MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C113 Certification Report

RSA Archer Suite v6.7

File name: ISCB-5-RPT-C113-CR-V1
Version: v1
Date of document: 9 Oct 2020
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999
www.cybersecurity.my

C113 Certification Report

RSA Archer Suite v6.7

9 Oct 2020

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C113 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C113-CR-D1
ISSUE:	v1
DATE:	9 Oct 2020
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 15 October 2020 and the Security Target (Ref[6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	30 September 2020	All	Initial draft
V1	9 October 2020	-	Final version

Executive Summary

The Target of Evaluation (TOE) is a RSA Archer Suite v6.7 comprises software that supports business-level management of governance, risk management, and compliance (GRC). It enables organisations to build an efficient, collaborative enterprise GRC program across IT, finance, operations and legal domains. It supports organisations in managing risk, demonstrating compliance, automating business processes, and gaining visibility into corporate risk and security controls. As the foundation for all RSA Archer Suite Solutions, the Suite allows users to adapt the solutions to their requirements, build their own applications, and integrate with other systems without touching code.

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2) Augmented ALC_FLR.2. This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]).

The evaluation was performed by BAE Systems Lab - MySEF and the evaluation was completed on 29 September 2020.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that RSA Archer Suite v6.7 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref[6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is RSA Archer Suite v6.7. It is a software product that supports business-level management of governance, risk management and compliance. As the foundation for all RSA Archer Suite Solutions, the suite allows users to adapt the solutions to their requirements, build their own applications and integrate with other systems without touching code.

2 Users access the TOE via a web-based graphical user interface (GUI). All users require an account in order to log on to the TOE. The user account specifies the user's groups and access roles. An access role is a collection of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete). The TOE controls user access to its objects (applications, questionnaires, records and fields) based on the access roles associated with users and with the groups to which the user belongs. An administrator can configure an advanced workflow to require users to electronically sign records. The electronic signature provides an additional layer of security by requiring users to re-authenticate before interacting with the records.

3 The Content API, Web Services API and RESTful APIs programmatically extend the functionality of the TOE to external applications through several classes and methods which expose many of its features, allowing for a high level of integration with other products. All users must be successfully identified and authenticated by the TOE before gaining access to any other TOE services.

4 The TOE provides capabilities to configure minimum strength requirements (e.g. minimum length, required character sets) for passwords. The TOE can be configured to track the number of consecutive failed authentication attempts and block further authentication attempts for a configurable time period when the configured threshold has been met. The TOE will terminate interactive sessions that have been idle for a configurable period of time.

5 The TOE is able to generate audit records of security-relevant events occurring on the TOE and provides administrators with the ability to review audit records stored in the audit trail.

6 There are four main components to RSA Archer Suite installation which are Web Application, Services, Instance Database and Configuration Database. In addition to the

Web Application, Services, and Instance Database components, the RSA Archer Suite distribution includes the RSA Archer Suite Control Panel, a configuration tool used to create and manage RSA Archer Suite instances. The control panel enables RSA Archer Suite administrators to manage installation settings, instance settings, and plugins, but is not itself part of RSA Archer Suite and is outside the TOE boundary.

