Beschreibung des Zertifizierungsverfahrens
IEC 62443 Industrial Security – Managementsysteme (Prozesse)

Zertifizierung

Inhaltsverzeichnis

1 EINLEITUNG 2

2 ZERTIFIZIERUNGSVERFAHREN 4

2.1 Auditvorbereitung 4
2.2 Stufe 1 Audit 5
2.3 Zertifizierungsaudit (Stufe 2 Audit) 6
2.4 Zertifikatserteilung 7

3 ÜBERWACHUNGSAUDIT 7

3.1 Rezertifizierungsaudit 8

4 ERWEITERUNGSAUDIT 9

5 ÜBERNAHME VON ZERTIFIZIERUNGEN ANDERER ZERTIFIZIERUNGSSTELLEN 9

6 ZERTIFIZIERUNG VON UNTERNEHMEN MIT MEHREREN STANDORTEN 9

7 MANAGEMENT VON NICHTKONFORMITÄTEN 10

Haben Sie Fragen zu der Leistungsbeschreibung? Wir helfen Ihnen gern weiter.

Sie erreichen uns per Mail info.tncert@tuev-nord.de oder persönlich von Montag bis Freitag zwischen 07:30 Uhr und 18:00 Uhr unter 0800 – 2457457.

TÜV NORD CERT GmbH

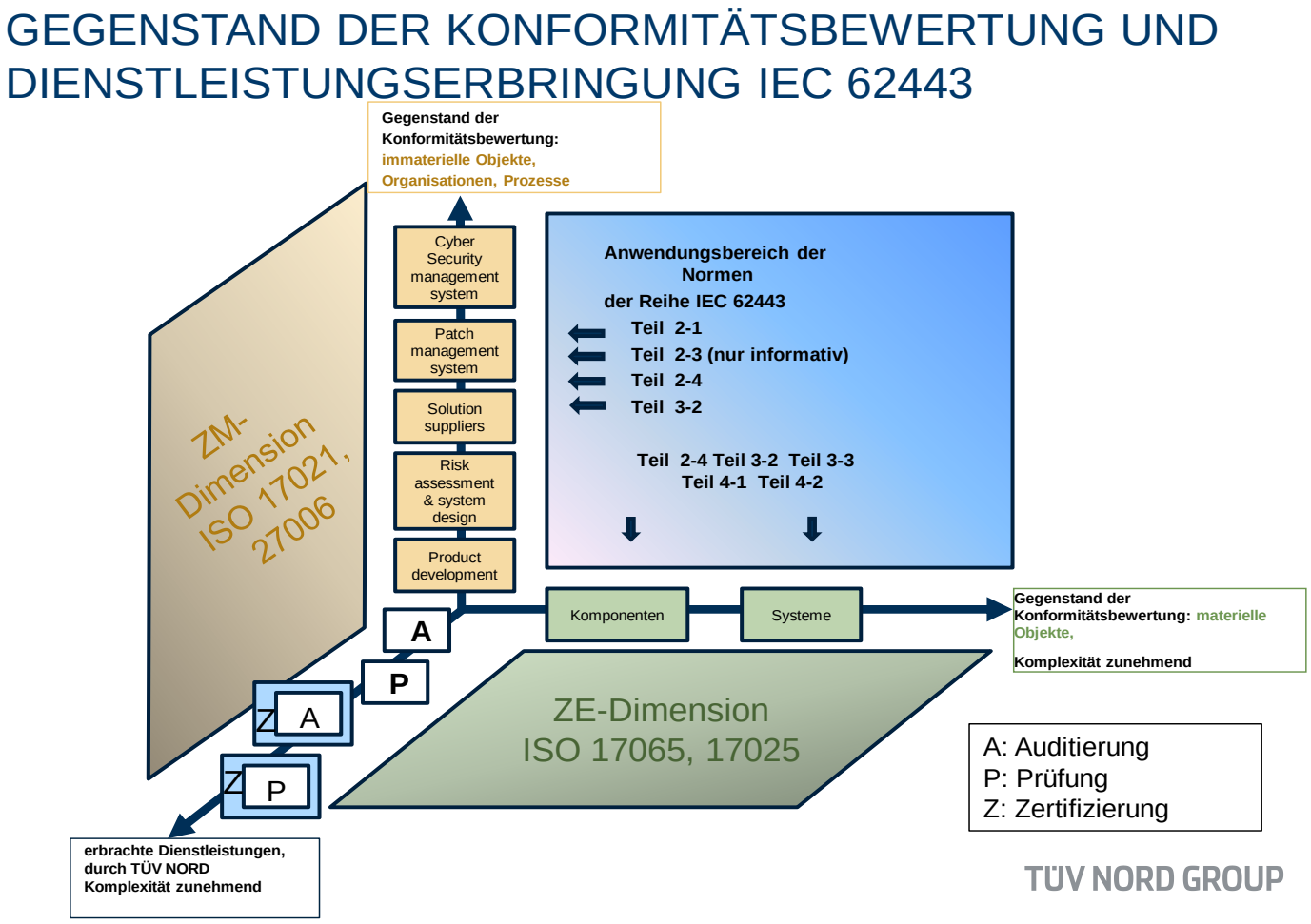
Langemarckstraße 20

45141 Essen

www.tuev-nord-cert.de

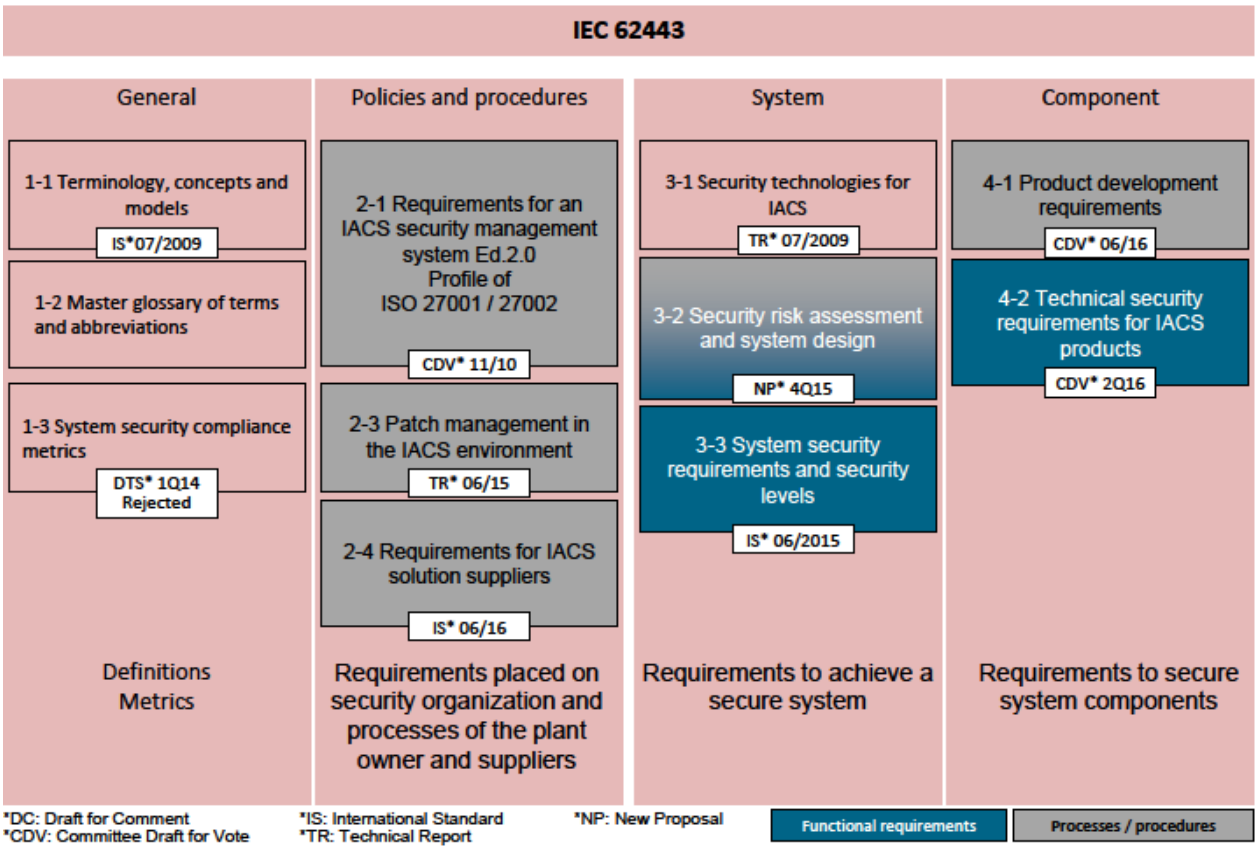
