CIS Certification Procedure IEC 62443-4-1 (d196) EN

CIS - Certification & Information Security Services GmbH

Headquarters

1010 Wien, Salztorgasse 2/3/7

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

© CIS 06.11.2026: Nachdruck und Vervielfältigung, auch auszugsweise, nur mit schriftlicher Genehmigung der CIS.

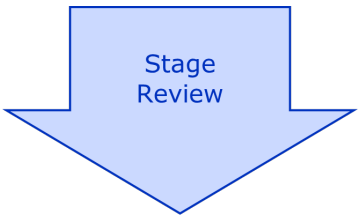
Inhalt

1 Certification Process Flow 3
2 Explanations Regarding the Certification Process 5
2.1 Application for Certification 5
2.2 Order 5
2.3 Product Development and Risk Review – Stage 1 Audit 5
3 Certification Audit—Stage 2 5
3.1 Certificate Issuance 6
3.2 Annual Monitoring (Conditions for Renewal) 6
3.3 Recertification 7
4 Maturity Level 7
4.1 Note on Maturity Level 7
4.2 Maturity Level 2 – Managed 7
4.3 Maturity Level 3 – Defined / Practiced 7
4.4 Maturity Level 4 – Improving 8
5 Certified Maturity Level 8
6 Changes to the Scope and Maturity Level 8
6.1 Increase in the Maturity Level 8
6.2 Reduction in the Maturity Level 9
6.3 Certificate Update 9
7 Changes regarding certification requirements: 9
8 Nonconformities 9
8.1 Nonconformity 9
8.2 Major Nonconformity 9
8.3 Minor Nonconformity 10
9 Certificate Transfer 10

1 Certification Process Flow



The customer submits a certification application and specifies the intended scope as well as the desired maturity level (ML2, ML3, or ML4). Based on the information provided in the application, the scope and duration of the audit, as well as the next steps in the certification process, are planned. Upon completion of this phase, the organization is added to the CIS registration list.



Organizations can have an optional stage review conducted even before the certification process begins. This review assesses whether the documented processes of the Secure Product Development Lifecycle (SDL) appear, in principle, to be suitable for meeting the requirements of IEC 62443-4-1 as well as the targeted maturity level. The Stage Review serves as preparation for certification and is not part of the certification decision.



During Audit Stage 1, the documented processes, procedures, and evidence related to the Secure Product Development Lifecycle are evaluated against the requirements of IEC 62443-4-1. This assessment determines whether the organization is fundamentally capable of achieving the requested maturity level. If it is determined that the requested maturity level is unlikely to be achieved, the customer may lower the requested maturity level before Audit Stage 2 is conducted.



During Audit Stage 2, the practical implementation and effectiveness of the documented processes within the defined scope are reviewed. This involves assessing whether the requirements of IEC 62443-4-1 are effectively implemented and whether the maturity level established during Audit Stage 1 has been achieved. Based on the audit findings, a recommendation is made regarding the certification decision.



Upon issuance of the certificate (Certificate Issuance & Right to Use License), the certified organization acquires the right to display proof of conformity. This certificate is valid for three years and may be used as evidence to build trust with third parties.



During the three-year certificate term, two surveillance audits are conducted at twelve-month intervals. These audits verify that the requirements of IEC 62443-4-1 continue to be met, that the implemented processes are being applied effectively, and that the certified maturity level is being maintained. A comprehensive recertification audit equivalent to a Stage 2 audit is therefore required. Successful recertification restores the right to use the CIS certificate and the CIS conformity mark for another three years.

2 Explanations Regarding the Certification Process

2.1 APPLICATION FOR CERTIFICATION

The completed d201 application form is used to prepare a quote based on the information provided. Here, the customer specifies which maturity level is to be reviewed.

2.2 ORDER

The order is finalized by returning the signed copy of the quote or order.

2.3 PRODUCT DEVELOPMENT AND RISK REVIEW – STAGE 1 AUDIT

The CIS Office will notify you in writing of the CIS staff members who will conduct the Stage 1 audit. The staff member(s) will contact you to schedule an appointment.

The purpose of the product development and risk review is to assess the company's interpretation of the standard's requirements based on the specific measures and precautions that have been implemented. Furthermore, the documentation of the existing product lifecycle for safe product development is reviewed and evaluated based on the customer's specified maturity level.

Prior to the audit, a detailed audit program is developed jointly to ensure that the audit is conducted in a cost-effective and efficient manner. After the audit, a comprehensive audit report is prepared, listing the company's strengths and areas for improvement, which serves as the basis for the company's continuous improvement process.

If the auditor determines that the maturity level under review has not been achieved, the customer has the option of lowering the maturity level to a lower one.

3 Certification Audit—Stage 2

Once Audit Stage 1 is complete, Audit Stage 2 will follow.

The Stage 2 audit will take place at your location.

CIS GmbH will provide you with the names of the audit team in writing; however, in justified cases, you may raise objections to individual team members.

