Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515

Version 1.0, 14 September 2026

Document reference: AISEP-EAL2-CR-2026-EFT-T062-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary 1

Introduction 3

Overview 3

Purpose 3

Identification 3

Target of Evaluation 5

Overview 5

Description of the TOE 5

TOE Functionality 5

TOE Physical Boundary 5

Architecture 6

Clarification of Scope 7

TOE Security Policy 8

Secure Delivery 8

Version Verification 8

Documentation and Guidance 8

Secure Usage 9

Evaluation 10

Overview 10

Evaluation Procedures 10

Functional Testing 10

Penetration Testing 10

Certification 12

Overview 12

Assurance 12

Certification Result 12

Recommendations 12

Annex – References and Abbreviations **14**

References 14

Abbreviations 15

Executive Summary

This report describes the findings of the IT security evaluation of Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515, developed by Rubrik Inc., against Common Criteria EAL2 augmented with ALC_FLR.2.

The Target of Evaluation (TOE) is Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515 a distributed platform consisting of Rubrik Security Cloud – Private (SC-P) and Rubrik Cloud Data Management (CDM). CDM is a Data Protection product that distributes data, metadata, and task management across a cluster, and SC-P permits administration and management of multiple Rubrik CDM clusters through a single web User Interface (UI).

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2, augmented with ALC_FLR.2, and that the evaluation was conducted in accordance with both the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs and was completed on 30 August 2026.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends that:

- Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.
- Access to all management interfaces (SSH and HTTPS interfaces for SC-P, SSH and HTTPS interfaces for CDM) should be restricted to controlled and trusted networks.
- Authentication factors (passwords and sensitive seed values for time-based second authentication factor) should be stored securely and should not be stored in the same location.
- Authentication credentials should not be re-used between SC-P and CDM user accounts.
- Password complexity rules should be configured in line with the *Australian Government Information Security Manual (ISM) [8]* best practices.
- Security administrators should confirm that the browser used to connect to the web administrative interfaces supports TLS 1.3, if required.
- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings. In particular, the Rubrik Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Guidance Documentation and Supplement documents must be followed for this TOE to be used in an evaluated configuration.
- The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE.
- System Auditors should review the audit trail generated and exported by the TOE periodically.
- The users should verify the integrity of the TOE software prior to installation by comparing the fingerprint of the downloaded software against the checksum value available from the download page link provided in the Rubrik Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Guidance Documentation and Supplement documents.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the *Security Target [10]* and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the *Common Criteria [1-7]*
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's *Security Target [10]* which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is the Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515 developed by Rubrik Inc.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515
TOE Type	Data Protection
TOE Software version	▪ Security Cloud – Private v2.4.12-p3-81 ▪ Cloud Data Management v9.2.3-p3-29515
Security Target	Rubrik, Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Security Target, Version 1.4, 27 August 2026
Evaluation Technical Report	Evaluation Technical Report 1.0 dated 30 August 2026 Document reference EFT-T062-ETR-1.0
Criteria	CC:2022r1
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2022-11-006, CEM:2022 Revision 1, November 2022
Conformance	EAL 2 augmented with ALC_FLR.2 (Flaw reporting procedures)

Developer	Rubrik Inc. 3495 Deer Creek Road, Palo Alto, CA 94304 United States of America
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515. It is a distributed TOE consisting of Cloud Data Management (CDM), a Data Protection product that distributes data, metadata, and task management across a cluster, and SC-P, which permits administration and management of multiple Rubrik clusters through a single web UI.

A Rubrik CDM cluster is a collection of objects that include sources from where data is getting backed up, targets where backups are stored, and security principals, including the users and service accounts that manages the cluster.

Rubrik Security Cloud - Private (SC-P) provides a global management view of the daily operations of the connected CDM clusters. SC-P apps monitor the protection and compliance status of CDM clusters, generating reports and charts using current and historical data about the health, protection, and compliance status of all of the objects that the CDM clusters protect.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.6 of the *Security Target [10].*

TOE Physical Boundary

The TOE is a software-only product. The TOE physical boundary comprises the software components that implement the TOE functionality, together with the associated guidance documentation required for secure operation. The components included within the TOE boundary are listed in *Table 1.*

Part of the TOE	Identification	Description
TOE Software	▪ SC-P: rscp-2-4-12-81.ova ▪ CDM: rubrik-image-9.2.3-p3-29515.ova	The TOE image is distributed as a VMware OVA file.
Product Documentation	▪ Rubrik CDM Version 9.2 CLI Guide (Rev. A3) ▪ Rubrik CDM Version 9.2 Install Guide (Rev. A0) ▪ Rubrik CDM Version 9.2 User Guide (Rev. A4) ▪ Rubrik Security Cloud - Private 2.4.12 CLI Reference (Rev A0)	Supporting product documentation available download through the Rubrik website in PDF formats.

