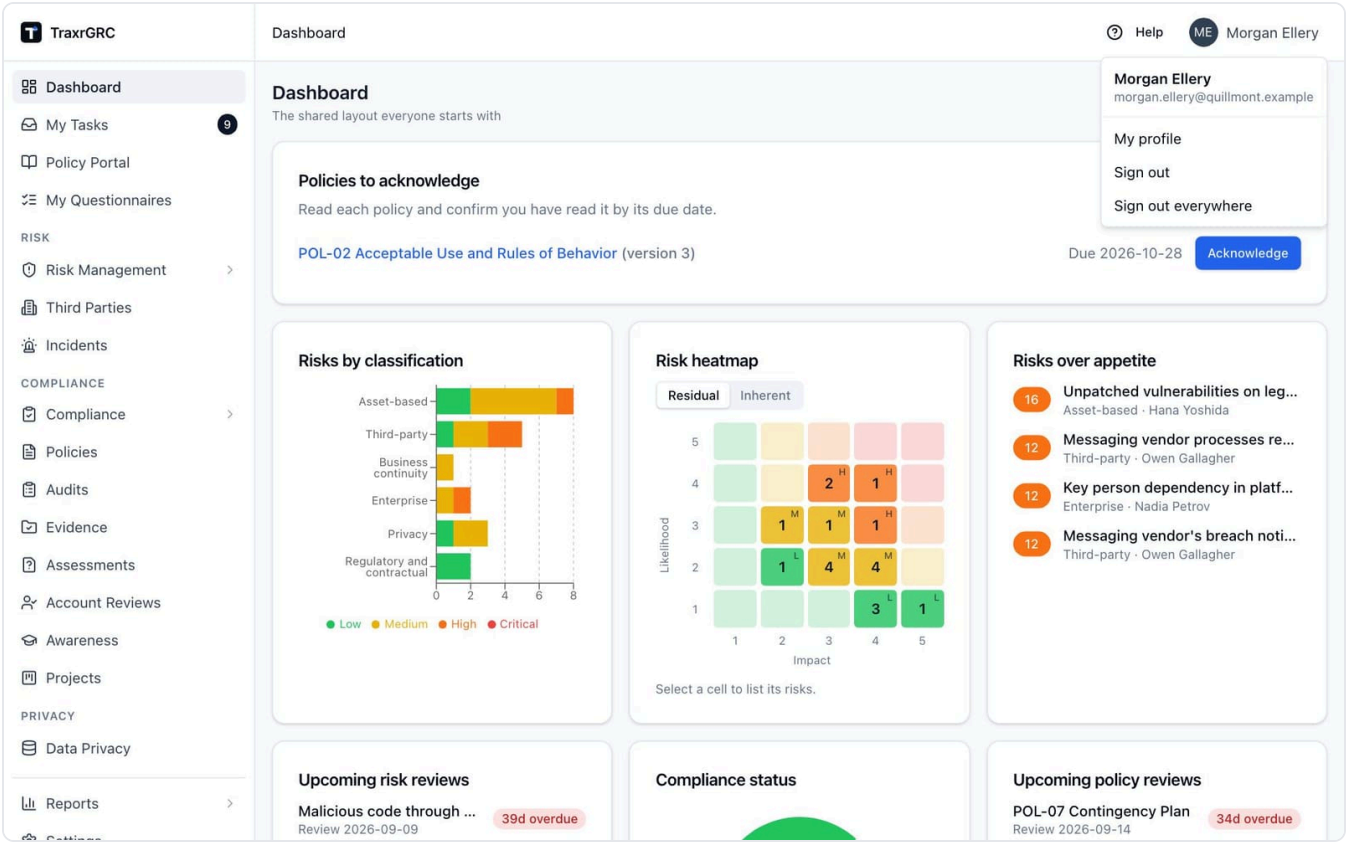


Figure 1.3. The user menu open in the header, showing My profile, Sign out and Sign out everywhere.

1.3.3 The Dashboard

The Dashboard is a grid of widgets: risks over appetite, upcoming reviews, compliance status, open incidents, control testing status and more. Everyone starts on the same shared layout, each widget counting only the records you may see; a widget for a module you cannot read is hidden. **Customize my dashboard** makes it your own to add, move and remove widgets, and **Reset to default** takes you back. When you have policies to acknowledge, a **Policies to acknowledge** card sits at the top.

Review chips follow one convention everywhere: red **Nd overdue** is past its date by N days, amber **due in Nd** is due within 14 days, gray **due in Nd** is later than that.

1.3.4 When a page is off limits

A page you have no permission for shows **403: Forbidden**, asks you to contact your administrator, and offers **Go to My Tasks** and **Policy Portal**. A link to something that does not exist shows **Page not found** with a **Back to dashboard** button.

Full details: User Manual, Getting Started, The app layout and The Dashboard.

1.4 Your profile and time zone

Open the user menu and choose **My profile**. The page has up to four parts: **Time zone**, **Sign-in security** (your **Password** and **Two-step verification**, when they apply to your account), **My policies** (policies to acknowledge and your acknowledgements) and **My notifications**.

TraxrGRC

Dashboard

My Tasks

Policy Portal

RISK

Risk Management

Third Parties

Incidents

COMPLIANCE

Compliance

Policies

Audits

Evidence

Assessments

Account Reviews

Awareness

Projects

PRIVACY

Data Privacy

Reports

Settings

My profile

Help

Dana Whitcombe

My profile

Signed in as dana.whitcombe@quillmont.example.

Time zone

Times are stored in UTC. Choose the zone you see them in, here and in emails and PDFs sent to you. Calendar dates such as due dates are never shifted. Every time shown names its zone.

Your time zone

America/New York

Show times in America/New York

Show times in UTC

Save

Sign-in security

Password

At least 8 characters, with a letter and a digit. Changing it signs you out everywhere else; this session stays signed in.

Current password

New password

Confirm new password

Change password

Two-step verification

With two-step verification on, signing in with your password or through LDAP also asks for a code from an authenticator app. Single sign-on relies on your identity provider instead.

Set up two-step verification

My policies

Policies to acknowledge

Nothing to acknowledge right now.

My acknowledgements

POL-02 Acceptable Use and Rules of Behavior (version 3)	2026-09-30 08:09 EDT
POL-05 Data Protection Policy (version 1)	2026-09-11 00:36 EDT
POL-02 Acceptable Use and Rules of Behavior (version 2)	2025-12-19 09:23 EST

My notifications

Figure 1.4. My profile, with the Time zone card, the Sign-in security cards and My policies.

Every time in TraxrGRC is stored in UTC. Until you choose a zone, you see UTC. To see times in your own zone:

1. In the **Time zone** card, pick **Your time zone** from the list (IANA names such as `America/New_York` or `Europe/London`).

2. Choose **Show times in** your zone, or **Show times in UTC**.
3. Click **Save**.

Every time on screen, in emails and in PDFs then names its zone, for example `2026-10-14 09:05 EDT`. Calendar dates such as due dates are never shifted: a due date is the same day for everyone, and what counts as today (and so as overdue) follows the organization's time zone, which an administrator sets. If your zone comes from your directory, SSO or provisioning, the list is grayed out and shows where it comes from; change it there.

Your password. If you sign in with a TraxrGRC password, change it under **Sign-in security**, in the **Password** card:

1. Enter your **Current password**.
2. Enter the **New password** twice, in **New password** and **Confirm new password**: at least 8 characters, with a letter and a digit.
3. Click **Change password**.

Your other sessions are signed out; this one stays signed in, and you receive an email confirming the change. If you sign in with SSO or your directory password, the card is not shown: change your password there. There is no "forgot password" link: if you have forgotten yours, an administrator sets a new one in **Settings → Users**.

Two-step verification. To protect a password or directory sign-in with a code from an authenticator app (Microsoft Authenticator, Google Authenticator, 1Password and others):

1. In the **Two-step verification** card, click **Set up two-step verification**.
2. In your authenticator app, add an account and scan the QR code shown. If you cannot scan it, type the setup key under it, or click **Open in authenticator app** on the device that has the app.
3. Enter the six-digit code the app shows and click **Confirm**.
4. Save the ten recovery codes shown, for example in a password manager, then click **I have saved my recovery codes**. They are not shown again; each works once if you lose your device.

TraxrGRC

Dashboard

My Tasks

Policy Portal

My Questionnaires

RISK

Risk Management

Third Parties

Incidents

COMPLIANCE

Compliance

Policies

Audits

Evidence

Assessments

Account Reviews

Awareness

Projects

PRIVACY

Data Privacy

Reports

Settings

My profile

Help

ME Morgan Ellery

My profile

Signed in as morgan.ellery@quillmont.example.

