Vendor Risk Assessment Report: OneTrust

Generated on: September 10, 2025

Vendor Risk Assessment Report: OneTrust

1. Executive Summary

OneTrust is a leading provider of enterprise privacy, security, and data governance software. The company demonstrates strong commitments to compliance, particularly with GDPR and CCPA, and actively engages in ESG initiatives. Financially, while it experienced a valuation adjustment, it shows strong annual recurring revenue growth and positive free cash flow, indicating a healthy financial outlook. OneTrust employs robust security measures, including data encryption and a formal information security program, and holds key certifications like SOC 2 and ISO 27001. Their customer support is tiered, offering various levels of assistance. Areas with insufficient public information include specific details on international sanctions impact, comprehensive disaster recovery plans, and formal uptime guarantees. Overall, OneTrust appears to be a robust and reliable vendor, especially in areas of data privacy and governance, though further inquiry into operational and specific geopolitical risk mitigation might be warranted for a complete assessment.

2. Vendor Profile

- **Vendor Name:** OneTrust
- **Main Focus:** Responsible AI Governance & Compliance Solutions, offering a unified platform for trust, risk, and compliance management.
- **Key Solutions:** AI Governance, Consent & Preferences, Data Use Governance, Privacy Automation, Tech Risk & Compliance, Third-Party Management.
- **Featured Products:** Consent Management Platform, DataGuidance, Third-Party Risk Management.
- **Regulatory Expertise:** Supports compliance with GDPR, DORA, and the EU AI Act.
- **Company Highlights:** Over 14,000 active customers (including 75 of the Fortune 100), 2,000+ employees, and 300+ patents.
- **Recent Activities/Recognition:** Released "The 2025 AI-Ready Governance Report," previewed new AI agents at TrustWeek, recognized in Forrester and IDC MarketScape reports for AI Governance and GRC software.

3. Risk Assessment Findings

Compliance

- **Does the vendor undergo annual SOC 2 Type 2 audits?** OneTrust undergoes SOC 2 audits and receives SOC 2 reports addressing the security, confidentiality, and availability of its services. While not explicitly stated as "annual" in all snippets, SOC 2 Type 2 reports assess controls over a period of time (typically 3 to 12 months) and are valid for one year, requiring annual audits for continuous compliance.
- **Is the vendor compliant with GDPR regulations?** OneTrust positions itself as a platform that helps companies comply with comprehensive data protection regulations like GDPR. They offer tools and solutions designed to operationalize GDPR requirements, build compliance programs, and assist with certification schemes like Europrivacy, which is approved by the European Data Protection Board (EDPB) for GDPR compliance.
- **Is the vendor CCPA compliant?** OneTrust provides solutions to help organizations manage and comply with the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA). They offer tools to automate consumer rights requests, enable opt-out of sale, and manage incident notifications, indicating their own adherence to these regulations.
- **Does the vendor have a documented privacy policy?** Yes, OneTrust has a publicly available "Privacy Notice" that covers the personal information they collect and how it is used.
- **How does the vendor handle data subject requests?** OneTrust offers automated solutions for handling Data Subject Access Requests (DSARs), Data Erasure Requests, and other privacy rights management. Data subjects can submit requests through OneTrust-hosted web forms, which are then queued and processed systematically, including identity verification, automated workflows, and secure communication through a customer portal.

ESG (Environmental, Social, and Governance)

- **Does the vendor have a stated commitment to diversity, equity, and inclusion?** Yes, OneTrust has a stated commitment to diversity, equity, and inclusion (DE&I). They formed a DE&I Council and have committed to funding projects that incorporate DE&I themes, supporting underrepresented communities. Internally, they have "Employee Trust Groups (ETGs)" such as Able, Asian, Black, Families, Interfaith, Latin, Pride, Veterans, and Women, which promote authenticity and inclusion in the workplace.
- **What are the vendor's environmental sustainability practices?** OneTrust has an Environmental Sustainability Policy and is committed to reducing its greenhouse gas emissions to align with the Paris Climate Agreement's goal of limiting global warming to 1.5 degrees Celsius by 2050. Their practices include efficient operations, transitioning away from fossil fuels, sourcing renewable energy, minimizing waste (e.g., eliminating single-use

plastics), and prioritizing partnerships with environmentally committed suppliers. They also offer an ESG and Sustainability Cloud product that helps organizations track and report on environmental metrics, including carbon accounting and emissions.

