|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Angaben zur Konformitätsbewertungsstelle (KBS)** | | | | | |
| Prüflaboratorium gemäß DIN EN ISO/IEC 17025 für eine Notifizierung nach VO 2019/881 Artikel 61 | | | | | |
| Zertifizierungsstelle gemäß DIN EN ISO/IEC 17065 für eine Notifizierung nach VO 2019/881 Artikel 61 | | | | | |
| Name der KBS: |  | | | | |
| Aktenzeichen: |  |  |  | | |
| Verfahrensnummer | Phase |  | | |
| Datum Begutachtung: |  | | | | |
| Begutachtungsvorgang: |  | | | | |
| Begutachtungstyp[[1]](#endnote-1): |  | | | | |
| KBS mit mehreren Standorten: | | | | Ja | Nein |
| Name / Anschrift begutachteter Standorte: | | | | | |

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
| **Angaben zum Begutachter** | | |
| Name: |  | |
| Status[[2]](#endnote-2): | SB | FB |
| **Gegenstand der Begutachtung** (Detaillierte Darstellung mit Angabe der Quellen der sektoralen Anforderungen) | | |

|  |
| --- |
|  |

Zusätzlich zum Bericht gemäß DIN EN ISO/IEC 17025 für Prüflaboratorien bzw. gemäß DIN EN ISO/IEC 17065 für Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen werden mit dieser Checkliste/diesem Bericht die speziellen Kriterien[[3]](#endnote-3) für Stellen, die an der Bewertung und Überprüfung von Produkten mit digitalen Komponenten, die entsprechend der VO 2019/881 zertifiziert werden, abgebildet.

**Die Checkliste enthält lediglich die speziellen Anforderungen des Cyber Security Acts und die durch delegierte Rechtsakte erlassenen Zusatzanforderungen, nicht die reinen Querverweise auf die grundlegende Akkreditierungsnormen DIN EN ISO/IEC 17025 bzw. DIN EN ISO/IEC 17065.**

**Werden die Prüftätigkeiten durch die Zertifizierungsstelle selbst durchgeführt, müssen in Teil II dieses Berichts beide Bereiche (Teil IIa und Teil IIb) ausgefüllt werden.**

Diese Checkliste/dieser Bericht wiederholt **NICHT** die bereits im Bericht zur DIN EN ISO/IEC 17025 bzw. DIN EN ISO/IEC 17065 aufgeführten objektiven Nachweise (ON) und eingesehenen Dokumente (ED) oder Text­passagen und Beschreibungen zu Abweichungen. Der zuständige Begutachter KANN jedoch ergänzende Dokumente und Anmerkungen notieren.

Im Interesse der Lesbarkeit wird grundsätzlich die männliche Form von Funktionsbezeichnungen verwendet; dies schließt die weibliche Form ein.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Teil Ia** | **Allgemeine Anforderungen für Zertifizierungsstellen und ITSEFs nach Anhang I des Cyber Security Acts** |  |  |  |  |  |
| Organisation | | | | | | |
| 1 | Eine KBS muss nach nationalem Recht gegründet und mit Rechtspersönlichkeit ausgestattet sein. |  |  |  |  |  |
| 2 | Bei einer KBS muss es sich um einen unabhängigen Dritten handeln, der mit der Einrichtung oder den IKT-Produkten, -Diensten oder -Prozessen, die er bewertet, in keinerlei Verbindung steht.  **Anmerkung: Siehe hierzu auch Teil 2 Zusatzanforderungen für ITSEFs für spezifsiche Interpretationen des Schemeowners** |  |  |  |  |  |
| 3 | Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte, -Dienste  oder -Prozesse bewertet, an deren Entwurf, Herstellung, Bereitstellung, Montage, Verwendung oder Wartung Unternehmen beteiligt sind, die von diesem Verband vertreten werden, kann als KBS gelten, sofern ihre Unabhängigkeit sowie die Abwesenheit jedweder Interessenkonflikte nachgewiesen sind. |  |  |  |  |  |
| 4 | Die KBS, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungs­betrieb des zu bewertenden IKT-Produkts, -Dienstes  oder -Prozesses noch Bevollmächtigter einer dieser Parteien sein. Dieses Verbot schließt nicht die Verwendung von bereits einer Konformitätsbewertung unterzogenen IKT-Produkten, die für die Tätigkeit der KBS nötig sind, oder die Verwendung solcher IKT-Produkte zum persönlichen Gebrauch aus. |  |  |  |  |  |
| 5 | Die KBS, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder direkt an Entwurf, Herstellung bzw. Bau, Vermarktung, Installation, Verwendung oder Instand­setzung dieser IKT-Produkte, -Dienste oder -Prozesse beteiligt sein, noch die an diesen Tätigkeiten beteiligten Parteien vertreten. Die KBS, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit ihren Konformitäts­bewertungstätigkeiten, beeinträchtigen können. Dieses Verbot gilt besonders für Beratungsdienste. |  |  |  |  |  |
| 6 | Falls eine KBS Eigentum einer öffentlichen Stelle oder Einrichtung ist oder von dieser betrieben wird, sind die Unabhängigkeit und die Abwesenheit von Interessenkonflikten zwischen der nationalen Behörde für die Cybersicherheits­zertifizierung und der sicherzustellen und zu dokumentieren. |  |  |  |  |  |
| 7 | Die KBSn müssen sicherstellen, dass die Tätigkeiten ihrer Zweigunternehmen oder Unterauftragnehmer die Vertraulichkeit, Objektivität oder Unparteilichkeit ihrer Konformitätsbewertungstätigkeiten nicht beeinträchtigen. |  |  |  |  |  |
