EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

STAR methodology

Version 1, February 2025

DOCUMENT HISTORY

Date	Version	Modification	Author’s comments
February 2025	V1	Creation	Endorsed for publication on 11/03/2025 by the ECCG

LEGAL NOTICE

LEGAL NOTICE

This publication is a state-of-the-art document as defined in Article 2 point 14 of Commission Implementing Regulation (EU) 2024/482.

This document is endorsed by the European Cybersecurity Certification Group (ECCG) in accordance with Article 48 paragraphs 2 and 3 of Commission Implementing Regulation (EU) 2024/482.

This document shall be updated whenever needed to reflect the developments and best practices in the field of the evaluation of sites. Updates of this document shall be submitted to the ECCG for endorsement.

This document shall be read in conjunction with Regulation (EU) 2019/881, the Commission Implementing Regulation (EU) 2024/482, its annexes, and where applicable supporting documentation that is made available.

This document is made publicly accessible through the EU cybersecurity certification website and is free of charge.

ENISA is not responsible or liable for the use of the content of this document. Neither ENISA nor any person acting on its behalf or on behalf of the maintenance of the scheme is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

CONTACT

Feedback or questions related to this document can be sent via the European Union Cybersecurity Certification website (https://certification.enisa.europa.eu/index_en).

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE

This state-of-the-art document as defined under Article 2 point 14 of Regulation (EU) 2024/482 is a supporting document under Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC).

The assurance class ALC "Life-cycle support" is addressing the aspect of establishing appropriate security controls and mechanisms at the developer's sites for the development, production, delivery and maintenance of the TOE. For some ALC assurance components (in particular for high assurance evaluations) the evaluator activities for this class usually include an on-site evaluation of these security controls and mechanisms. The security controls and mechanisms documented and implemented by the site are often applicable to other TOEs of the same developer and also from other developers, especially where the TOE follows the same life-cycle support processes.

The ability to transfer the evaluation evidences and results of the ALC class that are achieved e.g., for an initial TOE to other (similar) TOEs and other ITSEFs or CBs reduces the effort of the developers, ITSEFs and CBs by removing duplicate activities and makes subsequent evaluation processes more efficient. Hereby, the ITSEF making re-use of ALC evaluation evidences and results already gained shall be able to demonstrate the assurance for the ALC class in the context of the re-using TOE. The information available in certification reports is insufficient for this transfer purpose as more detailed information about ALC-related evaluation evidences and results and in particular accompanying site audits is needed by the re-using ITSEF for its fulfilment of evaluation activities. The "Site Technical Audit Report" (STAR) is designed to contain and provide the necessary information to support re-use of ALC-related evaluation evidences and results across (similar) TOEs and between ITSEFs and CBs.

The objective of the present document is to set up a framework, formal process and methodology surrounding the STAR that supports harmonization between the CBs and ITSEFs under the EUCC Scheme for the re-use of results achieved in the framework of ALC evaluation activities. Such harmonization will allow, in particular:

- to conduct a site audit by an ITSEF under control of one CB,
- to clearly define the STAR validity period,
- to efficiently re-use the results of such site audit by another ITSEF under control of another CB within a product certification procedure.

1.2 NORMATIVE REFERENCES

Regulations

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Implementing Regulation (EU) 2024/482 on establishing the Common Criteria-based cybersecurity certification scheme (EUCC)[1], as amended by Implementing Regulation 2024/3144.

Standards

Note: Unless otherwise specified, the versions of the Common Criteria and Common Evaluation Methodology standards defined in Article 2 of the EUCC scheme apply.

[1] Available at http://data.europa.eu/eli/reg_impl/2024/482/oj

EUCC state-of-the-art documents[2]

Note: Unless otherwise specified, the latest version of referenced state-of-the-art documents applies.

Minimum Site Security Requirements (MSSR)

1.3 ACRONYMS

CAB	Conformity assessment body
CB	Certification body
CC	Common Criteria for Information Technology Security Evaluation as defined the EUCC
CEM	Common Methodology for Information Technology Security Evaluation as defined the EUCC
CSA	Cybersecurity Act
EAL	Evaluation Assurance Level
EC	European Commission
ENISA	European Union Agency for Cybersecurity
ETR	Evaluation technical report
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and communications technology
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information technology
ITSEF	Information Technology Security Evaluation Facility
ST	Security target
STAR	Site Technical Audit Report
TOE	Target of evaluation
TS	Technical specification
TSFI	TOE security function interfaces

[2] Available at https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

2. STAR METHODOLOGY

2.1 SCOPE OF THE METHODOLOGY

The present document in its current version is explicitly bound and restricted to physical audits.

2.2 CONTEXT OF USE

A first ITSEF (hereinafter called ITSEF-1) has performed all required ALC evaluation activities under EUCC validated by a CB (hereinafter called CB-1). The Site Technical Audit Report (STAR) produced by ITSEF-1 and approved by CB-1 contains the minimum information for re-use of the ALC related evaluation results (including site audit). A second ITSEF (hereinafter called ITSEF-2) wants to re-use these ALC related evaluation results for a TOE evaluation under EUCC together with a CB (hereinafter called CB-2).

2.3 STAR OWNER

The STAR owner is ITSEF-1. Sharing of the STAR shall be authorised by the body which had requested the site audit.

2.4 CONTENT OF THE STAR

EUCC guidelines for a STAR template supporting this state-of-the-art document should be established to present all information elements a STAR should contain and to describe the minimum set of required information to establish the extent for re-use of already achieved ALC evaluation results for a site in subsequent certification procedures.

