Assessment summary

The Qlik Cloud Service (QCS) system is a Software-as-a-Service (SaaS) data analytics platform that enables Qlik's customers to obtain insights into their data.

Depending on the classification and risk tolerance of their customers, the QCS system may host information that is highly sensitive. To ensure that the security measures implemented across the QCS system are commensurate to the sensitivity of the information it may host, Qlik Technologies Incorporated (Qlik) has sought assurance of adherence to controls identified in the Australian Cyber Security Centre's (ACSC) Information Security Manual (ISM).

The objective of the assessment was to provide Qlik and Australian Government Cloud consumers visibility of the implementation state and effectiveness of security controls relevant to the operation and authorisation of the systems at the PROTECTED classification.

The assessment was based on Australian government security guidance sourced from:

- The Australian Government Information Security Manual (ISM), June 2022
- Cloud assessment requirements defined in the Australian Cyber Security Centre (ACSC) Anatomy of a Cloud Assessment and authorisation publication

The assessment was completed between November and December 2023 by Joshua Yeo, a certified Information Security Registered Assessor Program (IRAP) assessor, of the cybersecurity consultancy Trustwave.

Assessment scope

Components that make up the QCS system are developed and managed by Qlik, and deployed on Amazon Web Services (AWS).

Several additional third party solutions are deployed and/or integrated with the QCS system, including MongoDB and Expel – who are other major third parties participating in the overall security posture of the QCS system. Some of these providers and solutions have been subjected to their own independent IRAP assessments, but all were subjected to Qlik's supply chain risk management processes to ensure they meet Qlik's criteria for security to achieve adequate security around consumer data.

Assessment findings

Qlik has demonstrated commitment to operating and maintaining the environment in line with ISM control objectives and requirements.

The QCS system environment was found to present a sound security maturity across all relevant ISM control domains, emphasising a defence-in-depth approach to all areas, to meet security control expectations at the PROTECTED level.

Trustwave has provided Qlik with a cloud security assessment report for the consumption of the Authorising Officer, internal stakeholders, Australian Government agencies, and other Qlik customers, where required. The assessment report details control state on a control-by-control basis, and details the consumer’s responsibilities when employing the service. An overview of operational responsibilities is provided as Appendix A – Shared Security Model, and the assessment report can be made available upon request from Qlik.

As Qlik service a global market, the QCS system possesses a capability to be configured to enable compatibility with a wide range of potential consumer technologies. A key consideration for consumers of the service at the PROTECTED level will be in selection of architecture, deployment models, and configurations to suit their risk profile and business needs. To support this, cloud consumer implementation requirements are provided as Appendix B – Customer Guide.

Edward Dexter

Director and IRAP assessor

Trustwave

This report has been produced by an ASD endorsed IRAP Assessor

Appendix A – Shared Security Model

The below section provides and overview of the QCS system, AWS, MongoDB and Expel and Cloud Consumer operational responsibilities.

Layer	Responsibility			
	Qlik	AWS	MongoDB*	Expel
Governance				
Incident Response	Yes	Yes	Yes	Yes
Backups	Yes	Yes	No	No
Technical				
Identity & Access Management	Yes	No	No	No
Security Monitoring	Yes	No	No	Yes
Application	Yes	No	No	No
Platform	Yes	Yes	Yes	No
Virtualisation	Yes (Non-production only)	Yes	No	No
Physical Hosts, Networking & Datacentre	Yes (Non-production only)	Yes	Yes	No

* Note that Qlik consumes the service offering from MongoDB that is deployed on AWS.

Appendix B – Customer Guide

The table below outlines the responsibilities of the consumer when deploying the Qlik Cloud Service within their organisation.

Guideline	Description	Customer Responsibility
Guidelines for Personnel Security	Management of unprivileged accounts	Management of all unprivileged accounts (as users of the service) by nominating an identity provider service compatible with the OpenID Connect protocol.
Guidelines for System Hardening	Authentication	Customer are required to nominate their own identity provider service to enforce passphrase and multifactor authentication requirements.
Guidelines for System Management	Client file backups	Customers are responsible for backing up the originals version of their own data that is uploaded to the QCS system. Note that Qlik provide backups of the QCS system, which will contain copies of the customer data uploaded to the system.
Guidelines for System Monitoring	Centralised logging	Logs generated by the QCS system can be exported from the system. The customer is responsible for consuming these logs to provide audit capability across customer managed systems and services.
Guidelines for Database Security	Client file data protections	Files uploaded to the QCS system are the responsibility of the customer, including backup, access permissions, classification and deletion.
Guidelines for Cryptography	Key management	If supplying their own key(s) to encrypt the platform, customers are responsible for the managing the protection, rotation and decommissioning of their key(s).
Guidelines for Data Transfers	Client file transfers	Customers are responsible for ensuring their file servers, or hosting systems providing integration to the QCS system (via connectors) are configured to meet Transport Layer Security (TLS) requirements to protect the file uploads in transit.