Time zone

Times are stored in UTC. Choose the zone you see them in, here and in emails and PDFs sent to you. Calendar dates such as due dates are never shifted. Every time shown names its zone.

Your time zone

America/New York

Show times in America/New York

Show times in UTC

Save

Sign-in security

Password

At least 8 characters, with a letter and a digit. Changing it signs you out everywhere else; this session stays signed in.

Current password

New password

Confirm new password

Change password

Two-step verification

With two-step verification on, signing in with your password or through LDAP also asks for a code from an authenticator app. Single sign-on relies on your identity provider instead.

Set up two-step verification

My policies

Policies to acknowledge

Read each policy and confirm you have read it by its due date.

POL-02 Acceptable Use and Rules of Behavior (version 3)

Due 2026-10-28

Acknowledge

My acknowledgements

You have not acknowledged any policy yet.

My notifications

Figure 1.5. The Sign-in security section of My profile, with the Password card and the Two-step verification card.

You cannot turn two-step verification off yourself. If you lose your device or run out of recovery codes, ask an administrator to reset it, then set it up again.

Full details: User Manual, Getting Started, My profile and Times and time zones.

TraxrGRC Quick Start Guide

14

1.5 Notifications

TraxrGRC notifies you by email; there is no in-app inbox. You receive three kinds of message:

Kind	Examples	Can you turn it off?
Reminders about your own work	A risk or policy review coming due or overdue, a control test due, a policy to acknowledge, an awareness program due	No. These stop when the work is done.
Notification rules	Emails set up by your administrators, for example when you are mentioned in a comment or a finding is assigned to you	Yes, per rule.
Scheduled reports	A report emailed to you on a schedule	Yes, per report.

To stop a notification rule or a scheduled report from emailing you:

1. Open **My profile**.
2. Under **My notifications**, find the rule in **Notification rules** or the report in **Scheduled reports**.
3. Turn its switch off. Turn it on again to resume.

Email works only once your administrator has configured outgoing mail.

Full details: User Manual, Getting Started, My notifications.

1.6 Working with lists

Every module list (risks, controls, policies, incidents and the rest) is the same table, so learning one teaches you all of them.

T

TraxrGRC

Dashboard

My Tasks13

Policy Portal

RISK

Risk Management

Risks

Controls

Assets

Business Units

Third Parties

Incidents

COMPLIANCE

Compliance

Policies

Audits

Evidence

Assessments

Account Reviews

Awareness

Projects

PRIVACY

Data Privacy

Risk Management > Risks

?

Help

DW Dana Whitcombe

Risks

Import

New risk

All

Asset-based

Third-party

Business continuity

Enterprise

Privacy

Regulatory and contractual

Search...

Filters

Export CSV

Saved

Columns

Title

Inherent

Residual

Status

Controls

Classification

Owner

Ransomware encrypts FieldDesk production data

15 - High

6 - Medium

Open

Control failing

Asset-based

Tomas Okafor

Moderate environment)

22

board-visibility

fedramp-boundary

Compromise of privileged cloud credentials

20 - Critical

8 - Medium

Open

Untested

Asset-based

Lena Haverkamp

FieldDesk US (FedRAMP Moderate environment)

2026-10-07 (overdue)

fedramp-boundary

Unpatched vulnerabilities on legacy worker images

16 - High

16 - High

Open

2 controls failing

Asset-based

Hana Yoshida

FieldDesk US (FedRAMP Moderate environment)

2026-10-16 (overdue)

fedramp-boundary

Support staff misuse customer data

8 - Medium

4 - Low

Open

Control failing

Asset-based

Kenji Arakawa

Support ticketing system

2027-09-19

Leavers keep access to SaaS tools

9 - Medium

6 - Medium

Open

Control failing

Asset-based

Rhea Castellano

Support ticketing system

2026-11-28

Malicious code through a third-party

12 - High

8 - Medium

Open

OK

Asset-based

Nadia Petrov

CI/CD pipeline

2026-09-09

Figure 1.6. The risk register table with the Saved menu open, showing a saved view named Over appetite, open.

Tool	How to use it
Search	Type in Search... above the table to match text across the searchable columns.
Column filters	Filters opens a panel with a filter per column: a text box (Contains...), a list starting with All , or a date picker. Filters apply as you type; each active filter shows as a chip you can remove, and Clear all removes them all.
Sorting	Click a column heading; click again to reverse.
Page size	Choose 10 / page , 25 / page (the default), 50 / page or 100 / page in the footer.
Columns	Columns shows or hides individual columns.
Saved	Saved lists your saved views and saves the current one (see below).
Export CSV	Export CSV downloads every row matching your current search, filters and sort, up to 5,000 rows.

To save a view you use often:

1. Set the search, filters, sort, page size and columns you want.

2. Click **Saved**, then **Save current view...**
3. Enter a **Filter name** and click **Save filter**.

Click a saved name in the **Saved** menu to reapply it, or its trash icon to delete it. Saved views are personal; nobody else sees them.

The page, sort and filters are also kept in the browser address, so you can bookmark a filtered list or send the link to a colleague. They still need permission to see the records.

Full details: User Manual, Getting Started, Shared UI conventions.

Tasks for everyone

These are the tasks most people are asked to do, whatever their role. Each one usually starts with an email containing a link; you can also start from the sidebar. **My Tasks**, right under **Dashboard**, lists everything waiting on you in one place, overdue first, with a link to where you act on each one; its sidebar entry shows how many there are.

2.1 Acknowledging a policy

Your organization may ask you to confirm that you have read a policy, for example the acceptable use policy or rules of behavior. Requests appear under **Policies to acknowledge** on the **Policy Portal**, the Dashboard and **My profile**, with a due date (red once overdue). You also get an email with a link, a reminder in the week before the due date, and one notice if the date passes.

1. Open **Policy Portal** in the sidebar.
2. Under **Policies to acknowledge**, click the policy's title, or **Acknowledge** to jump to the acknowledgment.
3. Read the policy. The panel below the text says which version you are asked to acknowledge and by when. **PDF** downloads the version you are reading.
4. Tick the attestation checkbox in that panel, for example "I have read and understood this policy."
5. Click **Acknowledge**.

Purpose

- Explain what every user may and may not do with Quillmont systems and customer data. These are the rules of behavior for FieldDesk (NIST SP 800-53 PL-4).

Scope

- Everyone with a Quillmont account, including contractors.

You must

- Use only company-managed devices for company work and keep them locked when unattended.
- Keep customer data inside FieldDesk and approved tools; never in personal email or storage.
- Report lost devices, suspected phishing and security incidents straight away.
- Use your security key for every sign-in that asks for it; never approve a sign-in you did not start.
- Use only approved AI assistants, and never paste customer or resident data into them.

You must not

- Share accounts, passwords or security keys.
- Access customer or resident records without a work reason linked to a ticket or work order.
- Install unapproved software or disable security tooling.

Consequences

- Breaches of these rules may lead to removal of access and disciplinary action.

Acknowledge version 3 of this policy by 2026-10-28. Confirm once you have read the policy above.

☐ I have read and will follow the Rules of Behavior, including the rule on AI assistants.

Acknowledge

< Collapse

Figure 2.1. The acknowledgment panel below a policy's text on the portal: the due date, the attestation checkbox and the Acknowledge button.

The panel changes to "You acknowledged version N on" followed by the time, and the policy moves to **My acknowledgements**. Your acknowledgement records the exact version and text you confirmed; it cannot be changed or withdrawn.

The portal also lists every policy in force under **Policies**. Type in **Search titles and descriptions** and click **Search** to find one.