- **What are the vendor's governance structures and ethical guidelines?** OneTrust's values are grounded in integrity, trust, and accountability, guided by a "Code of Trust" to ensure ethical and legal actions. They have an interdisciplinary AI Governance Committee that manages their AI Governance program, aligning with applicable AI Governance laws. Their products, such as OneTrust Ethics, support ethical data processing, awareness training for employees, and due diligence for third parties.

Financial

- **Has the vendor experienced any significant financial distress in the past 3 years?** OneTrust experienced a "down round" in July 2023, where its valuation decreased from $5.1 billion to $4.5 billion. However, the company's CEO stated that annual recurring revenue (ARR) doubled to $400 million from 2021, and they expect to surpass $500 million in ARR in 2024 while maintaining positive free cash flow. This indicates continued growth and financial health rather than significant financial distress.
- **What is the vendor's financial stability rating?** Insufficient information to provide a confident answer. No formal financial stability rating from a recognized agency was found in the search results.
- **Has the vendor been profitable for the last 3 years?** OneTrust has reported "maintaining positive free cash flow". While positive free cash flow is a strong indicator of financial health, the search results do not explicitly state whether the company has been profitable in terms of net profit for the last three years.
- **What is the vendor's annual revenue?** As of September 2025, OneTrust has reached $500 million in annual recurring revenue (ARR). They expected to surpass $500 million in ARR later in 2024. In July 2023, their CEO stated that ARR had doubled to $400 million from 2021.

Fourth-Party

- **How does the vendor assess and manage the risks associated with its own supply chain?** OneTrust has a framework for vendor risk management that includes due diligence, identification of contractual privacy and security controls, and ongoing management and monitoring of third-party suppliers (vendors, service providers, and processors) from onboarding to offboarding. Their approach also integrates sustainable and ethical practices into the supply chain through supplier due diligence and ESG target tracking.
- **Does the vendor utilize any significant sub-processors or third-party providers for critical services?** Yes, OneTrust utilizes significant sub-processors and third-party providers for critical services. Their listed subprocessors include Microsoft Corporation (Azure Hosting Services), Amazon Web Services, Inc. (Hosting and Infrastructure), Confluent Inc. (Data

streaming and messaging platform), Databricks, Inc. (Data processing and analytics platform), and Cloudflare, Inc. (Content Delivery Network and DDoS Protection).

Geopolitical

- **How might international sanctions or trade restrictions impact the vendor's ability to provide services?** Insufficient information to provide a confident answer. Publicly available information does not detail the potential impact of international sanctions or trade restrictions on OneTrust's ability to provide services.
- **Where are the vendor's data centers and operations located, and what are the geopolitical risks associated with those regions?** OneTrust's headquarters are in Atlanta, Georgia, United States. Their operations are global, with co-headquarters in London, UK, and additional offices in Bangalore, Melbourne, Munich, San Francisco, and New York. For data centers, they utilize Microsoft Azure and Amazon Web Services, with specific hosting locations often determined by customer agreements. OneTrust's Data Processing Addendum outlines measures for transferring data to countries outside the EEA to ensure compliance with EU Data Protection Law. The search results do not specify geopolitical risks associated with these regions.

Privacy

- **Does the vendor have a publicly available privacy policy?** Yes, OneTrust has a publicly available "Privacy Notice".
- **How does the vendor handle personal data in accordance with privacy regulations?** OneTrust collects personal information to deliver products and services, for marketing, and to manage its websites. They employ appropriate technical, organizational, and administrative security measures to protect personal data from loss, misuse, and unauthorized access. Personal data is processed primarily for providing services to customers, and OneTrust commits not to retain, use, or disclose data for purposes other than the permitted purpose. They also provide automated solutions for handling data subject requests, enabling individuals to exercise their rights in accordance with privacy regulations like GDPR and CCPA.

