C095 Certification Report

RSA Archer Suite v6.3

File name: ISCB-5-RPT-C095-CR-v1
Version: v1
Date of document: 30 May 2018
Document classification: PUBLIC

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

C095 Certification Report

RSA Archer Suite v6.3

30 May 2018

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C095 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C095-CR-v1
ISSUE:	v1
DATE:	30 May 2018

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – 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 30 May 2018 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 associated certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) 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	20 May 2018	All	Initial draft of certification report
v1	23 May 2018	All	Final certification report
v1	30 May 2018	I,ii,iv	Certified date

Executive Summary

The Target of Evaluation (TOE) is RSA Archer Suite v6.3 from RSA.

The TOE 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.

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 Applied Intelligence MySEF (Malaysia Security Evaluation Facility) and completed on 27 April 2018.

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 v6.3 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 TOE 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 functionality defined in the Security Target (Ref [6]) that was subsequently evaluated is as follows:

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

1.2 TOE Identification

3 The details of the TOE are identified in

4 Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C095
TOE Name	RSA Archer Suite
TOE Version	v6.3
Security Target Title	RSA Archer Suite v6.3 Security Target
Security Target Version	Version 0.7
Security Target Date	17 April 2018
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 with Augmented 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 Applied Intelligence – MySEF (Malaysia Security Evaluation Facility) Level 28, Menara Binjai, 2 Jalan Binjai, 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

5 There are no organisational security policies that have been defined regarding the use of the TOE.

1.4 TOE Architecture

6 The TOE includes both logical and physical boundaries as described in Section 2.2.3 and 2.2.4 of the Security Target (Ref [6]).

7 The TOE architecture consists of the following components:

1) Web Application:

   The RSA Archer Suite application runs on a web server. This application requires Microsoft Internet Information Service (IIS) and Microsoft .NET Framework 4.6.1.

2) Services - the services complement the Web application and include the following:
   a) RSA Archer Suite Cache
   b) RSA Archer Suite Configuration
   c) RSA Archer Suite Instrumentation
   d) RSA Archer Suite LDAP Synchronization
   e) RSA Archer Suite Job Engine
   f) RSA Archer Suite Queueing
   g) RSA Archer Suite Workflow

3) Instance Database:

   The Instance Database stores the RSA Archer Suite content for a specific instance. There can be multiple instances based on the business structure and product licensing. For

example, there might be individual instances for each office location or region or for development, test, and production environments.

4) Configuration Database:

The configuration database is a central repository for configuration information for the web application and services servers.

1.4.1 Physical Boundaries

8 The TOE physical boundaries are described in Section 2.2.3 of the Security Target (Ref [6]).

9 The following diagram is a representation of the physical boundaries of the TOE and its components:

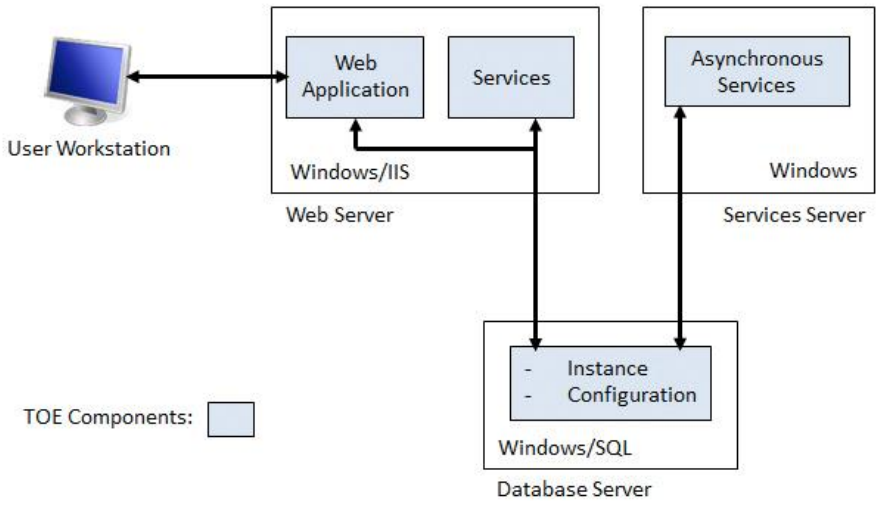

Figure 1: TOE Physical Boundaries

1.4.2 Logical Boundaries

10 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

11 **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.

12 **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.

13 **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.

14 **Security Management:** Authorised administrators manage the security functions and TSF data of the TOE via the web-based GUI.

15 **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.

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 In addition to the Web Application, Services, and 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.

19 The TOE can be deployed in single and multi-server configurations, depending on business requirements.

For optimal scalability and performance, RSA recommends a multi-server configuration. This configuration includes dedicated servers for hosting the web application and the services. Each server plays a specific role within the TOE configuration.

Although not recommended, the TOE can also be installed in a basic configuration consisting of a single server that hosts the web application and services.

Regardless if the TOE is deployed in a single or multi-server configuration, the databases are installed on a dedicated server known as the database server.

20 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 requirement for using functions and services outside of the evaluated configuration.

1.6 Assumptions

21 This section summarises the assumptions regarding the operational environment and the intended usage of the TOE, as described in the Security Target (Ref [6]):

a) There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

b) The TOE software critical to security policy enforcement will be protected from unauthorised physical modification.

c) The operational environment of the TOE will provide mechanisms to protect data communicated to and from remote users from disclosure and modification.

d) The operational environment of the TOE will provide reliable time sources for use by the TOE.

e) The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.

1.7 Evaluated Configuration

22 As stated in the ST (Ref [6]), there are four (4) main components of the TOE that make up the evaluated configuration, namely the Web Application, Services, Instance Database and Configuration Database.

23 The TOE components can be deployed in single and multi-server configurations, depending on business requirements. RSA however recommends a multi-server configuration. This configuration includes dedicated servers for hosting the web application and the services.

24 Regardless if the TOE is deployed in a single or multi-server configuration, the databases are installed on a dedicated server known as the database server, as stated in Section 2.2.3 of the ST (Ref. [6]).

25 The TOE presents a graphical user interface (GUI), a Web Services API, and RESTful 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

26 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.

27 The delivery procedure requirement 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.

28 The TOE delivery procedures are as follows:

- Pre-Delivery and Delivery Activities: The TOE is developed in-house. The development activities of the TOE are performed at RSA facilities. The implementation representation is stored at a secure facility at the RSA headquarters. Access controls are set on the server that stores the TOE, thus only authorised users are provided access. RSA uses an automated source code configuration management system. Before the TOE may be delivered, it must first be approved for release. In order to be approved, the TOE must undergo acceptance testing until it successfully meets the defined acceptance criteria. The

testing of the TOE is conducted throughout the development process. Once testing has been completed successfully, the product is then approved for release.

- TOE Download: Once the testing is verified as successful, the installation package is ready for upload to the RSA SecureCare Online (SCOL) website. A member of the RSA team takes the installation package and uploads it, making it available for subsequent download to a purchasing customer. The communications channel while uploading the installation package is secured by SSL. As the product is only available via download, this is considered the entire process from manufacturing to distribution.

29 All delivery process details are described in Section 2 of the Secure Delivery Life Cycle documentation.

1.9 Documentation

30 It is important that the TOE is used in accordance with the guidance documentation in order to ensure secure usage of the product.

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product.

- RSA Archer Suite Overview Guide 6.3, October 2017
- RSA Archer Suite Platform Administrator's Guide 6.3, October 2017
- RSA Archer Suite Platform Installation and Upgrade Guide 6.3, October 2017
- RSA Archer Suite Platform Planning Guide 6.3, Revision 1, October 2017
- RSA Archer Suite Security Configuration Guide 6.3, Revision 1, October 2017
- RSA Archer Suite Platform User's Guide 6.3, October 2017
- RSA Archer Suite Qualified and Supported Environments 6.3, October 2017
- RSA Archer Suite RESTful API Reference Guide 6.3, October 2017
- RSA Archer Suite Web Services API Reference Guide 6.3, October 2017
- RSA Archer Suite What's New Guide 6.3, October 2017
- RSA Archer Suite Control Panel Guide 6.3, October 2017
- RSA Archer Suite Download Verification Guide 6.3, October 2017

2 Evaluation

31 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. The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

- The evaluators' testing consisted of independent testing efforts, which comprise both functional and penetration test cases to address testing requirements for ATE_IND.2 and AVA_VAN.2 evaluation components.
- For functional testing, the focus was on testing the claimed security functionality (SFRs within the ST) through the interfaces specified in the functional specification (TSFI). For the penetration testing, the effort was limited to attacks that are commensurate to an attacker with equal or less than Basic attack potential. The testing approach for both testing commensurate with the respective assurance components (ATE_IND.2 and AVA_VAN.2).

2.1.1 Life-cycle support

2.1.1.1 Configuration Management Capability

33 The evaluators confirmed that the TOE provided for evaluation is labelled with its reference.

34 The evaluators confirmed that the TOE references used are consistent.

35 The evaluators examined the method of identifying configuration items and determined that it describes how configuration items are uniquely identified.

36 The evaluators examined the configuration items in the configuration item list and determined that they are identified in a way that is consistent with the CM documentation.

2.1.1.2 Configuration Management Scope

37 The evaluators confirmed that the configuration list includes the following set of items:

- the TOE itself;
- the parts that comprise the TOE; and
- the evaluation evidence required by the SARs in the ST.

38 The evaluators confirmed that the configuration list uniquely identifies each configuration item.

39 The evaluators confirmed that the configuration list indicates the developer of each TSF relevant configuration item.

2.1.1.3 TOE Delivery

40 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.

2.1.1.4 Flaw Reporting Procedures

41 The evaluators 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.

42 The evaluators 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.

43 The evaluators 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.

44 The evaluators 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.

45 The evaluators 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.

46 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.

47 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.

2.1.2 Development

2.1.2.1 Architecture

48 The evaluators examined the security architecture description and 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.

49 The security architecture description describes the security domains maintained by the TSF.

50 The initialisation process described in the security architecture description preserves security.

51 The evaluators examined the security architecture description and concluded that it contains sufficient information to demonstrate that the TSF is able to protect itself from tampering by untrusted active entities. The security architecture description presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed.

2.1.2.2 Functional Specification

52 The evaluators examined the functional specification and determined that:

- the TSF is fully represented,
- it states the purpose of each TSF Interface (TSFI),
- the method of use for each TSFI is given,

53 The evaluators also examined the presentation of the TSFI and determined that:

- it completely identifies all parameters associated with every TSFI,
- it completely and accurately describes all error messages resulting from an invocation of each SFR-enforcing TSFI,

54 The evaluators also confirmed that the developer supplied tracing that links the SFRs to the corresponding TSFIs.

2.1.2.3 TOE Design Specification

55 The evaluators examined the TOE design and determined that the structure of the entire TOE is described in terms of subsystems. The evaluators also determined that all subsystems of the TSF are identified. The evaluators determined that interactions between the subsystems of the TSF were described.

56 The evaluators examined the TOE and determined that each SFR supporting or SFR-non-interfering subsystem of the TSF was described such that the evaluators could determine that the subsystem is not SFR-enforcing.

57 The evaluators found the TOE design to be a complete, accurate, and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

58 The evaluators examined the TOE design and determined that it provides a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

59 The evaluators determined that the TOE design contained a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.

60 The evaluators determined that all SFRs were covered by the TOE design, and concluded that the TOE design was an accurate instantiation of all SFRs.

2.1.3 Guidance documents

2.1.3.1 Operational Guidance

61 The evaluators examined the operational user guidance and determined that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. For each role, the secure use of available TOE interfaces is described. The available security functionality and interfaces are described for each user role – in each case, all security parameters under the control of the user are described with indications of secure values where appropriate.

62 The operational user guidance describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.

63 The evaluators examined the operational user guidance (in conjunction with other evaluation evidence and determined that the guidance identifies all possible modes of operation of the

TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

64 The evaluators determined that the operational user guidance describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

65 The evaluators found that the operational user guidance is clear and reasonable.

2.1.3.2 Preparation Guidance

66 The evaluators examined the provided delivery acceptance documentation and determined that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.

67 The evaluators determined that the provided installation procedures describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

68 The evaluators performed all user procedures necessary to prepare the TOE during testing and determined that the TOE and its operational environment can be prepared securely using only the supplied preparative user guidance.

2.1.4 IT Product Testing

69 Testing at EAL2 consists of assessing developer tests, performing independent functional tests, and conducting penetration tests. The TOE testing was conducted by the evaluators of BAE Systems Applied Intelligence 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

70 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, 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).

2.1.4.2 Independent Functional Testing

71 At EAL2, 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.

72 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.

Test ID	Description	SFRs
TEST-IND-001-GUI	• 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. • 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 the TSF shall maintain security roles and security attributes belonging to individual users. • 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 authorised users are able to perform management of TSF data functions, and able to modify the behaviour of security management functions. • 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 TSF shall display an advisory warning message regarding unauthorised use of the TOE.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.3.1, FIA_AFL.1.1, FIA_AFL.1.2, FIA_ATD.1.1, FIA_SOS.1.1 , FIA_UAU.2.1, FIA_UAU.5.1, FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.6.1, FIA_UID.2.1, FMT_MTD.1.1(1), FMT_MTD.1.1(2), FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FTA_SSL.3.1, FTA_SSL.4.1 , FTA_TAB.1.1
TEST-IND-002-GUI	• Verify that the TSF shall enforce the Discretionary Access Control SFP on subjects, objects, and operations based on security and object attributes. • 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.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.3.1, FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4,

Test ID	Description	SFRs
	• 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. • Verify that the TSF shall enforce the Discretionary Access Control SFP to provide permissive default values for security attributes that are used to enforce the SFP. • Verify that the TSF shall allow the Application, Questionnaire, and Sub-form owner, Application Builder administrator, Workspace and Dashboard administrator, and System Administrator 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 TSF provides security management functions to manage the security attributes of objects within the Discretionary Access Control SFP.	FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_REV.1.1, FMT_REV.1.2, FMT_SMF.1.1
TEST-IND-003-GUI	• 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. • Verify that the TSF restricts the ability to enable and disable data privacy function to sysadmin. • 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 TSF shall be able to deny session establishment based on IP address and calendar date.	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.2.1, FAU_SAR.3.1, FMT_MOF.1.1, FMT_REV.1.1, FMT_REV.1.2, FMT_SMF.1.1, FTA_TSE.1.1
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 the TSF shall maintain security roles and security attributes belonging to individual users.	FAU_GEN.1.1, FAU_GEN.1.2, FIA_UAU.2.1, FIA_UID.2.1, FMT_MTD.1.1(2), FMT_SMF.1.1, FMT_SMR.1.1,

Test ID	Description	SFRs
	• 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.	FMT_SMR.1.2, FTA_SSL.4.1
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 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.	FAU_GEN.1.1, FAU_GEN.1.2, FIA_UAU.2.1, FIA_UID.2.1, FMT_MTD.1.1(2), FMT_SMF.1.1, FMT_SMR.1.1, FMT_SMR.1.2, FTA_SSL.4.1

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

2.1.4.3 Penetration Testing

74 The evaluators performed 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, and TOE design and security architecture description.

75 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 (specialist 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.

76 The penetration tests focused on:

a) General network vulnerability scan

b) Common web vulnerability scan

c) Input and data validation

d) Insecure direct object references

e) Unrestricted file upload

f) Missing function level access control

77 The results of the penetration testing demonstrate that the TOE is resistant to an attacker possessing a basic attack potential. However, it is important to ensure that the TOE is used only in its evaluated configuration and in a secure environment as specified in the Security Target (Ref [6]).

2.1.4.4 Testing Results

78 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target (Ref [6]) and its functional specification. In addition, the documentation supplied as evidence for the EAL2 Augmented ALC_FLR.2 Common Criteria evaluation of the TOE was analysed to identify possible vulnerabilities.

3 Result of the Evaluation

79 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 v6.3 performed by BAE Systems Applied Intelligence MySEF.

80 BAE Systems Applied Intelligence MySEF found that RSA Archer Suite v6.3 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 (EAL2) Augmented ALC_FLR.2.

81 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

82 EAL 2 Augmented ALC_FLR.2 provides assurance by a full Security Target and analysis of the SFRs in that Security Target (Ref [6]), using functional and interface specifications, guidance documentation and a basic description of the design and architecture of the TOE, to understand the security behaviours of the TOE.

83 The analysis is supported by an 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 an attacker possessing a Basic attack potential.

84 EAL 2 Augmented ALC_FLR.2 also provides assurance through use of a configuration management system, evidence of secure delivery procedures and flaw reporting procedures (ALC_FLR.2).

3.2 Recommendation

85 The following recommendations are made:

a) 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.

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 Policy (MyCC_P1), v1d, CyberSecurity Malaysia, February 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1c, February 2016.

[6] RSA Archer Suite v6.3 Security Target, Version 0.7, 17 April 2018

[7] EAU000605.01-S045-ETR1.0, Evaluation Technical Report, Version 1.0, 8 May 2018

A.2 Terminology

A.2.1 Acronyms

Table 2: 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
TOE	Target of Evaluation

Acronym	Expanded Term
API	Application Programming Interface
GUI	Graphical user interface
GRC	Governance, Risk management, and Compliance
REST	Representational state transfer—a software architecture for distributed systems, including RESTful API web services
SSL	Secure Sockets Layer

A.2.2 Glossary of Terms

Table 3: 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.

Term	Definition and Source
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 ---