| 8 | Die KBS und ihre Mitarbeiter müssen die Konformitäts­bewertungstätigkeiten mit höchster beruflicher Integrität und der erforderlichen fachlichen Kompetenz in dem betreffenden Bereich durchführen; sie dürfen keinerlei Einflussnahme durch Druck oder Vergünstigungen, auch finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse ihrer Konformitätsbewertungsarbeit auswirken könnte, insbesondere keinem Druck und keiner Einflussnahme durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben. |  |  |  |  |  |
| 9 | Eine KBS muss in der Lage sein, die bei der Konformitäts­bewertung anfallenden Aufgaben, die ihr mit dieser Verordnung übertragen wurden, auszuführen, unabhängig davon, ob diese Aufgaben von ihr selbst oder in ihrem Namen und unter ihrer Verantwortung ausgeführt werden. Jegliche Unterauftragsvergabe oder die Inanspruchnahme von externem Personal sind angemessen zu dokumentieren, dürfen nicht über Vermittler erfolgen und bedürfen einer schriftlichen Vereinbarung, in der unter anderem Vertraulichkeitsaspekte und Interessenkonflikte geklärt werden. Die betreffende KBS übernimmt die volle Verantwortung für die durchgeführten Aufgaben. |  |  |  |  |  |
| 10 | Eine KBS muss jederzeit, für jedes Konformitätsbewertungs­verfahren und für jede Art, Kategorie und Unterkategorie von IKT-Produkten -Diensten oder -Prozessen über Folgendes verfügen:   * 1. das erforderliche Personal mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;   2. Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt wird, um sicherzustellen, dass die Verfahren transparent sind und wiederholt werden können. Sie muss über angemessene Regelungen und Verfahren verfügen, bei denen zwischen den Aufgaben, die sie als nach Artikel 61 notifizierte Stelle wahrnimmt, und ihren anderen Tätigkeiten unter­schieden wird; L 151/68 Amtsblatt der Europäischen Union 7.6.2019 DE   3. Verfahren zur Durchführung von Tätigkeiten, bei denen die Größe eines Unternehmens, die Branche, in der es tätig ist, seine Struktur, der Grad an Komplexität der jeweiligen Technologie der ICT-Produkte, -Dienste  oder -Prozesse und der Umstand, dass es sich um Massenfertigung oder Serienproduktion handelt, gebührend berücksichtigt werden. |  |  |  |  |  |
| 11 | Eine KBS muss über die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben verfügen, die mit der Konformitätsbewertung verbunden sind, und Zugang zu allen benötigten Ausrüstungen und Einrichtungen haben. |  |  |  |  |  |
| 12 | Die Personen, die für die Durchführung der Konformitäts­bewertungstätigkeiten zuständig sind, müssen Folgendes besitzen:   1. eine solide Fach- und Berufsausbildung, die alle Tätigkeiten der Konformitätsbewertung umfasst; 2. eine ausreichende Kenntnis der Anforderungen, die mit den durchzuführenden Konformitätsbewertungen verbunden sind, und die entsprechende Befugnis, solche Bewertungen durchzuführen; 3. angemessene Kenntnis und angemessenes Verständnis der geltenden Anforderungen und Prüfnormen; 4. die Fähigkeit zur Erstellung von Bescheinigungen, Protokollen und Berichten als Nachweis für durchgeführte Konformitätsbewertungen |  |  |  |  |  |
| 13 | Die Unparteilichkeit der KBSn, ihrer obersten Führungsebene, des für Bewertungen zuständigen Personals der KBS und ihrer Unterauftragnehmer muss gewährleistet sein. |  |  |  |  |  |
| 14 | Die Vergütung für die oberste Leitungsebene und das für Bewertungen zuständige Personal der KBS darf sich nicht nach der Anzahl der durchgeführten Konformitätsbewertungen oder deren Ergebnissen richten. |  |  |  |  |  |
| 15 | Die KBS müssen eine Haftpflicht­versicherung abschließen, sofern die Haftpflicht nicht aufgrund des nationalen Rechts vom Mitgliedstaat übernommen wird oder der Mitgliedstaat selbst unmittelbar für die Konformitätsbewertung verantwortlich ist. |  |  |  |  |  |
| 16 | Die KBS und ihre Mitarbeiter, Gremien, Tochterunternehmen, Unterauftragnehmer und alle verbundenen Stellen oder Mitarbeiter externer Gremien einer KBS müssen die Vertraulichkeit wahren, und die Informationen, die sie bei der Durchführung ihrer Konformitätsbewertungsaufgaben nach dieser Verordnung oder nach einer nationalen Vorschrift zur Durchführung dieser Verordnung erhalten, fallen unter die berufliche Schweigepflicht, außer wenn eine Offenlegung aufgrund von Rechtsvorschriften der Union oder des Mitgliedstaats, denen diese Personen unterliegen, erforderlich ist und außer gegenüber den zuständigen Behörden der Mitgliedstaaten, in denen sie ihre Tätigkeiten ausüben. Die Rechte des geistigen Eigentums sind zu schützen. Die KBS muss über dokumentierte Verfahren in Bezug auf die Anforderungen dieser Nummer verfügen. |  |  |  |  |  |