2.5 STAR CREATION DATE

The creation date of a STAR shall be the related initial (i.e., first) audit date.

The ALC-related evaluation activities for a site are accompanied by corresponding audit activities. It might be useful or necessary respectively to perform those audit activities in several audits' events, in particular it might happen that the resolution of audit findings is examined within a subsequent audit. However, relevant for the STAR creation date is the first audit event in that set of audits.

2.6 STAR VALIDATION AND APPROVAL

An initial STAR corresponds to the initial audit and its results. It shall provide a record of the initial audit and include all identified findings as observations of type major non-conformities and minor non-conformities. Hereby, an audit finding is classified as “major non-conformity” if the identified issue depicts the non-fulfilment of the ALC-related evaluation criteria, whereas an audit finding of category “minor non-conformity” addresses a slight deficiency in the fulfilment of the ALC-related evaluation criteria without any severe security impact and that could be solved by improvement.

The developer, ITSEF-1 and CB-1 shall strive to agree during the site audit or immediately afterwards on the planning how the developer intends to resolve the identified deficiencies, and how the developer will provide corresponding evidence about start and completion of each correction and/or mitigation. A corresponding acceptable action plan serves for the identification of the corrective and/or mitigation actions with associated deadlines.

While working on the resolution of the identified findings according to the action plan, the progress of the corrective and/or mitigation actions shall be monitored and the STAR continuously be maintained. However, the STAR shall remain in a preliminary status until:

- CB-1 approves all findings (of any type) and related actions have been suitably closed, or;
- CB-1 approves all findings of type major non-conformities and related actions have been suitably closed or re-categorized as minor non-conformities, and CB-1 together with the developer and ITSEF-1 agrees upon an acceptable action plan for the remaining minor non-conformities.

In case of an action plan, ITSEF-1 shall verify the complete and suitable implementation during a subsequent suitable verification process in timely manner and inform CB-1 about the results correspondingly.

The STAR content shall be validated and approved by CB-1. Only a complete STAR version without any open site audit issues of type major non-conformities shall be delivered to CB-1 for validation and approval. However, this final STAR shall list all open remaining audit issues of type minor non-conformities, if any. The delivery of the STAR to CB-

1 opens the validation process, whereby validation means that CB-1 determines that the STAR is a correct and consistent subset of the full audit report written by ITSEF-1 and validated previously by CB-1. The approval of the STAR means acceptance of that STAR by CB-1 and defines the beginning of the validity period from which on the STAR for the site can be re-used for other evaluation/certification procedures.

Delivery, validation and approval of a STAR during an ongoing certification procedure is optional, and validation and approval of the STAR are not bound to the finalisation of that certification procedure[3].

Note: Prerequisite for the approval of a STAR is that all required ALC evaluation activities are performed and the final resolution of any identified findings is achieved in the sense of that no open audit issues of type major non-conformities exist and, if applicable, an acceptable action plan for minor non-conformities is agreed upon.

2.7 STAR VALIDITY

The STAR shall only be considered valid after approval by CB-1, in accordance with previous section that provides details on validation and approval. Only a valid STAR is allowed to be re-used in subsequent certification procedures.

The time period from the initial audit to the approval by CB-1 should not be longer than 6 months. At this time potentially a re-audit may be required. The decision for such re-audit is with the CB.

The approval date set by the CB-1 holds as the first day of the site approval and validity of the STAR. The approval date might be directly displayed in the STAR document itself (e.g., by incorporation of the approval date by ITSEF-1 on behalf of CB-1), or alternatively recorded in a separate approval sheet that is provided by CB-1 and linked to the STAR document.

CB-1 shall establish the end date validity of the STAR, that shall not exceed 30 months starting from the initial audit date.

2.8 STAR RE-USE

For a certification procedure, re-use of already achieved ALC related evaluation results for a site might be of interest for ITSEF-2 whereby such re-use may be intended to be supported by a corresponding valid STAR. It is the responsibility of ITSEF-2 to explain to its CB-2 why and how such re-use of those ALC results (including site audit) as outlined in the related STAR can be performed. The developer of the TOE under evaluation by ITSEF-2 is responsible to provide information to ITSEF-2 on how the site is integrated in the TOE life-cycle. Based upon this information ITSEF-2 shall determine whether re-use is possible and if so explain that to its CB-2.

An official validation and approval of the STAR by CB-1 is required to allow for re-use of the already achieved ALC related evaluation results addressed and covered by that STAR. Hereby, two cases for a STAR may occur:

- Official validation and approval by CB-1 already available: nothing to be done for permission of re-use of the STAR;
- Official validation and approval by CB-1 not (yet) available: ITSEF-2 contacts ITSEF-1, and ITSEF-1 informs ITSEF-2 when the validation and approval of the STAR by CB-1 is available; re-use of the STAR is permitted only in case approval of the STAR granted by CB-1.

In any case, for re-use of the STAR, ITSEF-2 shall check the authenticity of the STAR and its approval date granted by CB-1. Hereby, corresponding evidence for such authenticity is to be provided by CB-1. This can be achieved e.g. directly by an authenticity evidence provided on the CB-1’s website or within a certification report of a related completed certification procedure, or by contact to CB-1 for performing that authenticity check.

[3] This does not exclude early re-use of a STAR in non-final status for such other evaluation/certification procedures, e.g. to support preparatory steps. However, approval of the STAR is required for its “official” re-use in the sense of the present STAR methodology.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu