

One Trust: G-Cloud Price List

Helping Public Sector organisations automate manual privacy, IT & third-party risk management processes to improve efficiency & reduce risk.

Contents.

Section 1 - Introduction

- About OneTrust & Public Sector Use Cases
- Introduction to OneTrust's Commercial Model
- Overview of OneTrust Solutions

Section 2 – Pricing

- Privacy Automation
- Third Party Management
- Tech Risk and Compliance
- Data & AI Governance
- Consent & Preferences (Cookies)

Appendix

- Consumption usage definitions

Section 1

Introduction & Background

onetrust

Founded in 2016, pioneering the Privacy market in response to business needs due to the increase in internet privacy regulation and laws.

2,500

Employees

14,000

Customers

300+

Patents

\$450M

Revenue



About One Trust

OneTrust is the leading platform for privacy, security, and third-party risk management. Widely used by public sector organisations to ensure compliance with global data protection laws and build trust with stakeholders.

It provides a comprehensive suite of tools that help automate privacy workflows, manage data subject requests, assess third-party risks, and maintain compliance with regulations such as the UK GDPR, DPA 2018, and Freedom of Information Act.

With experience serving over 14,000 customers globally across all industries, OneTrust brings deep, cross-sector expertise that positions it well to meet the complex compliance and risk management needs of UK public sector bodies—now the fastest-growing sector for OneTrust in the UK.

Public Sector Use Cases

Public sector organisations can strengthen their data protection posture, reduce compliance risk, and build public trust in how they manage and protect personal information. OneTrust software is particularly relevant in the following areas:

- **Data Privacy Compliance:** Helps ensure adherence to UK GDPR and the Data Protection Act by managing records of processing activities (RoPAs), data mapping, and data subject access requests (DSARs).
- **Third-Party Risk Management:** Enables public sector organisations to assess, monitor, and mitigate risks associated with external vendors and service providers, which is critical for safeguarding citizen data and maintaining service integrity.
- **Incident and Breach Management:** Supports rapid response and reporting processes for data breaches, a requirement under UK GDPR and ICO guidance.
- **Policy and Consent Management:** Ensures transparency in citizen data use through centralised consent tracking and policy updates, aligning with ethical standards and regulatory obligations.
- **Audit and Accountability:** Provides robust documentation and audit trails, simplifying ICO audits and supporting internal governance processes.

One Trust Commercial Model

OneTrust has evolved its commercial model to better align with the way public sector organisations use and scale their trust, risk, and compliance capabilities. Moving away from a module-based subscription approach, OneTrust now delivers its platform as a unified suite where **core functionality is baked in by default**.

Instead of selecting and purchasing individual modules, customers gain access to the full breadth of platform capabilities—**with usage tied to the specific stream they are operating in, whether privacy, third-party management, tech risk and compliance, data & AI governance, or cookie consent**—and simply pay according to the **consumption tier** that matches their operational footprint across either **users, assets & vendors**.

This new consumption-based model provides clearer cost predictability, easier scalability, and more transparent alignment between investment and value delivered. It ensures organisations only pay for the level of usage they need while maintaining flexibility as their requirements evolve.

Suite solutions designed to enable responsible use of Data & AI

Collect —
transparently and
with consent

Consent & Preferences

Built for:
Marketing &
Privacy Teams

Govern —
automate compliance
and risk operations

Privacy Automation

Built for:
Security & Privacy
Operations Teams

Third-Party Management

Built for:
Procurement, Security,
Privacy & Risk Teams

Tech Risk & Compliance

Built for:
Security &
IT Risk Teams

Use —
apply and enforce
data use policies

Data & AI Governance

Built for:
Data Governance & AI
Governance Teams

Section 2

OneTrust Price List

Solution
Overview

Privacy Automation

Built for:
Security & Privacy
Operations Teams

Privacy Automation Capability

How it helps

Data & Activity Mapping (ROPA)

Build an evergreen data & activity map

Maintain a central view into personal data processing across your data assets, processing activities, and vendors to auto-generate record of processing activities (RoPA), identify data transfers, and manage privacy posture.

Privacy Impact Assessments (DPIA)

Perform privacy risk assessments & mitigation

Streamline privacy risk assessments with AI-assisted workflows that identify, evaluate, and mitigate risks across processing activities, assets, and projects, ensuring compliance and accountability from design to deployment.

Incident Management

Manage privacy incidents & notification

Respond to privacy incidents with speed and precision. Centralize intake, investigation, and notification workflows to meet regulatory timelines and reduce breach impact.

Data Subject Request (DSR) Automation

Automate data subject request (DSR) fulfillment

Automate intake, identity verification, fulfillment, and response for data subject requests—reducing manual effort and ensuring timely, compliant responses across global privacy regulations.

Integrations

Third-party integrations for additional automation

Connect with third-party business applications to trigger workflows, sync data, and initiate mitigation actions, improving visibility and driving automation by embedding privacy into your business operations.

DataGuidance Research

The largest, most trusted source for regulatory research

Leverage trusted intelligence from over 2,000 legal experts across 300 jurisdictions, integrated into OneTrust Copilot and automated workflows for PIAs, DSRs, RoPA, incident response, AI impact assessments, and more.

Privacy Automation Price List

	Advanced	Enterprise	Privacy Automation Base	Privacy Automation Suite
	Feature-limited	Full feature access	Automate core internal privacy operations	Comprehensive solution to automate all privacy use cases
Data & Activity Mapping (ROPA) Build an evergreen data & activity map	Historically Licensed individually	Historically Licensed individually	✓	✓
Privacy Impact Assessments (DPIA) Perform privacy risk assessments & mitigation			✓	✓
Incident Management Manage privacy incidents & notification			✗	✓
Data Subject Request (DSR) Automation Automate data subject request (DSR) fulfillment			✗	✓
Integrations Third-party integrations for additional automation	✗	✓	✓	✓
DataGuidance Research The largest, most trusted source for regulatory research	✗	✗	✓	✓
Insights Dashboard (Power BI) Customizable reporting and analytic capabilities.	✗	✓	✓	✓

Privacy Automation Base		
	Paid Users	
Assets	5	10
500	£39,555.00	£59,737.00
1000	£46,821.00	£67,003.00
2000	£61,352.00	£81,533.00
Unlimited	£92,840.00	£113,021.00

Privacy Automation Suite		
	Paid Users	
Assets	5	10
500	£66,599.00	£96,871.00
1000	£78,708.00	£108,980.00
2000	£102,962.00	£133,198.00
Unlimited	£163,471.00	£193,743.00

Solution Overview

Third-Party Management

Built for:
Procurement, Security,
Privacy & Risk Teams

TPRM Capability	How it helps
Third Party Risk Foundations Vendor inventory, workflows and attributes to manage full third-party lifecycle	Helps the department centrally manage the full lifecycle of third-party suppliers—ensuring consistent onboarding, assessment, mitigation, and contracting processes.
Integrations Intra-platform and 3rd party integrations to automate end-to-end processes.	Automates manual tasks by connecting internal systems and external tools, improving efficiency and accuracy across procurement and risk workflows.
Insights Dashboard Customizable reporting and analytic capabilities with Power BI	Provides clear, customizable reporting that helps the department track risk trends and make evidence-based decisions.
Integrated Risk Exchange Risk ratings data from multiple providers to inform risk assessment & continuous monitoring.	Supplies up-to-date risk ratings from multiple providers to strengthen assessment quality and ongoing monitoring of suppliers.
Third Party Due Diligence Workflows Workflows to screen third parties for ethics and compliance risks	Enables structured, repeatable checks to identify ethics and compliance risks before working with third parties.
Integrated Dow Jones Screening Screening data to monitor for sanctions, bribery, adverse media and other ethics related risks.	Continuously screens vendors for sanctions, bribery, and adverse media to help the department meet regulatory and ethical standards.

Third Party Management Price List

	Advanced	Enterprise	TPRM Base	TPRM Suite
	Feature-limited	Full feature access	TPM solution package with integrated risk intelligence	TPM solution package with multi-domain coverage
Third Party Risk Foundations Vendor and Engagements inventory, workflows and attributes to manage full third-party lifecycle from onboarding, assessments, mitigation and contracting.	✓	✓	✓	✓
Insights Dashboard (Power BI) Customizable reporting and analytic capabilities.	✗	✓	✓	✓
Integrated Risk Exchange Risk ratings data from multiple providers to inform risk assessment & continuous monitoring.	✗	✓	✓	✓
Integrations Third-party integrations for additional automation	✗	✓	✓	✓
Third Party Due Diligence Workflows Workflows to screen third parties for ethics and compliance risks	Standalone	Standalone	✗	✓
Integrated Dow Jones Screening Screening data to monitor for sanctions, bribery, adverse media and other ethics related risks.	Standalone	Standalone	✗	✓

Third Party Management Base		
	Paid Users	
Vendors	5	10
500	£84,100.00	£104,100.00
1000	£104,100.00	£143,500.00
2000	£134,100.00	£173,500.00

Prices above 2000 vendors available upon request

Third Party Management Suite		
	Paid Users	
Vendors & Screenings	5	10
1000	£123,160.00	£172,410.00
2000	£147,160.00	£196,410.00
5000	£192,126.00	£241,376.00

Prices above 5000 vendors available upon request

Solution
Overview

Tech Risk &
Compliance

Built for:
Security &
IT Risk Teams

TRC Capability	How it helps
Compliance Automation Build, scale, and automate the InfoSec compliance process for internal and third-party audits	Centrally manage compliance, and automatically generate required controls and evidence tasks based on your operations. Collect once, comply many with our proprietary shared evidence framework to remove duplication and complexity.
IT Security & Risk Management Identify and assess IT and cyber risk to make better risk-informed decisions	Proactively identify, measure, mitigate, and monitor IT risk by automating IT risk assessment lifecycle.
Enterprise Policy Management Streamline your policy creation and review process.	A central dashboard to manage, monitor, edit, update, and audit all policies, standards, and procedures across different languages.
Integrations Third-party integrations for additional automation	Connect with third-party business applications to automate evidence collection, build risk registers and map framework compliance across multiple systems.
Insights Dashboard Customizable reporting and analytic capabilities with Power BI	Provides clear, customizable reporting that helps the department track risk trends and make evidence-based decisions.

Tech Risk and Compliance Price List

	Standard, Advanced	Enterprise	Tech Risk & Compliance
	Feature-limited	Full feature access	Comprehensive solution to automate all GRC use cases
Compliance Automation Build, scale, and automate the InfoSec compliance process for internal and third-party audits	Historically Licensed individually	Historically Licensed individually	✓
IT Security & Risk Management Identify and assess IT and cyber risk to make better risk-informed decisions			✓
Enterprise Policy Management Streamline your policy creation and review process.			✓
Integrations Third-party integrations for additional automation			✓
Insights Dashboard Customizable reporting and analytic capabilities with Power BI	✗	✓	✓

Tech Risk & Compliance			
	Paid Users		
Assets	10	25	
1000	£81,964.00		£127,661.00
2000	£105,619.00		£151,316.00
Unlimited	£225,471.00		£271,167.00

Solution
Overview

Consent & Preferences

Built for:
Marketing &
Privacy Teams

C&P Capability	How it helps
Web & App Audits Scan websites & mobile app to cookies, tags and tracking technologies.	Maintain a central view into personal data processing across your data assets, processing activities, and vendors to auto-generate record of processing activities (RoPA), identify data transfers, and manage privacy posture.
User Experience Design Pre-built regulatory templates and customisable user experiences for CMP.	Respflows to meet regulatory timelines and reduce breach impact.
Consent Rate Optimisation A/B testing & analytics on CMP performance.	Automate intake, identity verification, fulfillment, and response for data subject requests—reducing manual effort and ensuring timely, compliant responses across global privacy regulations.
Web Forms & Preference Centers Customisable first party data collection points.	Configure data collection web forms and preference centers using dynamic and logic-based displays to capture durable identifiers and preference choices.
Unified Customer Profiles User profiles storing all forms of consent.	Create profiles that contain all consent and preference-related information in one place, even linking anonymous consent with known-user consent.
Integrations Third-party integrations for additional automation	Connect with third-party business applications to trigger workflows, sync data, and initiate mitigation actions, improving visibility and driving automation by embedding privacy into your business operations.
Insights Dashboard Customizable reporting and analytic capabilities with Power BI	Provides clear, customizable reporting that helps the department track risk trends and make evidence-based decisions.

Consent & Preferences Price List

	Enterprise	Consent Management Platform	Universal Consent & Preference Management
	Full feature access	Obtain consent for purposes such as analytics, advertising and compliance.	Collect first-party including product, communications, and channel preferences.
Web & App Audits Scan websites & mobile app to cookies, tags and tracking technologies.	Historically Licensed individually	✓	✗
User Experience Design Pre-built regulatory templates and customisable user experiences for CMP.		✓	✗
Consent Rate Optimisation A/B testing & analytics on CMP performance.		✓	✗
Web Forms & Preference Centers Customisable first party data collection points.		✗	✓
Unified Customer Profiles User profiles storing all forms of consent.		✗	✓
Insights Dashboard Customizable reporting and analytic capabilities with Power BI	✓	✓	✓
Integrations Third-party integrations for additional automation	✓	✓	✓

Consent Management Platform		
Average Daily Unique Visitors		
20,000		£16,145.00
50,000		£28,254.00
100,000		£36,326.00
200,000		£42,381.00

Prices above 200,000 ADUV available upon request

Universal Consent & Preference Management		
Data Subjects		
1 Million		£27,555.00
3 Million		£64,478.00
5 Million		£93,367.00
10 Million		£148,481.00

Prices above 10 Million Data Subjects available upon request

Solution
Overview

AI Governance

Built for:
Data Governance & AI
Governance Teams

AI Gov Capability	How it helps
Intake and inventory A central intake process helps a public body track all AI-related initiatives across departments, directorates, or agencies.	Creates a single, central register of all AI systems across the organisation. This ensures visibility, accountability, and compliance with governance requirements.
AI Assessment Templates Pre-built or customisable assessment templates (e.g., DPIAs, AI risk assessments, algorithmic impact assessments) standardise how AI risks are evaluated.	Provides structured templates for risk, ethical, and regulatory assessments. This ensures consistent and repeatable evaluation across all departments.
Automated risk flagging & mitigation This feature automatically detects high-risk factors—such as sensitive data use, automated decision-making, or potential discrimination—and suggests mitigation actions.	Automatically identifies potential high-risk issues within AI projects and highlights them early. This enables prompt mitigation and strengthens defensible governance.
Integrations OneTrust integrates with commonly used AI platforms, enabling monitoring and policy enforcement directly where models are built or deployed.	Connects governance controls directly to the AI tools, platforms, and models in use. This ensures real-time oversight and reduces reliance on manual tracking.
Systemic risk scoring, tiering & reporting These features provide organisation-wide risk scoring, model tiering, and dashboards so leadership can understand the overall AI risk landscape.	Scores and categorises AI systems based on their risk profile. This helps leaders prioritise oversight and maintain transparent, organisation-wide reporting.

AI Governance Price List

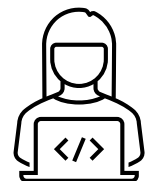
AI Governance	
Comprehensive solution to automate AI use cases	
Intake and inventory A central intake process to track all AI-related initiatives	✓
AI Assessment Templates Pre-built or customisable assessment templates	✓
Automated risk flagging & mitigation Detects high-risk factors—such as sensitive data use	✓
Integrations Enabling monitoring and policy enforcement directly where models are built or deployed.	✓
Systemic risk scoring, tiering & Reporting Dashboards Risk scoring, model tiering, and dashboards so leadership can understand the overall AI risk landscape.	✓

AI Governance			
Admin Users			
Projects	5	10	
100	£48,123.00		£82,028.00
250	£52,653.00		£96,558.00
500	£67,184.00		£102,089.00

Above 500 projects prices available upon request,.

Appendix

Key Activities For Paid And Free Users



“Paid Users” are individuals who create, configure and manage program elements & workflows, initiate key actions and perform system administrative activities.

- 1

Create and Manage Program Elements

Create & manage key program elements such as Data Map, DSRs, Exchange, Inventories (Third Party, Assets, Policies, Processing Activities, etc.) and Libraries (Controls, Risks, etc.).
- 2

Design, Configure & Oversee Workflows

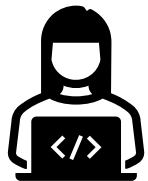
Create workflows & automation rules around program elements to automate manual tasks. Configure & manage templates. Create & provision dashboards & reports. Access DataGuidance for regulatory guidance.
- 3

Initiate Key Actions

Distribute or assign assessments such as PIA/DPIA, Third Party or Control assessments. Create, distribute, and assign tasks. Approve Assessments. Assign approvers.
- 4

Platform Administration

Set up integrations, perform bulk import/export, assign user permissions & permissions or manage other system administrative activities.



“Free Users” are individuals who contribute by responding and completing requests (e.g., assessments, tasks), triggering actions for program owners (e.g., launch assessments, raise issues, incidents) and viewing status as needed.

- 1

Contribute Key Information

Upload key information, documents or submit evidence. Create & submit issues & incidents.
- 2

Launch or Complete Assessments

Create & launch assessments via the self-service portal. Complete an assessment that the user is invited to complete. Trigger actions for paid users via self-service portal.
- 3

Perform Assigned Actions

Complete tasks assigned by paid users such as a DSR sub-task. Attest to a policy.
- 4

View Status Of Key Program Elements

View status for provisioned program inventory elements (i.e. assets, vendors). View specific dashboards and reports provisioned by paid users.

Privacy Automation

User Definitions

Roles	Paid or Free	Description
Assessments Manager	Paid	- Responsible for overseeing privacy assessment initiatives. - Have administrative permissions to configure templates, launch templates and approve responses.
Data Mapping Automation Manager	Paid	- Oversee data mapping processes. - Have administrative permissions to configure inventories, launch & review assessments, scan systems for data, generate key reports.
DataGuidance User	Paid	This is not an assignable role in the product, but every Privacy Automation user receives access to DataGuidance.
Incidents Manager	Paid	- Manage all aspects of privacy incidents. - Have administrative permissions to create, edit and manage incidents.
Integration Manager	Paid	- Configure & manage workflow connections between external systems and the OneTrust platform. - Set up custom connections, create system credentials, retrieve & alter data throughout the platform, investigate detailed logs, add systems.
Privacy Officer	Paid	- Designed for users who require access across capabilities. - Have access to most Privacy functions in the product and have administrative permissions across all core capabilities.
Privacy Rights Automation Manager	Paid	- Oversee their organization's data subject access requests and related policies. - Have administrative permissions to configure web forms, process requests, build workflows and respond to data subjects.
Site Admin	Paid	Manage the OneTrust application. Root organization level users have complete access to the application & all permissions enabled by default. Lower hierarchy organizations' Site Admins have access to most permissions at their organizational group and below.

Incident General User	Free	View and edit incidents they're assigned. Can access and edit incidents without the ability to delete or configure incident settings.
Project Owner	Free	Can launch assessments, review inventory data, view scan results, and complete other everyday business tasks. Have limited to administrative, destructive, and configuration function access.
Project Respondent	Free	- Can log into the application and access a list of all assessments assigned to them. - Can be assigned assessments, risks, and needs more information requests, respond to assigned assessments, & add comments.
Project Viewer	Free	Read-only access - can view information but cannot make any changes or respond to assessments.
Invited User	Free	- Invited users can only access assessments which they have been invited to complete and only through the link provided to them via email. - Invited users are added by email address from an assessment. Invited users cannot be created on the Users screen.
Employee	Free	- Employees have read-only access and can respond to Courses, Disclosures, or Policies from the Employee Portal. - Can only take action on items that have been shared or assigned to them.

Privacy Automation: Asset Inventory

Assets

Assets are any data, devices, or other components within an organization that support information-related activities.

Add New

Export

My Default View >

Search By Name or ID

☐	ID	Name ↑	Managing Organization	Hosting Location	Type	IT Owner	Status	Created Date
☐	13	Adobe Analytics	Marketing	South Africa	Application	David Franc	Active	10/20/2017
☐	159	AI Discovery	OneTrust	Unknown	File System	Kethaki Ashwin Demo0 User	Active	08/31/2023
☐	160	AI Discovery - ML	OneTrust	Unknown	File System	Kethaki Ashwin Demo0 User	Active	08/31/2023
☐	7	AirWatch	IT	Australia	Application	Quentin Bourne	Active	09/11/2017
☐	73	Amazon AWS S3	OneTrust	United States	Database	Johnathan Looney	Active	05/10/2021
☐	92	Amazon S3 - UK	OneTrust	United States	Database	Johnathan Looney	Active	08/18/2021
☐	147	Amazon SageMaker	OneTrust	United States	Software	Shea Murphy	Active	03/31/2023
☐	107	Amazon Web Services	OneTrust	United States	Database	Aaron Peiken	Active	03/04/2022
☐	95	Aurora MySQL AWS	OneTrust	United States	Database	Tim Wilson	Active	11/23/2021
☐	96	Aurora Postgres AWS	OneTrust	United States	Database	Tim Wilson	Active	11/23/2021
☐	93	AWS Health	OneTrust	United States	Software	- - - -	Active	10/25/2021
☐	97	Azure Databricks	OneTrust	United States	Database	Doug Boykin	Active	11/23/2021

< 1 2 3 4 5 6 >

Go to page Go

Showing 1-20 of 107 | 20/page ▼

View Deleted Records

- What:
- Assets refer to the objects added to the inventory in the product for risk tracking.
 - These are typically databases, data lakes, data warehouses, file shares, applications, websites, apps or devices.
 - A customer may choose to track at any level of granularity.
 - Includes archived/pending/active assets.
- Contractual Definition:
- Maximum count of **asset inventory records with processing activities** a customer may have in the cloud services.

Third Party Management

User Definitions

Roles	Paid or Free	Description
Exchange Manager	Paid	Exchange Managers are responsible for managing all aspects of vendors in the Exchange. Fully authorized in the Third-Party Risk Exchange module and can add vendors from the Exchange, request exchange assessments, and edit Exchange template rules.
TPDD Compliance Manager	Paid	Compliance Managers are responsible for the daily management of third party due diligence, including review of assessment responses and screening results.
TPDD Site Admin	Paid	TPDD Site Administrators have access to the global setup menu and the setup options within the TPDD module. This role is designed for designated individuals responsible for user and system setups specific to Third-Party Due Diligence.
Vendor Manager	Paid	Vendor Managers are responsible for managing all aspects of third-party risk management. Users with this role are fully authorized in the Third-Party Risk Management module and can create, edit, and manage vendors, engagements, and contracts, as well as configure vendor settings.
Site Admin	Paid	Manage the OneTrust application. Root organization level users have complete access to the application & all permissions enabled by default. Lower hierarchy organizations' Site Admins have access to most permissions at their organizational group and below.
Business Owner	Free	Business owners collaborate on Audits by providing evidence for control testing and issues remediation. Users with this role have access to view and completed assigned tasks.
TPDD Enhanced Due Diligence Requestor	Free	Enhanced Due Diligence Requesters are allowed to view and order enhanced due diligence reports in TPDD.
Vendorpedia Assessment Coordinator	Free	- Vendorpedia Assessment Coordinators are responsible for working with vendors to assist with, assign, & complete assessment requests. - Can access assessments in Third-Party Risk Exchange and Third-Party Risk Management to assist with these assessments.
Project Owner	Free	Can launch assessments, review inventory data, view scan results, and complete other everyday business tasks. Have limited to administrative, destructive, and configuration function access.
Project Respondent	Free	- Can log into the application and access a list of all assessments assigned to them. - Can be assigned assessments, risks, and needs more information requests, respond to assigned assessments, & add comments.
Project Viewer	Free	Read-only access - can view information but cannot make any changes or respond to assessments.
Invited User	Free	- Invited users can only access assessments which they have been invited to complete and only through the link provided to them via email. - Invited users are added by email address from an assessment. Invited users cannot be created on the Users screen.
Employee	Free	- Employees have read-only access and can respond to Courses, Disclosures, or Policies from the Employee Portal. - Can only take action on items that have been shared or assigned to them.

Third Party Risk Management: Vendor Inventory

Vendors									
Vendors are third parties that market and sell goods and services.									
My Default View > Search By Name or ID Add New Export ...									
ID	Name ↑	Organization	Type	Criticality	Vendor Rating	Primary Vendor Contact	Business Owner	Status	
36	Amazon.com, Inc.	OneTrust	Technology	High	A	Frederick.Smith@aws.com (External)	Arshdeep Sood	Active	
15	Atlassian, Inc.	OneTrust	Technology	Medium	B	Quentin Bourne	- - -	Active	
7	Cisco Systems, Inc.	Corporate	Technology	High	B	Wole Falana	Sam Parker	Pending	
136	Coronis Healthcare	OneTrust	Technology	Critical	B	- - -	Shea Murphy	Active	
10	Dell	IT	Technology	Medium	A	David Franc	Jeanne Lee	Active	
16	Dropbox, Inc.	OneTrust	Technology	High	A	Quentin Bourne	Doug Boykin (Disabled)	Active	
9	Facebook, Inc.	Marketing	Technology	Medium	C	Catherine Williams	Catherine Williams	Active	
120	Fateh Textile Mills	OneTrust	Supplier	- - -	B	Alexander FOnke	A Jason Smith	Active	
129	GE Healthcare	OneTrust	Technology	High	B	Aaron Peiken	Achint Sehgal	Active	
34	Google LLC	OneTrust	Technology	High	A	googleContact@email.com (External)	Catherine Williams	Active	
4	Mavenlink	Corporate	Operations	High	A	Eric Kent (External)	David Franc	Active	
1	Microsoft Corporation	OneTrust	Technology	Critical	A	Quentin Bourne	- - -	Active	

What:

- Third-Party or Vendor Inventory refers to the objects put the inventory for risk tracking.
- These are simply the third parties that an organization does business with.
- A customer may choose to track at any level of granularity.
- Customers can monitor number of Asset Records via the Third-Party Inventory tab in the product.

Contractual Definition:

- **“Third Parties”** means the maximum vendor inventory as identified by a unique record number that Customer may have in the Cloud Services.