| 17 | Abgesehen von Nummer 16 schließen die Anforderungen dieses Anhangs in keiner Weise der Austausch von technischen Informationen und regulatorischen Leitlinien zwischen einer KBS und einer Person, die eine Zertifizierung beantragt oder deren Beantragung in Erwägung zieht, aus. |  |  |  |  |  |
| 18 | KBS müssen ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter und angemessener Geschäfts­bedingungen ausüben, wobei sie in Bezug auf Gebühren die Interessen der KMU berücksichtigen. |  |  |  |  |  |
| 19 | Die KBS müssen die Anforderungen der einschlägigen Norm erfüllen, die gemäß der Verordnung (EG) Nr. 765/2008  für die Akkreditierung der KBS, die die Zertifizierung von  IKT-Produkten, -Diensten oder -Prozessen vornehmen, harmonisiert ist. |  |  |  |  |  |
| 20 | Die KBS müssen sicherstellen, dass die für die Konformitäts­bewertung eingesetzten Prüflabors den Anforderungen der einschlägigen Norm entsprechen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Labors, die Tests durchführen, harmonisiert ist. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Teil IIa** | **Spezifische Zusatzanforderungen an ITSEFs** |  |  |  |  |  |
| 6 | [General] The requirements for the competence of testing  and calibration laboratories defined in ISO/IEC 17025:2017 complemented by the requirements defined in ISO/IEC TS 23532-1:2021. |  |  |  |  |  |
| 6.2.1 | **Independence**  The independence criteria from CSA Annex point 2 shall apply to the ICT product, ICT process, ICT service under evaluation.  The ITSEF shall inform its clients of any activity of its legal entity including being a designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process that might be related to the type of products of the clients. |  |  |  |  |  |
| 6.2.2 | **Impartiality**  ISO/IEC 17025:2017, “4.1 Impartiality”  The ITSEF must ensure a strict separation of its responsibilities to maintain impartiality. This can be achieved within the same legal entity by meeting the requirements of EN ISO/IEC 17025 for impartiality. Additionally, an ITSEF is required to implement an ongoing risk analysis process to continuously assess its risks. The following list of activities (which builds on EA-2/20 G: 2020) of the ITSEF shall not be considered as “consultancy”:  a) Preparation of evaluation documentation and evidence in accordance with the rules defined in Annex B ‘Collection of developer evidence’.  b) Providing general training or guidance on best practices and state-of-the-art, under the following condition:  - This activity shall exclude recommendations regarding the implementation of a specific architecture or mechanism.  c) Providing technical analysis of product failures (including vulnerabilities), under the following conditions:   * The scope shall be clearly presented in the contract; * The delivery of the activity shall be limited to diagnosis; * The ITSEF personal shall commit to not recommend solutions and this commitment shall be recorded by the ITSEF   d) Participation to R&D projects, studies and to the maintenance of the EUCC scheme related to or emcompassing the categories of ICT products and technologies for which the ITSEF is accredited (e.g.: high level study into general market/design/production trends within the overall sector, feasibility studies on certification schemes reusing EUCC certification, mapping between EUCC certification and other regulations, participation to the definition and update of EUCC state-of-the-art documents and guidance), under the condition that:   * The ITSEF shall allow the results to be made publicly available   e) Development of tools for certification activities (e.g.: tools to support the development of PPs or STs, test benches, code review tools), including the possibility to register a patent and/or a user licence for it), under the conditions that:   * The ITSEF shall establish an analysis before project launch in order to verify there is no impact on conformity assessment or on assessed parties which might be competitors; * The activity shall relate to the complete sector, and shall neither be for the ITSEF nor for an individual industrial, and the ITSEF shall provide collective and transparent communication; * There shall not be subsequent certification of a ICT product related to a patent; * There shall not be any user licence resulting to collective certification.   f) Delivery of services that could be conformity assessment but out of the accreditation scope with regard to notification (e.g. Common Criteria assessment of a product outside EUCC certification process for national security purpose).  