



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

C124 Certification Report

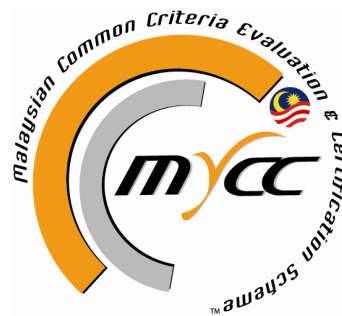
Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4

File name: ISCB-5-RPT-C124-CR-v1

Version: v1

Date of document: 29 April 2022

Document classification: PUBLIC



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



C124 Certification Report

Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4

29 April 2022

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: C124 Certification Report

DOCUMENT REFERENCE: ISCB-5-RPT-C124-CR-v1

ISSUE: v1

DATE: 29 April 2022

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND
DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2022

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (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, 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 17 May 2022, 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 authorised provided the report is reproduced in its entirety.

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	21 April 2022	All	Initial draft
V1	29 April 2022	All	Final version

Executive Summary

The Target of Evaluation (TOE) is Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4. The TOE 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 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 MySEF and the evaluation was completed on 30 March 2022.

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 <https://www.cybersecurity.my/mycc/> and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at <https://www.commoncriteriaportal.org/>

It is the responsibility of the user to ensure that Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4 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	Document Authorisation	ii
Copyright Statement		iii
Foreword		iv
Disclaimer		v
Document Change Log		vi
Executive Summary		vii
Index of Tables		ix
Index of Figures		ix
1 Target of Evaluation		1
1.1	TOE Description	1
1.2	TOE Identification	3
1.3	Security Policy	4
1.4	TOE Architecture	4
1.4.1	Logical Boundaries	4
1.4.2	Physical Boundaries	5
1.5	Clarification of Scope	7
1.6	Assumptions	7
1.6.1	Operational Environmental assumptions	7
1.7	Evaluated Configuration	8
1.8	Delivery Procedures	10
1.8.1	TOE Delivery Procedures	10
2	Evaluation	14
2.1	Evaluation Analysis Activities	14
2.1.1	Life-cycle support	14
2.1.2	Flaw Reporting Procedures	14
2.1.3	Development	15
2.1.4	Guidance documents	16
2.1.5	IT Product Testing	16
3	Result of the Evaluation	24

3.1 Assurance Level Information	24
3.2 Recommendation.....	24
Annex A References.....	26
A.1 References.....	26
A.2 Terminology.....	26
A.2.1 Acronyms	26
A.2.2 Glossary of Terms	27

Index of Tables

Table 1: TOE Identification	3
Table 2: Assumptions for the TOE Environment	8
Table 3: Independent Functional Test	17
Table 4: List of Acronyms.....	26
Table 5: Glossary of Terms.....	27

Index of Figures

Figure 1 – TOE.....	5
Figure 2 – Test environment components.....	9

1 Target of Evaluation

1.1 TOE Description

- 1 The Target of Evaluation (TOE) is Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4. The TOE is a software that support business-level management of governance, risk management, and compliance. As the foundation for all Archer Suite Solutions, the Suite allows users to adapt the solutions to their requirements, build their own applications, and integrate with other systems without touching code. This report also will refer to the previous TOE identification as RSA Archer Suite v6.9.1.2 with the RSA Archer Mobile App V1.4 due to the Developer re-branding. The terms are interchangeable in this document.
- 2 Users access the TOE via a web-based graphical user interface (GUI) or via the TOEs Mobile application. The RSA Archer Mobile application provides remote users the ability to complete their Advanced Workflow actions (edit records and add comments) on-the-go. All users require an account in order to log on to the TOE. The user account specifies the user's groups and access roles. An access role is a collection of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete). The TOE controls user access to its objects (applications, questionnaires, records and fields) based on the access roles associated with users and with the groups to which the user belongs. Administrators can select the application fields and layouts for mobile end users. An administrator can configure an advanced workflow to require users to electronically sign records. The electronic signature provides an additional layer of security by requiring users to re-authenticate before interacting with the records. The Mobile App does not support electronically signed records.
- 3 The Content API, Web Services API, Mobile App API and RESTful APIs programmatically extend the functionality of the TOE to external applications through several classes and methods which expose many of its features, allowing for a high level of integration with other products. All users must be successfully identified and authenticated by the TOE before gaining access to any other TOE services.
- 4 The TOE provides capabilities to configure minimum strength requirements (e.g., minimum length, required character sets) for passwords. The TOE can be configured to track the number of consecutive failed authentication attempts and block further authentication attempts for a configurable time period when the configured threshold

has been met. The TOE will terminate interactive sessions that have been idle for a configurable period of time.

