ReliSec

Penetration Test Summary

Web Application, API and MCP Penetration Test

Client:	Risk Quilt Ltd
Report Reference:	RIQU-PT-RISKQUILT-PLATFORM-06-2026
Summary Version:	1.0
Date:	29/06/2026
Classification:	Approved for Distribution

| SECURITY **BEYOND THE CHECKBOX**

Introduction

This document is a summary of the full penetration testing report produced by ReliSec Ltd for Risk Quilt Ltd following a security assessment conducted from 22 to 25 June 2026. The complete report, including detailed findings, evidence, and remediation guidance, is available upon request under NDA.

Executive Summary

ReliSec was contracted by Risk Quilt Ltd to conduct a security assessment of its RiskQuilt Web Application, underlying API infrastructure, and MCP integration. Overall, the assessment identified fourteen security findings, comprising ten low and four informational severity findings.

The RiskQuilt platform is a multi-tenant governance, risk and compliance tool currently in the final weeks before its commercial launch. The platform enables organisations to manage risk registers, controls, actions, obligations, and events across multiple subscription tiers, and includes a custom artificial intelligence integration built on the Model Context Protocol for AI assistant connectivity.

The engagement was conducted over a four-day period from 22 to 25 June 2026, targeting the multi-tenant GRC SaaS platform hosted on Google Cloud Platform with Cloudflare CDN, including the platform's OIDC authentication framework, three MCP endpoints, and the riskadmin administrative CLI. This engagement also naturally served as a full retest of all findings from the initial penetration test conducted in April 2026.

No critical or high-severity findings were identified during this latest engagement. The platform's core security posture, specifically tenant isolation, SQL injection defences, session management, and file upload controls, is strong for a pre-launch product.

The platform's core security architecture performed well under test. Cross-tenant data isolation remains robust, with comprehensive IDOR testing conducted bidirectionally between the two test tenants across the REST API and all three MCP endpoints. No access violations were identified in either direction, confirming that the tenant boundary enforcement observed in the first engagement has been maintained and extended to the new MCP integration. SQL injection testing was conducted directly against the Go API layer with the Cloudflare WAF bypassed, and all tested payloads were stored as inert data consistent with thorough use of parameterised queries. Object-level Role-Based Access Control (RBAC), introduced since the first engagement to support granular read and write permissions on individual objects, was found to be correctly enforced server-side across all tested endpoints.

Session management is also well implemented. The platform supports a range of production-grade identity providers including Google Workspace, Microsoft Entra ID, and custom OIDC configurations, with a guided switching workflow that correctly invalidates all existing sessions when a provider change is committed. The magic link authentication flow provides a low-friction onboarding path for tenants that have not yet configured their own identity provider. File upload controls introduced in response to the first engagement are effective. Malicious image uploads are now rejected by

content inspection regardless of MIME type or file extension and evidence files are served from signed URLs on a separate origin. Core security response headers are consistently applied and Cloudflare edge protection is in place with the Managed Ruleset, OWASP Core Ruleset, rate-limiting rules, and leaked credential detection all active and operating in blocking mode.

A full summary of the remediation status of all findings from the first engagement is presented in the Retest Summary section of the full report. In total, all high and medium-severity findings have been fully remediated and are formally closed, representing a significant improvement in the platform's security posture over a two-month period.

The fourteen findings identified during this engagement are concentrated in three areas: MCP integration authentication, server-side input validation, and retained infrastructure disclosure. All are addressable before launch without architectural change.

Visual Summary

The assessment identified the following number of security vulnerabilities:

Component	Critical	High	Medium	Low	Informational
Core Platform (Web App + Main API)	0	0	0	6	3
MCP Integration	0	0	0	3	1
LLM API	0	0	0	1	0
Overall	0	0	0	10	4

Scope and Duration

Risk Quilt Ltd contracted ReliSec to conduct a security assessment of the following assets.

22/06/2026 to 25/06/2026

Asset	Note
https://pentest.riskquilt.com	RiskQuilt web application - primary testing target
https://pentest.riskquilt.com/api/v1/	RiskQuilt API - Go backend
https://pentest.riskquilt.com/api/v1/mcp/{slug}	MCP standard endpoint - read and general tool access, slug-based per-tenant routing
https://pentest.riskquilt.com/api/v1/mcp-admin/{slug}	MCP admin endpoint - administrative tools, requires standard MCP connection to function
https://pentest.riskquilt.com/api/v1/mcp-import/{slug}	MCP import endpoint - bulk data operations, may be retired by client
https://www.riskquilt.com/signup-pentest/	Self-service tenant signup form - free first month model with manual conversion to paid

riskadmin CLI	Administrative CLI tool

ReliSec was provided with access to the following accounts:

Account	Note
sarah.chen@brinecroft.co.uk	Pre-seeded Tenant Admin Owner - demo tenant, Flex subscription. Available across all IdPs (Google, Entra, Auth0).
tom.granger@brinecroft.co.uk	Test user - available across all IdPs
priya.kapoor@brinecroft.co.uk	Test user - available across all IdPs
david.okafor@brinecroft.co.uk	Test user - available across all IdPs
lisa.sheridan@brinecroft.co.uk	Test user - available across all IdPs
james.whitfield@brinecroft.co.uk	Test user - available across all IdPs
pentest1@relisec.co.uk	Created during testing - admin for relisec-pentest-1 tenant (ID: 557035df-e1af-4916-9efd-2478d3a0cb8b). Used for bot-protection bypass confirmation and cross-tenant IDOR setup.

Assessment Limitations

The security assessment was conducted exclusively on systems listed in the above scope as agreed upon by the client. Any third-party components that provide or receive data from the items in scope, or other organisational systems not listed above, are not included in this security assessment.

No testing was conducted with the intention of causing Denial-of-Service (DoS) to any Risk Quilt Ltd assets.

Testing was conducted against the pentest environment (https://pentest.riskquilt.com) with Cloudflare WAF enabled in blocking mode. The tester's IPv4 addresses (109.153.173.128 and 100.94.242.69) were whitelisted for WAF bypass on day three of the engagement to assess the platform’s security posture from an application-level perspective.

GCP infrastructure, Terraform configuration, Stripe Checkout, and a source code review were out of scope and were not assessed.