g) Development of a test protocol (e.g.: development of a test bed to develop ITSEFs’ and/or CBs’ skills or to support and/or monitor their accreditation or authorisation), under the conditions that:   * The validation of the method shall satisfy the requirements of ISO/IEC 17025; * The ITSEF shall provide a generic test or inspection protocol, publicly available, or; * The ITSEF may only provide a specific test or inspection protocol that is non publicly available for the benefit of evaluation and certification activities outside of its scope of accreditation.   Where an activity is considered as acceptable with conditions, the ITSEF shall demonstrate the fulfillment of conditions and provide detailed proofs of this to the NAB. |  |  |  |  |  |
| 6.2.3. | **Confidentiality**  EUCC, “24.2 SECURITY OF INFORMATION” ISO/IEC 17025:2017, “4.2 Confidentiality” Additional requirement to ISO/IEC TS 23532-1:2021, 4.2.6  The exclusions indicated by ISO/IEC TS 23532-1:2021 4.2.6 need to be noted and justified in the ETR to the responsible CB. If the responsible CB considers that access to this information is relevant to perform the certification decision, it can be a cause for rejecting the requested certificate.  The ETR for composition needs to include all information necessary for the composition, it has to be technically relevant, while taking into account the confidentiality of sensitive information.  Additional requirement to ISO/IEC TS 23532-1:2021, 4.2.8  The scope of the policies, procedures and security manual to ensure the protection of proprietary information shall also cover and protect the following:   1. Handling of personal data, where applicable. 2. Information necessary for  * the effective implementation of the EUCC scheme, in particular for the purpose of accreditation assessments, * effective collaboration between the involved authorities and bodies, * the handling of publicly unknown and subsequently detected vulnerabilities in the TOE in the process of, or after certification, and * the handling of complaints.  1. The case of subcontracting, and in the situation where the ITSEF uses other facilities (e.g., third parties independent of both the ITSEF and the company(ies) developing and producing the TOE), appropriate security measures shall be applied to protect the vendor’s information and samples as well as the relevant the know-how and evaluation and testing approaches and their results of the ITSEF. 2. Protection under scenarios of unavailability or lack of accessibility of the ITSEF main location, remote evaluation activities, both from home-office of the evaluators, or from the manufacturer site. 3. The ITSEF should ensure that information that is required by a user or users (i.e. those accessing the evaluation information) for a short period, is retrievable when this period expires. 4. The ITSEF shall implement mechanisms that allow setting a fixed duration for users’ access to confidential information. 5. Confidential information that requires temporary access to be given to a set of users to perform a specific task such as assessments from NABs should not be permanently handed to the possession such temporary users. They should only have access for the duration of the activity. 6. Confidential information about an evaluation activity should be restricted to the ITSEF staff involved in the specific evaluation activity.   In particular, the policies, procedures and security manual to ensure the protection of proprietary information shall also cover and include the following measures:   1. The information system shall include tools that provide encryption functionalities for non-public Information at rest. These tools should be referenced by an ENISA or a National guidance document. Encryption tools that are deployed for security of information are expected to be in compliance with, by order of precedence:  * EU and national regulation regarding the protection of sensitive information, * recommendations, guidance and opinions from the competent cybersecurity authorities of the member state, * recommendations from the ECCG.  1. Secure electronic storage and communication must be achieved for non-public Information through accepted and recognised cryptographic methods and algorithms. The ITSEF shall refer to and comply with ENISA or National cryptography guidelines for further guidance. 2. ITSEF staff shall be trained on information handling and sign agreements of compliance with information security obligations to maintain data secrecy. The ITSEF shall keep these agreements as per Retention of records.   Every staff member shall sign an NDA before he/she is granted access to non-public information. In governmental organizations where there are binding legal regulations on information secrecy, these rules shall be leading, unless they interfere with EU law. The ITSEF shall maintain a updated information security workshop schedule for staff involved in the EUCC scheme process. The workshop shall be performed on a regular basis and include updates on relevant regulatory changes.  Evaluation contracts between ITSEFs and their customers shall identify which parties will have access to the evaluation evidence and findings that are part of the certification process and that have for the purpose of certification and certification maintenance of the ICT product and compliance, a need-to-know right, subject to accreditation assessments and/or other scheme defined processes and procedures. The CB, the NAB where necessary for the purpose of accreditation, and the NCCA where necessary for the purpose of it’s monitoring and supervision tasks, shall be informed about these contract obligations. |  |  |  |  |  |
| 6.2.4 | **Competence**  The ITSEF, their evaluators and, if applicable, the relevant staff of their subcontracted partiess shall be required to have the necessary expertise and experience in performing the specific testing activities to determine the product’s resistance against specific attacks (penetration testing).  The ITSEF shall define and operate a competence management system for the evaluators where:   * The elements of competence, competency levels and the measurement of the elements of competence are drawn from ISO/IEC 19896-1:2018, and if they differ, they shall be commensurate with the objectives that are defined and at least be equivalent to the elements defined by ISO/IEC 19896-1:2018. The ITSEF needs to demonstrate this. * The knowledge, skills, experience and education, and the applicable requirements for the evaluators are drawn from ISO/IEC 19896-3:2018, and if they differ, they shall be commensurate with the objectives and be at least equivalent to the requirements defined by ISO/IEC 19896-3:2018. The ITSEF needs to demonstrate this. * The knowledge required for evaluating security assurance requirement classes is specified based on Annex B of ISO/IEC 19896-3:2018. * The knowledge required for evaluating security functional requirement classes is specified based on Annex C of ISO/IEC 19896-3:2018. * The knowledge required for evaluating specific technologies and exercising different evaluation technique types are to be specified by the ITSEF using the classification provided in Annex (SoA ITSEF).   The ITSEF may use other classification criteria, as long as it can be mapped to the one provided in Annex. Such mapping, and the supporting rationale, shall be made available to the CB the ITSEF is subcontracted with, the NABs and NCCA. |  |  |  |  |  |
| 6.2.5 | **Facilities**  Additional requirement to ISO/IEC TS 23532-1:2021, 6.3.1.1  Network isolation must ensure the integrity of the test results and their confidentiality. |  |  |  |  |  |
| 6.2.6 | **Subcontracting**  EUCC, “7. NOTIFICATION AND AUTHORISATION OF CABS, FUNCTIONING OF CABS AND SUBCONTRACTORS”  ISO/IEC 17025:2017, “6.6 Externally provided products and services”  The ITSEF shall operate according to defined procedures ensuring that:   * The use of a subcontracted third-party facility is outlined in the evaluation plan, approved by the manufacturer or provider and by the CB and compliant with the obligations under the CSA, Annex 1 of the CSA and the EUCC while the ITSEF remains responsible for the work done. The subcontacted third-party shall be subject to the accreditation procedure for the subcontracted tasks it is performing; * If the ITSEF uses equipment at a third-party facility as specified in the sub-contracting, the evaluator shall be present and instruct the equipment operating personnel. To instruct the operating personnel, evaluators shall have the required knowledge of the subcontract with the third-party, the TOE, the equipment, and the purpose and scope of the evaluation. |  |  |  |  |  |
| 6.2.7 | **Non-Compliance**  EUCC, “13. RULES RELATED TO NON-COMPLIANCE”  The ITSEF shall support the CB’s, for which it performed evaluation activities, in their handling of non-compliances in the conditions under which the evaluation of the certification takes place, by defining and operating a process where:   * They identify within the scope of their tasks potentially impacted certified ICT products, from those TOEs evaluated by the ITSEF that contributed to the certification of the ICT product. * They perform where deemed necessary by the CB, or at the discretion of the NCCA, a series of re-evaluation tasks on one or more certified ICT products. * If the ITSEF that performed evaluation activities on behalf of a certified product, proves to be non-compliant, the NCCA handling the non-compliance with the responsible CB may appoint an other supporting ITSEF to perform certain evaluation activities. |  |  |  |  |  |
| 6.2.8 | Retention of Records  EUCC, “15. RETENTION OF RECORDS BY A CAB”  ISO/IEC 17025:2017, “7.5 Technical records”,  “8.4 Control of records”  The record system shall include all records and other related documents produced in connection with each evaluation; the recording shall be updated, accurate and complete to enable the course of each evaluation to be traced and reproduceable.  All records shall be securely and accessibly stored for a period of at least five (5) years after the final date of the certificate validity, with the exception of running investigations related non-compliance and complaint handling and their respective legal remedy procedures.  All records related to the handling of non-compliances and/or complaints not related to the evaluation shall be kept for a period of at least five (5) years after the non-compliance and/or complaint was handled and all related (legal) procedures are closed.  In case a different expiration date of the certificate has been attributed in accordance with the conditions of Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES of the EUCC, it shall be taken into account for the new calculation of the retention period of the records, with the same rules in this section.  New or revised information related to the activities described under Chapter 12, CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES of the EUCC shall be added to the previous records for the evaluation. |  |  |  |  |  |
| 6.2.9 | **Ensuring the validity of results**  ISO/IEC 17025:2017, “7.7.2 Monitoring of laboratory performance”  This clause requires that a laboratory shall monitor its performance by comparison with the results of other laboratories. In particular, the ITSEF needs to demonstrate that it is having a planning and where already the benchmarking is performed a demonstrated proof of participation and result report.  Further guidance is needed how to apply this requirement on CC laboratories, also to ensure a level playing field within Europe. |  |  |  |  |  |
| 6.2.10 | **Management System documentation**  ISO/IEC 17025:2017, “8.2 Management system documentation (Option A)”  Additional requirement to ISO/IEC TS 23532-1:2021, 8.2.8  Procedures for evaluation should be written with a level of detail that would allow a technical competent evaluator to perform the evaluation without further guidance. |  |  |  |  |  |
| 6.2.11 | **Quality process** EUCC, “11. RULES FOR MONITORING COMPLIANCE” ISO/IEC 17025:2017, “8.8 Internal audits”  The management process of the ITSEF shall explicitly ensure conformity with all the applicable requirements and obligations of the EUCC, including the requirements associated to handle complaints. |  |  |  |  |  |
| 6.2.12 | **Composite evaluations**  EUCC, “8. SPECIFIC EVALUATION CRITERIA AND METHODS”  The ITSEF shall operate according to defined procedures that ensure that, where an ICT product undergoes a composite product evaluation, necessary including where needed sensitive information that is reused from the initial evaluation is provided to the ITSEF performing the composite evaluation. This information shall be shared in the form of an evaluation technical report (ETR) for composition, based on the template provided by ENISA.  The information sharing in the case of composite evaluation must take place in full cooperation between the CBs, i.e. the CB that has certified the base component and the one handling the composite evaluation.  Besides the relevant documentation which should be exchanged, there must exist a communication channel between all involved parties to clarify technical problems. All parties/bodies, esp. the ITSEF which is responsible for the composition ETR must support this approach. |  |  |  |  |  |
| 6.2.13 | **Monitoring compliance**  EUCC, “11. RULES FOR MONITORING COMPLIANCE”  Monitoring compliance of certified ICT products with the requirements of the European cybersecurity certificates: Manufacturers, developers and any other holders of a cybersecurity certificate shall have procedures and processes in place that allow to demonstrate their continued compliance with the specified cybersecurity requirements under their certification.  The CB must carry out an assessment of the criticality of the reported irregularities with the support of the ITSEF if necessary.  To support compliance monitoring, ITSEFs shall define a set of compliance monitoring processes that ensure that, for TOEs evaluated by the ITSEF:   * They carry out an active cybersecurity-oriented technology watch, and keep themselves informed and continuously updated on the main discovered vulnerabilities and attack techniques relevant to their scope of assessment, * They systematically carry out a search for publicly known vulnerabilities in connection with the products being assessed, * They report to their CB any vulnerability they are aware of that affects the compliance of a certified ICT product with the certification requirements, in accordance with the provisions of the EUCC scheme, * They support the CB, and upon request the NCCA, in the implementation of their compliance monitoring obligations and processes.   The ITSEF of a certified ICT product shall be involved by the NCCA in monitoring activities, where the NCCA deems it necessary.  The monitoring activity may under circumstances consist, among other things, in the re-assessment of the ICT product by the ITSEF upon request of the CB, accompanied - if necessary - by an audit subject to the monitoring activities (for example compliance of the complaints procedure, events of a security incident, …). |  |  |  |  |  |
| 6.2.14 | **Patch Management**  EUCC, “12. CONDITIONS FOR ISSUING, MAINTAINING, CONTINUING AND RENEWING CERTIFICATES”  EUCC, “41. ANNEX 15: PATCH MANAGEMENT”  Among the evaluation services related to ICT product certification that the ITSEF provides, patch management may be included upon request by the applicant. Patch management is associated to vulnerability handling and may also be used for the maintenance activities of certificates.  The ITSEF shall provide such services based on defined procedures and methods that ensure their conformity with the requirements laid out for ITSEFs in Annex II Article II.4 of the EUCC Regulation. |  |  |  |  |  |
| **Teil IIb** | **Zusatzanforderungen an Zertifizierungsstellen** | | | | | |
| 8.2.1 | **Independence**  The independence criteria from CSA Annex point 2 shall apply to the ICT product, ICT process, ICT service under evaluation.  The CB shall inform its clients of any activity of its legal entity including being a designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process that might be related to the type of products of the clients. |  |  |  |  |  |
| 8.2.2 | **Certification body personnel**  [ISO/IEC 17065:2012], 6.1 Certification body personnel  [ISO/IEC 17065:2012], 6.1.2 Management of competence for personnel involved in the certification process  The CB shall establish, implement and maintain a procedure for management of competencies of certifiers where:   * The elements of competence, competency levels, knowledge, skills, experience and education shall comply with the specific requirements for certifiers brought by the revision of ISO/IEC 19896, once available; * The knowledge required for certifying specific technologies and exercising different evaluation technique types are to be specified by the CB using the classification provided in Annex I, Technology and evaluation technique types.   The CB may use other classification criteria, as long as it can be mapped to the one provided in Annex I, Technology and evaluation technique types. Such mapping, and the supporting rationale, shall be made available to the NABs and NCCA. |  |  |  |  |  |
| 8.2.3 | **Resources for evaluation**  [ISO/IEC 17065:2012], 6.2 Resources for evaluation  ISO/IEC 17065:2012 allows for two options as regards resources for evaluation:   * The use of the CB internal resources, either directly employed by the CB or under its direct control; * The use of external resources, which might belong to different legal entities or may be other parts of the same legal entities.   ISO/IEC 18045:2022 states in §9.2.2 and §9.2.3 that the evaluator and the certifier roles **shall be fulfilled by different entities**. Moreover, ISO/IEC TS 23532 that applies to ITSEF performing CC evaluations, states that: “To maintain impartiality, the laboratory shall maintain proper separation between evaluators and other personnel inside the laboratory or outside the laboratory, but inside the parent organization.”  Therefore, in the EUCC context, only the use of external resources shall be possible as illustrated in the following figures. ITSEFs, whether they belong to the same organization or are part of a different organization than the CB, shall be seen as subcontractors/outsourced resources in the sense of ISO/IEC 17065:2012.  