

# CIS Zertifizierungsverfahren IEC 62443-4-1 (d196)

**CIS** - Certification & Information  
Security Services GmbH

**Headquarters**

1010 Wien, Saltzorgasse 2/3/7

Tel.: +43 1 532 98 90  
Fax: +43 1 532 98 90 89  
[office@cis-cert.com](mailto:office@cis-cert.com)  
[www.cis-cert.com](http://www.cis-cert.com)

© CIS 01.10.2026: Nachdruck und Vervielfältigung, auch auszugsweise, nur mit schriftlicher Genehmigung der CIS.

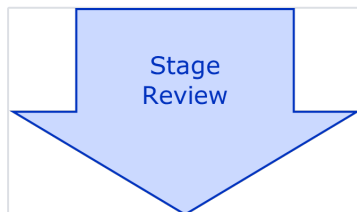
## Inhalt

|                                                                              |           |
|------------------------------------------------------------------------------|-----------|
| <b>1 Ablauf des Zertifizierungsverfahrens.....</b>                           | <b>3</b>  |
| <b>2 Erläuterungen zum Zertifizierungsablauf.....</b>                        | <b>5</b>  |
| 2.1 Antrag auf Zertifizierung.....                                           | 5         |
| 2.2 Auftrag .....                                                            | 5         |
| 2.3 Produktentwicklung und Risk Review – Audit Stage 1 .....                 | 5         |
| <b>3 Zertifizierungsaudit- Audit Stage 2.....</b>                            | <b>5</b>  |
| 3.1 Zertifikatsausstellung.....                                              | 6         |
| 3.2 Jährliche Überwachung (Bedingungen für die Aufrechterhaltung) .....      | 6         |
| 3.3 Re-Zertifizierung .....                                                  | 7         |
| <b>4 Maturity Level.....</b>                                                 | <b>7</b>  |
| 4.1 Maturity Level 2 – Managed .....                                         | 7         |
| 4.2 Maturity Level 3 – Defined / Practiced .....                             | 7         |
| 4.3 Maturity Level 4 – Improving .....                                       | 7         |
| <b>5 Ermittlung des Maturity Levels .....</b>                                | <b>8</b>  |
| 5.1 Beispiele .....                                                          | 8         |
| <b>6 Änderungen des Geltungsbereichs und des Maturity Levels .....</b>       | <b>8</b>  |
| 6.1 Erhöhung des Maturity Levels .....                                       | 9         |
| 6.2 Reduzierung des Maturity Levels.....                                     | 9         |
| 6.3 Zertifikatsanpassung.....                                                | 9         |
| <b>7 Änderungen bezüglich der Anforderungen an die Zertifizierung: .....</b> | <b>9</b>  |
| <b>8 Nichtkonformitäten .....</b>                                            | <b>10</b> |
| 8.1 Nichtkonformität .....                                                   | 10        |
| 8.2 Wesentliche Nichtkonformität (Major Nonconformity) .....                 | 10        |
| 8.3 Geringfügige Nichtkonformität (Minor Nonconformity) .....                | 10        |
| <b>9 Zertifikatsübernahme .....</b>                                          | <b>10</b> |

## 1 Ablauf des Zertifizierungsverfahrens



Der Kunde stellt einen Zertifizierungsantrag und legt den angestrebten Geltungsbereich sowie den gewünschten Maturity Level (ML2, ML3 oder ML4) fest. Auf Grundlage der Antragsangaben werden Auditumfang, Auditdauer und die weiteren Schritte des Zertifizierungsverfahrens geplant. Mit Abschluss dieser Phase wird die Organisation in die CIS-Registrationsliste aufgenommen.



Organisationen können bereits vor Beginn des Zertifizierungsverfahrens ein optionales Stage Review durchführen lassen. Dabei wird beurteilt, ob die dokumentierten Prozesse des Secure Product Development Lifecycle (SDL) grundsätzlich geeignet erscheinen, die Anforderungen der IEC 62443-4-1 sowie den angestrebten Maturity Level zu erfüllen. Das Stage Review dient der Vorbereitung auf die Zertifizierung und ist nicht Bestandteil der Zertifizierungsentscheidung.