	▪ Rubrik Security Cloud - Private 2.4.12 Install and Upgrade Guide (Rev A0) ▪ Rubrik Security Cloud - Private 2.4.12 User Guide (Rev A0)	
Security Guidance	Rubrik, Inc. Security Cloud-Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515; Guidance Documentation Supplement Document Version: v1.2	The Common Criteria Guidance supplement for the TOE. The security guidance is available for download through the Rubrik website in PDF formats.

Architecture

The TOE is a distributed software-only solution comprising Rubrik Security Cloud - Private (SC-P) v2.4.12-p3-81 and Cloud Data Management (CDM) v9.2.3-p3-29515. CDM distributes data, metadata, and task management across a cluster, while SC-P provides a centralized web-based interface for the administration and management of connected CDM clusters. SC-P collects information from connected CDM instances and presents aggregated operational, protection, compliance, inventory, event, and reporting information through a single management interface.

CDM comprises the Cloud-Scale File System, Distributed Metadata Service, Cluster Management, Distributed Task Framework, Data Management, and an administrative interface. These components operate together to store and manage versioned data, maintain distributed metadata, coordinate cluster operations, distribute tasks across cluster nodes, and provide administrative access. The internal CDM components communicate with corresponding components on other nodes using a Thrift RPC protocol implemented over TLS-protected channels.

In the evaluated configuration, the TOE is deployed as virtual appliances on VMware vSphere environments. SC-P is installed from an SC-P OVA image and CDM is installed from a Rubrik Edge OVA image. Administrators interact with the TOE through a secure web interface, while SC-P receives audit and operational information from connected CDM clusters. *Figure 1* below illustrates the TOE physical boundary and the relationship between the TOE components and supporting environment.

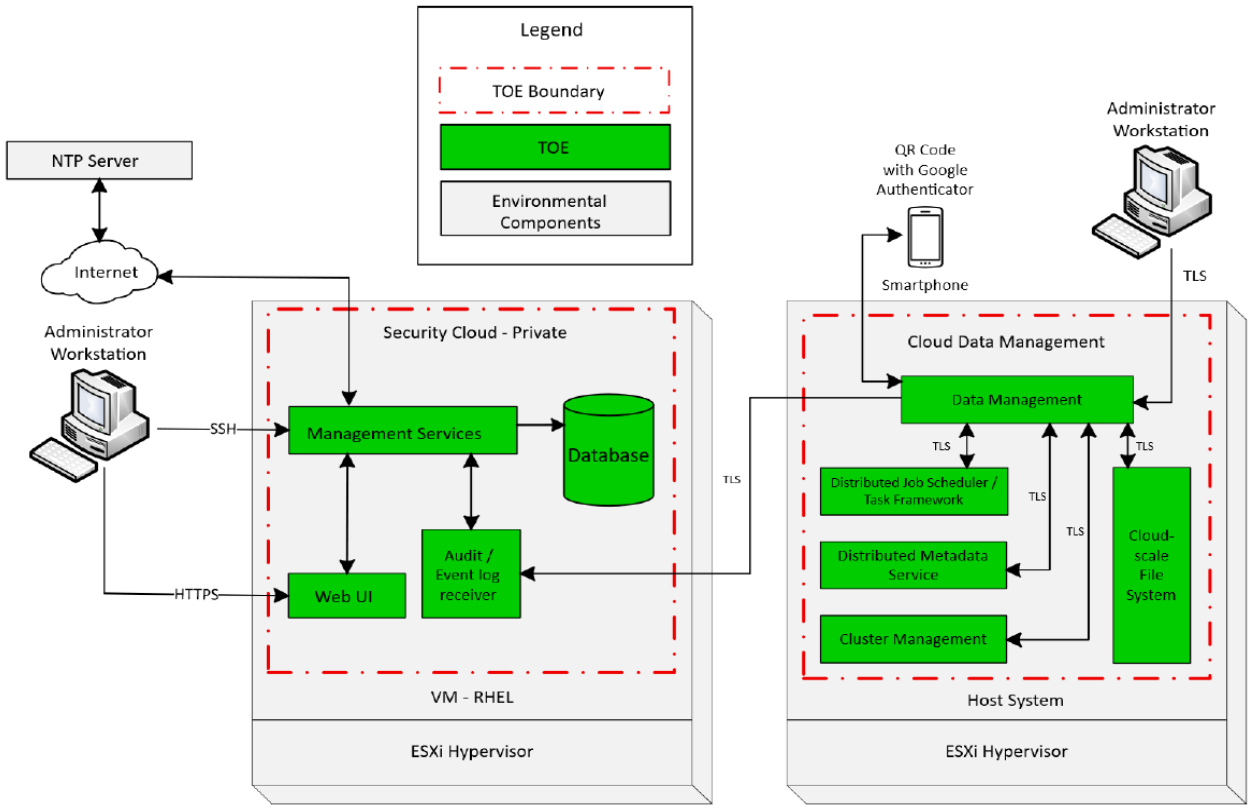

Figure 1- TOE Architecture

NOTE: The TOE should be used with Google Authenticator.

Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the *Security Target [10].*

Non-TOE Hardware/Software/Firmware

The TOE is software-only solution. Yet, it does require following external components to operate securely and as evaluated. These items are outside the TOE boundary and must be present and correctly configured in the operational environment.

- Two VMware ESXi hypervisors, which are the host servers for SC-P and Rubrik Edge running in a VM (a VM running Rubrik Edge is necessary for setting up CDM). Rubrik Virtual Cluster is a set of CDM instances; within the TOE test environment there is only one CDM instance.
- Administrator Workstation, used for external communication with the SC-P Management Services via SSH, with the SC-P Web UI via HTTPS, and with the CDM Data Management via TLS.
- Smartphone, connected to CDM Data Management via a QR code using Google Authenticator, implementing time-based password for secure authentication.

- NTP Server, which provides time synchronization for the TOE.

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual [8]* for policy relating to using an evaluated product in an unevaluated configuration.

TOE Security Policy

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. *The Security Target [10]* contains a summary of the functionality that is evaluated.

Secure Delivery

TOE Delivery Procedures

The TOE software may be downloaded using the Rubrik Inc. Support website. Customers must have an active Rubrik Inc. Support portal account in order to download the TOE software. Prospective customers must submit an account request form (*https://support.rubrik.com/s/login/SelfRegister*) or contact Rubrik Inc. Sales in order to create an account and gain access the TOE software downloads.

Customers with active Rubrik Inc. Support accounts can access the following link to download the TOE software:

- Product page: https://support.rubrik.com/s/documentationdetail?id=a5B8Y000000gBOLUA2

The TOE is distributed as a VMware OVA file. The filenames of each are as follows:

- **SC-P OVA:** rscp-2-4-12-81.ova
- **CDM OVA:** rubrik-image-9.2.3-p3-29515.ova

Installation of the TOE

The *Configuration Guides [9]* contains all relevant information for the secure configuration of the TOE.

Version Verification

The TOE software downloads may be verified against transmission corruption by a checksum provided on the downloads page. Before installing the TOE, generate the checksum of the downloaded files and compare against the hash provided on the respective SC-P and CDM download pages.

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased by the consumer, and it titled as:

- *Guidance documentation, Rubrik; Security Cloud-Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): 2+; Document Version: v1.2, 27 August 2026*

All Common Criteria guidance material is available at *https://www.commoncriteriaportal.org.*

The Australian Government Information Security Manual is available at *https://www.cyber.gov.au/ism [8].*

Secure Usage

The evaluation of the TOE took into account certain organisational security policies to be followed in its operational environment. These policies must be followed in order to ensure the security objectives of the TOE are met:

- The TOE is installed on the appropriate, dedicated hardware and operating system.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.
- The IT environment provides the TOE with the necessary reliable timestamps.
- The TOE software will be protected from unauthorized modification.
- The TOE is located within a controlled access facility.
- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 2022 Revision 1 [1][2][3][4][5][7]*.