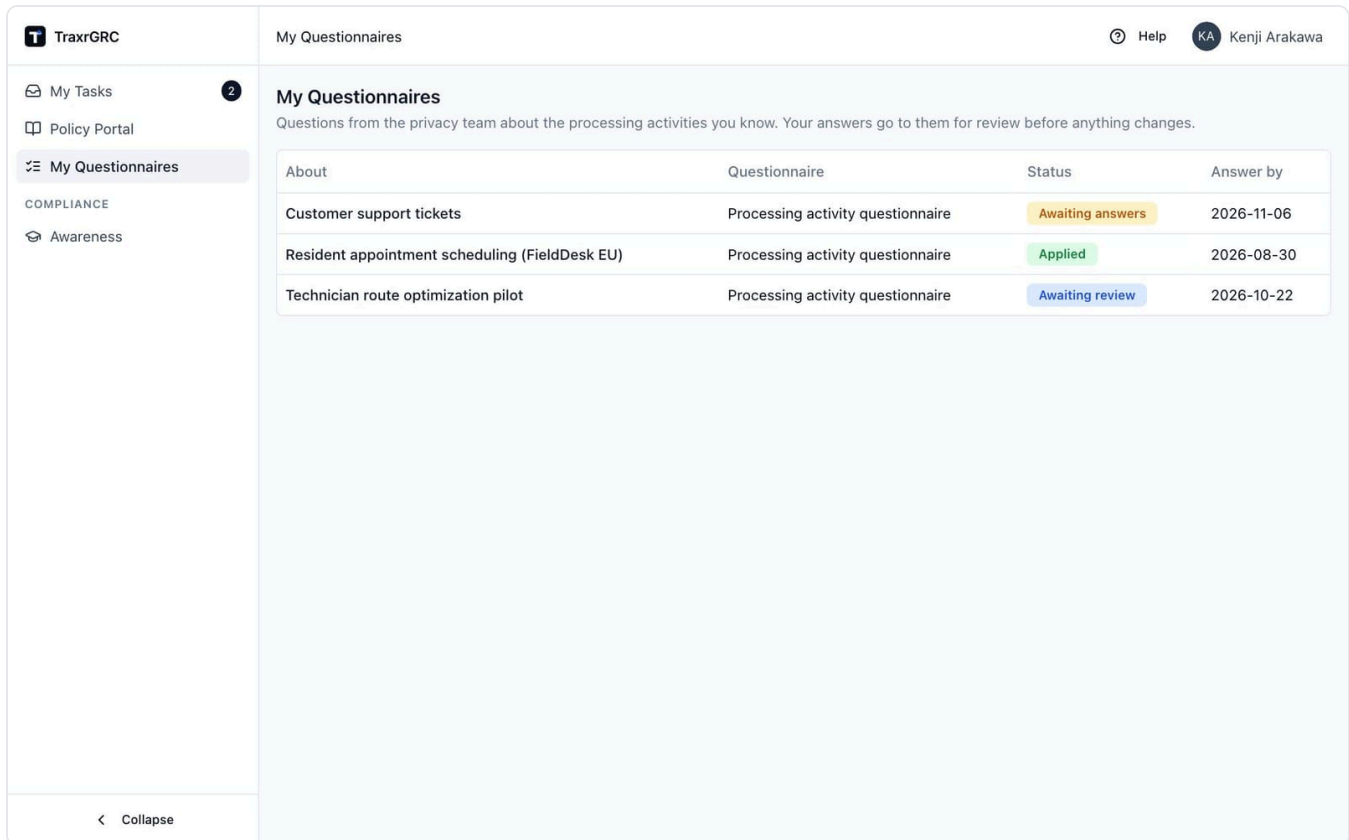
Full details: User Manual, Policy Management, Policy portal and acknowledgements.

2.2 Answering a data mapping questionnaire

If you are a **Data Liaison**, the privacy team asks you to describe the processing activities you know: what personal data a business process uses, why, where it comes from and who receives it. Nothing changes on the privacy records until the privacy team has reviewed your answers.

1. Open **My Questionnaires** in the sidebar (or follow the link in the email). The list shows what each questionnaire is **About**, the **Questionnaire**, its **Status** and the **Answer by** date, in red once overdue.
2. Click the activity name to open the questionnaire. The header shows who sent it, the answer-by date and any message.

3. Answer the questions. For an activity that already has a record, the answers start from what the record holds today: correct and complete them.
4. Click **Save draft** to keep work in progress, or **Submit answers** when every required question is answered.



About	Questionnaire	Status	Answer by
Customer support tickets	Processing activity questionnaire	Awaiting answers	2026-11-06
Resident appointment scheduling (FieldDesk EU)	Processing activity questionnaire	Applied	2026-08-30
Technician route optimization pilot	Processing activity questionnaire	Awaiting review	2026-10-22

Figure 2.2. My Questionnaires as a Data Liaison sees it, listing an open annual check and earlier questionnaires with their statuses.

Once you submit, the questionnaire becomes read-only, its status shows **Awaiting review**, and the sender is emailed. It later shows **Applied** or **Rejected**.

Annual checks. Once a year the privacy team may ask you to confirm a record is still accurate. An annual check opens with the current answers and a **Nothing has changed** button: click it if nothing has changed, or correct the answers and click **Submit answers**.

Full details: User Manual, Data Privacy, Data mapping questionnaires.

2.3 Completing awareness training

Awareness programs are training material with a short test. Open **Awareness** in the sidebar to see your programs and their due dates. If **Awareness** is missing from your sidebar, you have no training assigned through the platform.

1. Open **Awareness** and click the program's title to read its training material on the **Content** tab.
2. Click **Take the test** (on the list, or in the program's header).
3. Check the pass score and due date under the title, then answer each question. More than one choice can be correct: tick every choice you believe is right. A question counts only when your selection matches exactly, and an unanswered question counts as wrong.
4. Click **Submit answers**. The counter beside it shows how many questions you have answered.

The screenshot shows the TraxrGRC interface. On the left is a sidebar with 'My Tasks' (3), 'Policy Portal', and 'COMPLIANCE' with an 'Awareness' sub-tab. The main header shows 'Awareness > Handling residents' data (EU support and dispatch)' with a 'Help' icon and user 'JP Jordan Pike'. The main content area is titled 'Handling residents' data (EU support and dispatch)' and includes the text 'Role-based module for staff who handle EU residents' data. Overdue for some.' and 'Pass score 100% · Due 2026-10-14'. Below this is a instruction box: 'Answer every question. Some may have more than one correct choice. Unanswered questions count as incorrect.' The test consists of three questions, each with checkbox options:

1. Residents' appointment data belongs to which organization as controller?
 - ☐ Quillmont
 - ☐ The utility that books the appointment
 - ☐ The technician
2. A resident emails support asking for a copy of their data. What do you do?
 - ☐ Send them a FieldDesk export
 - ☐ Log it as a data subject request and pass it to the utility and the DPO
 - ☐ Tell them to ask their utility and close the ticket
3. Which access notes are appropriate to record?
 - ☐ "Side gate code needed"
 - ☐ "Resident is undergoing chemotherapy"
 - ☐ "Dog in back garden"

At the bottom is a 'Submit answers' button and a counter '0/3 answered'. A 'Collapse' link is at the bottom left of the sidebar.

Figure 2.3. The test page as a staff member sees it, with checkbox choices for each question and the Submit answers button.

The result screen shows your score and a **Passed** or **Failed** badge, with each question marked right or wrong. The correct answers are never shown. If you failed, click **Back to program**, reread the material and use **Retake the test**; you can retake as often as you like. A pass is never lost by a later lower score, and once you pass, the due-date reminders stop.

Full details: User Manual, Security Awareness, Taking a test.

2.4 Comments and mentions

Most record pages (risks, controls, policies, incidents, projects and others) have a **Comments** tab for discussion that stays with the record.

1. Open the record and click **Comments**.

2. Type in **Add a comment...** (up to 4,000 characters).
3. To bring a colleague in, write @ followed by their email address, for example `@jane@example.com`.
4. Click **Post comment**.