Im Audit Stage 1 werden die dokumentierten Prozesse, Verfahren und Nachweise des Secure Product Development Lifecycle hinsichtlich der Anforderungen der IEC 62443-4-1 bewertet. Dabei wird geprüft, ob die Organisation grundsätzlich in der Lage ist, den beantragten Maturity Level zu erreichen. Sofern festgestellt wird, dass der beantragte Reifegrad voraussichtlich nicht erreicht werden kann, kann der Kunde den beantragten Maturity Level vor Durchführung des Audit Stage 2 reduzieren.



Im Audit Stage 2 wird die praktische Umsetzung und Wirksamkeit der dokumentierten Prozesse innerhalb des festgelegten Geltungsbereichs überprüft. Dabei wird beurteilt, ob die Anforderungen der IEC 62443-4-1 wirksam umgesetzt werden und der im Audit Stage 1 zugrunde gelegte Maturity Level erreicht wird. Auf Basis der Auditfeststellungen erfolgt die Empfehlung für die Zertifizierungsentscheidung.



Mit der Ausstellung des Zertifikats (Certificate Issuance & Right to Use Licence) erwirbt die zertifizierte Organisation das Recht zur Führung eines Konformitätsnachweises. Dieser wird mit einer 3-jährigen Gültigkeit ausgestellt und darf als vertrauensbildender Nachweis gegenüber Dritten verwendet werden.



## Surveillance Audit

Während der dreijährigen Zertifikatslaufzeit werden zwei Überwachungsaudits im Abstand von jeweils zwölf Monaten durchgeführt. Dabei wird überprüft, ob die Anforderungen der IEC 62443-4-1 weiterhin erfüllt werden, die eingeführten Prozesse wirksam angewendet werden und der zertifizierte Maturity Level aufrechterhalten wird. Es ist daher ein vollumfängliches Rezertifizierungsaudit im Umfang eines Stage 2 Audits erforderlich. Durch eine erfolgreiche Rezertifizierung kann erneut das 3-jährige Recht zur Führung des CIS-Zertifikates und des CIS-Konformitätszeichens erworben werden.

## 2 Erläuterungen zum Zertifizierungsablauf

---

### 2.1 ANTRAG AUF ZERTIFIZIERUNG

Das ausgefüllte Antragsformular d201 wird verwendet, um auf Basis der Angaben ein Angebot zu erstellen. Hier gibt der Kunde bekannt, welches Maturity Level geprüft werden soll.

### 2.2 AUFTRAG

Der Auftrag wird abgeschlossen durch Retournierung der unterfertigten Zweitschrift des Angebotes oder Bestellung.

### 2.3 PRODUKTENTWICKLUNG UND RISK REVIEW – AUDIT STAGE 1

Das CIS-Office gibt Ihnen schriftlich die CIS-Mitarbeiter bekannt, die das Stage 1 Audit durchführen. Der (die) Mitarbeiter nehmen mit Ihnen Kontakt zwecks Terminvereinbarung auf.

Das Produktentwicklungs- und Risk-Review hat zum Ziel, die unternehmensbezogene Interpretation der Normforderungen auf Grundlage durchgeführter konkreter Maßnahmen und Vorkehrungen zu beurteilen. Weiters wird die Dokumentation des existierenden Lebenszyklus für eine sichere Produktentwicklung auf Basis des angegebenen Maturity Levels des Kunden geprüft und beurteilt.

Vor dem Audit wird gemeinsam ein detailliertes Audit-Programm erstellt, so dass eine ökonomische und effiziente Audit-Durchführung sichergestellt wird. Nach dem Audit wird ein umfassender Auditbericht erstellt, in dem die Stärken und Verbesserungspotentiale aufgelistet werden und als Grundlage für den kontinuierlichen Verbesserungsprozess im Unternehmen vorliegen.

Sollte hier durch den/die Auditor:In erkannt werden, dass das zu prüfende Maturity Level nicht erreicht wird, hat der Kunde die Möglichkeit das Maturity Level auf ein niedrigeres zu reduzieren.

## 3 Zertifizierungsaudit- Audit Stage 2

---

Nach Abschluss des Audit Stage 1 erfolgt das Audit Stage 2.

Das Audit Stage 2 findet bei Ihnen vor Ort statt.