If you agree to the audit team, the lead auditor will schedule an audit appointment with you.

In Stage 2 of the audit, the practical implementation and effectiveness of the Secure Development Lifecycle (SDL) within the defined scope are reviewed. This involves assessing whether the requirements of IEC 62443-4-1 are being effectively implemented based on the maturity level confirmed in the Stage 1 audit.

The assessment specifically covers the evaluation of the following process areas: security management, security requirements definition, secure by design, secure implementation, security verification and validation testing, management of security-related issues, security

update management, and security guidelines. The evaluation is based on appropriate samples drawn from the product development process.

A written audit report on the results of Stage 2 of the audit will be prepared and provided to the client. The report includes an assessment of the Secure Development Lifecycle's compliance with the requirements of IEC 62443-4-1, as well as the effectiveness of the processes applied within the scope of the audit.

If any nonconformities are identified during the audit that would prevent the issuance of the certificate, these must be corrected within three months, and evidence of the corrective actions taken must be provided to CIS.

The certificate specifies the certified scope of the Secure Development Lifecycle as well as the maturity level determined during Audit Stage 1 and confirmed during Audit Stage 2.

Upon successful completion of Audit Stage 2, the audit team leader submits a recommendation to CIS GmbH to grant certification. The final certification decision is made by a CIS GmbH auditor who is independent of the audit process.

3.1 CERTIFICATE ISSUANCE

Once the report has been approved or any discrepancies have been resolved, CIS GmbH will issue the certificate. The certificate's validity period begins on the date of the CIS management's decision.

3.2 ANNUAL MONITORING (CONDITIONS FOR RENEWAL)

The date of the first surveillance audit is based on the date of the certification decision. CIS GmbH will notify the client of the assigned auditor(s) prior to the surveillance audit. The auditor will contact the client to schedule the audit. Depending on the scope, complexity, and risk situation, monitoring can be conducted on-site, remotely, or using a combination of both.

The surveillance audit focuses on determining whether the certified Secure Development Lifecycle (SDL) continues to be effectively implemented and whether the requirements of IEC 62443-4-1 are being met within the defined scope. Particular attention is paid to changes in development processes, the organization, locations, and the certified scope, as well as to new or modified development projects. In addition, the audit evaluates the handling of security incidents and vulnerabilities, security updates and their management, internal audits, corrective actions, and the ongoing effectiveness of established security processes.

A written report will be prepared on the results of the surveillance audit. If any nonconformities are identified, they must be corrected through appropriate corrective actions. Evidence of the implementation and effectiveness of these actions must be provided to the CIS auditors.

If the effectiveness of the implemented measures cannot be assessed based on the submitted evidence, an additional follow-up audit may be required.

If the surveillance audit is completed successfully, the auditor will submit a recommendation to CIS GmbH to renew the certificate. The final decision on whether to maintain the certification is made by the appropriate department at CIS GmbH.

If identified nonconformities are not effectively corrected within the specified timeframes, or if ongoing compliance with the requirements of IEC 62443-4-1 cannot be demonstrated, the certification may be revoked.

Note:

The CIS certification process does not provide for any suspension of certification.

3.3 RECERTIFICATION

After 3 years, a Stage 2 recertification audit will be conducted.

4 Maturity Level

IEC 62443-4-1 evaluates not only whether requirements for the Secure Product Development Lifecycle are met, but also how systematically and sustainably these requirements are implemented within the organization. So-called Maturity Levels (ML) are used for this purpose. The target maturity level is defined as early as the request for proposal stage and is assessed during the Stage 1 audit.

4.1 NOTE ON MATURITY LEVEL

The intended Maturity Level (ML) is assessed during the Stage 2 audit within the defined scope of the audit and the estimated audit duration. If evidence is found for individual controls that goes beyond the ML being assessed, this may be documented in the audit report. This does not constitute confirmation of a higher ML, as that level was not fully subject to assessment. This information is provided solely as a guide regarding implementation that goes beyond the audited ML.

4.2 MATURITY LEVEL 2 – MANAGED

At this maturity level, the processes for safe product development are documented and formally established within the organization. Responsibilities, procedures, and requirements are defined and described in a traceable manner. The organization can demonstrate that the necessary processes are in place and are being managed.

Key feature: Documented and controlled processes.

4.3 MATURITY LEVEL 3 – DEFINED / PRACTICED

In addition to the requirements of Maturity Level 2, the defined processes are applied in practice and effectively implemented. The organization can demonstrate that the guidelines are consistently applied in day-to-day development activities and that safe product development is an integral part of established workflows.

Key feature: Documented processes are demonstrably put into practice.

4.4 MATURITY LEVEL 4 – IMPROVING

In addition to the requirements of Maturity Level 3, the organization continuously monitors and improves its processes. Weaknesses, opportunities for improvement, and new security requirements are systematically analyzed and integrated into the product development process. Decisions are based on key performance indicators, experience, and the results of reviews, audits, and security analyses.

Key feature: Continuous improvement in safe product development.

5 Certified Maturity Level

The certified maturity level indicates that all controls specified in IEC 62443-4-1 meet the specified maturity level. The assessment is based on the maturity level requirements defined in IEC 62443-4-1 for the controls specified in the standard.

6 Changes to the Scope and Maturity Level

The certificate holder must immediately notify the CIS of any planned or actual changes that may affect the certified scope or the certified maturity level. The IEC 62443-4-1 certification covers both the defined scope of the Secure Development Lifecycle and the certified maturity level.

Changes may include, in particular:

- Expansion or restriction of the scope,
- Inclusion of additional locations or organizational units,
- Inclusion of additional product areas, product families, or development processes,
- significant changes to the Secure Development Lifecycle,
- Increase in the certified maturity level,
- Voluntary reduction of the certified maturity level at the request of the certificate holder.

CIS management will assess the impact of the change and decide on the next steps. Depending on the nature, scope, and risk potential of the change, CIS may conduct a document review, a special audit, or a full certification process.

6.1 INCREASE IN THE MATURITY LEVEL

An increase in a certified maturity level is considered an extension of the certification. The certificate holder must demonstrate, through appropriate evidence and an audit, that all requirements of the higher maturity level applied for are effectively implemented. The assessment may take place as part of a special audit or a regular surveillance or recertification audit.

6.2 REDUCTION IN THE MATURITY LEVEL

A reduction in the certified maturity level may only be made at the request of the certificate holder and is treated as a change to the scope of certification.

If audits reveal deviations that jeopardize the maintenance of the certified maturity level, the matter will be handled in accordance with the regulations governing nonconformities and certificate revocation. There is no automatic downgrade of the certified maturity level.

6.3 CERTIFICATE UPDATE

Following a successful evaluation, the approved changes will be reflected in the certificate and the associated certification documents. The remaining term of the certificate generally remains unchanged, unless a different decision is made as part of the certification process.

7 Changes regarding certification requirements:

Changes to certification requirements—such as changes to the standards under which certification was granted—will be communicated to all certified customers via email. Should further explanatory information be necessary, it will be published on the website or via newsletter.

8 Nonconformities

8.1 NONCONFORMITY

Nonconformity = Failure to meet a requirement of IEC 62443-4-1 or a Secure Product Development Lifecycle (SDL) process applied within the certified scope, relative to the desired/ assessed maturity level.

Nonconformity occurs when the requirements of IEC 62443-4-1, documented procedures, established processes, or their effective application are not met.

8.2 MAJOR NONCONFORMITY

A major nonconformity impairs the Secure Product Development Lifecycle’s (SDL) ability to effectively achieve the intended results regarding the secure development, maintenance, and retirement of development processes.

Nonconformities may be classified as significant, in particular, if:

1. there is substantial doubt that a required SDL process will be effectively established, implemented, or maintained;
2. there is significant doubt that the organization systematically meets the requirements of IEC 62443-4-1;
3. a key process area of IEC 62443-4-1 is missing or is not effectively implemented,

4. several minor nonconformities collectively indicate a systematic failure of the same SDL process;
5. the effectiveness of the certified development process cannot be demonstrated.
6. At least **90% of all evaluated controls** must meet or exceed the maturity level stated on the certificate. If more than 90% of the assessed controls fall below the audited maturity level, this constitutes a material nonconformity.

8.3 MINOR NONCONFORMITY

A minor nonconformity does not impair the organization's ability to achieve the defined objectives of the Secure Product Development Lifecycle (SDL) within the organization or the essential requirements of IEC 62443-4-1.

It constitutes an isolated deviation that does not indicate a systematic failure of an SDL process and does not have a significant impact on the organization's ability to meet the requirements of IEC 62443-4-1.

Individual controls with a maturity level that is no more than one level below the audited maturity level may be assessed as minor nonconformities, provided that they do not exceed 10 percent of the audited controls and do not exhibit any characteristics of a serious nonconformity.

9 Certificate Transfer

In principle, existing certificates may be accepted, provided that the certification was issued by an accredited certification body and the requirements for recognition are met.

Prior to the transfer, CIS conducts a so-called pre-transfer review. This review assesses the validity of the existing certificate, the results of previous audits, the status of any nonconformities, and other relevant information. The decision regarding the transfer must be made before a surveillance or recertification audit is conducted.

The assessment is based on a document review and may be supplemented by additional remote or on-site activities, depending on any outstanding nonconformities or risks.

If the transfer is completed successfully, the existing certification cycle—including the certificate’s original term—will remain in effect. Subsequent certification will then be carried out by CIS within the existing certification cycle.

If the equivalence or validity of the existing certification cannot be sufficiently demonstrated, or if the requirements for recognition are not met, the certification will not be recognized. In this case, a standard initial certification process must be carried out.

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Salztorgasse 2/3/7

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

© CIS 06.11.2026:
Nachdruck und Vervielfältigung,
auch auszugsweise, nur mit schrift-
licher Genehmigung der CIS.