- 5 The TOE able to generate audit records of security-relevant events occurring on the TOE and provides administrators with the ability to review audit records stored in the audit trail.
- 6 There are five main components to an RSA Archer Suite installation which are Web Application, Services, Instance Database, Configuration Database and Archer IRM Mobile or RSA Archer Mobile App.
- 7 RSA Archer Suite distribution also 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.

1.2 TOE Identification

8 The details of the TOE are identified in Table 1: TOE Identification below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C124
TOE Name	Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4
TOE Version	v6.9.1.2 and V1.4
Security Target Title	Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4 Security Target
Security Target Version	V1.0
Security Target Date	8 April 2022
Assurance Level	Evaluation Assurance Level 2 Augmented ALC_FLR.2
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2 Augmented ALC_FLR.2
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive, Columbia, Maryland 21046, The United States of America
Developer	RSA 13200 Metcalf Avenue, Suite 300 Overland Park, Kansas 66213, The United States of America
Evaluation Facility	BAE Systems Lab - MySEF Level 28, Menara Binjai, 2 Jalan Binjai 50450 Kuala Lumpur, Malaysia

1.3 Security Policy

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

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

- 11 The logical boundary of the TOE is summarized below:

- Security Audit

The TOE generates audit records of security relevant events that include at least the date and time of the event, subject identity and outcome for security events. The TOE provides 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 & 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 or with a SAML 2.0 or Federation Single Sign-on (SSO) capable Identity Provider 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 locally defined user account passwords and provides a mechanism to lock a user account after a configured number of consecutive failed attempts to logon.

When using the SSO authentication method, the user is authenticated based on assertions of Identity Providers (IDPs). The user enters their username and

password at the Identity Provider for authentication and the response is enforced by the TOE. For locally defined accounts, the TOE performs the authentication.

- 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 configuration using the RSA Archer Suite Control Panel.

The TOE can be configured to allow connections to the Web Application only from designated IP addresses, and to deny session establishment outside specified times, days of the week, or dates.

1.4.2 Physical Boundaries

- 12 The physical boundaries of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