Die CIS GmbH gibt Ihnen schriftlich die Namen des Auditorenteams bekannt, wogegen Sie in begründeten Fällen Einwände gegen einzelne Teammitglieder vorbringen können.

Sofern Sie dem Auditorenteam zustimmen, wird der leitende Auditor einen Audittermin mit Ihnen vereinbaren.

Im Audit Stage 2 wird die praktische Umsetzung und Wirksamkeit des Secure Development Lifecycle (SDL) innerhalb des festgelegten Geltungsbereichs überprüft. Dabei wird bewertet, ob die Anforderungen der IEC 62443-4-1 auf Basis des im Stage 1 Audit bestätigten Maturity Levels wirksam umgesetzt werden.

Die Begutachtung umfasst insbesondere die Bewertung der Prozessbereiche Security Management, Security Requirements Definition, Secure by Design, Secure Implementation, Security Verification and Validation Testing, Management of Security-related Issues, Security Update Management sowie Security Guidelines. Die Bewertung erfolgt anhand geeigneter Stichproben aus dem Produktentwicklungsprozess.

Über das Ergebnis des Audit Stage 2 wird ein schriftlicher Auditbericht erstellt und dem Auftraggeber zur Kenntnis gebracht. Der Bericht beinhaltet die Bewertung der Konformität des Secure Development Lifecycle mit den Anforderungen der IEC 62443-4-1 sowie die Wirksamkeit der im Geltungsbereich angewendeten Prozesse.

Sofern im Zuge des Audits Abweichungen erkannt werden, die eine Ausstellung des Zertifikates verhindern, sind diese innerhalb von drei Monaten zu beheben und die durchgeführten Maßnahmen gegenüber CIS nachzuweisen.

Auf dem Zertifikat werden der zertifizierte Geltungsbereich des Secure Development Lifecycle sowie das im Audit Stage 1 festgelegte und im Audit Stage 2 bestätigte Maturity Level angegeben.

Nach positivem Abschluss des Audit Stage 2 wird vom Audit-Teamleiter die Empfehlung auf Zertifikatserteilung an die CIS GmbH gestellt. Die endgültige Zertifizierungsentscheidung erfolgt durch einen von der Auditdurchführung unabhängigen Auditor der CIS GmbH.

## 3.1 ZERTIFIKATSAUSSTELLUNG

Nach positiver Bewertung des Berichtes bzw. allfälliger Erledigungen von Abweichungen erfolgt die Zertifikatsausstellung durch die CIS GmbH. Die Gültigkeit des Zertifikates wird ab dem Zeitpunkt der Entscheidung der CIS-Geschäftsführung berechnet.

## 3.2 JÄHRLICHE ÜBERWACHUNG (BEDINGUNGEN FÜR DIE AUFRECHTERHALTUNG)

Der Termin der ersten Überwachung orientiert sich am Datum der Zertifizierungsentscheidung. Die CIS GmbH gibt dem Auftraggeber vor dem Überwachungsaudit den/die zuständigen Auditor/en bekannt. Dieser nimmt mit dem Auftraggeber Kontakt auf und vereinbart einen Audittermin. Die Überwachung kann abhängig von Umfang, Komplexität und Risikosituation vor Ort, remote oder in kombinierter Form durchgeführt werden.

Das Überwachungsaudit konzentriert sich auf die Feststellung, ob der zertifizierte Secure Development Lifecycle (SDL) weiterhin wirksam angewendet wird und die Anforderungen der IEC 62443-4-1 im festgelegten Geltungsbereich erfüllt werden. Besonderes Augenmerk wird dabei auf Änderungen der Entwicklungsprozesse, der Organisation, der Standorte, des zertifizierten Geltungsbereichs sowie auf neue oder geänderte Entwicklungsprojekte gelegt. Darüber hinaus werden der Umgang mit Security Incidents und Schwachstellen, Security Updates und deren Steuerung, interne Überprüfungen, Korrekturmaßnahmen sowie die fortlaufende Wirksamkeit der etablierten Security-Prozesse bewertet.

Über das Ergebnis des Überwachungsaudits wird ein schriftlicher Bericht erstellt. Sofern Abweichungen festgestellt werden, sind diese durch geeignete Korrekturmaßnahmen zu beheben. Die Umsetzung und Wirksamkeit der Maßnahmen ist den CIS-Auditoren nachzuweisen.

Kann die Wirksamkeit der umgesetzten Maßnahmen nicht anhand der eingereichten Nachweise beurteilt werden, kann ein zusätzliches Nachaudit erforderlich sein.

Bei positivem Abschluss des Überwachungsaudits wird vom Auditor die Empfehlung auf Weiterführung des Zertifikats an die CIS GmbH gestellt. Die endgültige Entscheidung über die Aufrechterhaltung der Zertifizierung erfolgt durch die hierfür zuständige Stelle der CIS GmbH.

Werden festgestellte Abweichungen nicht innerhalb der vorgegebenen Fristen wirksam behoben oder kann die fortlaufende Konformität mit den Anforderungen der IEC 62443-4-1 nicht nachgewiesen werden, kann die Zertifizierung entzogen werden.

#### Anmerkung:

Im CIS-Zertifizierungsverfahren ist keine Aussetzung der Zertifizierung vorgesehen.

### 3.3 RE-ZERTIFIZIERUNG

Nach Ablauf von 3 Jahren wird ein Re-Zertifizierungsaudit im Umfang eines Stage 2 durchgeführt.

## 4 Maturity Level

---

Die IEC 62443-4-1 bewertet nicht nur, ob Anforderungen an den Secure Product Development Lifecycle erfüllt werden, sondern auch, wie systematisch und nachhaltig diese Anforderungen innerhalb der Organisation umgesetzt werden. Hierzu werden sogenannte Maturity Levels (ML) verwendet. Der angestrebte Reifegrad wird bereits im Rahmen der Angebotsanfrage festgelegt und im Stage-1-Audit bewertet.

### 4.1 MATURITY LEVEL 2 – MANAGED

Auf diesem Reifegrad sind die Prozesse zur sicheren Produktentwicklung dokumentiert und organisatorisch festgelegt. Verantwortlichkeiten, Verfahrensanweisungen und Anforderungen sind definiert und nachvollziehbar beschrieben. Die Organisation kann nachweisen, dass die erforderlichen Prozesse vorhanden sind und gelenkt werden.

Kernmerkmal: Dokumentierte und gesteuerte Prozesse.

### 4.2 MATURITY LEVEL 3 – DEFINED / PRACTICED

Zusätzlich zu den Anforderungen des Maturity Level 2 werden die definierten Prozesse in der Praxis angewendet und wirksam umgesetzt. Die Organisation kann nachweisen, dass die Vorgaben im Entwicklungsalltag dauerhaft genutzt werden und die sichere Produktentwicklung Bestandteil der etablierten Arbeitsabläufe ist.

Kernmerkmal: Dokumentierte Prozesse werden nachweislich gelebt.

### 4.3 MATURITY LEVEL 4 – IMPROVING

Zusätzlich zu den Anforderungen des Maturity Level 3 überwacht und verbessert die Organisation ihre Prozesse kontinuierlich. Schwachstellen, Verbesserungspotenziale und neue Sicherheitsanforderungen werden systematisch analysiert und in den Produktentwicklungsprozess integriert. Entscheidungen basieren auf Kennzahlen, Erfahrungen sowie Ergebnissen aus Reviews, Audits und Sicherheitsanalysen.

Kernmerkmal: Kontinuierliche Verbesserung der sicheren Produktentwicklung.

## 5 Ermittlung des Maturity Levels

---

Der zertifizierte Maturity Level beschreibt den erreichten Reifegrad der Produktentwicklungsprozesse im Geltungsbereich der Zertifizierung. Die Bewertung erfolgt auf Basis der in der IEC 62443-4-1 definierten Anforderungen und Controls.

Für die Ermittlung des erreichten Maturity Levels gelten folgende Grundsätze:

- Der auf dem Zertifikat ausgewiesene Maturity Level bestätigt, dass kein Control unter dem Reifegrad **Maturity Level minus 1** bewertet wurde.
- Mindestens **90 % aller bewerteten Controls** müssen den auf dem Zertifikat ausgewiesenen Maturity Level erreichen oder übertreffen.

Werden diese Voraussetzungen nicht erfüllt, ist eine Zertifizierung für den beantragten Reifegrad nicht möglich.

### 5.1 BEISPIELE

#### Zertifizierung auf Maturity Level 2

- Mindestens 90 % der Controls müssen Level 2 oder höher erreichen.
- Einzelne Controls dürfen auf Level 1 liegen.

#### Zertifizierung auf Maturity Level 3

- Kein Control darf unter Level 2 bewertet sein.
- Mindestens 90 % der Controls müssen Level 3 oder höher erreichen.

#### Zertifizierung auf Maturity Level 4

- Kein Control darf unter Level 3 bewertet sein.
- Mindestens 90 % der Controls müssen Level 4 erreichen.

## 6 Änderungen des Geltungsbereichs und des Maturity Levels

---

Der Zertifikatsinhaber hat der CIS geplante oder bereits eingetretene Änderungen unverzüglich bekanntzugeben, sofern diese Auswirkungen auf den zertifizierten Geltungsbereich oder das zertifizierte Maturity Level haben können. Die IEC 62443-4-1 Zertifizierung umfasst sowohl den festgelegten Geltungsbereich des Secure Development Lifecycle als auch das zertifizierte Maturity Level.

Änderungen können insbesondere umfassen:

- Erweiterung oder Einschränkung des Geltungsbereichs,

- Aufnahme zusätzlicher Standorte oder Organisationseinheiten,
- Einbeziehung weiterer Produktbereiche, Produktfamilien oder Entwicklungsprozesse,
- wesentliche Änderungen des Secure Development Lifecycle,
- Erhöhung des zertifizierten Maturity Levels,
- freiwillige Reduzierung des zertifizierten Maturity Levels auf Antrag des Zertifikatsinhabers.

Die Geschäftsführung der CIS beurteilt die Auswirkungen der Änderung und entscheidet über die weitere Vorgehensweise. Abhängig von Art, Umfang und Risikopotenzial der Änderung kann die CIS eine Dokumentenprüfung, ein Sonderaudit oder ein vollständiges Zertifizierungsverfahren durchführen.

## 6.1 ERHÖHUNG DES MATURITY LEVELS

Die Erhöhung eines zertifizierten Maturity Levels gilt als Erweiterung der Zertifizierung. Der Zertifikatsinhaber hat durch geeignete Nachweise und ein Audit nachzuweisen, dass sämtliche Anforderungen des beantragten höheren Reifegrades wirksam umgesetzt werden. Die Bewertung kann im Rahmen eines Sonderaudits oder eines regulären Überwachungs- bzw. Re-Zertifizierungsaudits erfolgen.

## 6.2 REDUZIERUNG DES MATURITY LEVELS

Eine Verringerung des zertifizierten Maturity Levels kann ausschließlich auf Antrag des Zertifikatsinhabers erfolgen und wird als Änderung des Zertifizierungsumfangs behandelt.

Werden im Rahmen von Audits Abweichungen festgestellt, die die Aufrechterhaltung des zertifizierten Maturity Levels gefährden, erfolgt die Behandlung gemäß den Regelungen für Nichtkonformitäten und Zertifikatsentzug. Eine automatische Herabstufung des zertifizierten Maturity Levels erfolgt nicht.

## 6.3 ZERTIFIKATSANPASSUNG

Nach erfolgreicher Bewertung werden die genehmigten Änderungen im Zertifikat und in den zugehörigen Zertifizierungsunterlagen berücksichtigt. Die verbleibende Zertifikatslaufzeit bleibt dabei grundsätzlich unverändert, sofern keine andere Entscheidung im Rahmen des Zertifizierungsverfahrens getroffen wird.

## 7 Änderungen bezüglich der Anforderungen an die Zertifizierung:

---

Änderungen bezüglich der Anforderungen an die Zertifizierung wie z.B. Änderung der Normen, nach denen die Zertifizierung erteilt wurde, werden allen zertifizierten Kunden per E-Mail zur Kenntnis gebracht. Sofern weiterführende erläuternde Hinweise erforderlich sein sollten, werden diese auf der Homepage oder per Newsletter veröffentlicht.

## 8 Nichtkonformitäten

---

### 8.1 NICHTKONFORMITÄT

Nichtkonformität = Nichterfüllung einer Anforderung der IEC 62443-4-1 oder eines im zertifizierten Geltungsbereich angewendeten Secure Product Development Lifecycle (SDL)-Prozesses bezogen auf den gewünschten/geprüften Maturity Level.

Eine Nichtkonformität liegt vor, wenn Anforderungen der IEC 62443-4-1, dokumentierte Verfahren, festgelegte Prozesse oder deren wirksame Anwendung nicht erfüllt werden.

### 8.2 WESENTLICHE NICHTKONFORMITÄT (MAJOR NONCONFORMITY)

Eine wesentliche Nichtkonformität beeinträchtigt die Fähigkeit des Secure Product Development Lifecycle (SDL), die beabsichtigten Ergebnisse hinsichtlich der sicheren Entwicklung, Pflege und Abkündigung von Entwicklungsprozessen wirksam zu erreichen.

Nichtkonformitäten können insbesondere dann als wesentlich eingestuft werden, wenn:

1. erheblicher Zweifel besteht, dass ein erforderlicher SDL-Prozess wirksam etabliert, umgesetzt oder aufrechterhalten wird;
2. erheblicher Zweifel besteht, dass die Organisation die Anforderungen der IEC 62443-4-1 systematisch erfüllt;
3. ein wesentlicher Prozessbereich der IEC 62443-4-1 fehlt oder nicht wirksam umgesetzt wird,
4. mehrere geringfügige Nichtkonformitäten gemeinsam auf ein systematisches Versagen desselben SDL-Prozesses hinweisen;
5. die Wirksamkeit des zertifizierten Entwicklungsprozesses nicht nachgewiesen werden kann.

### 8.3 GERINGFÜGIGE NICHTKONFORMITÄT (MINOR NONCONFORMITY)

Eine geringfügige Nichtkonformität beeinträchtigt die Fähigkeit Unternehmens nicht, die definierten Zielsetzungen des Secure Product Development Lifecycle (SDL) im Unternehmen oder die wesentlichen Anforderungen der IEC 62443-4-1 zu erreichen.

Sie stellt eine einzelne Abweichung dar, die kein systematisches Versagen eines SDL-Prozesses erkennen lässt und keine erhebliche Auswirkung auf die Fähigkeit der Organisation hat, die Anforderungen der IEC 62443-4-1 zu erfüllen.

## 9 Zertifikatsübernahme

---

Eine Übernahme bestehender Zertifikate ist grundsätzlich möglich, sofern die Zertifizierung von einer akkreditierten Zertifizierungsstelle ausgestellt wurde und die Voraussetzungen für eine Anerkennung erfüllt sind.

Vor der Übernahme führt CIS eine sogenannte Pre-Transfer-Prüfung durch. Dabei werden die Gültigkeit des bestehenden Zertifikats, die Ergebnisse der bisherigen Audits, der Status allfälliger Nichtkonformitäten sowie weitere relevante Informationen bewertet. Die Entscheidung über die Übernahme muss vor der Durchführung eines Überwachungs- oder Re-Zertifizierungsaudits erfolgen.

Die Bewertung erfolgt anhand einer Dokumentenprüfung und kann, abhängig von offenen Nichtkonformitäten oder Risiken, durch zusätzliche Remote- oder Vor-Ort-Aktivitäten ergänzt werden.

Wird die Übernahme erfolgreich abgeschlossen, bleibt der bestehende Zertifizierungszyklus einschließlich der ursprünglichen Laufzeit des Zertifikats erhalten. Die weitere Zertifizierung erfolgt anschließend innerhalb des bestehenden Zertifizierungszyklus durch CIS.

Kann die Gleichwertigkeit oder Gültigkeit der bestehenden Zertifizierung nicht ausreichend nachgewiesen werden oder werden die Voraussetzungen für eine Übernahme nicht erfüllt, erfolgt keine Zertifikatsübernahme. In diesem Fall ist ein reguläres Erstzertifizierungsverfahren durchzuführen.



**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](mailto:office@cis-cert.com)  
[www.cis-cert.com](http://www.cis-cert.com)

© CIS 01.10.2026:  
Nachdruck und Vervielfältigung,  
auch auszugsweise, nur mit schrift-  
licher Genehmigung der CIS.