1 EINLEITUNG

Das Zertifizierungsverfahren des Managementsystems (Industrial Security) folgt den Anforderungen des Konformitätsbewertungsprogramms: „Dienstleistungen im Bereich Industrial Security nach Normen der Reihe IEC 62443“ (CERT-310-VA001) und bildet hier spezifisch den Teil des Konformitätsbewertungsprogramms ab, dessen Gegenstand die immateriellen Objekte (=Organisationen,und Prozesse) sind. Dies wird in der nachfolgenden Grafik dargestellt. Das hier beschriebene Zertifizierungsverfahren von Managementsystemen wird demzufolge in der linken Ebene (gelber Bereich) abgebildet.

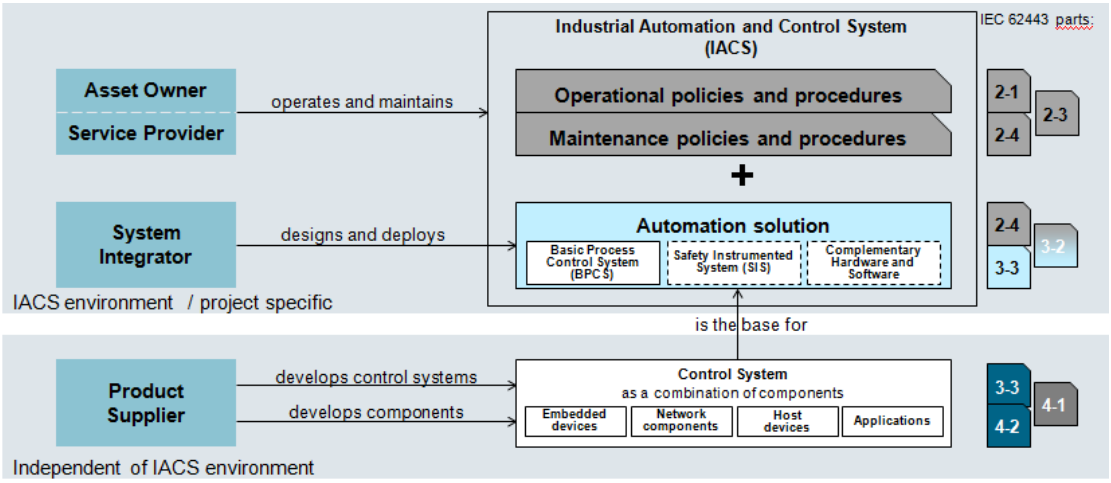


Weitere Details zur grundsätzlichen Einordung und Abgrenzung der Dienstleistung sowie den handelnden Parteien können dem Konformitätsbewertungsprogramm: „Dienstleistungen im Bereich Industrial Security nach Normen der Reihe IEC 62443“ (CERT-310-VA001) entnommen werden.

Das Zertifizierungsverfahren des Managementsystems (Industrial Security) besteht aus der Angebots- und Vertragsphase, der Auditvorbereitung, der Durchführung des Audits Stufe 1 mit Bewertung der Management-Dokumentation, der Durchführung des Audits Stufe 2, der Zertifikatserteilung und der Überwachung/Rezertifizierung.
Die Auditoren werden von der Zertifizierungsstelle der TÜV NORD CERT GmbH entsprechend der Zulassung für die Branche und Qualifikation ausgewählt.
Der Betrachtungsumfang richtet sich nach den jeweils anwendbaren Normenteilen der IEC 62443:



in Verbindung mit nachfolgenden Zusammenhängen der Normenteile:



2 ZERTIFIZIERUNGSVERFAHREN

2.1 Auditvorbereitung

Zunächst erfolgt die Sichtung der eingereichten Unterlagen zur Feststellung der Zertifizierbarkeit des Systems. Bei positivem Ergebnis findet ein Kick-Off Meeting beim Kunden statt zur Definition des genauen Betrachtungsgegenstandes und Festlegung der Grenzen des Zertifizierungsumfangs.