Security

- **Describe the vendor's data encryption practices for data at rest and in transit.** OneTrust encrypts data in transit using TLS 1.2 and data at rest using Azure Transparent Data Encryption AES-256. For their SaaS mode, database encryption is achieved by default with Transparent Data Encryption, supported by Azure. The application also encrypts sensitive data with an encryption key, and connections to SQL Server and MongoDB use HTTPS.
- **Does the vendor have a formal information security program in place?** Yes, OneTrust has a formal information security program. Security is embedded throughout their business, including employee training and third-party onboarding, with risk-based controls and

processes to safeguard data. Their Data Processing Addendum outlines policies for information security incident management and supplier relationships, indicating a structured program. The presence of SOC 2 and ISO 27001 certifications further confirms a formal program.

- **What is the vendor's incident response plan in case of a data breach?** OneTrust has an Incident & Breach Response solution, which, while primarily a product for their customers, reflects their internal approach to managing the full lifecycle of personal data incidents. This includes automated workflows for intake, analysis, investigation, reporting, and monitoring, tailored to relevant breach notification laws. Their Data Processing Addendum also states they have policies to reduce the impact of security incidents.
- **Does the vendor have a documented information security policy?** Yes, the existence of their ISO 27001 certification implies a documented Information Security Management System (ISMS), which includes formal policies. Their Data Processing Addendum also refers to established policies for security incident management and technology procurement.
- **Does the vendor have SOC 2 certification?** Yes, OneTrust has been audited and received SOC 2 reports addressing the security, confidentiality, and availability of its services.
- **Does the vendor have ISO 27001 certification?** Yes, OneTrust holds ISO/IEC 27001 certification for its Information Security Management System. They also hold ISO/IEC 27701 (Privacy Information Management System) and ISO/IEC 27017 (Information Security for Cloud Service Providers) certifications.
- **Has the vendor experienced any security breaches in the last 3 years?** The available search results, including a security rating report from UpGuard that monitors data breaches and cybersecurity incidents, do not indicate any publicly known security breaches experienced by OneTrust in the last three years.
- **How does the vendor handle security incident response?** OneTrust handles security incident response through a structured approach that includes centrally managing incidents, automating tasks, and maintaining records for compliance and notification. They leverage their DataGuidance intelligence to tailor response workflows based on applicable laws and integrate with other security tools. Their processes aim to streamline investigation, automate root cause analyses, and ensure accountability.

Service Delivery

- **What specific metrics are included in the SLA (e.g., response times, resolution times, uptime guarantees), and how are breaches of the SLA handled?** OneTrust publishes Service Level Objectives (SLOs) for its APIs, which are stated as objectives rather than guarantees. For example, Universal Consent & Preference Management APIs aim for 99% availability, and specific APIs target 99.99% or 99.95% uptime. Response time objectives for certain APIs are typically less than 500 ms. For support, they offer a "4-hour target first time

response (Sev1)" under their "Essentials Plus Success" package. Comprehensive details on how breaches of a formal Service Level Agreement (SLA) are not publicly available.

- **What are the vendor's escalation procedures for critical issues or service disruptions?** Insufficient information to provide a confident answer. Specific escalation procedures for critical issues or service disruptions are not publicly detailed in the provided search results.
- **Describe the vendor's customer support model (e.g., 24/7, tiered support, dedicated account managers).** OneTrust offers a tiered customer support model through various "Success Packages". These packages include digital self-help resources, community forums, office hours, and technical support. Their "Essentials Plus Success" package provides support Monday to Friday, 8 AM to 11 PM GMT, with online case management and a 4-hour target first-time response for Severity 1 issues. They are known for robust customer support services, including documentation, training programs, and responsive teams.

Operational

- **What is the vendor's disaster recovery plan?** Insufficient information to provide a confident answer on OneTrust's specific internal disaster recovery plan. While OneTrust provides best practices for customers implementing their solutions on-premises, including replication and failover strategies, and their products address business continuity management, a detailed public document of their own internal disaster recovery plan was not found.
- **What is the vendor's uptime guarantee?** OneTrust provides Service Level Objectives (SLOs) for its APIs, such as 99% availability for Universal Consent & Preference Management APIs and 99.99% or 99.95% for specific APIs. However, these are explicitly stated as "objectives only and not a commitment or guarantee". A formal uptime guarantee is not publicly available.
- **Does the vendor have a business continuity plan?** Insufficient information to provide a confident answer on OneTrust's specific internal business continuity plan. While OneTrust offers products that support business continuity management for their customers and emphasizes business resilience, a detailed public document outlining their own internal business continuity plan was not found.

4. Recommendations

- **For Compliance and Security:** OneTrust demonstrates high adherence to compliance standards (GDPR, CCPA, SOC 2, ISO 27001) and strong security practices. It is recommended to review their latest SOC 2 Type 2 report and ISO certifications for detailed control implementations and audit results.
- **For ESG:** Their strong commitment to DE&I and environmental sustainability aligns with responsible vendor selection. Organizations should leverage OneTrust's publicly available DE&I and environmental sustainability policies for internal benchmarking if applicable.

- **For Financial Stability:** While OneTrust's ARR growth is strong and free cash flow is positive, the lack of a formal financial stability rating and explicit net profitability statements for the last three years suggests that a deeper financial due diligence might be beneficial. Requesting detailed financial statements or a third-party financial assessment is recommended.
- **For Fourth-Party Management:** Their comprehensive framework for managing risks associated with sub-processors and supply chain is a strong point. Requesting their sub-processor list and understanding their due diligence process for these entities is advisable.
- **For Geopolitical Risks:** Due to insufficient public information regarding the impact of international sanctions and specific geopolitical risks of their data center locations, a direct inquiry should be made to OneTrust to understand their strategies and resilience plans in these areas.
- **For Service Delivery and Operational Aspects:** While customer support is tiered, specific escalation procedures for critical issues, comprehensive SLA metrics (beyond SLOs), formal uptime guarantees, and a detailed internal disaster recovery plan are not fully transparent from public sources. It is recommended to request a detailed SLA document and their internal BCP/DRP for a thorough understanding of their operational resilience and service commitments.

5. Validated References

- OneTrust Targeted Data Discovery & Integration Workflow FAQ | MyOneTrust ✓
- OneTrust-Software for Data Protection and Data Governance - 8awake ✓
- API Service Level Objectives - OneTrust Developer Portal ✓
- Your complete guide to General Data Protection Regulation (GDPR) compliance - OneTrust ✓
- OneTrust Customers Saw 227% ROI, New Study Reveals | AWS ChicagoTest ✓
- OneTrust on Track to Surpass $500M in ARR as Demand for Responsible Data and AI Solutions Skyrockets ✓
- OneTrust Announces Recipients of DE&I Grant Commitment ✓
- OneTrust Launches OneTrust GRC Solution for Integrated Risk Management - PR Newswire ✓
- OneTrust Raises $150M As It Cuts Its Valuation - Crunchbase News ✓
- Privacy Overview - OneTrust ✓
- OneTrust Security Rating, Vendor Risk Report, and Data Breaches - UpGuard ✓
- Culture and Values | OneTrust ✓
- List of Subprocessors | MyOneTrust ✓
- Best Practices: Managing Data Subject Rights & Requests | MyOneTrust ✓
- SOC 2 Compliance | Solutions - OneTrust ✓
- OneTrust | Company Overview & News - Forbes ✓
- Support and Services - OneTrust ✓
- Contact Us - OneTrust ✓
- OneTrust Privacy Notice ✓

- General Data Protection Regulation (GDPR) Compliance | Solutions | OneTrust ✓
- OneTrust Trust Center ✓
- OneTrust Privacy Incident Management - GOV.UK ✓
- OneTrust Updates Incident & Breach Response Solution ✓
- The Ultimate Guide to ESG Sustainability | Blog - OneTrust ✓
- ESG & Sustainability Cloud - OneTrust Developer Portal ✓
- OneTrust Data Processing Addendum ✓