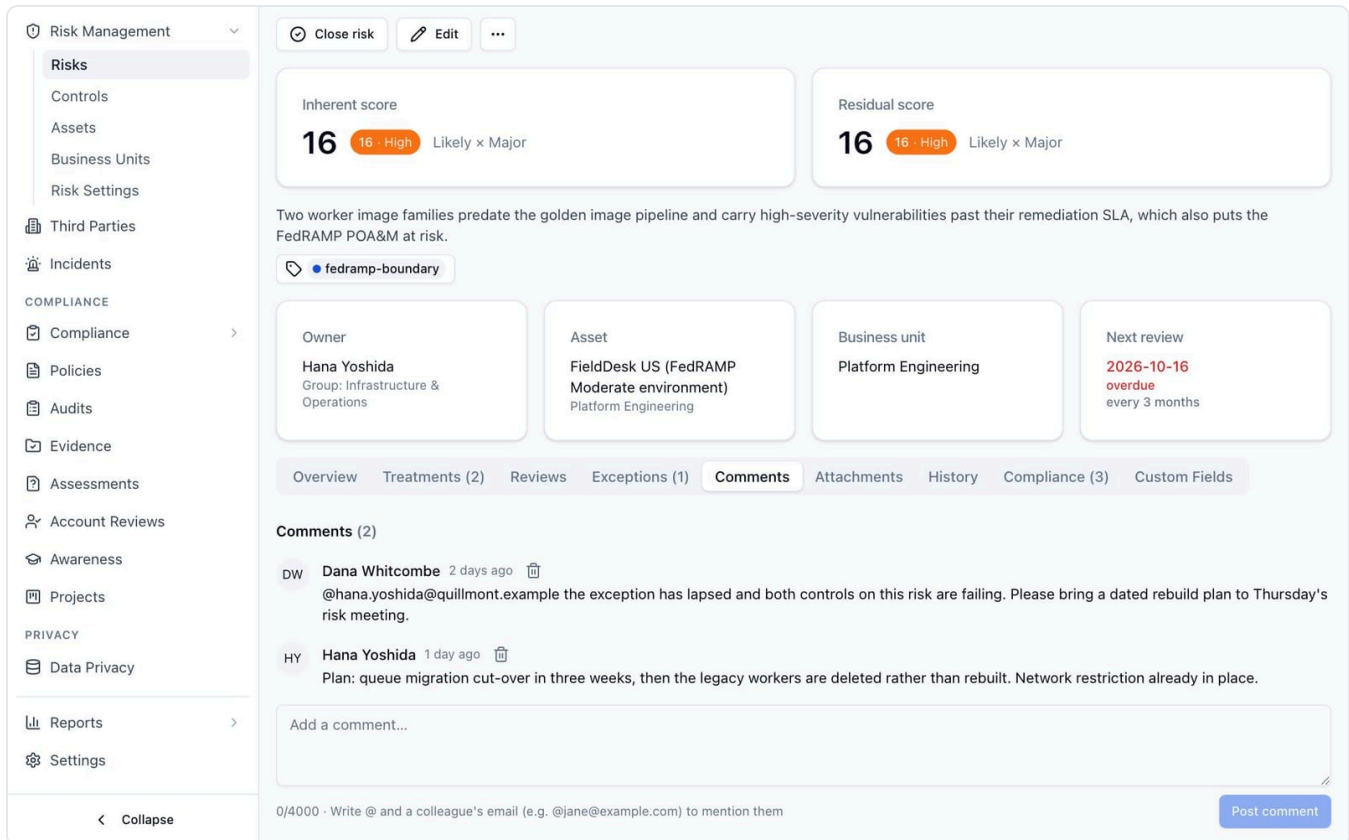


Figure 2.4. The Comments tab of a risk, with a comment that mentions a colleague by email address and the reply below it.

A mentioned colleague is emailed a link to the record when your administrator has set up a notification rule for mentions and the colleague may see the record. The email never contains the comment itself. You can delete your own comments.

Full details: User Manual, Getting Started, Comments.

2.5 Attachments

Supporting documents go on the record's **Attachments** tab. On a control, a compliance requirement or an account review, add files as evidence instead: **Add evidence** on its **Evidence** tab, then upload on the evidence's **Files** tab.

1. Open the record and click **Attachments**.
2. Click **Upload file** and choose the file.

Files can be up to 25 MB, of these types: PDF, PNG, JPG, JPEG, GIF, WEBP, BMP, TXT, CSV, LOG, DOC, DOCX, XLS, XLSX, PPT, PPTX and ZIP. The file's contents must match its extension. Each person can store up to 2 GB unless an administrator changed the limit. Click a file's name to download it.

Every record also has a **History** tab listing each change: what happened, who did it, when and which fields changed.

Full details: User Manual, Getting Started, Attachments and History tabs.

Your first week as a GRC lead

This chapter is a short, ordered path for the person setting up and running the program. Each section is one task: a few numbered steps, one figure and a pointer to the User Manual section that covers it in full. Work through them in order; later tasks use records created by earlier ones.

3.1 Before you start

The tasks below assume the built-in **GRC Manager** role (full access to the risk and compliance modules) or administrator rights. Check with your administrator that:

Item	Why it matters
You are in a group carrying the GRC Manager role	Without it, the New buttons and edit actions in this chapter do not appear.
Outgoing email is configured	Acknowledgement requests, reminders and assessment links are sent by email.
Colleagues have accounts and groups	Owners, approvers and acknowledgement audiences are chosen from active users, groups and roles.
Incident classifications exist	A new installation has none; they are added from the incidents list (see Log an incident).

The GRC Manager role does not include Settings. Risk Settings (the scoring scales, matrix and appetite bands) and the Settings screens are for administrators; the defaults are a 5 × 5 matrix with Low, Medium, High and Critical bands, where High and Critical are over appetite.

3.2 Register an asset

Assets are the things you protect: systems, applications, data stores, facilities. Risks and incidents link to them.

1. Open **Risk Management → Assets**.
2. Click **New asset**.
3. Enter the **Name**, and optionally the **Business unit**, **Owner**, **Owner group** and **Description**.
4. If the asset is a system that holds personal data, tick **A system that holds or processes personal data** and fill in **Hosting country** and **Categories of personal data held**.
5. Click **Create asset**.

Name	Business unit	Owner	Risks	Labels
FieldDesk US (FedRAMP Moderate environment) System, United States	Platform Engineering	Tomas Okafor	4 linked	Labels
FieldDesk EU region System, Ireland	Platform Engineering	Tomas Okafor	1 linked	Labels
Customer identity service System, United States	Platform Engineering	Lena Haverkamp	0 linked	Labels
Corporate identity provider System, United States	Infrastructure & Operations	Hana Yoshida	0 linked	Labels
Analytics data warehouse System, United States	Platform Engineering	Nadia Petrov	0 linked	Labels
Corporate email and collaboration suite System, United States	Infrastructure & Operations	Hana Yoshida	0 linked	Labels
HR information system System, Ireland	People & Culture	Rhea Castellano	0 linked	Labels
Payroll platform System, United States	Finance	Grace Mbeki	0 linked	Labels
Support ticketing system System, United States	Customer Success	Kenji Arakawa	2 linked	Labels
CRM System, United States	Sales & Marketing	Bianca Holm	0 linked	Labels
Marketing website and forms System, Ireland	Sales & Marketing	Thao Lindgren	0 linked	Labels

Figure 3.1. The asset catalog, with systems that hold personal data marked by a System badge and their hosting country.

To load many assets at once, click **Import**, download the template, fill it in and import it back. The same import works for risks, controls, policies, third parties, incidents and projects.

Full details: User Manual, Risk Management, Assets; Getting Started, Importing from CSV.

3.3 Record a risk

1. Open **Risk Management** → **Risks** and click **New risk**.
2. Enter a **Title** and **Description**.
3. Choose the **Classification** (the register tab it belongs to: Asset-based, Third-party, Business continuity or Enterprise on a new installation) and the **Asset** you just registered.
4. Set an **Owner** and, optionally, an **Owner group**.
5. Choose the **Inherent likelihood** and **Inherent impact**: the risk before any action is taken.
6. Keep **Review frequency (months)** at 12 or change it, and leave **Schedule first review** ticked so the first review is booked.
7. Click **Create risk**.

New risk ×

Inherent likelihood and impact set the starting score; treatments reduce the residual.

Title

e.g. Data breach of customer database

Description

Classification

Asset-based

Asset

None

Owner

None

Owner group

None

Inherent likelihood

Rare (1)

Inherent impact

Insignificant (1)

Review frequency (months)

12

☒ Schedule first review (due in 12 months)

Cancel Create risk

Figure 3.2. The New risk dialog with classification, owner, inherent likelihood and impact, and review frequency.

The risk opens in the register with its inherent score; its residual score starts equal to it. Open the risk to add what you are doing about it:

1. On the risk page, open the **Treatments** tab and click **Add treatment**.
2. Choose the **Strategy** (mitigate, accept, transfer or avoid) and **Status**.
3. For a mitigation, set **Reduce likelihood by** and **Reduce impact by** (0 to 4) and describe it in **Description**.
4. Click **Add treatment**.

Figure 3.3. The Add treatment dialog with strategy, status, linked control and the likelihood and impact reductions.

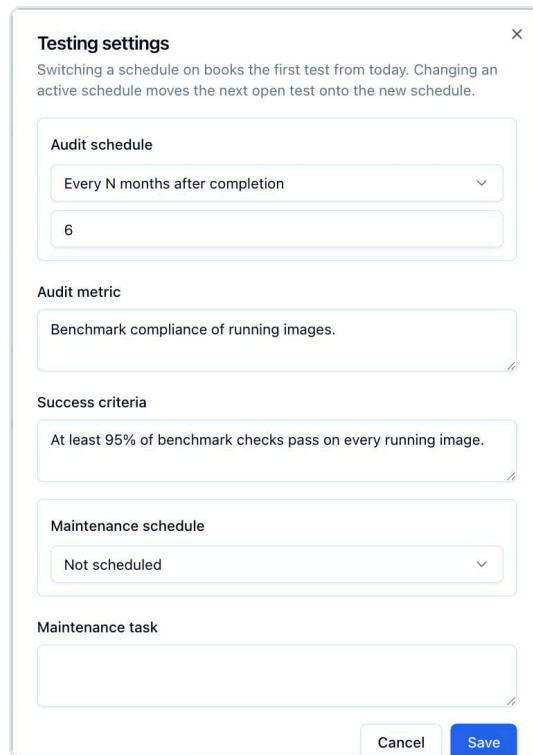
Only an **implemented** mitigation lowers the residual score. When the residual score lands in an over-appetite band, the risk shows a red banner and appears in the **Risks over appetite** dashboard widget. Leave **Linked control** at **None** for now; you link a control in the next task.

Full details: User Manual, Risk Management, Creating a risk, How scoring works and Treatments.

3.4 Add a control and record a test

Controls are shared: one control can treat risks, satisfy compliance requirements and carry audit findings.

1. Open **Risk Management → Controls** and click **New control**.
2. Enter the **Name**, choose the **Type** (Policy, Process, Technical, Physical or Other) and **Status** (Planned, Active or Retired), set the **Owner** and optionally the **Owner group** and **Description**.
3. Click **Create control**.
4. Click the control's name to open it, then click **Testing settings**.
5. Under **Audit schedule**, choose **Every N months after completion** and enter the months, or **Fixed dates each year**. Describe the **Audit metric** (what you measure) and the **Success criteria** (what counts as a pass).
6. Click **Save**. The first audit is booked and appears on the **Audits** tab.



Testing settings [X]

Switching a schedule on books the first test from today. Changing an active schedule moves the next open test onto the new schedule.

Audit schedule

Every N months after completion [v]

6

Audit metric

Benchmark compliance of running images.

Success criteria

At least 95% of benchmark checks pass on every running image.

Maintenance schedule

Not scheduled [v]

Maintenance task

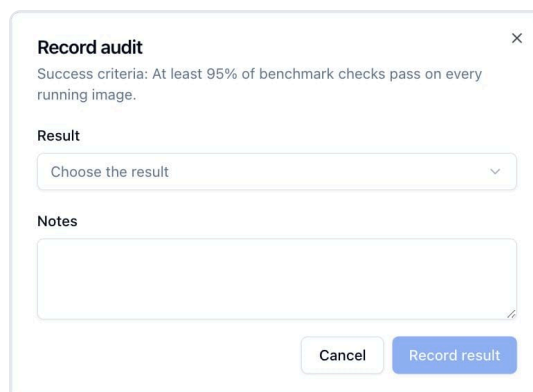
[Empty text field]

Cancel Save

Figure 3.4. The Testing settings dialog with the audit schedule, audit metric, success criteria and maintenance schedule.

When you have performed the test:

1. On the control's **Audits** tab, click **Record result** on the scheduled audit. You can record it before its date.
2. In the **Record audit** dialog, which repeats the success criteria, choose the **Result, Pass or Fail**, and add **Notes**.
3. Click **Record result**. The next audit is booked from the schedule.



Record audit [X]

Success criteria: At least 95% of benchmark checks pass on every running image.

Result

Choose the result [v]

Notes

[Empty text field]

Cancel Record result

Figure 3.5. The Record audit dialog for a scheduled control audit, showing the success criteria, the Pass or Fail result and the notes field.

Add the evidence (a report, a screenshot, an export) with **Add evidence** on the result, then upload its files on the evidence's **Files** tab. A failed audit marks the control **Failed** and emails its owner.

Finally, link the control to your risk: open the risk, edit its treatment with the pencil icon, choose the control in **Linked control** and click **Save changes**. From then on, a failing or overdue control flags the risk **Control failing** on the register. Retiring the control later removes the treatment's reduction from the risk's residual score.

Full details: User Manual, Risk Management, Controls and Scheduling and recording control tests.

3.5 Load a framework and analyze a requirement

A framework (NIST SP 800-53, ISO/IEC 27001, the GDPR, your own internal standard) is loaded as a *package* of requirements. TraxrGRC does not bundle licensed frameworks; you import the clause structure from a file you are licensed to use.

Prepare a CSV file with a header row and one row per clause:

```
code,name,description,parent_code,kind
AC,Access Control,,,heading
AC-1,Policy and Procedures,Develop and maintain an access control policy.,AC,
AC-2,Account Management,Manage system accounts.,AC,
```

`parent_code` builds the tree, and `kind` is `requirement` (the default when blank), `additional` or `heading`. A JSON file in the export format works too.

1. Open **Compliance** → **Packages** and click **Import**.
2. In the **Import compliance package** dialog, choose your file.
3. For a CSV file, enter the **Package name** and, optionally, the **Standard** and **Version**.
4. Check the preview of the item tree. If the dialog lists errors, fix the file and choose it again: the whole file is rejected when any row fails.
5. Click **Commit import**.

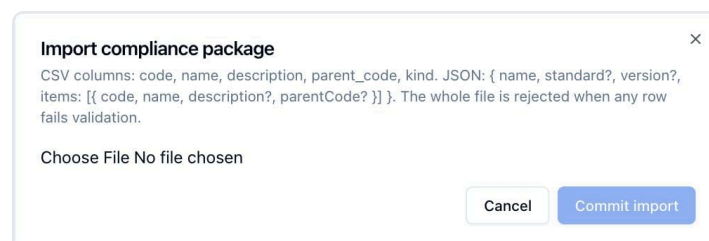


Figure 3.6. The Import compliance package dialog, before a file is chosen.

Every requirement gets an analysis with the status **Not reviewed**. To analyze one:

1. Open **Compliance → Analyses** and choose the package's tab.
2. Click the requirement's row to open it.
3. In the **Analysis** card, choose the **Status** (Compliant, Partially compliant, Not compliant or Not applicable), assign an **Owner** and write your reasoning in **Analysis notes**.
4. Click **Save analysis**.
5. Under **Mapped controls, policies and risks**, click **Map controls** and tick the control you created. Each tick saves straight away. **Map policies** and **Map risks** work the same way.
6. Add supporting files as evidence: **Add evidence** on the **Evidence** tab.

TraxrGRC

Dashboard

My Tasks

Policy Portal

My Questionnaires

RISK

Risk Management

Third Parties

Incidents

COMPLIANCE

Compliance

Analyses

Packages

Gaps

POA&M

Catalog

Policies

Audits

Evidence

Assessments

Account Reviews

Awareness

Projects

PRIVACY

Data Privacy

Reports

Settings

Compliance > Analyses > CM-2 Baseline Configuration

Help

Morgan Ellery

NIST SP 800-53 Rev 5 Moderate > CM Configuration Management > CM-2 Baseline Configuration

CM-2 Baseline Configuration

Partially compliant

At risk

Low

Moderate

High

NIST SP 800-53 Rev 5 (5.2.0) Moderate baseline

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [Assignment: organization-defined frequency];

2. When required due to [Assignment: organization-defined circumstances] ; and

3. When system components are installed or upgraded.

Sub-items (3)

CM-2(2) Baseline Configuration | Automation Support for Accuracy and Currency

Partially compliant

CM-2(3) Baseline Configuration | Retention of Previous Configurations

Compliant

CM-2(7) Baseline Configuration | Configure Systems and Components for High-risk Areas

Not reviewed

Analysis - last reviewed 2026-08-28 09:04 EDT

Status

Partially compliant

Owner

Hana Yoshida

Analysis notes

Golden images cover all but two legacy worker families.

Save analysis

Statement and organization-defined values (NIST SP 800-53 Rev 5) - 0 of 2 set

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [Assignment: organization-defined frequency];

2. When required due to [Assignment: organization-defined circumstances] ; and

3. When system components are installed or upgraded.

frequency cm-02_odp.01

Not set

circumstances cm-02_odp.02

Not set

Save values

Other frameworks

+ Link requirement

Indicated by

No linked requirements indicate this one.

Indicates

This requirement indicates no linked requirements.

Mapped controls, policies and risks

Controls: Failed

Controls

Map controls

Hardened baseline images (CIS Level 1)

Failed

Policies

Map policies

POL-08 Configuration Management Plan

Not published

Risks

Map risks

Unpatched vulnerabilities on legacy worker images

open

Remediation projects

In remediation

Link projects

Create project from this gap

Figure 3.7. A partially compliant requirement at risk: the Analysis card, the mapped controls, policies and risks, and an overdue remediation project.

A requirement you mark compliant or partially compliant shows **At risk** when its evidence disagrees: a mapped control failed, is overdue or retired, or a mapped policy is unpublished or past review. An open audit finding on a mapped control is listed on the requirement, with **Add to POA&M** when no POA&M item tracks it. For a gap, **Create project from this gap** starts a remediation project linked to the

requirement, and **Compliance → Gaps** lists every open gap. To mark a whole domain at once, tick rows on the Analyses page and use **Set status....**

Full details: User Manual, Compliance Management, Importing a package and Working on an item.

3.6 Publish a policy and request acknowledgement

A policy goes live in four stages: write it, have it approved, publish it, and put it on the Policy Portal. Approval needs a second person: you cannot approve your own request unless an administrator has relaxed separation of duties.

1. Open **Policies** and click **New policy**. Enter the **Title**, and optionally a **Description**, **Owner**, **Owner group** and **Review frequency (months)**, then click **Create policy**.
2. Open the policy. On the **Content** tab, click **Edit content**, write the policy in the **Markdown source** pane (the **Preview** pane shows the result) and click **Save content**.
3. On the **Approvals** tab, click **Submit version 1 for approval**.
4. Your approver opens the policy, clicks **Approve** on the pending card, optionally adds a **Note** (it becomes the version's change note) and confirms with **Approve**.
5. Click **Publish v1** in the page header. The policy becomes **Published** with an immutable version 1, and its first review is booked one review frequency after it takes effect.

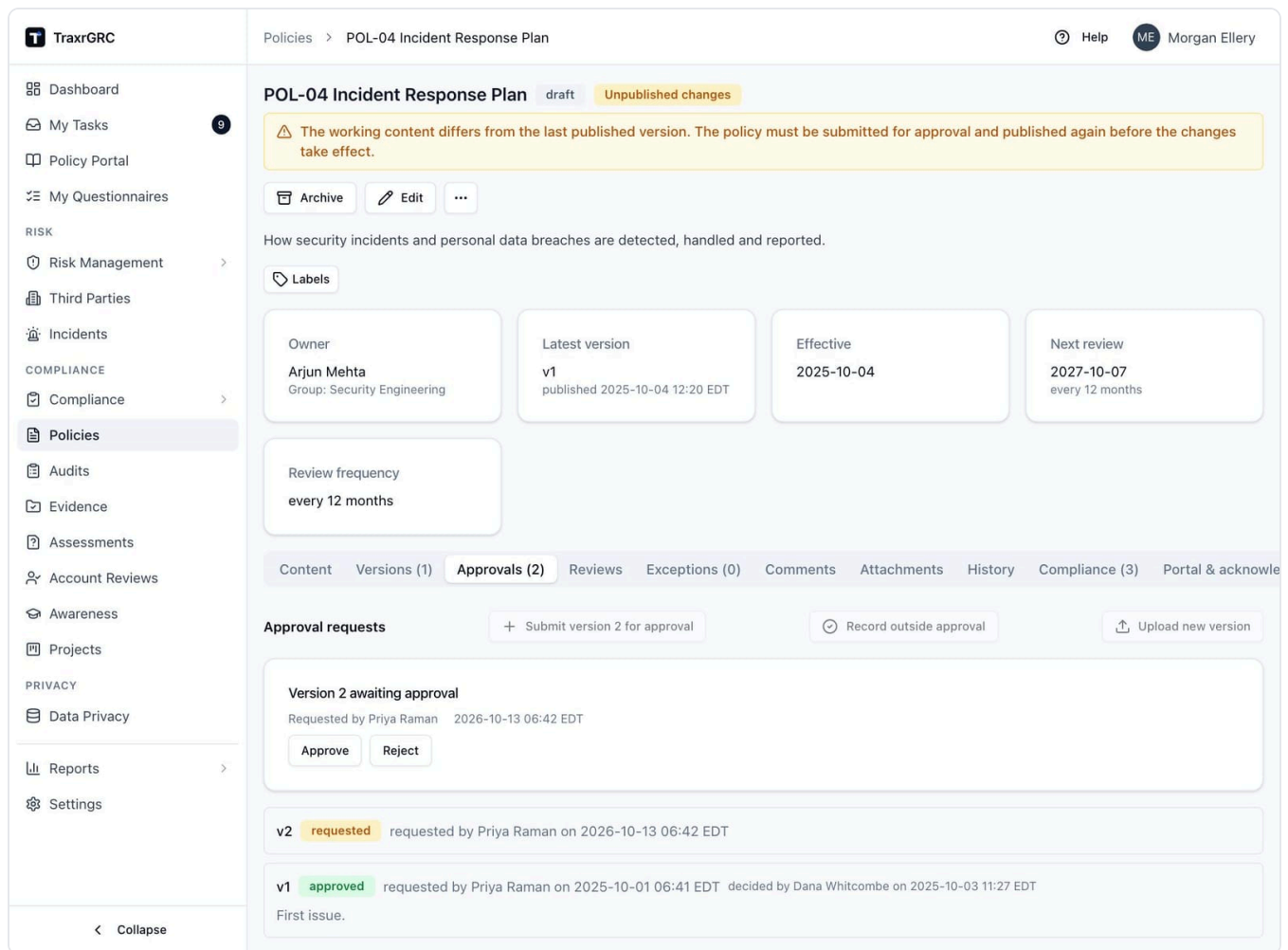


Figure 3.8. The Approvals tab with a version awaiting approval, its Approve and Reject buttons, and earlier approvals listed below.

If the content changes after submission, the approval is withdrawn automatically; submit again. If your organization approves policies outside the tool (a board signature, for example), an administrator can allow **Record outside approval** in place of steps 3 and 4.

To put the policy in front of staff and ask them to acknowledge it:

1. Open the policy's **Portal & acknowledgements** tab.
2. Under **Policy portal**, click **Publish to the portal**. This needs `policies:update` and `policies:review` ; the GRC Manager role has both.
3. Under **Acknowledgement requests**, click **Request acknowledgement**.
4. In the **Request acknowledgement of version 1** dialog, turn on **Everyone (every active user)**, or tick the **Users, Groups and Roles** to ask.
5. Check the **Due date** (30 days ahead by default) and, optionally, write the **Attestation (optional)** text people confirm.
6. Click **Send request**.

Figure 3.9. The Request acknowledgement dialog, with the audience choices, the due date and the attestation.

Everyone asked is emailed a link and reminded before the due date. The **Completion** table on the same tab shows who has acknowledged, who is outstanding and who is overdue, and exports to CSV.

Full details: User Manual, Policy Management, The draft → approval → publish workflow and Policy portal and acknowledgements.

3.7 Log an incident

A new installation has no incident classifications. Add a few first (this needs `incidents:update` at the *all* level):

1. Open **Incidents** and click **Classifications**.
2. Type a **Name** (for example `Phishing`) and a **Sort** number, and click **Add**. Repeat for each category you use.

Then log the incident:

1. On the incidents list, click **New incident**.
2. Enter a **Title** (the only required field) and a **Description** of what happened.
3. Choose the **Classification**, the affected **Asset** or **Third party**, and the **Owner** or **Owner group** handling it.
4. Click **Create incident**.

Figure 3.10. The New incident dialog with its title, description, classification, asset, third party, owner and owner group fields.

The incident opens with status **open**. Record progress in **Comments** and evidence in **Attachments**. When it is resolved, click **Close**, write the **Resolution** and click **Close incident**. If personal data is involved, **Assess as personal data breach** on the incident starts the 72-hour notification clock.

Full details: User Manual, Incident Management, Creating an incident, Closing and reopening an incident and Personal data breaches.

3.8 Send a third-party assessment

Online assessments send a questionnaire to a vendor contact, who answers through a personal link without an account. You need a template first; a new installation has none.

1. If the vendor is not registered yet, open **Third Parties**, click **New third party**, fill in the dialog and click **Create third party**.
2. Open **Assessments**. On the **Templates** tab, click **New template**, enter the **Title** and optionally a **Description** and **Owner**, and click **Create template**.
3. Click the template's title to open it. Click **Add question** for each question, choose its **Answer type**, whether it takes **Evidence files** and whether an answer is required, then click **Save questions**.
4. On the **Requests** tab, click **New request**.
5. Choose the **Template**, the **Third party (optional)**, and enter the **Contact name** and **Contact email**.
6. Choose **Repeat** (for example **Annually**) and a **Due date (optional)**. Tick **Email the link to the contact, with a reminder a week before the due date** to have TraxrGRC send it.

7. Click **Create request**. The **Request created** dialog shows the public link with a **Copy** button; if you did not tick the email option, send the link yourself. Click **Done**.

New assessment request ×

The contact receives a single-use link to a public questionnaire; the result lands back here with a weighted score.

Template ▼

Title Defaults to the template title

Third party (optional) None ▼

Contact name

Contact email

Repeat Does not repeat ▼

☐ Email the link to the contact, with a reminder a week before the due date

Due date (optional) mm/dd/yyyy 📅

Cancel Create request

Figure 3.11. The New assessment request dialog with the template, third party, contact, repeat, email and due date fields.

Anyone holding the link can answer, so share it only with the intended contact. When the contact submits, the request shows **Completed** with a score; open it to accept or flag each answer, send answers back for rework, or raise a third-party risk from an answer.

Full details: User Manual, Online Assessments, Templates and the question editor, Requests and Reviewing answers.

3.9 Run a report

1. Open **Reports → Report Center**. Each card is one report: Risk Register, Compliance Status, Exceptions, Reviews Due, Awareness Completion, Incidents and Policy Acknowledgements.
2. Click a card, for example **Risk Register**.
3. Set the filters and click **Apply filters**. **Reset** clears them.
4. Click **Download CSV** to save the filtered rows for a spreadsheet or an evidence pack.
5. To email the report regularly, click **Schedule**. The **New scheduled report** dialog keeps your filters; give it a **Name**, set the **Frequency**, **Time**, **Time zone** and **Recipients**, and click **Create schedule**. Scheduled reports are listed under **Reports → Scheduled**.

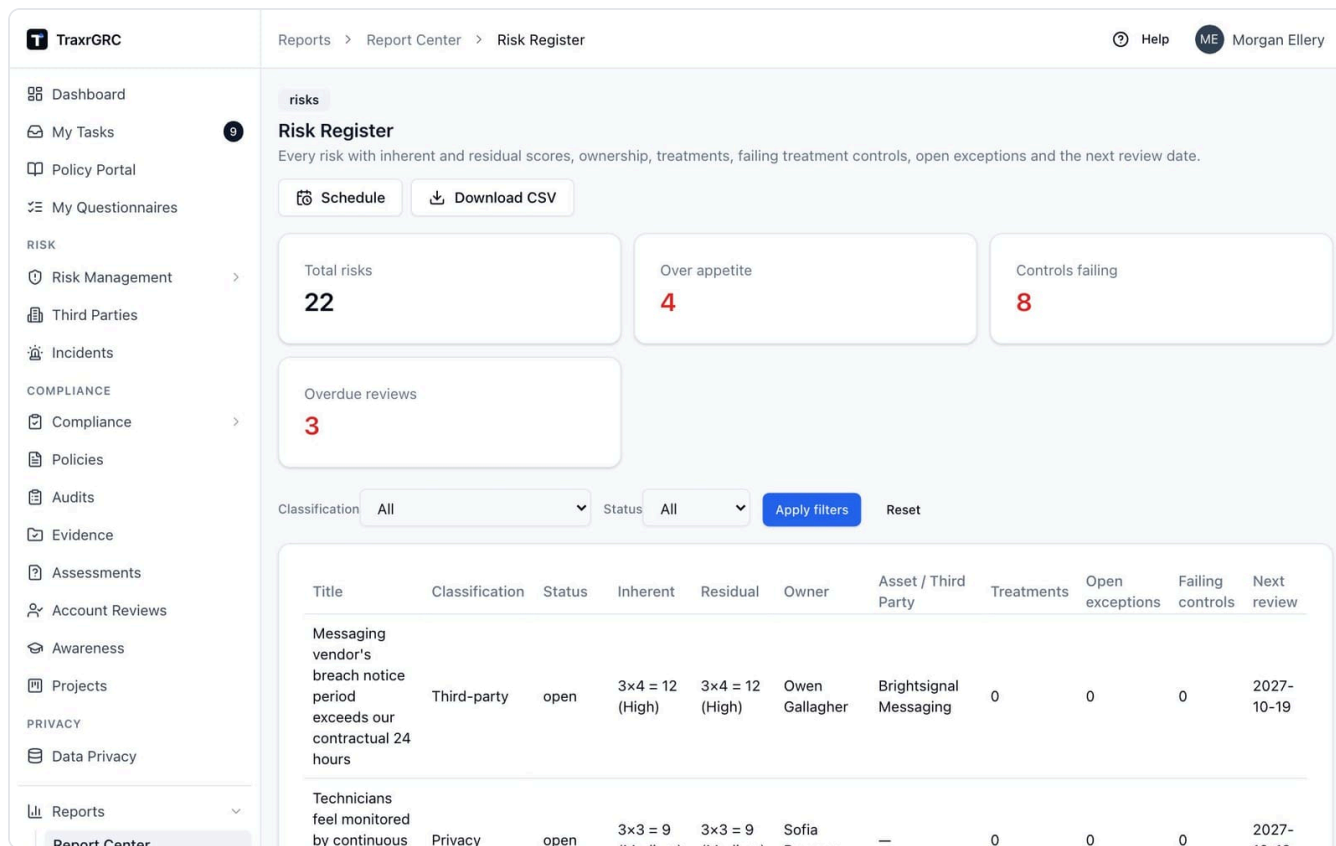


Figure 3.12. The Risk Register report: summary cards with red counts for risks over appetite and failing controls, the Classification and Status filters, and the results table.

Every report applies the reader's permissions, so two people can see different rows in the same report. For a board-ready view of one framework, open the package under **Compliance → Packages** and click **Report** to download the compliance PDF.

Full details: User Manual, Report Center.

3.10 Keep it running: reviews

Every risk, policy and record of processing carries a review date, and proving that reviews happen on time is much of what an auditor asks for. Make a weekly habit of finding what is due:

1. Open **Reports → Report Center** and click **Reviews Due**.
2. Tick **Overdue only** and click **Apply filters** to list every past-due risk, policy and data privacy review with its owner.
3. Click **Schedule** to have the list emailed to you every week.

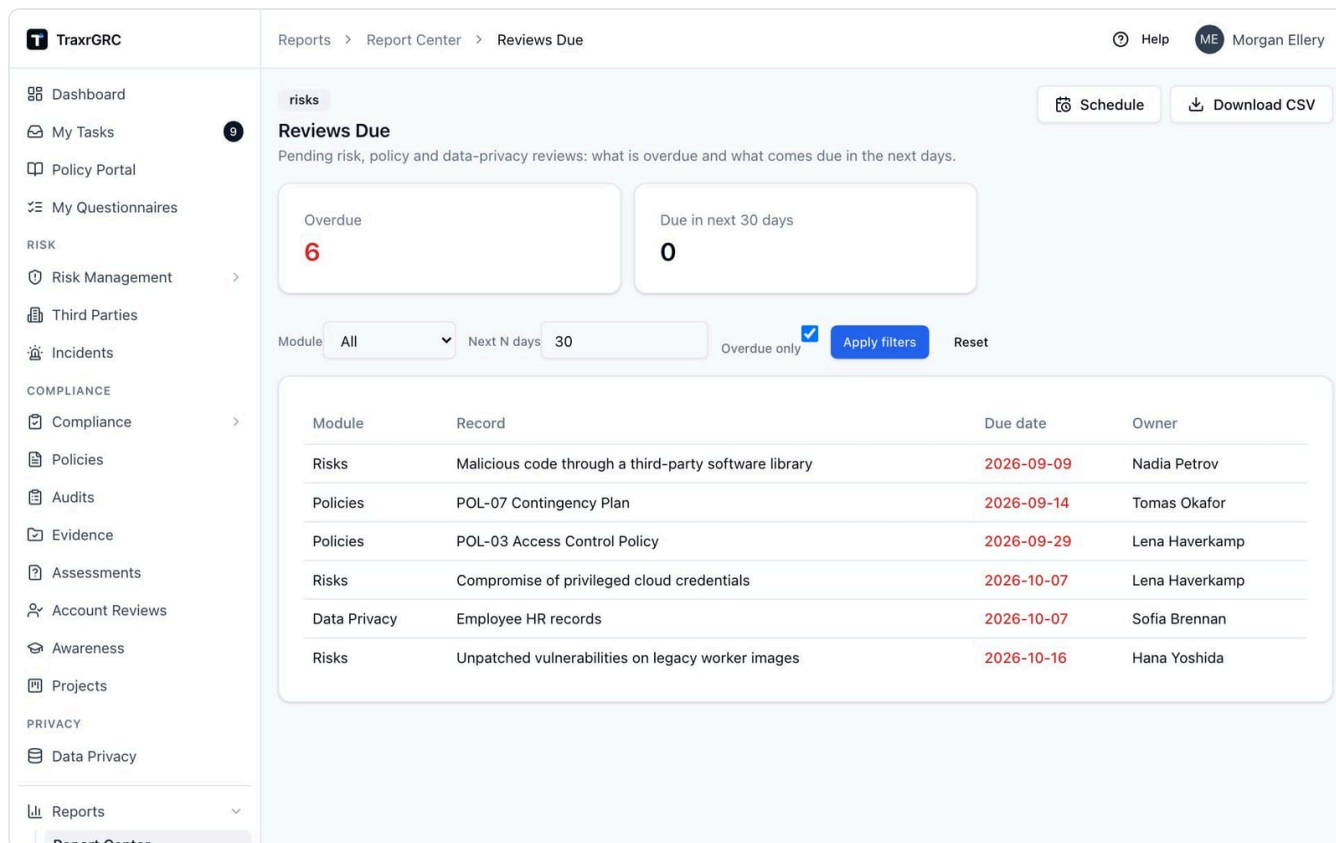


Figure 3.13. The Reviews Due report with Overdue only ticked, listing past-due risk, policy and data privacy reviews with their due dates in red.

To complete a risk review (this needs `risks:review` ; the GRC Manager role has it):

1. Open the risk and click the **Reviews** tab.
2. Under **Upcoming reviews**, click **Complete review**.
3. Choose the **Result: Approved** (fine as it is), **Changes required** (follow-up needed) or **Accepted over appetite** (the risk stays over appetite by explicit decision). Add **Notes** on what you checked. Accepting over appetite also asks for a justification, an expiry date and optionally an approver: it raises an exception request, and the risk is accepted only once someone approves it.
4. Click **Complete review**.

The screenshot displays the TraxrGRC interface for a risk titled "Compromise of privileged cloud credentials". The interface is divided into a sidebar on the left and a main content area on the right. The sidebar contains navigation links for Dashboard, My Tasks, Policy Portal, My Questionnaires, RISK, Risk Management, Controls, Assets, Business Units, Risk Settings, Third Parties, Incidents, COMPLIANCE, Compliance, Policies, Audits, Evidence, Assessments, Account Reviews, Awareness, and Projects. The main content area shows the risk details, including the risk name, scores (Inherent score: 20 Critical, Residual score: 8 Medium), a description of the risk, and a list of reviews. The "Upcoming reviews" section shows a review due on 2026-10-07, which is marked as "overdue". The "History" section shows a completed review on 2026-03-28 by Lena Haverkamp.

Figure 3.14. The Reviews tab of a risk with an overdue scheduled review and the history of completed reviews.

The review is recorded with your name and the time, the next review is booked at the risk's review frequency from today, and **Next review** moves everywhere it is shown. Policies have a **Reviews** tab that works the same way.

Full details: User Manual, Risk Management, Reviews; Policy Management, Reviews tab; Report Center, Reviews Due.

3.11 What you have built

By the end of the week your program holds an asset, a scored risk with a treatment, a tested control linked to both the risk and a compliance requirement, a framework under analysis, a published policy with acknowledgements coming in, an incident record, a vendor assessment in flight and a report you can schedule. The Dashboard now reflects all of it. From here, the same patterns repeat: add records, link them, review them on schedule, and let the reports and widgets show where attention is needed.

Where to go next

4.1 User Manual chapters by role

The User Manual is the complete reference. Start with the chapters for your role:

Role	Chapters
Every user	Getting Started; Policy Management (Policy portal and acknowledgements); Security Awareness (Taking a test)
Data Liaison	Data Privacy (Data mapping questionnaires)
Risk owner	Risk Management (The risk detail page, Treatments, Reviews, Exceptions)
Control owner	Risk Management (Controls); Internal Audits (Working with findings)
Compliance manager	Compliance Management; Projects; Report Center
Policy owner or approver	Policy Management
Vendor or third-party risk manager	Third-Party Management; Online Assessments
Security operations	Incident Management
Data Protection Officer	Data Privacy; Incident Management (Personal data breaches); Third-Party Management (Data protection)
Internal auditor	Internal Audits; Account Reviews; Report Center
CISO or executive	Getting Started (The Dashboard); Report Center

4.2 The Administrator's Guide

Read the Administrator's Guide to install and run TraxrGRC: deployment, the first administrator, sign-in with SAML SSO or LDAP, outgoing email, users, groups and roles, notification rules, branding, backups and the audit log.

Every Settings screen has a card on the **Settings** page, shown only to people who may open it. The **Settings** entry in the sidebar appears for anyone with at least one card: administrators see them all, and

a GRC Manager, for example, sees **Custom Fields**, **Notifications** and **Audit Log**.

4.3 The REST API

Scripts and other systems can read and maintain records through the REST API at `/api/v1`. The machine-readable OpenAPI document is served at `/api/v1/openapi` on your installation and needs no token.

1. A user with Create on API tokens (an administrator, by default) creates a token at `/settings/api-tokens`, with a name, an optional expiry date and the module scopes it may use.
2. The token, starting with `aat_`, is shown once. Store it safely.
3. Send it in the `Authorization` header:

```
curl -H "Authorization: Bearer aat_your_token_here" \  
https://grc.example.com/api/v1/risks
```

A token acts as the user who created it, limited to its scopes, and every change it makes is recorded in the audit log.

Full details: User Manual, REST API.

4.4 Getting help

- **A module or button is missing.** Your role does not grant it. Ask your administrator which group to join.
- **An email never arrived.** Check that outgoing email is configured, and on **My profile** that you have not switched the rule or report off.
- **You cannot sign in.** Read the message under the form (see Signing in) and contact your administrator; they can reset a password, reset two-step verification after a lost device, or reactivate an account in **Settings → Users**.

Index

A

Acknowledgement 11, 18, 24, 32
Acknowledging a policy 18
Add a control and record a test 27
Answering a data mapping questionnaire 19
Approval workflow 32
Asset 24, 25
Attachment 22
Attachments 22
Audit finding 6, 8, 9, 29
Audit log 40

B

Before you start 24

C

Classification 34
Comment 21
Comments and mentions 21
Completing awareness training 20
Control 6, 25, 27, 29, 40
CSV import 15, 24, 29

D

Dashboard 7, 11, 25, 39
Data Liaison 7, 19, 40
Data map 19

E

Evidence 22, 27, 29
Export 15

F

Finding your way around 8

G

Getting help 41

Group 9, 24, 32

H

History 22

K

Keep it running: reviews 37

L

Load a framework and analyze a requirement 29

Log an incident 34

N

NIST SP 800-53 29

Notification rule 15, 40

Notifications 15

O

Owner 24, 25, 27, 32, 34, 40

P

Password 7, 11

Password change 11

Personal data breach 34

POA&M 29

Policy portal 6, 7, 9, 11, 18, 32, 40

Publish a policy and request acknowledgement 32

Q

Questionnaire 6, 19

R

- Record a risk 25
- Register an asset 24
- Remediation project 6, 29
- Report schedule 15, 36
- Residual risk 25
- Review 6, 11, 25, 32, 37, 40
- Risk appetite 24, 25, 37
- Risk score 25
- Run a report 36

S

- SAML 7, 11, 40
- Send a third-party assessment 35
- Session 7, 10
- Signing in 7

T

- The Administrator's Guide 40
- The Dashboard 11
- The header and user menu 10
- The REST API 41
- The sidebar 9
- Third party 6, 35
- Time zone 11
- Treatment 25, 27
- Two-step verification 7, 11

U

- User 7, 9, 10, 11, 32, 40, 41
- User Manual chapters by role 40

V

- Version 18, 32

W

- What TraxrGRC does 6
- What you have built 39
- When a page is off limits 11
- Working with lists 15

Y

Your profile and time zone 11