Der mit dem Kunden zu definierende Auditumfang umfasst neben der Definition der Grenzen des Zertifizierungsumfangs auch die Spezifikation von Standorten, Organisationseinheiten, Tätigkeiten und Prozessen. Die Auditkriterien zur Feststellung der Konformität und Wirksamkeit des Managementsystems richten sich nach den jeweiligen Anforderungen des der Bewertung zu Grunde gelegten Normenteils der IEC 62443. Je nach Festlegung der Auditziele wird das Managementsystem nach den Kriterien der IEC 62443-2-1 (Implementierung eines Security-Managementsystem), IEC 62443-2-4 (Security-Anforderung für IACS-Service-Provider) und/oder IEC 62443-3-2 (Risikobeurteilung und Systemgestaltung) bewertet. Die Durchführung der Bewertung richtet sich hierbei nach der in diesem Dokument beschriebene Vorgehensweise.

Sollten bei dem Unternehmen besondere Umstände vorhanden sein, welche darüberhinausgehende Absicherungen bzgl. der Vertraulichkeit erfordern, so kann eine zusätzliche Vertraulichkeitsvereinbarung geschlossen werden.

Sollten beim Auftraggeber vertrauliche oder sensitive Dokumente / Aufzeichnungen vorhanden sein, die den Auditoren nicht zugänglich gemacht werden können, so ist die Zertifizierungsstelle vorher darüber zu unterrichten. Die Zertifizierungsstelle beurteilt vor dem Audit, ob ohne Einsicht in diese Dokumente / Aufzeichnungen ein adäquates Audit durchgeführt werden kann.

Abschließend werden entsprechend die, für das Projekt notwendigen, Kompetenzen bezüglich des Personals ermittelt und die jeweiligen Rollen für die Evaluierung, Bewertung und Zertifizier-Entscheidung festgelegt.

Im Rahmen der Vorbereitung auf die Überwachungs- bzw. Rezertifizierungsaudits ist das Unternehmen verpflichtet, der Zertifizierungsstelle wesentliche Änderungen in der Aufbau- und Ablauforganisation ihres Unternehmens mitzuteilen

2.2 Stufe 1 Audit

Das Audit der Stufe 1 wird durchgeführt, um

- einen Überblick und ein Review der Managementsystem-Dokumentation gemäß den Anforderungen des Standards zu erhalten,
- die Planung für das Stufe 2 Audit zu ermöglichen,
- den Status der Organisation bezüglich der Erfüllung der Anforderungen für das Stufe 2 Audit basierend auf das Managementsystem und dessen Leitlinien und –Ziele.

Das Unternehmen trifft alle erforderlichen Arrangements, um das Audit zu ermöglichen, einschließlich der Bereitstellung der Dokumente zu Dokumentenbewertung, dem Zugang zu allen Bereichen, Aufzeichnungen (einschließlich der Internen Audits und Berichte zum Managementreview), des Personal zur Begleitung der Zertifizierungs-, Überwachungs- und Re-Zertifizierungsaudits und der Beseitigung von Schwachstelen. Das Unternehmen stellt alle aktuellen Dokumente 4 Wochen vor dem Audit zur Verfügung.

Das Stufe 1 Audit beinhaltet u. a. eine Dokumentenbewertung. Die Zertifizierungsstelle stellt aufgrund der Unternehmensangaben fest, wo das Stufe 1 Audit stattfinden wird.

Die Organisation erhält einen Bericht über die Ergebnisse des Stufe 1 Audits einschließlich der Bewertung der Managementdokumentation und der damit vorhandenen Möglichkeit eventuelle

Nichtkonformitäten bis zum Stufe 2 Audit zu beseitigen. Dieser Bericht kann auch Aussagen zu unklaren Punkten beinhalten.

Falls im Audit Stufe 1 Nichtkonformitäten festgestellt wurden, sind diese vom Kunden bis zum Audit Stufe 2 zu beheben.

Kann abschließend nicht positiv festgestellt werden, dass der Kunde für das Audit der Stufe 2 bereit ist, erfolgt der Abbruch des Zertifizierungsverfahrens nach dem Audit Stufe 1.

Für die Koordinierung der Tätigkeiten des Audits Stufe 1 und ggf. die Abstimmung der beteiligten Auditoren untereinander ist der leitende Auditor verantwortlich.

2.3 Zertifizierungsaudit (Stufe 2 Audit)

Das Stufe 2 Audit wird gemäß dem abgestimmten Auditplan durchgeführt. Das Unternehmen hat das Recht Auditoren abzulehnen.
Das Audit beginnt mit einem Einführungsgespräch, in dem sich die Teilnehmer vorstellen. Das Vorgehen im Audit wird erläutert. Im Rahmen des Audits im Unternehmen überprüfen und bewerten die Auditoren die Wirksamkeit des eingeführten Managementsystems.
Während des Audit ermöglicht das Unternehmen den Zugang zu Aufzeichnungen aus den relevanten Geschäftsbereichen die im Geltungsbereich der Zertifizierung.
Im Audit werden u. a. folgende Punkte betrachtet:

- Dokumente, auf denen die Bewertung des Managementsystem beruht,
- Nachweise über Managementreview und interne Audits, das diese eingeführt, wirksam und gepflegt werden,
- die Wirksamkeit des Managementsystem in dem Geltungsbereich der Zertifizierung,
- Nutzung des Zertifikates und Zertifizierungszeichen (soweit vorhanden)
- Einsprüche gegen das Managementsystem

Wirksamkeit der Korrekturmaßnahmen bzgl. von Nichtkonformitäten aus vorangegangenen Audits.

Das Unternehmen hat die Pflicht, alle Einsprüche gegen das Managementsystem sowie deren Behandlung aufzuzeichnen und dies im Audit zugänglich zu machen.

In einem Abschluss-Gespräch werden die Auditergebnisse, einschließlich der dokumentierten Nichtkonformitäten, dem Unternehmen mitgeteilt. Nichtkonformitäten sind durch das Unternehmen zu untersuchen und geeignete Korrekturmaßnahmen einzuleiten. Ein entsprechender Nachweis ist zu erbringen. Nichtkonformitäten können zu neuen / geänderten Dokumenten / Verfahren und/ oder einem Nachaudit führen. Der Auditleiter entscheidet über den Umfang und Bereich des Nachaudits. Nur Aspekte die für die Nichtkonformitäten zutrafen werden auditiert.

Nachdem alle Korrekturmaßnahmen implementiert sind wird der Auditbericht erstellt.

2.4 Zertifikatserteilung

Die Erteilung des Zertifikates erfolgt mit der positiven Prüfung des Zertifizierungsverfahrens durch die Zertifizierungsstelle. Der Prüfende darf nicht an der Auditierung beteiligt gewesen sein.
Das Zertifikat kann nur dann erteilt werden, wenn alle Nichtkonformitäten behoben sind, d. h. wenn die Korrekturmaßnahmen vom Audit-Team angenommen bzw. verifiziert sind.

Die Zertifikate haben eine Gültigkeit von 3 Jahren.

3 ÜBERWACHUNGSAUDIT

Innerhalb der Gültigkeit des Zertifikates (3 Jahre) sind Überwachungsaudits einmal jährlich durchzuführen.
Folgende Punkte werden in dem Überwachungsaudit betrachtet:

- Wirksamkeit des Managementsystems im Geltungsbereich an ausgesuchten Beispielen
- korrekte Nutzung des Zertifikates und des Zertifizierungszeichens
- Einsprüche gegen das Managementsystem
- Wirksamkeit der Korrekturmaßnahmen bzgl. der Nichtkonformitäten aus vorangegangenen Audits

In einem Abschluss-Gespräch werden die Auditergebnisse, einschließlich der dokumentierten Nichtkonformitäten, dem Unternehmen mitgeteilt. Das Unternehmen erhält einen Auditbericht.

Neukunden:

Das auditrelevante Datum für das jährliche Überwachungsaudit, das dem Zertifizierungsaudit folgt, darf nicht später als 12 Monate nach dem letzten Tag des Audits der Stufe 2 liegen.

Bestandskunden:

Das auditrelevante Datum für das jährliche Überwachungsaudit ist das Gültigkeitsdatum des gültigen Zertifikats (Tag und Monat) minus 1 Monat.