Testing methodology was drawn from *Common Methodology for Information Technology Security, Version 2022 Revision 1 [6]*.

The evaluation was carried out in accordance with the operational procedures of the *Australian Information Security Evaluation Program [8].*

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security were also upheld [12].*

Functional Testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators found that the developer tests covered all Security Functional Requirements specified in the *Security Target [10].*

The evaluators examined the TOE prior to testing and determined that the test configuration was consistent with the configuration under evaluation as specified in the *Security Target [10]*. The evaluators followed the user installation and configuration guidance to ensure that the TOE had been installed correctly and was in a known state prior to conducting testing.

The evaluators drew upon the developer testing evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The evaluators also devised and conducted additional functional testing.

Penetration Testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the TOE and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The evaluator performed a vulnerability analysis of the TOE in order to identify any potential security vulnerability in the TOE, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)

- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for exploitation.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the 01 July 2026 coinciding with the conclusion of the evaluation.

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that *security target [10]*, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through the use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the *Security Target [10]* and **has met** the requirements of Common Criteria EAL2 augmented with ALC_FLR.2 (Flaw reporting procedures).

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the *Evaluation Technical Report [11]*, the Australian Certification Authority **certifies** the evaluation of Rubrik SC-P and CDM v2.4.12-p3-81 and v9.2.3-p3-29515 performed by the Australian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual [8].*

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance documentation is followed, the Australian Certification Authority also recommends:

- Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

- Access to all management interfaces (SSH and HTTPS interfaces for SC-P, SSH and HTTPS interfaces for CDM) should be restricted to controlled and trusted networks.
- Authentication factors (passwords and sensitive seed values for time-based second authentication factor) should be stored securely and should not be stored in the same location.
- Authentication credentials should not be re-used between SC-P and CDM user accounts.
- Password complexity rules should be configured in line with the *Australian Government Information Security Manual (ISM) [8]* best practices.
- Security administrators should confirm that the browser used to connect to the web administrative interfaces supports TLS 1.3 if required.
- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings. In particular, the Rubrik Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Guidance Documentation Supplement document must be followed for this TOE to be used in an evaluated configuration.
- The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE.
- System Auditors should review the audit trail generated and exported by the TOE periodically.
- The users should verify the integrity of the TOE software prior to installation by comparing the fingerprint of the downloaded software against the checksum value available from the download page link provided in the Rubrik Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Guidance Documentation and Supplement documents.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2022-11-001, CC:2022 Revision 1, November 2022*
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2022-11-002, CC:2022 Revision 1, November 2022*
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2022-11-003, CC:2022 Revision 1, November 2022*
4. *Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the Specification of Evaluation Methods and Activities, CCMB-2022-11-004, CC:2022 Revision 1, November 2022*
5. *Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined Packages of Security Requirements, CCMB-2022-11-005, CC:2022 Revision 1, November 2022*
6. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2022-11-006, CEM:2022 Revision 1, November 2022*
7. *Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-2025-001, Version 1.2, Published 15-October-2025*
8. *Australian Government Information Security Manual: https://www.cyber.gov.au/ism*
9. *Guidance documentation, Rubrik; Security Cloud-Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): 2+; Document Version: v1.2, 27 August 2026*
10. *Security Target for Rubrik, Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Security Target, Version 1.4, 27 August 2026*
11. *Evaluation Technical Report for Rubrik, Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515, Version 1.0, 30 August 2026* (Document reference EFT-T062-ETR 1.0)
12. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
13. *AISEP Policy Manual (APM): https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ACA	Australian Certification Authority
ALC_FLR	Assurance in Life Cycle – Flaw Remediation
ASD	Australian Signals Directorate
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CDM	Cloud Data Management
EAL2	Evaluation Assurance Level 2
HTTPS	Hypertext Transfer Protocol Secure
NTP	Network Time Protocol
.ova	Open Virtual Appliance format for virtual machine
PMC	Polaris / Rubrik Management Console
QR Code	Quick Response Code
SC-P	Security Cloud – Private (by Rubrik)
SFR	Security Functional Requirement
SLA	Service Level Agreement
SSH	Secure Shell
ST	Security Target document
TLS	Transport Layer Security
TOE	Target of Evaluation
UI	User Interface
VM	Virtual Machine

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate