MOSTI
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

CyberSecurity MALAYSIA
An agency under MOSTI

C073 Certification Report

RSA Archer GRC Platform v6.1

File name: ISCB-3-RPT-C073-CR-v1
Version: v1
Date of document: 14 September 2016
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

Securing Our Cyberspace

C073 Certification Report
RSA Archer GRC Platform v6.1

14 September 2016

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

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 5, Sapura@Mines
No 7, Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
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 14 September 2016, 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).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	1st September 2016	All	Initial draft
v1	6th September 2016	Executive Summary, 1.1, 1.2, 1.4.1, 1.5, 1.8, Annex A.1	Update executive summary, scope, logical boundaries, delivery procedures, reference

Executive Summary

RSA Archer GRC Platform v6.1 is the TOE for this Evaluation Assurance Level EAL 2+ evaluation. This TOE is a software product which supports business level management of governance, risk management and compliance. As the foundation for all RSA Archer GRC Solutions, the Platform allows users to adapt the solution to their requirements, build their own applications and integrate with other systems without touching code.

The TOE enables users to address particular business needs using solutions, which consist of applications and questionnaires that are containers for specific types of data records such as incidents, controls, policies or assets. The applications define the content and behaviour of the individual records while questionaries have unique features that allow users to access the content of a particular target application.

Users access the TOE via a web-based graphical user interface (GUI) and are required to have an account to log into the TOE. Each user account specifies the user's groups and access roles that control user privileges (create, read, update and delete) and control user access to objects (applications, questionnaires, record and fields).

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

The TOE scope of evaluation covers various major security functions described as below:

a) Security Audit: The TOE generates the 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 authorized administrators with the ability to read the audit events.
b) 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 Discretionary Access Control covers the scope of applications, questionnaires, sub-forms, records, fields, workspace, dashboards and iViews.
c) Identification & Authentication: The TOE identifies and authenticates all users of the TOE before granting the users access to the TOE. Each user must have an account on the TOE to access the TOE that associates the user's identity with the user's password, any assigned group and any assigned access roles.
d) Security Management: Authorized administrators manage the security functions and TSF data of the TOE via the web-based GUI.
e) 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. Moreover, the TOE displays a banner message on the user login page, the content of which is specified during initial configuration using the RSA Archer GRC Control Panel. The TOE also 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.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 RSA Archer GRC Platform v6.1 is the TOE for this Evaluation Assurance Level EAL 2+ evaluation. This TOE is a software product which supports business level management of governance, risk management and compliance. As the foundation for all RSA Archer GRC Solutions, the Platform allows users to adapt the solution to their requirements, build their own applications and integrate with other systems without touching code.

2 The TOE enables users to address particular business needs using solutions, which consist of applications and questionnaires that are containers for specific types of data records such as incidents, controls, policies or assets. The applications define the content and behaviour of the individual records while questionaries have unique features that allow users to access the content of a particular target application.

3 Users access the TOE via a web-based graphical user interface (GUI) and are required to have an account to log into the TOE. Each user account specifies the user's groups and access roles that control user privileges (create, read, update and delete) and control user access to objects (applications, questionnaires, record and fields).

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

5 The TOE scope of evaluation covers various major security functions described as below:

a) Security Audit: The TOE generates the 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 authorized administrators with the ability to read the audit events.

b) 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 Discretionary Access Control covers the scope of applications, questionnaires, sub-forms, records, fields, workspace, dashboards and iViews.

c) Identification & Authentication: The TOE identifies and authenticates all users of the TOE before granting the users access to the TOE. Each user must have an account on the TOE to access the TOE that associates the user's identity with the user's password, any assigned group and any assigned access roles.

d) Security Management: Authorized administrators manage the security functions and TSF data of the TOE via the web-based GUI.

e) 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. Moreover, the TOE displays a banner message on the user login page, the content of which is specified during initial configuration using the RSA Archer

GRC Control Panel. The TOE also 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.

1.2 TOE Identification

6 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	C073
TOE Name	RSA Archer GRC Platform v6.1 (RSA Archer)
TOE Version	v6.1
Security Target Title	RSA Archer GRC Platform 6.1 Security Target
Security Target Version	v1.0
Security Target Date	5 August 2016
Assurance Level	Evaluation Assurance Level 2 (EAL 2+) Augmented with ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (Ref [2])
Methodology	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1, Revision 4 (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 and Developer	RSA 13200 Metcalf Avenue, Suite 300, Overland Park, KS 66213
Evaluation Facility	BAE Systems Lab - MySEF

1.3 Security Policy

7 There are no organisational security policies defined regarding the use of the TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

9 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 in Table 2:

Table 2: Logical Boundaries

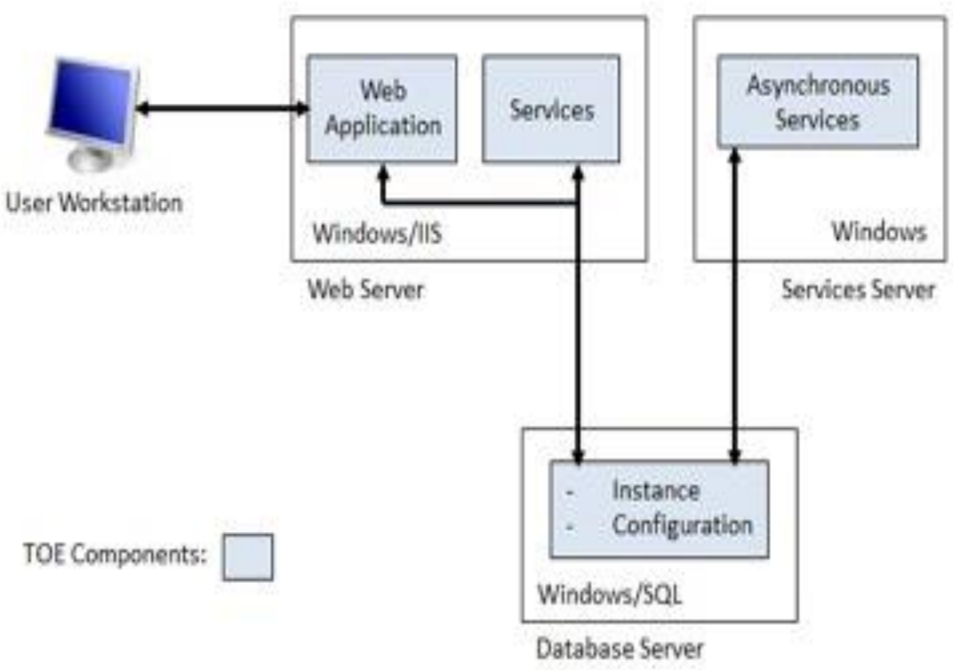
Security Component	Description
Web Subsystem	This TOE component consists of the end user interface pages, management applets, dashboards and workspaces which account for much of the TOE's operations as well as the applications which run on the TOE. It represents the front-end layer that is presented to TOE users and administrators through its TOE Security Function Interfaces, which are as follows: • Web Graphical User Interface (GUI) • Web Services Application Programming Interface (Web API) • RESTful API
Administration Subsystem	This TOE component consists of C# code and Windows Communication Foundation (WCF) services. While it does not contain any external interfaces, it accounts for much of the TOE's security functionality. It represents middle-tier application logic responsible for enforcing many of the SFRs claimed for the TOE. It is responsible for user management, security roles, access control, application management, security audit, as well as other non-security related management features.
Database Logic Subsystem	This TOE component represents the Structured Query Language (SQL) stored procedures which handle all of the TOE database operations. None of the TOE subsystems can act directly upon TOE user data; rather, data operations must be processed via the invocation of a stored procedure called by this subsystem.
Job Management Subsystem	This TOE component enforces session expiration and provides various options for integration of the TOE with external applications. It contains several transporters that call out to external servers to retrieve data feeds that are imported into TOE

	applications. Several external interfaces are found in this subsystem, but none enforce security functionality.
Applications Subsystem	This TOE component accounts for the middle-tier C# application logic that pertains to the applications which run on the TOE. While much of its functionality is omitted from the TOE, it does provide security functionality, such as access control and auditing.
Queuing Subsystem	This TOE component does not provide any security functionality. It is responsible for maintaining full-text indexes which are referenced by the Web Subsystem for its full-text search function.
Advanced WorkFlow Subsystem	This TOE component does not provide any security functionality. It is responsible for processing workflows defined by users in the Web Subsystem.
Cache Subsystem	This TOE component, which does not provide any security functionality, supports the caching solution for reducing the number of calls from the Web Subsystem to the database by storing metadata, which consists of language, application, solution and values list data.

1.4.2 Physical Boundaries

10 The following Figure 1 is representing the physical boundaries of the TOE and its components.

Figure 1: Physical Boundaries of the TOE



11 The TOE is primarily accessible via a web browser through the web GUI TSFI, but it can also be programmatically invoked via the Web and RESTful APIs. Several management applications, which are integral to the TOE and therefore included within the TOE boundary, are available to authorized administrators through the Web GUI, including Access Control, Appearance, Application Builder, Discussion Forums, Integration, Management Reports, Notifications, Training and Awareness, and Workspaces and Dashboards. Additionally, much of the Access Control application's feature set is exposed via the Web and RESTful APIs.

12 In addition, the RSA Archer distribution includes the RSA Archer GRC Control Panel, a configuration tool used to create and manage RSA Archer GRC Platform instances. The control panel enables RSA Archer GRC Platform administrators to manage installation settings, instance settings, and plugins, but is not itself part of RSA Archer GRC Platform and is outside the TOE boundary. Administrators can configure TOE installation behaviour including the Login Banner field during initial installation using the Control Panel.

1.5 Clarification of Scope

13 The TOE is designed in order to support business level management of governance, risk management and compliance. As the foundation for all RSA Archer GRC Solutions, the Platform allows users to adapt the solution to their requirements, build their own applications and integrate with other systems without touching code.

14 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The TOE is the software that enables users to address particular business needs using solutions, which consist of applications and questionnaires that are containers for specific types of data records such as incidents, controls, policies or assets.

15 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

16 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE, which has been defined in the Security Target (Ref [6]).

1.6.1 Usage assumptions

17 Assumptions for the TOE usage as listed in Security Target:

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 unauthorized physical modification.

1.6.2 Environment assumptions

18 Assumptions for the TOE environment listed in Security Target are:

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

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

1.7 Evaluated Configuration

19 There are four main components of the TOE, namely the RSA Archer GRC Platform web application, services that complement the web application, instance database that stores the TOE content for a specific instance, and the configuration database that serves as a central repository for configuration information for the web application and services servers.

20 The TOE can be deployed in a single or multi-server configuration depending on business requirements. However, the ST and the guidance documentation recommend a multi-server configuration for the TOE. The TOE comprises the software and database, and requires specific qualified software components in its operational environment. This information is comprehensively described in the Security Target (Ref [6]).

21 During testing, the TOE was set up in a multi-server configuration that consisted of the web application and the databases on two separate servers that was connected in an internal network. A client PC was used to access the web application over HTTPS, as mandated in the ST.

1.8 Delivery Procedures

22 Delivery procedures of the TOE consist of:

a) **Security Environment**

The main threats that apply to the delivery of the TOE are: the wrong product could be delivered from RSA to the customer; a third party attacker could attempt to replace the TOE with an imitation unit during TOE delivery; and a third-party attacker could attempt to sabotage the TOE during delivery.

However, the TOE is not uniquely vulnerable during the delivery phase therefore the level of sophistication of threats to delivery is considered to be low. The delivery procedures ensure that the integrity and authenticity of the TOE are maintained and that they are verifiable by the customer and by RSA after delivery has been completed.

b) **Pre-Delivery and Delivery Activities for software and documentation**

i. Software

The TOE is developed in-house. Before the TOE may be delivered, it must first have been tested by the RSA Quality Engineering (QE) team. Once approved for release by QE team, the TOE then becomes the “Master” version. The Release Engineer (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 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 GA, depending on scheduling.

Moreover, RSA uses WinRAR as the tool to create the Archer installation package. The Archer installation package includes authenticity verification via a password-protected self-extraction package and CRC[1] validation for file integrity. CRC is an error-detecting non-secure hash function. WinRAR runs a hash function on the installation package and a value is determined. This value is sent as part of the installation package. Once the package is downloaded, and extracted, the hash function is run again automatically and a comparison to the previous hash value is made. If the value is different from the original value, then an error message is given.

ii. Documentation

RSA Archer Technical Publications team creates and maintain all guidance documentation. 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.

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.

c) **Customer Product Verification.**

[1] CRC = Cyclic redundancy check

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 authorized account to be able to access the installation package and TOE Documentation on the RSA Archer Community website.

1.9 Documentation

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

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

a) RSA Archer GRC 6.1 Platform User Guide, June 2016

b) RSA Archer GRC 6.1 Platform Administrator Guide, June 2016

c) RSA Archer GRC 6.1 Platform Download Verification, June 2016

d) RSA Archer GRC 6.1 Platform Installation and Upgrade Guide, June 2016

e) RSA Archer GRC 6.1 Platform Security Configuration Guide, June 2016

f) RSA Archer GRC 6.1 Platform Sizing Performance Guide, June 2016

g) RSA Archer GRC 6.1 Platform Web Services API Reference Guide, June 2016

2 Evaluation

25 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2+ Augmented with ALC_FLR.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

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

2.1.1 Life-cycle support

27 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.

28 The evaluators examined the delivery documentation including flaw remediation procedures 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

29 The evaluators analysed 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).

30 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 behaviour of the SFR-enforcing subsystems.

31 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.

2.1.3 Guidance documents

32 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.

2.1.4 IT Product Testing

33 Testing at EAL2+ Augmented with ALC_FLR.2 consists of assessing developer tests, performing independent function tests, and performing penetration tests. The TOE testing was conducted by evaluators from BAE Systems Lab – MySEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of developer Tests

34 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).

35 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

36 At EAL2+ Augmented with ALC_FLR.2, independent functional testing is the evaluation testing conducted by the evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

37 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 3: Independent Functional Test

Identifier	Description	Results
D001	• Audit of start-up and shutdown of audit function. • Audit consist date and time of event, type of event, subject identity (if applicable), and outcome (success or failure) of event. • Auditable events such as access role creation / modification / deletion, user login / logout, password change, assigning role. • Associate each auditable event with the identity of the user that caused the event, suitable for user to interpret the information.	**PASS.** Result as expected.

Identifier	Description	Results
D002	• Enforce discretionary access control SFP on users, TOE objects and TOE operations. • Enforce discretionary access control SFP to subject and object attributes. • Enforce additional rules to determine if an operation among controlled subjects and controlled objects is allowed.	**PASS.** Result as expected.
D003	• Detect an administrator-configurable positive integer of unsuccessful authentication attempts on user account login. • Require each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. • Re-authenticate the user under the conditions of interactive user session duration exceeds configured Static Session Timeout value.	**PASS.** Result as expected.
D004	• Enforce the discretionary access control SFP to provide permissive default values for security attributes that are used to enforce the SFP. • The TSF shall restrict the ability to query, modify, delete, or create user accounts and user groups to System Administrator and user with access control rights. • Restrict the ability to revoke access roles associated with the users under the control of the TSF to System Administrator and user with access control rights. • Able to maintain and associate user with roles.	**PASS.** Result as expected.
D005	• Terminate an interactive session after a System Administrator or user with access control rights configurable time interval of session inactivity. • Allow user-initiated termination of user's own interactive session. • Display advisory warning regarding unauthorized use of the TOE before establish user session. • Deny session establishment based on IP address, time of day, day of week and calendar date.	**PASS.** Result as expected.

Identifier	Description	Results
F001	• Audit records are protected from unauthorised modifications or deletion. • Ensure that only System Administrator role or user with access control rights can view the TOE audit trail file. • Ensure that the identity of the user that caused the event can be traced from audit logs	**PASS.** Result as expected.
F002	• TOE is able to restrict the ability to create or delete user account only to System Administrator role or user with access control rights. • User needs to be authenticated and identified as System Administrator role or user with access control rights before user creation or deletion.	**PASS.** Result as expected.
F003	• Demonstrate that the TOE can terminate inactive sessions by an administrator – configured period of time. • Demonstrate that only System Administrator role or user with access control rights are able to set time duration for inactive session.	**PASS.** Result as expected.

2.1.4.3 Penetration Testing

38 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.

39 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 (elapse 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.

40 The penetration tests focused on:

a) General Vulnerability Scan

b) Injection Attacks

c) Cross-Site Scripting (XSS)

d) Security Misconfiguration

e) Broken Authentication and Session Management

f) Sensitive Data Exposure

g) Invalidated Redirects and Forwards

h) Missing Function Level Access Control

i) Insecure Direct Object Reference

j) SQL Injection

41 The results of the penetration testing note 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 4.2 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

42 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.

3 Result of the Evaluation

43 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 GRC Platform v6.1 performed by BAE Systems Lab – MySEF.

44 BAE Systems Lab - MySEF, found that RSA Archer GRC Platform v6.1 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL 2+ Augmented with ALC_FLR.2)

45 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

46 EAL 2+ Augmented with ALC_FLR.2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

47 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.

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

3.2 Recommendation

49 To ensure secure usage of the product, below are additional recommendations for TOE users:

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.

b) The user should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

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

d) System Auditor should review the audit trail generated and exported by the TOE periodically.

e) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected, commensurate with the sensitivity of the TOE keys.

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 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1e, CyberSecurity Malaysia, August 2016.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1d, August 2016.

[6] RSA Archer GRC Platform 6.1 Security Target, Version 1.0, 5 August 2016.

[7] RSA Archer GRC Platform 6.1 Evaluation Technical Report, Version 1.0, 22 August 2016.

[8] RSA Archer GRC 6.1 Common Criteria Flaw Remediation Document, version 1.1, 28 July 2016

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
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile

Acronym	Expanded Term
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
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.

Term	Definition and Source
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 ---