MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C107 Certification Report

RSA ARCHER SUITE V6.5

File name: ISCB-5-RPT-C107-CR-v1
Version: v1
Date of document: 26 August 2019
Document classification : PUBLIC

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

CyberSecurity Malaysia
(726630-U)
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C107 Certification Report

RSA ARCHER SUITE V6.5

26 August 2019

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:	C107 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C107-CR-v1
ISSUE:	v1
DATE:	26 August 2019
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 3rd Sep 2019, 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	7 August 2019	All	Initial draft
d2	22 August 2019	19	Revised draft
v1.0	26 August 2019	All	Baselined

Executive Summary

The Target of Evaluation (TOE) is RSA Archer Suite v6.5. It comprises software that supports business-level management of governance, risk management, and compliance (GRC). It enables organizations to build an efficient, collaborative enterprise GRC program across IT, finance, operations and legal domains. It supports organizations in managing risk, demonstrating compliance, automating business processes, and gaining visibility into corporate risk and security controls.

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 with 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 31 May 2019.

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 V6.5 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 RSA Archer Suite v6.5 is a software product 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.

2 The TOE includes the following security functions:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

1.2 TOE Identification

3 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	C107
TOE Name	RSA Archer Suite
TOE Version	V6.5
Security Target Title	RSA Archer Suite v6.5 Security Target
Security Target Version	V0.3
Security Target Date	18 February 2019
Assurance Level	Evaluation Assurance Level 2 Augmented with 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 with ALC_FLR.2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046
Developer	RSA 13200 Metcalf Avenue, Suite 300 Overland Park, Kansas 66213
Evaluation Facility	BAE Systems Lab - MySEF

1.3 Security Policy

4 There is no organisational security policies defined regarding the use of TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

6 The TOE consists of security functions provided by the TOE that are identified in the Security Target (Ref [6]).

Table 2: RSA Archer Suite Logical Boundaries

Security Audit	The TOE generates audits 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 authorized 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 authorized 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 and 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	Authorized administrators manage the security 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 configurations 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

7 The hardware requirements in the operational environment are determined by the size of the deployment and are summarized in the table below.

Table 3: RSA Archer Suite Physical Boundaries

Size	Content Records	Concurrent Users	Description	Element
Very Small Single-Host Environment	Up to 75,000	Up to 10	Web, Services, and Database Servers all on the same server.	2 CPU Cores 8 GB RAM
Small Environment	Up to 100,000	Up to 100	Combined Web and Services Server with a separate Database Server.	For all servers: 4 CPU Cores 16 GB RAM
Medium Environment	Up to 250,000	Up to 250	Two Web Servers, one for Advanced Workflow and one for Web Application, one Services Server, and one Database Server.	For Web and Services Servers: 4 CPU Cores 16 GB RAM For Database Servers: 8 CPU Cores 48 GB RAM
Large Environment	Up to 750,000	Up to 750	Four Web Servers, two Services Servers with Advanced Workflow, and one Database Server.	For Web and Services Servers: 8 CPU Cores 24 GB RAM For Database Servers: 16 CPU Cores 96 GB RAM
Very Large Environment	More than 750,000	More than 750	Contact your RSA sales representative for very large environment recommendations.	
Offline Access Laptop	Up to 1,000	1	Standalone computer that can manual sync	2 CPU Cores 6 GB RAM

Size	Content Records	Concurrent Users	Description	Element
			with RSA Archer for offline use.	

8 The TOE comprises the software and database components listed in Section 2.2.1 of the Security Target (Ref [6]).

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

- Windows Server 2012 R2 or 2016 Standard or Datacenter edition
- Internet Information Services Version 8.5 or 10 (included in Windows Server 2012 R2 or 2016)
- 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 4.6.1 or 4.6.2

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

- Windows Server 2012 R2 or 2016 Standard or Datacenter edition
- Java Runtime Environment (JRE) 8
- Microsoft .NET Framework 4.6.1 or 4.6.2
- Microsoft Sync Framework 2.1 (for offline access)

11 The Instance and Configuration database require the following in the operational environment:

- Windows Server 2012 R2 or 2016 Standard or Datacenter edition
- Microsoft SQL Server SP1 (64-bit), Microsoft SQL Server 2016 Enterprise Edition or Microsoft SQL Server 2017 (64-bit)

12 Users accessing the TOE from a client computer require:

- One of the following supported browsers:
  - Internet Explorer 11
  - Internet Explorer Edge*
  - Chrome 69*
  - Firefox 62 or 60 (ESR)*

- Safari 11*

*These browsers do not support RSA Archer Administrator pages that require Silverlight.

13 The TOE must be configured to require the use of HTTPS to access the TOE from external clients. The TOE documentation provides the guidance necessary to configure the TOE in this fashion.

14 The following diagram is a representation of the physical boundaries of the TOE and its components.

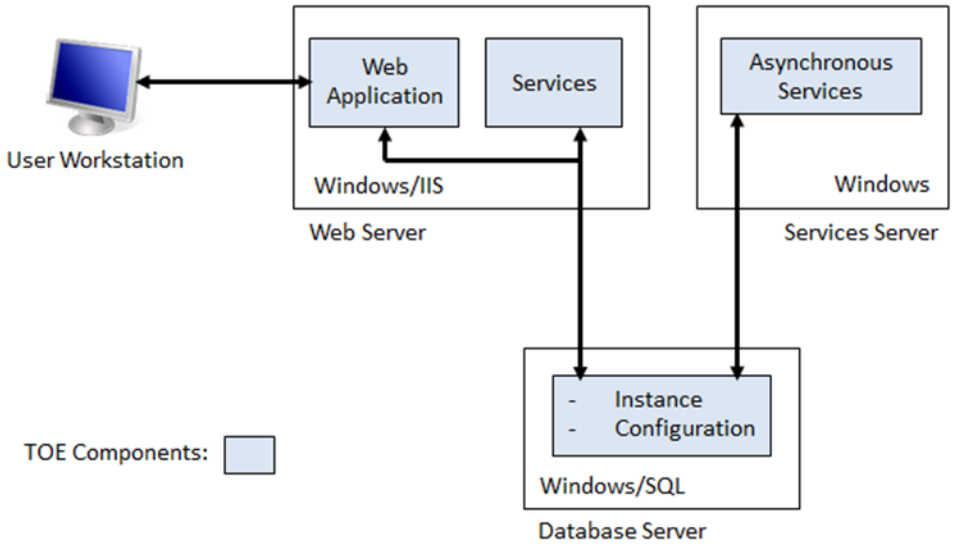

Figure 1: TOE Physical Boundaries

1.5 Clarification of Scope

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

16 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]).

17 Potential consumers of the TOE are advised that some functions and services of the overall product have not 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.

18 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.

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 Operational Environment Assumptions

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

Table 4: Assumptions for the TOE environment

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

1.7 Evaluated Configuration

21 The TOE may be deployed in a number of configurations consistent with the requirements identified in this Security Target (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 Synchronization, 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.
- Configuration Database – a central repository for configuration information for the web application and services servers.

22 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).

23 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 setting, 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

24 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.

25 The delivery procedures should consider, if applicable, issues such as:

- ensuring that the TOE received by the consumer corresponds precisely to the evaluated version of the TOE;
- avoiding or detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;

- avoiding unwanted knowledge of distribution of the TOE to the consumer: there might be cases where potential attackers should not know when and how it is delivered;
- avoiding or detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

1.8.1 TOE Delivery

1.8.1 Software Delivery

26 All delivery of RSA Archer software is done electronically. The product is either downloaded from Flexera or is provided through the SaaS product offering. The client must have an authorized account to be able to access the installation package and TOE Documentation on the RSA Archer Community Website.

1.9 Flaw Reporting Procedures

27 The evaluator 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.

28 The evaluator 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.

29 The evaluator 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.

30 The evaluator 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.

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

32 The evaluators 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.

33 The evaluators 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.

34 Therefore, the evaluator confirms that the information provided meets all requirements for content and presentation of evidence.

2 Evaluation

36 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 with ALC_FLR.2. The evaluation was performed conformant to the ISCB Product Certification Schemes Policy (Product_SP) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

38 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.

39 The evaluators confirmed that the configuration list includes TOE itself, the parts that comprise the TOE the evaluation evidence required by the SARs in the the Security Target (Ref [6]).

40 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 Development

41 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).

42 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.

43 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.

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

2.1.3 Guidance documents

45 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.

46 The evaluators confirmed that the TOE guidance fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

47 Testing at EAL 2 Augmented with 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.

2.1.4.1 Assessment of Developer Tests

48 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 their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

49 At EAL 2 Augmented with 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.

50 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 5: Independent Functional Test

TEST ID	DESCRIPTIONS	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 user 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,	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	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.	
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	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	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, iView and Effective Permission Investigation Console access to the owner or user granted administrator rights. • Verify that a user session will be automatically logged out after the configured time interval of user inactivity has passed. • 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	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	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. • 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 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. • To test that the TOE shall be able to deny session establishment based on calendar date.	
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	Passed. Result as expected.

TEST ID	DESCRIPTIONS	RESULTS
	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.	
TEST-IND-005-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 TOE is able to generate an audit record for security relevant events performed by users.	Passed. Result as expected.
TEST-IND-006-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 of objects within the scope of Discretionary Access Control belonging to individual users.	Passed. Result as expected.

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

2.1.4.3 Penetration testing

52 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.

53 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack 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 requirement for exploitation

54 The penetration tests focused on:

a) General network vulnerability scan;

b) Common web 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.

55 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 a secure environment as specified in Section 4 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

56 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all tests conducted were PASSED as expected.

3 Result of the Evaluation

57 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of RSA ARCHER SUITE V6.5 performed by BAE Systems Lab – MySEF.

58 BAE Systems Lab – MySEF found that RSA ARCHER SUITE V6.5 upholds the claims made in the Security Target (Ref [6]) and supporting documentations and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 Augmented with ALC_FLR.2.

59 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

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

61 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.

62 EAL 2 Augmented with ALC_FLR.2 also provides assurance through use of a configuration management system, the secure delivery procedures, and evidence of flaw remediation procedures.

3.2 Recommendation

63 The Malaysian Certification Body (MyCB) is strongly recommends that:

a) The users should make themselves familiar with the developer guidance provided with the TOE, and to pay attention to all security warnings as well as to observe the

operational environment requirements and assumptions defined in the applicable Security Target (Ref [6]).

b) The users must maintain the confidentiality, integrity and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.

c) The System Administrator should review the audit trail generated and exported by the TOE periodically.

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] ISCB Product Certification Schemes Policy (Product_SP), v1b, CyberSecurity Malaysia, March 2018.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v1a, March 2018.

[6] RSA Archer Suite v6.5 Security Target, Version 0.3, 18 February 2019.

[7] RSA Archer Suite v6.5, Evaluation Technical Report, Version 1.0, 6 August 2019.

A.2 Terminology

A.2.1 Acronyms

Table 6: 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
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 7: 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
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.

Term	Definition and Source
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 ---