Neukunden und Bestandskunden:

- Das auditrelevante Datum steuert sämtliche Folgeaudits (Überwachungs- und Rezertifizierungsaudits).
- Jedes Überwachungsaudit einschließlich der Prüfung, Annahme und ggf. Verifizierung von Maßnahmen zur Korrektur von Nichtkonformitäten, der Erstellung des Auditberichts und der Freigabe durch die Zertifizierungsstelle ist spätestens 3 Monate nach dem auditrelevanten Datum abzuschließen.
- Im Rahmen der Jahresüberwachung kann ein Überwachungsaudit frühestens 3 Monate vor dem auditrelevanten Datum durchgeführt werden.

Erlaubte Toleranz bei der Durchführung der jährlichen Überwachungsaudits: auditrelevantes Datum -3/+ 0 Monate.

3.1 Rezertifizierungsaudit

Rezertifizierungsaudits müssen – einschließlich der Prüfung von Maßnahmen zur Korrektur von Nicht-konformitäten – vor dem Ablauf der Geltungsdauer des Zertifikats abgeschlossen sein.
Im Rezertifizierungsaudit findet eine Überprüfung der Dokumentation des Managementsystems des Unternehmens sowie ein Audit vor Ort statt, wobei die Ergebnisse des/der vorangegangenen Überwachungsprogramms(e) über die Laufzeit der Zertifizierung zu berücksichtigen sind. Es werden alle Normanforderungen auditiert.
Tätigkeiten zu Rezertifizierungsaudits können ein Audit der Stufe 1 erfordern, wenn es signifikante Änderungen im Managementsystem oder im Zusammenhang mit den Tätigkeiten des Unternehmens gibt (z. B.: Gesetzesänderungen).

4 ERWEITERUNGSAUDIT

Soll der Geltungsbereich des bestehenden Zertifikates erweitert werden, so kann das durch ein Erweiterungsaudit geschehen. Die Durchführung des Erweiterungsaudits kann im Rahmen eines Überwachungsaudits, Rezertifizierungsaudits oder zu einem eigens angesetzten Termin erfolgen.

Die Gültigkeitsdauer eines Zertifikates ändert sich dadurch nicht. Ausnahmen sind schriftlich zu begründen.

5 ÜBERNAHME VON ZERTIFIZIERUNGEN ANDERER ZERTIFIZIERUNGSSTELLEN

Generell können nur Zertifikate von akkreditierten Zertifizierungsstellen übernommen werden. Organisationen mit Zertifikaten, die von nicht akkreditierten Zertifizierungsstellen ausgestellt wurden, sind als Neukunde zu behandeln.

Es ist ein „Pre-Transfer-Review“ durch eine kompetente Person der übernehmenden Zertifizierungsstelle durchzuführen, das in der Regel aus der Durchsicht wichtiger Dokumente sowie einem Besuch beim Kunden besteht.

Ausgesetzte Zertifikate oder solche, bei denen die Gefahr einer Aussetzung besteht, dürfen nicht übernommen werden. Offene Abweichungen sollten, soweit praktikabel, noch vor der Übernahme mit dem bisherigen Zertifizierer geklärt werden. Anderenfalls müssen sie im Audit behandelt werden.

Das weitere Überwachungsprogramm richtet sich nach dem bisherigen.

6 ZERTIFIZIERUNG VON UNTERNEHMEN MIT MEHREREN STANDORTEN

Wird ein Unternehmen, das mehrere Standorte unterhält, nach IEC 62443 zertifiziert, so sind diese Standorte ebenfalls zu auditieren. Die Zertifizierung von Unternehmen mit mehreren Produktionsstätten/Niederlassungen/Standorten etc. mit ähnlichem Tätigkeitsprofil und unter einem einheitlichen Managementsystem erfolgt durch die Anwendung eines Stichprobenverfahrens.

7 MANAGEMENT VON NICHTKONFORMITÄTEN

Für jede Nichtkonformität ist vom Unternehmen eine Ursachenanalyse durchzuführen und entsprechende Korrekturmaßnahmen sind zu implementieren. Das Unternehmen hat die Pflicht in Abhängigkeit der Schwere der Nichtkonformität, das Audit-Team innerhalb von 90 Tagen entweder über die festgelegten Korrekturmaßnahmen und Zieltermine oder über die Umsetzung der Korrekturmaßnahmen zu unterrichten. Wird diese Frist nicht eingehalten, gilt das Audit als nicht bestanden. Es kann kein Zertifikat erteilt werden bzw. das Zertifikat wird zurückgezogen.