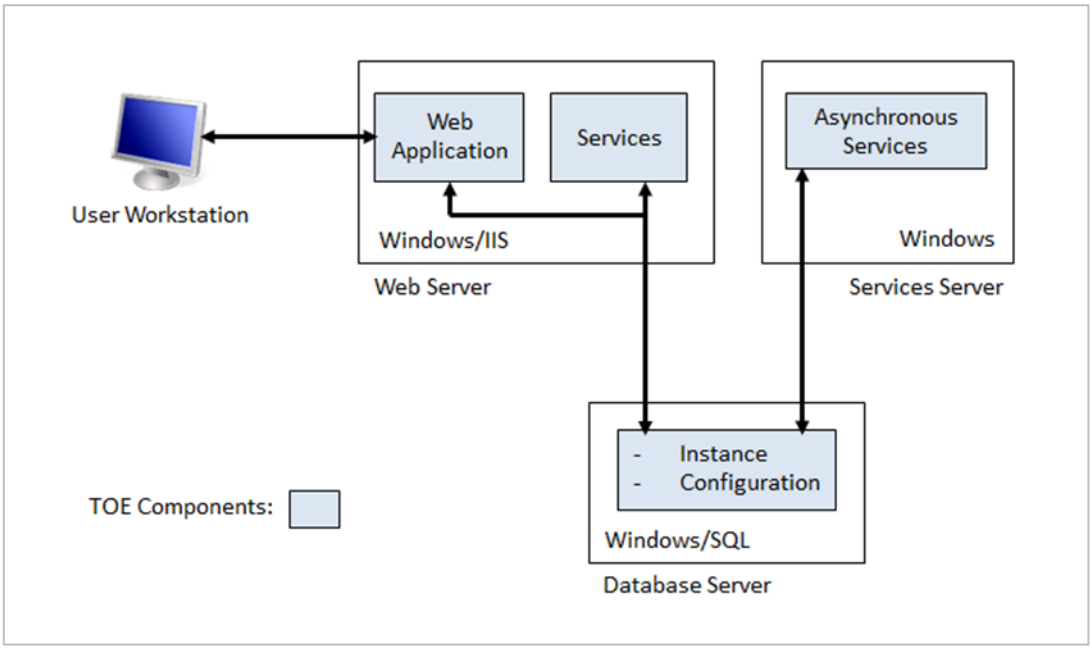

Figure 1 - TOE Environment Components

1.2 TOE Identification

7 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C113
TOE Name	RSA Archer Suite v6.7
TOE Version	V6.7
Security Target Title	RSA Archer Suite v6.7 Security Target (Ref [6])
Security Target Version	V1.0
Security Target Date	29 September 2020
Assurance Level	Evaluation Assurance Level 2 Augmented ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2 Augmented ALC_FLR.2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, The United States of America
Developer	RSA Security LLC 13200 Metcalf Avenue, Suite 300 Overland Park, Kansas 66213, The United States of America
Evaluation Facility	BAE Systems Applied Intelligence Malaysia Lab - MySEF Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

8 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture

9 The TOE consist of logical and physical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

10 The logical scope of TOE is described based on security functions provided by the TOE.

- Security Audit

  The TOE generates audit records of security relevant events that include at least the date and time of the event, subject identity and outcome for security events. The TOE provides authorised administrators with the ability to read the audit events.

  The TOE relies on its operational environment to store the audit records and to provide the system clock information that is used by the TOE to timestamp each audit record.

- User Data Protection

  The TOE implements a Discretionary Access Control security function policy (SFP) to control access by authorised users to the resources it manages. The scope of the Discretionary Access Control SFP covers applications, questionnaires, sub-forms, records, fields, workspaces, dashboards, and iViews.

- Identification & Authentication

  The TOE identifies and authenticates all users of the TOE before granting them access to the TOE. Each user must have an account on the TOE in order to access the TOE. The account associates the user's identity with the user's password, any assigned groups, and any assigned access roles. The TOE enforces minimum requirements for the construction of user passwords and provides a mechanism to lock a user account after a configured number of consecutive failed attempts to logon.

- Security Management

  Authorised administrators manage the security management functions and TSF data of the TOE via the web-based GUI.

- TOE Access

  The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.
  The TOE displays a banner message on the user login page. The content of the message is specified during initial configuration using the RSA Archer Suite Control Panel.
  The TOE can be configured to allow connections to the Web Application only from designated IP addresses, and to deny session establishment outside specified times, days of the week, or dates.

1.4.2 Physical Boundaries

11 The TOE boundary consists of the RSA Archer Suite itself, which accounts for the user interface tier, application tier and database tier components. Excluded from the boundary are the solutions and individual non-management applications that run on the platform, the RSA Archer Suite instance database, and the configuration database.

12 The Web Application requires the following components in its operational environment:

- Windows Server 2012 R2, 2016, or 2019 Standard or Datacenter edition
- Internet Information Services Version 8.5 or 10 (included in Windows Server 2012 R2, 2016, or 2019)
- Microsoft Office 2010 or 2013 Filter Packs (to enable indexing of MS Office files). This in turn requires Microsoft Filter Pack 2.0 or later
- Microsoft .NET Framework 4.7.2 or 4.8

13 The Services component requires the following in its operational environment:

- Windows Server 2012 R2, 2016, or 2019 Standard or Datacenter edition
- Java Runtime Environment (JRE) 8 (required only for the cache service)
- Microsoft .NET Framework 4.7.2 or 4.8
- Microsoft Windows 10 (for offline access).

14 The Instance and Configuration databases require the following in the operational environment:

- Windows Server 2012 R2, 2016, or 2019 Standard or Datacenter edition
- Microsoft SQL Server 2016 SP 1 (64-bit), Microsoft SQL Server 2016 Enterprise Edition or Microsoft SQL Server 2017 (64-bit).

15 Users accessing the TOE from a client computer require:

- One of the following supported browsers:
  - Internet Explorer 11
  - Microsoft Edge 42*
  - Chrome 76*
  - Firefox 60.9 (ESR)* or 69*
  - Safari 12*

  * These browsers do not support RSA Archer Administrator pages that require Microsoft Silverlight.
- Microsoft Silverlight 5.1 (required for administration)

1.5 Clarification of Scope

16 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

17 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref [6]).

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

1.6 Assumptions

19 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environment and requirements for secure operation of the TOE as defined in the Security Target (Ref [6]).

1.6.1 Environmental assumptions

20 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 2 : Assumptions for the TOE operational environment

Assumption	Statements
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains..
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorised physical modification.
A.SECURE_COMMS	The operational environment of the TOE will provide mechanisms to protect data communicated to and from remote users from disclosure and modification.
A.TIME	The operational environment of the TOE will provide reliable time sources for use by the TOE.
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.

1.7 Evaluated Configuration

21 As stated in the ST (Ref [6]), there are four (4) main components that make up the TOE in its evaluated configuration:-:

- Web Application – the RSA Archer Suite application that runs on a web server.
- Services – the services complement the Web application, such as RSA Archer Suite Cache, RSA Archer Suite Configuration, RSA Archer Suite Instrumentation, RSA Archer Suite LDAP Synchronisation, RSA Archer Suite Job Engine, RSA Archer Suite Queueing and RSA Archer Suite Workflow.

- Instance Database – stores the RSA Archer Suite content for a specific instance. It can be multiple instances based on the business structure and product licensing.
- Configuration Database – a central repository for configuration information for the web application and services servers.

During the testing activities, the TOE components were deployed in a multi-server configuration, which consists of the web server, services server and database server (instance and configuration).

The TOE presents a Web graphical user interface (Web GUI), Web Services API, RESTful API and Content API. The RSA Archer Suite distribution includes the RSA Archer Suite Control Panel, which is a configuration tool that allows administrators to manage installation settings, instance settings, and plugins. The RSA Archer Suite Control Panel is only used for initial configuration of the TOE and is outside the TOE boundary.

1.8 Delivery Procedures

22 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.

23 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

24 Pre Delivery and Delivery Activities

- The TOE is the RSA Archer Suite v6.7, a software-only platform for delivering business use case workflow and reporting applications for Enterprise Risk in all its forms, via a code-free fully configurable tool. The TOE itself is comprised of software and documentation.

25 Software

- The TOE is developed in-house. The development activities of the TOE are performed at RSA facilities in Overland Park, Kansas, Bedford, Massachussetts, and Bangalore, India. The implementation representation is stored at a secure facility at the RSA headquarters. Access controls are set on the server that stores the TOE, so only authorised users are able to access it. RSA uses an automated source code configuration management system. For more detailed information,

the RSA Archer Suite 6.7 Common Criteria Configuration Management document can be referenced.

- Before the TOE may be delivered, it must first be approved for release. In order to be approved, the TOE must undergo acceptance testing by the RSA Quality Engineering (QE) team until it successfully meets the defined acceptance criteria. The QE department, together with the project management and development teams, defines the acceptance criteria and testing methods necessary to obtain a product release. This involves defining a threshold for release of few-to-no critical or high-severity bugs and also a threshold for release with a percentage of passed tests as provided by the test cases. The testing of the TOE is conducted throughout the development process. Early in the development process, sparse testing is conducted every night on each nightly build and QE reports the test results back to the Engineering department by 10 AM the next morning. As the product gets closer to finalization, QE begins testing fewer builds, but the testing is done in a more rigorous manner. Two weeks prior to the final release of the TOE is the final release candidate phase of testing. During these two weeks, QE tests the TOE thoroughly according to the defined acceptance criteria.
- Once the product has completed the QE testing successfully, QE approves the product for release. It then becomes the "Master" version. The RE includes the approved version of the product installer and the approved version of the technical documentation in the self-extracting package (zip). When complete, the RE makes the zip file available to the QE team for one final pass of installer testing. Once the testing is verified as successful, the QE team tells a member of the Production Support (PS) team that the installation package is ready for upload to the RSA SecureCare Online (SCOL) website. A member of the RSA Operations team takes the installation package which is considered the "Master" version of the TOE and uploads it to SCOL, making it available for subsequent download by the purchasing customer. The communications channel to SCOL while uploading the installation package, is secured by Secure Sockets Layer (SSL). Since the product is only available via download, this is considered the entire process from manufacturing to distribution.
- RSA Archer is also available as a Software as a Service (SaaS) delivery model. This allows customers to purchase licensed software that is hosted by Archer instead of purchasing the software and hosting it in-house. The SaaS Operations team places the build into the test environment and then migrates the build into

production 30-45 days following General Availability (GA), depending on scheduling.

- RSA uses WinRAR as the tool to create the Archer installation package. WinRAR runs a hash function on the installation package and a value is determined. This value is sent as part of the installation package. The end user downloads a md5sum program and generates a checksum value for the RSA Archer file. The resulting checksum is compared with the RSA Archer provided checksum. If the two checksum values do not match, the downloaded file may be corrupt. If this happens, download the RSA Archer file again and use the md5sum utility to generate another checksum value.

26 Documentation

- All guidance documentation is created and maintained in-house by the RSA Archer Technical Publications team. The RSA Archer Technical Publications team is located in the United States in Overland Park, Kansas and Bedford, Massachussetts. The TOE documentation is available online for the proper installation, administration, and use of the TOE.
- All guidance documentation is stored within RSA Archer's Configuration Management (CM) documentation control system for version control. For more information, the RSA Archer Suite 6.7 Common Criteria Configuration Management document can be referenced.
- Throughout the testing process of the TOE software, feedback is provided to the Technical Publications team about the TOE documentation. In addition, RSA's technical support and professional services teams provide feedback to the Technical Publications team about the TOE documentation. As a final review before publication, the Technical Publications team does a copy edit on the TOE documentation.
- All guidance documentation is available online and can be downloaded from the RSA Archer Community website. Since the TOE documentation is only available via download, this is considered the entire process from manufacturing to distribution.

27 Customer Product Verification

- All delivery of RSA Archer software is done electronically. The product is either downloaded via RSA SCOL or is provided through the SaaS product offering. The

client must have an authorised account to be able to access the installation package and TOE Documentation on the RSA Archer Community website.

- When a client either purchases the product or requests an updated license, Customer Order Management (COM) submits a request electronically through SAP, an internal customer order system, which sends a request to the License Tool (LT). The LT creates the license and key and sends them to Archer Activation Service (AAS) which is used by customers to perform online license authorisation. The LT then returns the key to SAP which stores and forwards it to Download Central (DLC). DLC then retrieves the Archer license file used for offline installations from the LT, and emails the key to the customer along with instructions. If the order is for SaaS, an email is sent by the LT to archer_saasops@emc.com, once the file has been loaded into the AAS. After they have completed creation of the required instances, the Archer SaaS Ops team uses the SaaSMailer app to send emails to the customer with their 'sysadmin' credentials, and to COM confirming the order is completed for revenue recognition.
- Once the client is successfully identified and authenticated to SCOL they are then able to access their installation package. The client is able to view the version of the software on the website where the package is downloaded. In addition, the client can view the version of the TOE once the version is installed. The communications channel while downloading the installation package is secured by SSL.

2 Evaluation

28 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 Augmented ALC_FLR.2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

29 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

30 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

31 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Flaw Reporting Procedures

32 The evaluators have examined the flaw remediation procedures documentation and determined that it describes the procedures used to track all reported security flaws in each release of the TOE which would produce a description of each security flaw in terms of its nature and effects.

33 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would identify the status of finding a correction to each security flaw and identify the corrective action for each security flaw.

34 The evaluators have examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.

35 The evaluators have examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

36 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would help to ensure every reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.

37 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.

38 The evaluators have examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

2.1.3 Development

39 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

40 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

41 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

42 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.4 Guidance documents

43 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

44 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed this assurance class.

2.1.5 IT Product Testing

45 Testing at EAL 2 Augmented ALC_FLR.2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by BAE Systems Lab - MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.5.1 Assessment of Developer Tests

46 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators' tests are consistent with the developers' test results defined in the evaluation evidences submitted.

2.1.5.2 Independent Functional Testing

47 At EAL 2 Augmented ALC_FLR.2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.

48 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 3 : Independent Functional Test

Test ID	Description	Results
TEST-IND-001-GUI	• Verify that the TSF shall display an advisory warning message regarding unauthorised use of the TOE. • Verify that the TSF shall maintain security roles and security attributes belonging to individual users, and associate users with roles. • Verify that the TSF shall provide a mechanism to verity that secrets meet the password requirements for all users accounts (except sysadmin and service accounts). • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TOE is able to restrict authorised users to perform management of TSF data functions, or to modify the behaviour of security management functions. • Verify that the TSF shall allow user-initiated termination of the user's own interactive session. • Verify that the TOE is able to generate an audit record for security relevant events performed by each user and provides an interface to view the audit records generated to authorised users.	Passed.

Test ID	Description	Results
TEST-IND-002-GUI	• Verify that the TSF shall maintain security roles and security attributes belonging to individual users • Verify that the TOE is able to detect when a configured amount of unsuccessful authentication attempts have occurred. • Verify that the TOE will lock the user account associated with the failed authentication attempt based on a configurable period of time, and re-authenticate a user if an interactive user session exceeds the configured Static Session Timeout value. • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TSF shall enforce rules to determine if an operation among controlled subjects/objects is allowed and authorised access of subjects to objects is allowed. • Verify that the TSF shall enforce the Discretionary Access Control SFP to restrict the ability to query/modify/delete the security attributes of an Application, Questionnaire, or Sub-form owner; field permissions; and Workspace, Dashboard and iView access to the owner or user granted administrator rights.	Passed.

Test ID	Description	Results
	• Verify that a user session will be automatically logged out after the configured time interval of user inactivity has passed. • Verify that the TSF shall allow user-initiated termination of the user's own interactive session. • Verify that the TOE is able to generate an audit record for security relevant events performed by each user and provides an interface to view the audit records generated to authorised users.	
TEST-IND-003-GUI	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TSF shall enforce rules to determine if an operation among controlled subjects/objects is allowed, and authorised access of subjects to objects is allowed, and deny access of subjects to objects for unauthorised users. • Verify that the TSF shall allow the authorised user to specify alternative initial values to override the default values when an object or information is created.	Passed.

Test ID	Description	Results
	• Verify that the TSF shall restrict the ability to revoke access roles associated with the users under the control of sysadmin and verify that the revocation is enforced immediately. • Verify that the TOE shall re-authenticate the user under the conditions of electronically sign records. • Verify that the TSF shall allow user-initiated termination of the user's own interactive session. • Verify that the TOE is able to generate an audit record for security relevant events performed by each user and provides an interface to view the audit records generated to authorised users.	
TEST-IND-004-Web API	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that authorised users are able to perform management of TSF data functions, and able to modify the behaviour of security management functions. • Verify that the TSF shall allow user-initiated termination of the user's own interactive session. • Verify that the TOE is able to generate an audit record for security relevant events performed by users.	Passed.

Test ID	Description	Results
TEST-IND-005-Content API	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TSF shall maintain security roles and security attributes belonging to individual users. • Verify that a user session will be automatically logged out after the configured time interval of user inactivity has passed. • Verify the TOE is able to generate an audit record for security relevant events performed by users.	Passed.
TEST-IND-006-RESTful API	• Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that authorised users are able to perform management of TSF data functions, and able to modify the behaviour of security management functions. • Verify that the TSF shall allow user-initiated termination of the user's own interactive session. • Verify that the TSF shall deny session establishment based on a restricted date, time of day, day of the week and user IP address.	Passed.

Test ID	Description	Results
	• Verify that the TOE is able to generate an audit record for security relevant events performed by users.	

49 All testing performed by the evaluators produced expected results and as such the TOE behaved as expected.

2.1.4.3 Vulnerability Analysis

50 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

51 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

2.1.4.4 Vulnerability testing

52 The penetration tests focused on:

a) General network vulnerability scan

b) Common web application vulnerability scan

c) Insecure direct object references

d) File upload restriction

e) Input and data validation

f) Missing function level access control

g) Content API brute-force testing

h) Input and data validation

53 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is used only in its evaluated configuration and in secure environment as specified in the Security Target (Ref [6]).

2.1.4.5 Testing Results

54 Tests conducted for the TOE produced expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. Therefore, the certifiers confirmed that all the test conducted were PASSED.

3 Result of the Evaluation

55 After due consideration during the oversight of the execution of the evaluation and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of RSA Archer Suite v6.7 which was performed by BAE Systems Lab - MySEF.

56 BAE Systems Lab - MySEF found that RSA Archer Suite v6.7 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 Augmented ALC_FLR.2.

57 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

58 EAL 2 Augmented ALC_FLR.2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.

59 The analysis is supported by independent testing of the 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.

60 EAL 2 Augmented ALC_FLR.2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

61 The Malaysian Certification Body (MyCB) strongly recommends that:

a) Potential purchasers of the TOE should consider the use of a certification authority (CA) signed certificate, as opposed to a self-signed certificate to fully secure access to the TOE environment.

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

c) Potential puchasers of the TOE should ensure there are appropriate security controls in the TOE operational environment to ensure protection of the database and its stored data.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2, December 2019.

[6] RSA Archer Suite v6.7 Security Target, Version 1.0, 29 September 2020.

[7] Evaluation Technical Report, Version 1.0, 29 September 2020.

A.2 Terminology

A.2.1 Acronyms

Table 4 : List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5 : Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---