GOAT Information Security Approach

Last updated 6th May 2025

We know information security is critical and we take this very seriously. Our systems are compliant with ISO 27001 controls which is globally recognised as the leading standard for information security management. GOAT Risk™ is also compliant with Payment Card Industry Data Security Standards (PCI DSS), and Azure Centre for Internet Security (CIS) 1.1.0 controls.

Protecting your data

GOAT is hosted on Microsoft Azure's cloud platform and benefits from knowledge, resources and a suite of scanning and security tools. GOAT has implemented the added protection of the Azure Front Door service which includes a suite of features including its Web Application Firewall (WAF) and protection against Distributed Denial of Service (DDoS). The data is stored in Microsoft's UK data centres (UK South and UK West locations). Billing details reside with and protected by 3rd party payment processing company Stripe.

Behind the systems

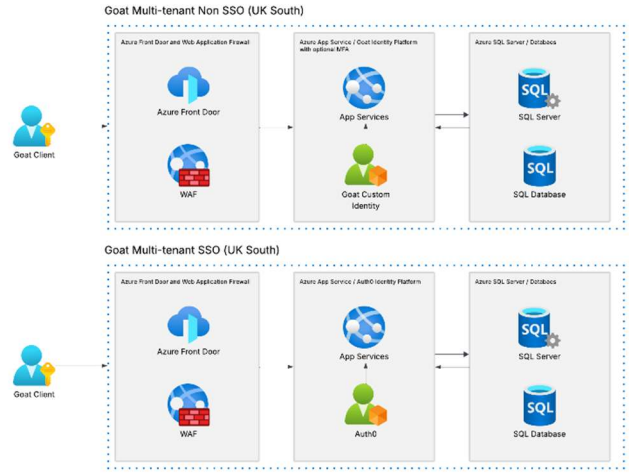
GOAT is a small company which means only a core team of trusted senior employees have access to the system and data. Whilst we benefit from an offshore 3rd party development partner with scalable resources, we keep them in a separate environment and they do not have access to the live system or client data. We conduct 3rd party penetration tests after major releases or annually as well as conducting our own Information Security Risk Assessment.

Technical details

- Daily security scans including patch management and activity alerts
- Source code analysis tool used before deployment to User Acceptance Testing (UAT) and Production environments
- Data transferred between users and GOAT are encrypted by Transport Layer Security (version 1.3) and Secure Sockets Layer (TLS/SSL) in transit and at rest (see https://learn.microsoft.com/en-us/azure/app-service/overview-tls)
- Separation of development, testing and dual instance production environments
- Client data backed up for 30 days
- Client data is not replicated in testing and UAT
- Single or two factor authentication available with minimum password controls
- Single sign on (SSO) via Auth0 available
- User passwords are encrypted
- Access controls and users managed by your Administrator, though risks and risk profiles can be locked by owners.

- Access controls by client down to risk level

Azure Architecture Diagram



Data Privacy Policy

https://www.goatrisksolutions.com/privacy-policy/

Suspicious activity

If you detect any suspicious activity or have any questions, please contact support@goatrisksolutions.com

Version and record of changes

Version	Key Changes	Date
1.0	First published	09/09/2020
1.1	Behind the systems • We conduct 3rd party penetration tests after major releases or annually	01/08/2021
1.2	Technical details - Inclusion of: • Separation of development, testing and dual instance production environments • Single or two factor authentication with minimum password controls • Client data backed up for 30 days	30/08/2022
1.3	Behind the systems • Removed GOAT imagery • Removed – we have discussed our risk appetite which is to go beyond minimum or even reasonable expectations by investing in security	28/02/2023
1.4	Introduction • Removed - GOAT Risk™ is also compliant with System and Organisation Controls Trust Service Principles (SOC TSP)	12/06/2024

1.5	Added download link and included Version and record of changes table	26/02/2025
1.6	Technical details - Inclusion of: • TLS/SSL details and hyperlink • Single sign on Added Azure Architecture Diagram	06/05/2025