Tech Risk & Compliance

User Definitions

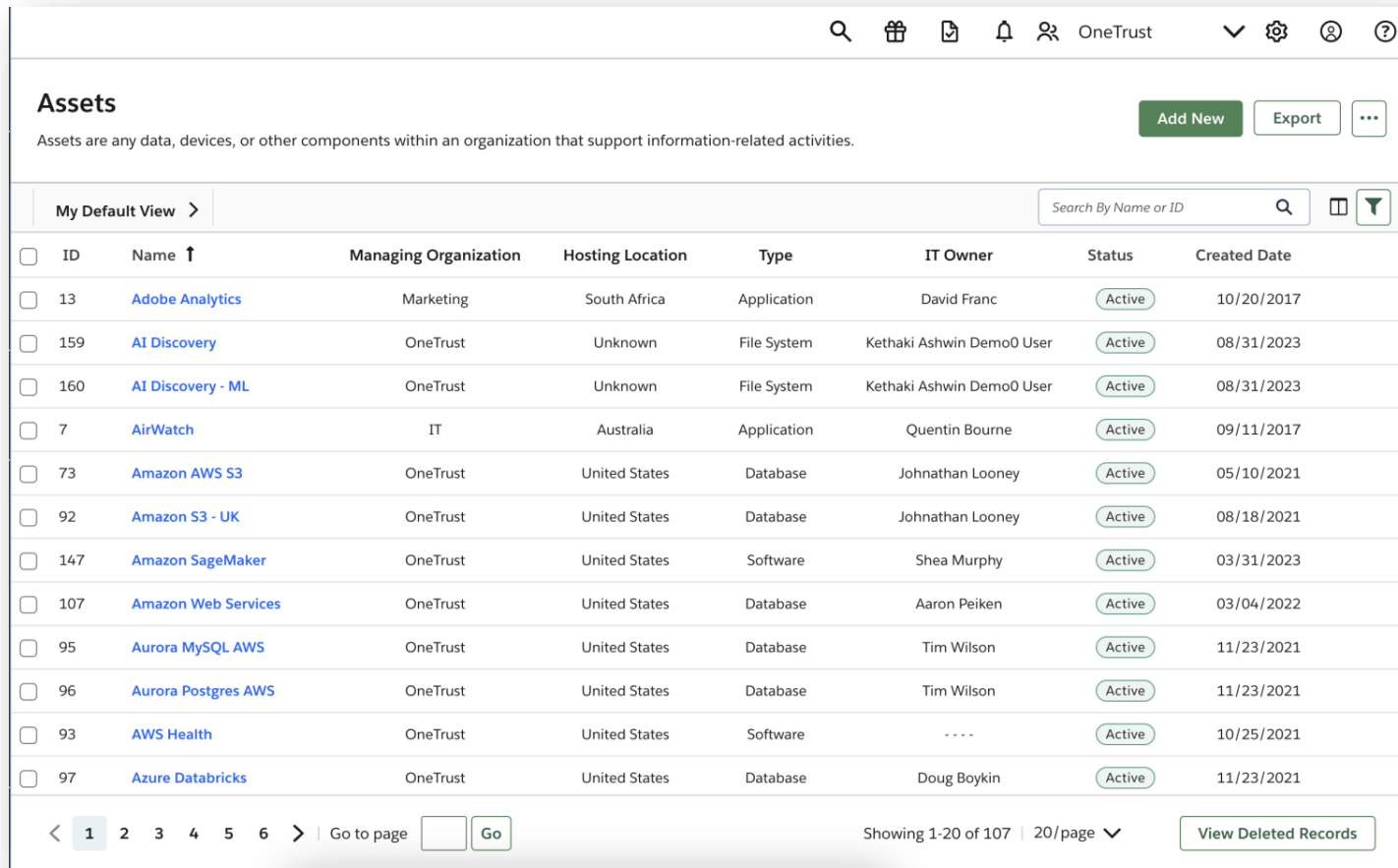
Roles	Paid or Free	Description
Answer Library Manager	Paid	This role allows user to create and manage Answer Libraries within the QRA module
Audit Manager	Paid	Audit Managers are responsible for managing all aspects of the audit process. Users with this role are fully authorized in the Audit Management module and can create and manage audits, workpapers, and findings as well as configure related audit settings.
Enterprise Policy Manager	Paid	Enterprise Policy Managers are responsible for managing all aspects of policy creation. Users with this role are fully authorized in the Policy Management module and can create, organize, and manage documents.
ERM Manager	Paid	ERM Managers are responsible for managing all aspects of the enterprise risk process. Users with this role are fully authorized in the Enterprise Risk Management module to manage and edit risk attributes, risk scoring, risk categories, risk assessments, and view reports.
Policy Owner	Paid	Policy Owners are responsible for reviewing the policies they were assigned. Users with this role are able to access the Policy Management module to manage all aspects of a policy and assign controls to a policy.
Tech Risk and Compliance Admin	Paid	Tech Risk & Compliance admins have access to fundamental capabilities in IT Security Risk, Compliance and Policy Management
Compliance Manager	Paid	A Compliance Manager has access to the Compliance Automation module and related settings.
Site Admin	Paid	Manage the OneTrust application. Root organization level users have complete access to the application & all permissions enabled by default. Lower hierarchy organizations' Site Admins have access to most permissions at their organizational group and below.

Tech Risk & Compliance

User Definitions

Roles	Paid or Free	Description
Auditor	Free	Auditors are responsible for reviewing the audit they were assigned. Users with this role are able to access the Audit Management module and can access and complete work on any audit, workpaper, and finding for which they were assigned.
EPM Policy View Only	Free	EPM Policy View Only users are responsible for viewing policies. Users with this role are able to access the Policy Management module and view policies without the ability to create, edit, delete, or download the policy.
EPM Procedure View Only	Free	EPM Procedure View Only users are responsible for viewing procedures. Users with this role are able to access the Policy Management module and view procedures without the ability to create, edit, delete, or download the procedure.
EPM Standard View Only	Free	EPM Standard View Only users are responsible for viewing standards. Users with this role are able to access the Policy Management module and view standards without the ability to create, edit, delete, or download the standard.
EPM View Only	Free	EPM View Only users are responsible for viewing policies, standards, and procedures. Users with this role are able to access the Policy Management module and view policies, standards, and procedures without the ability to create, edit, delete, or download the documents.
Policy Attestation Respondent	Free	Policy Attestation Respondents are responsible for reviewing the attestations they were assigned. Users with this role are able to access the Self Service Portal to review, acknowledge, and attest policies.
Trust Profile Viewer	Free	Trust Profile Viewers are responsible for viewing Trust Profiles in the Vendor Portal. Users with this role are able to access the Vendor Portal and view Trust Profiles without the ability to modify the profiles in any way.
Questionnaire Respondent	Free	Questionnaire Respondents are responsible for taking action on questions or requests assigned to them from the Vendor Portal. Users with this role are able to access the Vendor Portal, but cannot create new requests or run the Auto Complete tool.
Project Owner	Free	Can launch assessments, review inventory data, view scan results, and complete other everyday business tasks. Have limited to administrative, destructive, and configuration function access.
Project Respondent	Free	- Can log into the application and access a list of all assessments assigned to them. - Can be assigned assessments, risks, and needs more information requests, respond to assigned assessments, & add comments.
Project Viewer	Free	Read-only access - can view information but cannot make any changes or respond to assessments.
Invited User	Free	- Invited users can only access assessments which they have been invited to complete and only through the link provided to them via email. - Invited users are added by email address from an assessment. Invited users cannot be created on the Users screen.
Employee	Free	- Employees have read-only access and can respond to Courses, Disclosures, or Policies from the Employee Portal. - Can only take action on items that have been shared or assigned to them.

Tech Risk & Compliance: Asset Inventory



Assets							
Assets are any data, devices, or other components within an organization that support information-related activities.							
My Default View > Search By Name or ID							
☐	ID	Name ↑	Managing Organization	Hosting Location	Type	IT Owner	Status
☐	13	Adobe Analytics	Marketing	South Africa	Application	David Franc	Active
☐	159	AI Discovery	OneTrust	Unknown	File System	Kethaki Ashwin Demo0 User	Active
☐	160	AI Discovery - ML	OneTrust	Unknown	File System	Kethaki Ashwin Demo0 User	Active
☐	7	AirWatch	IT	Australia	Application	Quentin Bourne	Active
☐	73	Amazon AWS S3	OneTrust	United States	Database	Johnathan Looney	Active
☐	92	Amazon S3 - UK	OneTrust	United States	Database	Johnathan Looney	Active
☐	147	Amazon SageMaker	OneTrust	United States	Software	Shea Murphy	Active
☐	107	Amazon Web Services	OneTrust	United States	Database	Aaron Peiken	Active
☐	95	Aurora MySQL AWS	OneTrust	United States	Database	Tim Wilson	Active
☐	96	Aurora Postgres AWS	OneTrust	United States	Database	Tim Wilson	Active
☐	93	AWS Health	OneTrust	United States	Software	----	Active
☐	97	Azure Databricks	OneTrust	United States	Database	Doug Boykin	Active

< 1 2 3 4 5 6 >

Go to page Go

Showing 1-20 of 107 | 20/page

[View Deleted Records](#)

What:

- Assets refer to the inventory objects added to the product for risk tracking.
- These are typically databases, data lakes, data warehouses, file shares, applications, websites, apps or devices.
- A customer may choose to track at any level of granularity.
- Customers can monitor number of Asset Records via the Inventory tab in the Product.

Contractual Definition:

- “Assets” means the maximum number of asset records as identified by a unique record number that the Customer may have in the Cloud Services.

AI Governance
User Definitions

Roles	Paid or Free	Description
AI Governance Manager	Paid	AI Governance Managers are responsible for overseeing all aspects of artificial intelligence policy and governance within the organization
Project Owner	Free	Can launch assessments, review inventory data, view scan results, and complete other everyday business tasks. Have limited to administrative, destructive, and configuration function access.
Project Respondent	Free	- Can log into the application and access a list of all assessments assigned to them. - Can be assigned assessments, risks, and needs more information requests, respond to assigned assessments, & add comments.
Project Viewer	Free	Read-only access - can view information but cannot make any changes or respond to assessments.
Invited User	Free	- Invited users can only access assessments which they have been invited to complete and only through the link provided to them via email. - Invited users are added by email address from an assessment. Invited users cannot be created on the Users screen.
Employee	Free	- Employees have read-only access and can respond to Courses, Disclosures, or Policies from the Employee Portal. - Can only take action on items that have been shared or assigned to them.