If the ITSEF ist part oft he same legal entity as the certification body, some additional requirements are to be fulfilled by the legal entity to which the CB and the ITSEF belong:   * Top-level management shall not be involved in certification decision, * Top-level management shall commit to preserve impartiality and prevent undue influence between certification and evaluation, * When another part of the same legal entity acts as ITSEF, CB and ITSEF shall have disjoint perimeters and operate independently in terms of: * Working procedures, * Competence management, * Resource allocation.   This implies some structural and organizational separation. Personnel involved in evaluation activities shall not be CB´s personnel and shall not be involved in the review and certification decision-making process. However, without prejudice to the previous requirements, Quality Management may be mutualized between both accredited bodies.  The CB shall take responsibility for all evaluation tasks outsourced to selected and approved ITSEFs. The outsourced activities, as well as the CB’s responsibility for those outsourced tasks, shall be reflected in the legally binding contract or agreement the CB establishes with its clients. |  |  |  |  |  |
| 8.2.4 | Requirements for CBs for the selection and approval of ITSEFs In response to ISO/IEC 17065:2012 §6.2.2.3, the CB shall have a legally binding contract or agreement in place with each ITSEF it’s working with, that includes specific provisions for:   * The respective roles and responsibilities of both the CB and the ITSEF regarding CC evaluation and certification tasks, in line with ISO/IEC 18045:2022 §9.2; * The management of confidentiality, in particular as regards sensitive and/or proprietary information shared by the sponsor/developer as part of certification evidence, and evaluation results; * Identification and prevention of conflict of interest, in line with ISO/IEC 17065:2012 6.1.3 item c).   **Note:** the ITSEF shall perform evaluation activities as specified in CEM work units and provide verdicts with regards to the conformance of the evaluated product with the specified security requirements; the CB shall review - and possibly discuss - the verdicts proposed by the ITSEF, and based on a final ETR, confirm those verdicts and make a certification decision that shall, when applicable, lead to the issuance of a EUCC certificate and certification report.  The CB shall maintain a list of selected and approved ITSEFs for the outsourcing of evaluation tasks as part of EUCC certification projects.  The CB shall have a process in place to assess:   * That selected and approved ITSEFs are appropriately accredited according to ISO/IEC 17025 and according to the state-of-the-art document “ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME”, for the scope of evaluation activities that are relevant for the activities of the CB; * That, at any time, the selected and approved ITSEFs continue to comply with rules and requirements covered by the contract or agreement they have with the CB.   Such process shall be documented in the CB’s operating procedures, and records of assessment and monitoring of the selected and approved ITSEFs shall be produced and securely stored for a period of at least five (5) years after the legally binding contract or agreement with an ITSEF has ceased to produce effect.  The CB shall have a process in place to implement corrective actions for any breaches of the contract or agreement with an ITSEF of which it becomes aware. |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Der Bericht wurde als Anhang zum Bericht gemäß**  **DIN EN ISO/IEC 17025**  **DIN EN ISO/IEC 17065 erstellt**[[4]](#endnote-4)**:** | | | | | |
| Ort: |  | Datum: |  | gez. *Name Begutachter:* | [[5]](#endnote-5) |

1. Unter Begutachtungstyp ist die Art der Begutachtung/die Begutachtungstechnik anzugeben, wobei mehrere Begutachtungs­typen im Rahmen einer Begutachtung zum Tragen kommen können. Bitte wählen Sie aus den folgenden Möglichkeiten das zutreffende Element bzw. die zutreffende Kombination von Elementen für die Angabe des Begutachtungstyps aus:

   Vor-Ort-Begutachtung / Fernbegutachtung / Witness-Audit (Vor-Ort) / Witness-Audit (Fernbegutachtung) / Witness-Prüfung / Dokumentenprüfung / Sonstige Begutachtungstätigkeit (bitte ggf. präzisieren) [↑](#endnote-ref-1)
2. Status im Begutachterteam: SB=Systembegutachter; FB=Fachbegutachter [↑](#endnote-ref-2)
3. Die speziellen Kriterien sind sowohl im Anhang der VO 2019/881, als auch in den einschlägigen „State-Of-The-Art-Dokumenten für Zertifizierungsstellen und ITSEFs zu finden. [↑](#endnote-ref-3)
4. Die Bewertung der Erfüllung der Anforderungen sowie die Empfehlung zur Akkreditierung sind im Begutachtungsbericht zur DIN EN ISO/IEC 17025 bzw. im Begutachtungsbericht zur DIN EN ISO/IEC 17065 dokumentiert. [↑](#endnote-ref-4)
5. Dieser Bericht wurde persönlich von am erstellt. [↑](#endnote-ref-5)