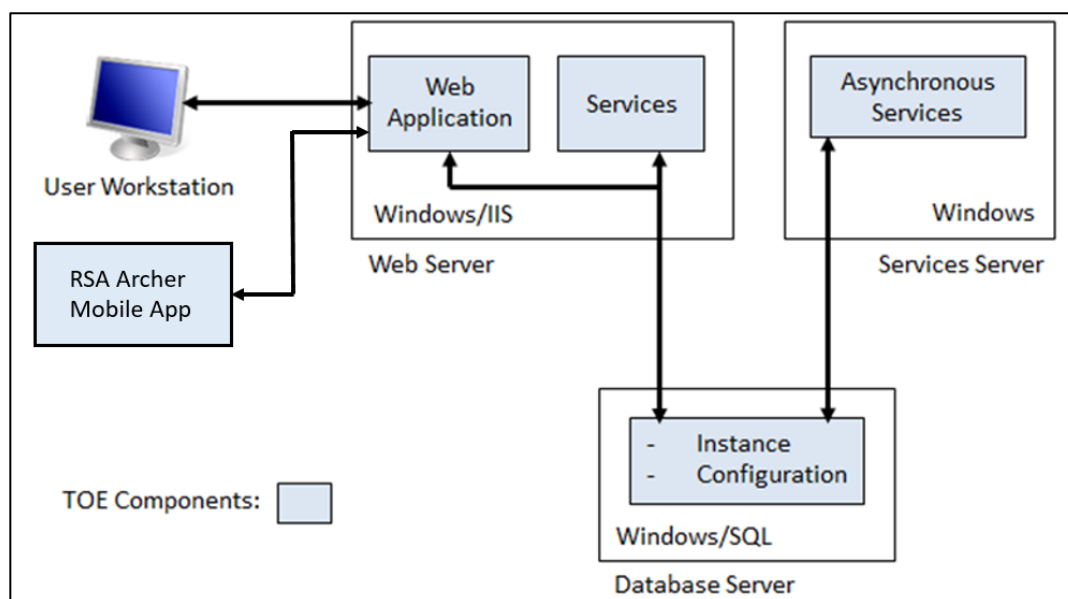


Figure 1 - TOE

- 13 The Web Application requires the following components in its operational environment:
- Windows Server 2012 R2, 2016, or 2019 Standard or Datacenter edition
 - Internet Information Services Version 8.5 or 10 (included in Windows Server 2012 R2, 2016, or 2019)
 - Microsoft Office 2019, 2016, or Office 365 (to enable indexing of MS Office files). This in turn requires Microsoft Filter Pack 2.0 or later
 - Microsoft .NET Framework 4.7.2 or 4.8
 - SAML 2.0 and Federation Single Sign-on capable Identity Providers
- 14 The Services component requires the following in its operational environment:
- Windows Server 2012 R2, 2016, or 2019 Standard or Datacenter edition
 - Microsoft .NET Framework 4.7.2 or 4.8
 - Microsoft Windows 10 (for offline access).
- 15 The Instance and Configuration databases require the following in the operational environment:
- Windows Server 2012 R2, 2016, or 2019 Standard or Datacenter edition
 - Microsoft SQL Server 2019, 2017 (both Standard and Enterprise editions are qualified).
- 16 The Archer IRM Mobile application requires the following in the operational environment:
- Android 8.0 (Android Oreo) and above (API Level 24+) obtained from Google Play store
 - iOS 12 and above (obtained from Apple store)
 - The RSA Archer Mobile app only works in an environment where RSA Archer is using a trusted Certificate Authority (CA) signed SSL certificate. RSA Archer Mobile application does not support self-signed certificates. The configured login type rejects requests if it is not communicating using valid public certificates.
 - Federation Single Sign-on capable Identity Providers - For mobile users to sync data between offline access or the mobile app and RSA Archer, they must log in to the mobile device and provide their RSA Archer credentials when prompted to sync.

17 Users accessing the TOE from a client computer require:

- One of the following supported browsers:
 - Internet Explorer 11
 - Microsoft Edge 86*
 - Chrome 86*
 - Firefox 78.3 (ESR)* or 81*
 - Safari 13*

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

- Microsoft Silverlight 5.1 (required for administration.)

18 The TOE must be configured to require the use of HTTPS to access the TOE from external clients and from the RSA Archer Mobile App. The Mobile App also requires the use of CA certificates. The TOE documentation provides the guidance necessary to configure the TOE in this fashion.

1.5 Clarification of Scope

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

20 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]).

21 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.

1.6 Assumptions

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

1.6.1 Operational Environmental assumptions

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

Table 2: Assumptions for the TOE Environment

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

1.7 Evaluated Configuration

- 24 This section describes the evaluated configurations of the TOE that are included within the scope of the evaluation.
- 25 As stated in the ST (Ref. [6]) there are five (5) main components that make up the TOE in its evaluated configuration:
- Web Application – the RSA Archer Suite application that runs on a web server.
 - Services – the services complement the Web application, such as RSA Archer Suite Cache, RSA Archer Suite Configuration, RSA Archer Suite Instrumentation, RSA Archer Suite LDAP Synchronisation, RSA Archer Suite Job Engine, RSA Archer Suite Queueing and RSA Archer Suite Workflow.
 - Instance Database – stores the RSA Archer Suite content for a specific instance. It can be multiple instances based on the business structure and product licensing.
 - Configuration Database – a central repository for configuration information for the web application and services servers.

- Archer IRM Mobile or RSA Archer Mobile App – The RSA Archer Mobile application provides remote users the ability to complete their Advanced Workflow actions on-the-go. Users can edit records and add comments while completing tasks. Administrators can select the fields and layouts for mobile end users. This configuration is performed from within RSA Archer Suite (not from Mobile App).
- 26 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).
- 27 The TOE presents a Web graphical user interface (Web GUI), Web Services API, RESTful API and Content API. In addition, the Mobile application presents the ability to complete their Advanced Workflow actions on-the-go.
- 28 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.

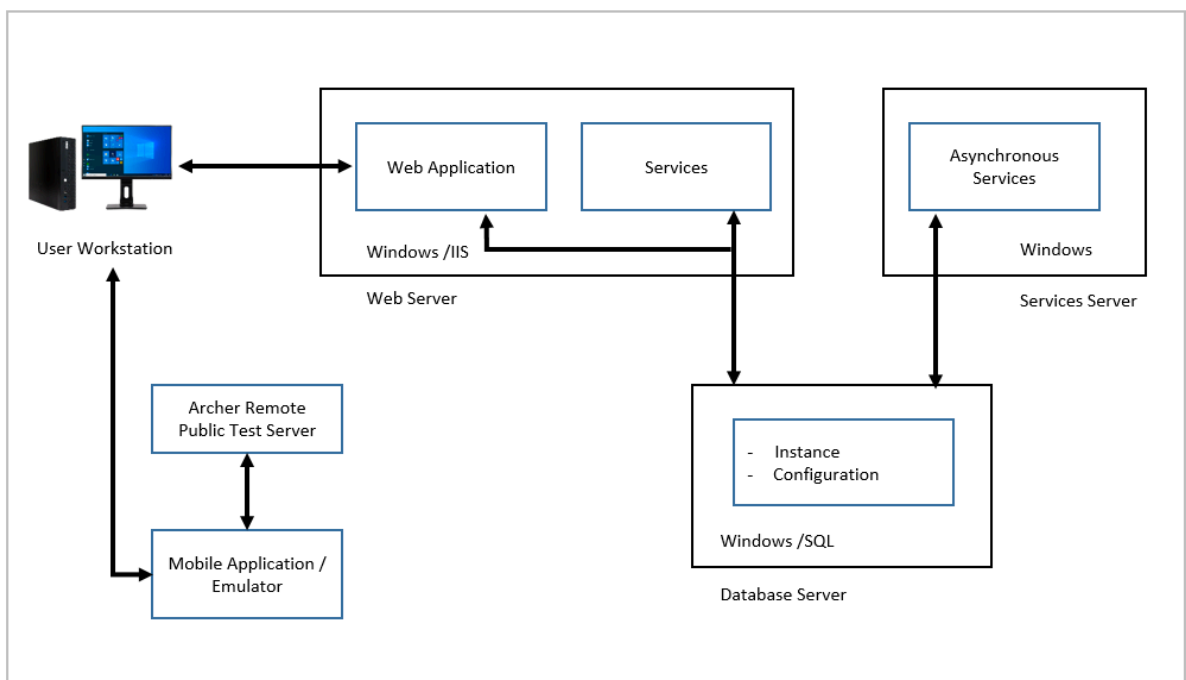


Figure 2 – Test environment components

1.8 Delivery Procedures

- 29 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.
- 30 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

- 31 Several procedures are necessary for Archer to maintain security of the TOE during distribution including the procedures that Archer follows during the production, packaging, and release of the TOE.
- 32 Pre-Delivery and Delivery Activities
- The TOE is the Archer Suite v6.9.1.2 with the Archer IRM Mobile v1.4, a software-only platform for delivering business use case workflow and reporting applications for Enterprise Risk in all its forms, via a code-free fully configurable tool. The TOE itself is comprised of software and documentation.
- 33 Software
- The TOE – Archer Suite and Archer IRM Mobile are developed in-house. The development activities of the TOE are performed at Archer facilities in Overland Park, Kansas, Bedford, Massachusetts, and Bangalore, India. The implementation representation is stored at a secure facility at the Archer headquarters. Access controls are set on the server that stores the TOE, so only authorized users are able to access it. Archer uses an automated source code configuration management system. For more detailed information, the Archer Suite 6.9.1.2 with Archer IRM Mobile v1.4 Common Criteria Configuration Management document can be referenced.
 - Before the TOE may be delivered, it must first be approved for release. In order to be approved, the TOE must undergo acceptance testing by the Archer Quality Engineering (QE) team until it successfully meets the defined acceptance criteria. The QE department, together with the project management and development teams, defines the acceptance criteria and testing methods necessary to obtain a product release. This involves defining a threshold for release of few-to-no critical or high-severity bugs and also a threshold for release with a percentage of passed tests as provided by the test cases. The testing of the TOE is

conducted throughout the development process. Early in the development process, sparse testing is conducted every night on each nightly build and QE reports the test results back to the Engineering department by 10 AM the next morning. As the product gets closer to finalization, QE begins testing fewer builds, but the testing is done in a more rigorous manner. Two weeks prior to the final release of the TOE is the final release candidate phase of testing. During these two weeks, QE tests the TOE thoroughly according to the defined acceptance criteria.

- Once the product has completed the QE testing successfully, QE approves the product for release. It then becomes the “Master” version. The 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 Archer Secure Care Online (SCOL) website. A member of the Archer 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.
- Archer IRM Mobile app is developed and it is uploaded to Play Store for Android app and uploaded to App store for iOS app. Customers can download the Archer IRM Mobile app based on the mobile operating system.
- Archer is also available as a Software as a Service (SaaS) delivery model. This allows customers to purchase licensed software that is hosted by Archer instead of purchasing the software and hosting it in-house. The SaaS Operations team places the build into the test environment and then migrates the build into production 30-45 days following General Availability (GA), depending on scheduling.
- Archer uses WinRAR as the tool to create the Archer installation package. WinRAR runs a hash function on the installation package and a value is determined. This value is sent as part of the installation package. The end user downloads a ‘md5sum’ program and generates a checksum value for the Archer file. The resulting checksum is compared with the Archer provided checksum.

If the two checksum values do not match, the downloaded file may be corrupt. If this happens, download the Archer file again and use your md5sum utility to generate another checksum value.

34 Documentation

- All guidance documentation is created and maintained in-house by the Archer Technical Publications team. The Archer Technical Publications team is located in the United States in Overland Park, Kansas and Bedford, Massachusetts. The TOE documentation is available online for the proper installation, administration, and use of the TOE.
- All guidance documentation is stored within Archer's Configuration Management (CM) documentation control system for version control. For more information, the Archer Suite 6.9.1.2 with Archer IRM Mobile v1.4 Common Criteria Configuration Management document can be referenced.
- Throughout the testing process of the TOE software, feedback is provided to the Technical Publications team about the TOE documentation. In addition, Archer's technical support and professional services teams provide feedback to the Technical Publications team about the TOE documentation. As a final review before publication, the Technical Publications team does a copy edit on the TOE documentation.
- All guidance documentation is available online and can be downloaded from the Archer Community website. Since the TOE documentation is only available via download, this is considered the entire process from manufacturing to distribution.

35 Customer Product Verification - Archer Suite 6.9.1.2

- All delivery of Archer software is done electronically. The product is either downloaded via Archer 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 Archer Community website.
- When a client either purchases the product or requests an updated license, Customer Order Management (COM) submits a request electronically through SAP, an internal customer order system, which sends a request to the License Tool (LT). The LT creates the license and key and sends them to Archer Activation Service (AAS) which is used by customers to perform online license authorization. The LT then returns the key to SAP which stores and forwards it

to Download Central (DLC). DLC then retrieves the Archer license file used for offline installations from the LT and emails the key to the customer along with instructions. If the order is for SaaS, an email is sent by the LT to archer.saas.ops@archerirm.com, once the file has been loaded into the AAS. After they have completed creation of the required instances, the Archer SaaS Ops team uses the SaaSMailer app to send emails to the customer with their sysadmin credentials, and to COM confirming the order is completed for revenue recognition.

- Once the client is successfully identified and authenticated to SCOL they are then able to access their installation package. The client is able to view the version of the software on the website where the package is downloaded. In addition, the client can view the version of the TOE once the version is installed. The communications channel while downloading the installation package is secured by SSL.

36 Customer Product Verification - Archer IRM Mobile App 1.4

- All delivery of Archer software is done electronically. The product is downloaded via Play Store for Android app or via App store for iOS App. The client must have an authorized account to be able to access the TOE Documentation on the Archer Community website.
- Once the client is successfully downloaded the App they are then able to access their Application on the Mobile device. Client can view the version of the TOE once the App is installed.

2 Evaluation

37 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 Requirement (MyCC_REQ) (Ref [4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

39 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.

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 Flaw Reporting Procedures

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

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

- 43 The evaluators have examined the flaw remediation procedures documentation and determined that it describes a means of providing the TOE users with the necessary information on each security flaw.
- 44 The evaluators have examined the flaw remediation procedures and determined that it describes procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.
- 45 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would help to ensure every reported flaw is corrected and that TOE users are issued remediation procedures for each security flaw.
- 46 The evaluators have examined the flaw remediation procedures and determined that the application of the procedures would result in safeguards that the potential correction contains no adverse effects.
- 47 The evaluators have examined the flaw remediation guidance and determined that the application of the procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

2.1.3 Development

- 48 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).
- 49 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.
- 50 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.
- 51 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.4 Guidance documents

- 52 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.
- 53 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.5 IT Product Testing

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

2.1.4.1 Assessment of Developer Tests

- 55 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

- 56 At EAL 2 Augmented ALC_FLR.2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.
- 57 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Table 3: Independent Functional Test

Test ID	Description	Security Function	Results
TEST-IND-001-GUI	<ul style="list-style-type: none"> 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 verify that secrets meet the password requirements for all users' accounts (except sysadmin and service accounts). Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. Verify that the TOE is able to restrict authorised users to perform management of TSF data functions, or to modify the behaviour of security management functions. Verify that the TSF shall allow user-initiated termination of the user's own interactive session. Verify that the TOE is able to generate an audit record for security relevant events performed by each user and provides an interface to view the audit records generated to authorised users. 	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, FIA_ATD.1.1, FIA_SOS.1.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FMT_MOF.1.1 ,FMT_SMF.1.1 FMT_SMR.1.1, FMT_SMR.1.2, FTA_SSL.4.1 , FTA_TAB.1.1	Passed

Test ID	Description	Security Function	Results
TEST-IND-002-GUI	<ul style="list-style-type: none"> • Verify that the TSF shall maintain security roles and security attributes belonging to individual users. • Verify that the TOE is able to detect when a configured amount of unsuccessful authentication attempts have occurred. • Verify that the TOE will lock the user account associated with the failed authentication attempt based on a configurable period of time, and re-authenticate a user if an interactive user session exceeds the configured Static Session Timeout value. • Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. • Verify that the TSF shall enforce rules to determine if an operation among controlled subjects/objects is allowed and authorised access of subjects to objects is allowed. • Verify that the TSF shall enforce the Discretionary Access Control SFP to restrict the ability to query/modify/delete the security attributes of an Application, Questionnaire, or Sub-form owner; field permissions; and Workspace, Dashboard, 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 	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FDP_ACC.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FIA_AFL.1.1, FIA_AFL.1.2, FIA_ATD.1.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UAU.6.1, FIA_UID.2.1, FMT_MSA.1.1, FTA_SSL.3.1, FTA_SSL.4.1	Passed

Test ID	Description	Security Function	Results
	<p>configured time interval of user inactivity has passed.</p> <ul style="list-style-type: none"> Verify that the TSF shall allow user-initiated termination of the user's own interactive session. Verify that the TOE is able to generate an audit record for security relevant events performed by each user and provides an interface to view the audit records generated to authorised users. 		
TEST-IND-003-GUI	<ul style="list-style-type: none"> Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. Verify that the TSF shall enforce rules to determine if an operation among controlled subjects/objects is allowed, and authorised access of subjects to objects is allowed, and deny access of subjects to objects for unauthorised users. Verify that the TSF shall allow the authorised user to specify alternative initial values to override the default values when an object or information is created. 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. 	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FDP_ACF.1.1, FDP_ACF.1.4, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UAU.6.1, FIA_UID.2.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_MTD.1.1 (1), FMT_MTD.1.1 (2), FMT_REV.1.1, FMT_REV.1.2, FTA_SSL.4.1	Passed

Test ID	Description	Security Function	Results
	<ul style="list-style-type: none"> Verify that the TSF shall allow user-initiated termination of the user's own interactive session. Verify that the TOE is able to generate an audit record for security relevant events performed by each user and provides an interface to view the audit records generated to authorised users. 		
TEST-IND-004-Web API	<ul style="list-style-type: none"> 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_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FMT_MTD.1.1 (2), FMT_SMF.1.1, FTA_SSL.4.1	Passed
TEST-IND-005-Content API	<ul style="list-style-type: none"> Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. Verify that the TSF shall maintain security roles and security attributes belonging to individual users. Verify that a user session will be automatically logged out after the 	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FMT_SMR.1.1, FMT_SMR.1.2, FTA_SSL.3.1	Passed

Test ID	Description	Security Function	Results
	<p>configured time interval of user inactivity has passed.</p> <ul style="list-style-type: none"> Verify the TOE is able to generate an audit record for security relevant events performed by users. 		
TEST-IND-006-RESTful API	<ul style="list-style-type: none"> Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. Verify that authorised users are able to perform management of TSF data functions, and able to modify the behaviour of security management functions. Verify that the TSF shall allow user-initiated termination of the user's own interactive session. Verify that the TSF shall deny session establishment based on a restricted date, time of day, day of the week and user IP address. 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, FAU_GEN.2.1, FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_UID.2.1, FMT_MTD.1.1 (2), FMT_SMF.1.1, FTA_TSE.1.1, FTA_SSL.4.1	Passed
TEST-IND-007-Mobile-App	<ul style="list-style-type: none"> Verify TSF shall authenticate user claimed identity depending on the authentication method chosen by the user. Verify that all users are successfully identified and authenticated based on authentication mechanisms and user attributes before allowing any other TSF-mediated actions. 	FIA_UAU.2.1, FIA_UAU.5.1, FIA_UAU.5.2, FIA_AFL.1.1, FIA_AFL.1.2, FMT_MSA.1.1, FDP_ACF.1.3, FAU_GEN.1.1,	Passed

Test ID	Description	Security Function	Results
	<ul style="list-style-type: none"> • 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 TOE users could perform assigned tasks or Advanced workflow actions via the mobile application. • 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. 	FAU_GEN.1.2, FAU_GEN.2.1	

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

2.1.4.3 Vulnerability Analysis

59 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.

60 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 equipment required for exploitation

2.1.4.4 Vulnerability testing

61 The penetration tests focused on:

- a) General network vulnerability scan
- b) Common web application vulnerability scan
- c) Insecure direct object references
- d) Mobile Application Interception
- e) Encrypted Communications
- f) Missing function level access control
- g) Content API brute-force testing
- h) Input and data validation (REST API)
- i) Source Code Review

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

2.1.4.5 Testing Results

63 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 the test conducted were PASSED as expected.

3 Result of the Evaluation

- 64 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 Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4 which is performed by BAE System Lab - MySEF.
- 65 BAE System Lab - MySEF found that Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4 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 ALC_FLR.2.
- 66 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

- 67 EAL 2 Augmented ALC_FLR.2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.
- 68 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.
- 69 EAL 2 Augmented ALC_FLR.2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

- 70 The Malaysian Certification Body (MyCB) is strongly recommended that:
- a) Potential purchasers of the TOE should consider the use of a certification authority (CA) trusted certificate, as opposed to a self-signed certificate to fully secure access to the TOE environment.

- b) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it can be suitably addressed.
- c) Potential purchasers of the TOE should ensure there are appropriate security controls in the TOE operational environment to ensure protection of the database and its stored data.
- d) Potential purchasers should consider the usage, practicality and security considerations and best practices of the mobile application before deploying it in their intended working environment.

Annex A References

A.1 References

- [1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July, 2014.
- [2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
- [3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
- [4] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.
- [5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.
- [6] Archer Suite v6.9.1.2 with the Archer IRM Mobile V1.4 Security Target, Version 1.0, 8 April 2022.
- [7] Evaluation Technical Report, Version 1.1, 13 April 2022.

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

Acronym	Expanded Term
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

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-to-day operation of an Evaluation and Certification Scheme . Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

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

--- END OF DOCUMENT ---