

Inhaltsverzeichnis

1. Geltungsbereich	1
2. Anmeldung und Zulassung zur Prüfung	1
3. Durchführung der Prüfung	2
4. Bewertung	2
5. Wiederholung der Prüfung.....	2
6. Zertifizierungsentscheidung	3
7. Überwachung	3
8. Rezertifizierung.....	3
9. Prüfungsunterlagen	3
10. Kosten.....	4
11. Änderungsdienst.....	4
Anlage 1 - Profildarstellung IT Administrator	5
Anlage 2 - Profildarstellung IT Project Coordinator	7
Anlage 3 - Profildarstellung IT Security Coordinator	9
Anlage 4 - Profildarstellung IT Solution Developer	11
Anlage 5 - Profildarstellung IT Tester	13
Anlage 6 - Profildarstellung Software Developer	15
Anlage 7 - Dokumentenmatrix	17

1. Geltungsbereich

Diese Prüfungs- und Zertifizierungsordnung (PZO) gilt für das Zertifizierungsverfahren für IT-Spezialisten entsprechend dem Programm zur Zertifizierung von Personen der DEKRA Certification GmbH, auf der Grundlage der DIN EN ISO 17024 in der jeweils gültigen Fassung und für die folgenden Profile:

- IT Administrator
- IT Project Coordinator
- IT Security Coordinator
- IT Solution Developer
- IT Tester
- Software Developer

Zusätzlich gelten die Allgemeinen Geschäftsbedingungen (AGB) (D-030-18) und die Allgemeinen Zertifizierungsbedingungen (AZB) (D-030-19) der DEKRA Certification GmbH.

Die Dienstleistungen der Zertifizierungsstelle stehen allen interessierten Personen offen und die DEKRA Certification GmbH garantiert die Gleichbehandlung aller Antragsteller durch die Festlegung objektiver Kriterien für die Zulassung, die Prüfung und die Zertifizierung.

Aus Vereinfachungsgründen wurde für Bezeichnungen durchgängig die männliche Form gewählt. Damit soll keine Benachteiligung eines Geschlechts verbunden sein; die Bezeichnungen erfassen die jeweilige weibliche Form ebenso.

2. Anmeldung und Zulassung zur Prüfung

Die Anmeldung zu einer Prüfung und Zertifizierung erfolgt schriftlich anhand des Antrags zur Zertifizierung für IT-Spezialisten (F-03S-13) und Bestätigung der PZO, AZB und AGB der DEKRA Certification GmbH.

Die Teilnahme an der unter **Punkt 1** genannten Prüfung unterliegt den folgenden Zulassungsvoraussetzungen:

- Berufsqualifizierender Bildungsabschluss in einem Beruf des IT-Bereichs **oder**
- Berufsqualifizierender Bildungsabschluss in einem sonstigen Beruf **und** danach eine mindestens einjährige Berufspraxis im IT-Bereich **oder**

- Mindestens vierjährige Berufspraxis im IT-Bereich

Die Nachweispflicht liegt beim Teilnehmer. Die Zertifizierungsstelle prüft die Vollständigkeit und formale Richtigkeit der Anmeldeunterlagen sowie das Vorliegen der Zulassungsvoraussetzungen und entscheidet über die Zulassung zur Prüfung.

3. Durchführung der Prüfung

Die Prüfung in dem entsprechenden Profil erfolgt schriftlich und besteht aus **zwei Prüfungsteilen**: Erstellung einer profilspezifischen Projektdokumentation in Heimarbeit sowie Präsentation des Projekts und Fachgespräch.

Im ersten Prüfungsteil dokumentiert der Teilnehmer sein für die Zertifizierung vorgesehenes Projekt in schriftlicher Form unter Verwendung der von DEKRA zur Verfügung gestellten Dokumentationsvorlage des jeweiligen Profils. In der Dokumentation ist das Projekt (ggf. auch mehrere Projekt) im Gesamtüberblick und in den einzelnen Prozessen zu beschreiben. Zusätzlich sind in der Regel 10 Schlüsselsituationen darzustellen. Die Dokumentation kann bei der Anmeldung eingereicht werden, muss jedoch spätestens 6 Monate nach dem Einreichen des Antrages zur Zertifizierung und Zulassungsbestätigung zum Zertifizierungsverfahren bei DEKRA Certification GmbH eingehen. Wird dieser Zeitraum überschritten, ist ggf. ein neues Zertifizierungsverfahren zu beantragen. Keine der in der Dokumentation beschriebenen Tätigkeiten und Schlüsselsituationen darf vom Zeitpunkt der Einreichung der Dokumentation gerechnet älter als 24 Monate sein. Die Unterlagen sind dann vollständig und korrekt, wenn eine vollständig ausgefüllte Dokumentation mit eidesstattlicher Versicherung der eigenen Leistung eingereicht wird. Die Prüfung der Dokumentation erfolgt im Regelfall binnen 8 Wochen gerechnet ab dem Zeitpunkt der Einreichung bis zur Mitteilung an den Teilnehmer.

Nach positiver Prüfung der Dokumentation finden **im zweiten Prüfungsteil** die Präsentation des Projekts sowie Fachgespräch statt. Prüfungstermine und Prüfungsorte werden mit der Zertifizierungsstelle abgestimmt. Die Prüfung findet dabei entweder vor Ort in Präsenz oder online (z. B. Videokonferenzsystem, GoToMeeting®, Microsoft Teams) statt. Bei einer Prüfungsabnahme online muss der Teilnehmer sicherstellen, dass die technischen Anforderungen erfüllt sind (z. B. stabile Internetverbindung, Webcam). Der Termin für die Präsentation und das Fachgespräch sollte in der Regel nicht später als 6 Wochen nach positiver Prüfung der Dokumentation stattfinden. Die Prüfung findet unter Ausschluss der Öffentlichkeit statt. In der 30-minütigen Präsentation soll der Teilnehmer durch eine zusammenhängende Darstellung der Tätigkeiten und seiner Kompetenz sein prozessübergreifendes Verständnis in der gewählten Spezialisierung nachweisen. Dieser Nachweis erfolgt durch die Präsentation des vom Teilnehmer durchgeführten Projekts (kurze Gesamtdarstellung des Projekts, ausgewählte Prozesse und Schlüsselsituationen). Dem Prüfer sind die Präsentationsfolien in einer digitalen Form zur Verfügung zu stellen. Im darauffolgenden 30-minütigen Fachgespräch wird die Vollständigkeit und Komplexität der vom Teilnehmer nachgewiesenen Prozesse und Kompetenzen vom Prüfer hinterfragt. Die fachliche Kompetenz des Teilnehmers ist auf der Grundlage der in der Dokumentation beschriebenen Prozesse zu überprüfen.

Alle Bestandteile der Prüfung müssen den Stand der Kompetenzen entsprechend den Anforderungen des jeweiligen Profils bestätigen (gemäß den **Profildarstellung in der Anlage dieser PZO**).

Die Prüfung erfolgt grundsätzlich in deutscher Sprache. Die Organisation der Prüfung liegt in der Verantwortung der Zertifizierungsstelle. Die Prüfung führt ein zugelassener und von der DEKRA Certification GmbH für diese Durchführung beauftragter Prüfer durch. Die Organisation der Prüfung vor Ort obliegt dem eingesetzten Prüfer.

4. Bewertung

Die Bewertung der Prüfung erfolgt durch den beauftragten Prüfer.

Die Dokumentationsprüfung ist erfolgreich bestanden, wenn mindestens 80 % der geforderten Tätigkeiten und Kompetenzen des jeweiligen Profils nachweislich erfüllt sind. Diese Feststellung obliegt dem zuständigen Prüfer. Bei einem negativen Prüfungsergebnis werden dem Teilnehmer die Ablehnungsgründe mitgeteilt.

Der Prüfer entscheidet nach dem Fachgespräch, ob der Teilnehmer seiner Ansicht nach, die Kompetenzen entsprechend den Anforderungen des jeweiligen Profils besitzt oder nicht. Das Prüfungsergebnis und die Prüfungsunterlagen werden der Zertifizierungsstelle übermittelt und gegen geprüft.

5. Wiederholung der Prüfung

Eine nicht bestandene Prüfung/Prüfungsteil kann einmal wiederholt werden. Die Anmeldung zu einer Wiederholungsprüfung erfolgt schriftlich anhand des Antrags zur Wiederholungsprüfung (F-03S-09) und Bestätigung der PZO, AZB und AGB der DEKRA Certification GmbH.

Die Wiederholungsprüfung muss im Regelfall innerhalb von 60 Tagen nach der Zertifizierungsentscheidung (Datum des Entscheides) beantragt werden. Der Termin der Wiederholungsprüfung wird von der DEKRA

Certification GmbH festgelegt.

6. Zertifizierungsentscheidung

Das Zertifizierungsgremium trifft die Zertifizierungsentscheidung in der Regel innerhalb von max. 3 Wochen nach dem Prüfungstermin. Weicht das Zertifizierungsgremium vom Votum des Prüfers ab, ist dies schriftlich zu begründen.

Bei bestandener Prüfung und erfolgreicher Zertifizierung wird das DEKRA Zertifikat in deutscher Sprache für die Laufzeit von max. 3 Jahren erteilt. Das Zertifikat beinhaltet die folgenden Angaben: vollständiger Name, Geburtsdatum und Titel (falls vorhanden) der zertifizierten Person, die erworbene Qualifikationsstufe, der Hinweis auf das Zertifizierungsprogramm, nachgewiesene Kenntnisse und Kompetenzen, DEKRA Logo, DEKRA Zeichen, Angaben zur Zertifizierungsstelle, Prüfungsdatum, Prüfungsort, Ausstellungsdatum, Ausstellungsort, Ablaufdatum des Zertifikates, eindeutige Zertifikatsnummer sowie die Unterschrift der verantwortlichen Person.

Die Zertifikatsinhaber werden in das zur Veröffentlichung für berechnigte Personen bestimmte Verzeichnis der zertifizierten Personen der DEKRA Certification GmbH aufgenommen. Das Zertifikat bleibt das Eigentum der DEKRA Certification GmbH. Die Nutzungsbedingungen für das Zertifikat sind in den AZB geregelt.

7. Überwachung

Die zertifizierte Person hat eigenverantwortlich ihren Kompetenzerhalt sicherzustellen. Die DEKRA Certification GmbH überwacht die Einhaltung der Nutzungsbedingungen für das Zertifikat. Dazu gehören – sofern im Gültigkeitszeitraum des Zertifikats eintretend – die Auswertung von Informationen von Aufsichtsbehörden, die Bewertung von Beschwerden und Informationen von interessierten Kreisen sowie von eingeleiteten rechtlichen Schritten in Bezug auf die zertifizierte Person.

8. Rezertifizierung

Eine Rezertifizierung kann vom Zertifikatsinhaber spätestens bis zu 3 Monaten nach dem Ablauf der Gültigkeit des aktuellen Zertifikates unter Verwendung des Antrags zur Rezertifizierung (F-03S-17) schriftlich bei DEKRA Certification GmbH beantragt werden. Später eingereichte Anträge werden nicht akzeptiert.

Voraussetzung für eine Rezertifizierung sind ein vollständiger und korrekter Antrag sowie die erfolgreiche Durchführung einer Rezertifizierungsprüfung. Zusammen mit dem Antrag ist eine Beschreibung von einem bzw. von mehreren Projekten über mindestens 24 Monate Beschäftigung/Tätigkeit in einem dem zertifizierten Profil zuzuordnenden Gebiet einzureichen. Das Projekt bzw. die Projekte müssen von Ihnen im Zeitraum der Zertifikatsgültigkeit durchgeführt worden sein. Bitte verwenden Sie dafür das Formular Projektblatt RZ (F-03S-16).

Bei der fachlichen Prüfung soll festgestellt werden, inwieweit der Kompetenzerhalt des IT-Spezialisten in Bezug auf den aktuellen Stand der Technik und Methodik gegeben ist. Dazu analysiert der Prüfer die vom IT-Spezialisten eingereichten Projektblätter auf nicht nachvollziehbare Gegebenheiten und nicht hinreichend durchgeführte Prozesse (gemäß der **Profildarstellung in der Anlage dieser PZO**). Es findet ein 60-minütiges Fachgespräch statt. Prüfungstermine und Prüfungsorte werden mit der Zertifizierungsstelle abgestimmt. Das Fachgespräch findet dabei entweder vor Ort in Präsenz oder online (z. B. Videokonferenzsystem, GoToMeeting®, Microsoft Teams) statt. Bei einer Prüfungsabnahme online muss der Teilnehmer sicherstellen, dass die technischen Anforderungen erfüllt sind (z. B. stabile Internetverbindung, Webcam). Der Termin sollte in der Regel nicht später als 6 Wochen nach positiver Prüfung der Projektblätter stattfinden. Die Prüfung findet unter Ausschluss der Öffentlichkeit statt. In dem Fachgespräch mit dem IT-Spezialisten wird überprüft, ob die zertifizierten Kenntnisse, Fähigkeiten und Kompetenzen aufrechterhalten wurden.

Bei erfolgreicher Rezertifizierung wird ein neues Zertifikat für weitere max. 3 Jahre ausgestellt. Das bisherige Zertifikat verliert seine Gültigkeit.

9. Prüfungsunterlagen

Alle Unterlagen zur Prüfung werden von der Zertifizierungsstelle elektronisch oder in Papierform archiviert aufbewahrt. Die Aufbewahrungsfrist beträgt 10 Jahre.

10. Kosten

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erstprüfung (inkl. Zertifizierung)	1.000,00 EUR	1.190,00 EUR
Wiederholungsprüfung Dokumentation	350,00 EUR	416,50 EUR
Wiederholungsprüfung Präsentation/Fachgespräch	350,00 EUR	416,50 EUR
Rezertifizierung	750,00 EUR	892,50 EUR

Abweichend von diesen Regelpreisen kann für Gruppenprüfungen eine angemessene Rabattierung vereinbart werden. Die Zustimmung dazu obliegt dem Industry Expert Personnel Certification.

11. Änderungsdienst

Der Teilnehmer bzw. die zertifizierte Person hat sich laufend eigenverantwortlich über Änderungen an den für den Zertifizierungsprozess relevanten Verfahren, Beschreibungen, Dokumenten und Formularen zu informieren. Die aktuellen Unterlagen sind auf der Website der DEKRA Certification GmbH erhältlich.

Anlage 1 - Profildarstellung IT Administrator

IT Administrator

Kurzbeschreibung:

IT Administratoren konfigurieren, betreiben, überwachen und pflegen IT-Systeme oder Netze. Dabei kann es sich um Software-, Hardware- oder vernetzte Systeme ebenso handeln wie um IT-Infrastrukturen, Datenbanken oder Unternehmensanwendungen (Unter den Begriff Unternehmensanwendung fallen ERP-Systeme sowie alle Anwendungen, die Geschäftsprozesse (auch Produktionsprozesse) im Unternehmen und über Unternehmensgrenzen hinweg unterstützen).

Arbeitsgebiete und Aufgaben:

IT Administratoren analysieren und bewerten den internen und externen Datenverkehr, kontrollieren und analysieren Datendurchsatz und Fehlerrate. Ebenso analysieren und bewerten sie den Bedarf an Soft- und Hardware, Systemen und IT-Infrastruktur (z. B. Netzwerke), planen entsprechende Beschaffungen, installieren und konfigurieren IT-Systeme und ihre Komponenten. Sie organisieren den Betrieb von IT-Systemen, einschließlich automatischer Updates und Backups sowie den Benutzersupport. Sie analysieren Probleme, isolieren und beheben fehlerhafte Zustände und erarbeiten proaktiv Richtlinien und Verfahren für den störungsfreien Betrieb. Sie erarbeiten neue technische Konzepte für den Systembetrieb und entwickeln die Systeme unter Beachtung der Auswirkungen der Veränderungen bedarfsgerecht und wirtschaftlich weiter. IT Administratoren setzen auch Sicherheitsmaßnahmen um und sichern den Systembetrieb gegen Angriffe von außen und von innen.

Kompetenzen:

Gemeinsame Kompetenzen aller IT-Spezialisten

- Lernbereitschaft
- Eigenverantwortung
- Selbstmanagement

Profilspezifische Kompetenzen

- Analytische Fähigkeiten
- Beurteilungsvermögen
- Systematisch-methodisches Vorgehen
- Kommunikationsfähigkeit
- Gewissenhaftigkeit
- Eigenverantwortung
- Lernbereitschaft
- Selbstmanagement

Prozessspezifische Kompetenzen

- Belastbarkeit
- Dialogfähigkeit/Kundenorientierung
- Entscheidungsfähigkeit
- Konfliktlösungsfähigkeit
- Konzeptionsstärke
- Kooperationsfähigkeit
- Planungsverhalten
- Problemlösungsfähigkeit
- Sprachgewandtheit
- Teamfähigkeit

Hauptprozesse und Tätigkeiten:

1. Überwachen des Systembetriebs

- 1.1. Durchführen der initialen Bereitstellung
- 1.2. Durchführen kontinuierlicher Überwachung
- 1.3. Analysieren von Störungen, Lösungen und Anforderungen
- 1.4. Identifizieren möglicher Probleme
- 1.5. Planen des Reportings
- 1.6. Erstellen regelmäßiger Reports
- 1.7. Informieren betroffener Stellen/Personen
- 1.8. Klassifizieren der Störung und Prüfen des Störungsmusters
- 1.9. Priorisieren der Störung
- 1.10. Analysieren der Störung
- 1.11. Ausarbeiten einer möglichen Lösung
- 1.12. Einrichten des Workarounds
- 1.13. Beheben der Störung
- 1.14. Durchführen von Tests
- 1.15. Weitergeben der Änderungsanforderung an Change Management

1.16. Dokumentieren der Störung

2. Durchführen von Änderungen

2.1. Analysieren der Anforderungen

2.2. Planen der Durchführung

2.3. Einholen der Durchführungsfreigabe

2.4. Erstellen einer Prozessdokumentation

2.5. Informieren betroffener Personen/Stellen

2.6. Planen des benötigten Ziel-Release

2.7. Schätzen der Aufwände

2.8. Entwickeln der Komponenten

2.9. Beschaffen der erforderlichen Komponenten

2.10. Erstellen und Konfigurieren des Release

2.11. Testen des Release

2.12. Integrieren des Release in den Produktivbetrieb

2.13. Testen der Funktion des Release im Produktivbetrieb

2.14. Dokumentieren des Release und der Konfigurationsänderungen

3. Umsetzen und Überwachen von IT-Sicherheitsmaßnahmen

3.1. Mitwirken bei der Planung der Umsetzung des Sicherheitskonzepts

3.2. Umsetzen der technischen Sicherheitsmaßnahmen

3.3. Durchführen kontinuierlicher Kontrollen

3.4. Bewerten des Prüfergebnisses

3.5. Prüfen der Sicherheitsmaßnahmen auf mögliche Verbesserungen

3.6. Dokumentieren und Kommunizieren des Verbesserungsbedarfs

3.7. Informieren betroffener Personen/Stellen

3.8. Erstellen einer Prozessdokumentation

4. Unterstützen von Benutzern

4.1. Annehmen von Anfragen

4.2. Prüfen und Klassifizieren der Anfragen

4.3. Einweisen von Benutzern

4.4. Unterstützen von Benutzern

4.5. Beraten von Mitarbeitern der Fachabteilungen

4.6. Dokumentieren der Unterstützungsleistungen

Anlage 2 - Profildarstellung IT Project Coordinator

IT Project Coordinator

Kurzbeschreibung:

IT Project Coordinator leiten IT-spezifische Projekte oder Teilprojekte mit vorgegeben Zielsetzungen und Ressourcenrahmen.

Arbeitsgebiete und Aufgaben:

IT Project Coordinator steuern und überwachen die Anforderungen, Rahmenbedingungen und Verläufe von IT-Projekten. IT Project Coordinator arbeiten mit Spezialisten aus den beteiligten Bereichen, Nutzern und Auftraggebern zusammen, entwickeln Ziel- und Sollvorgaben und steuern deren Erreichung, lösen auftretende Konflikte, analysieren und behandeln potenzielle Risiken mit angemessenen Maßnahmen. Sie steuern technologische und personelle Ressourcen so, dass die Projektergebnisse anforderungsgerecht, d. h. qualitätsgerecht, zeitgerecht und im geplanten Budgetrahmen erreicht werden. Sie sorgen für leistungsfördernde Arbeitsbedingungen für die Projektmitarbeiter. IT Project Coordinator pflegen eine angemessene Beziehung zum Auftraggeber und halten gegenüber der Geschäftsführung oder einem Lenkungsausschuss die Projektergebnisse transparent. IT Project Coordinator haben im Projektteam eine Vorbild- und Steuerungsfunktion.

Kompetenzen:

Gemeinsame Kompetenzen aller IT-Spezialisten

- Lernbereitschaft
- Eigenverantwortung
- Selbstmanagement

Profilspezifische Kompetenzen

- Kommunikationsfähigkeit
- Belastbarkeit
- Beurteilungsvermögen
- Fachübergreifende Kenntnisse
- Eigenverantwortung
- Lernbereitschaft
- Selbstmanagement

Prozessspezifische Kompetenzen

- Analytische Fähigkeiten
- Dialogfähigkeit/Kundenorientierung
- Entscheidungsfähigkeit
- Ergebnisorientiertes Handeln
- Folgebewusstsein
- Konfliktlösungsfähigkeit
- Kooperationsfähigkeit
- Planungsverhalten
- Problemlösungsfähigkeit
- Systematisch-methodisches Vorgehen
- Teamfähigkeit

Hauptprozesse und Tätigkeiten:

1. Vorbereiten des Projekts

- 1.1. Mitwirken bei der Prüfung der Machbarkeit
- 1.2. Einholen der Freigabe vom Entscheider
- 1.3. Koordinieren der Anforderungsanalyse
- 1.4. Koordinieren der Erstellung des Fachkonzepts
- 1.5. Analysieren von Umfeld und Stakeholderinteressen
- 1.6. Analysieren der Projektrisiken
- 1.7. Festhalten der Rahmenbedingungen für das Projekt
- 1.8. Identifizieren der kritischen Erfolgsfaktoren
- 1.9. Schätzen der Aufwände und Kosten
- 1.10. Erstellen eines vorläufigen Phasen- und Terminplans
- 1.11. Präsentieren des Projekts beim Entscheider
- 1.12. Zusammenstellen des Projektteams
- 1.13. Durchführen eines internen Kick-Offs

2. Planen des Projekts

- 2.1. Planen der Projektphasen und Projektstruktur
- 2.2. Auswerten der Stakeholder- und Umfeldanalyse
- 2.3. Einrichten des Risikomanagements
- 2.4. Planen der Einsatzmittel/Ressourcen
- 2.5. Beschreiben der Arbeitspakete

- 2.6. Schätzen der Aufwände pro Arbeitspaket
- 2.7. Erstellen des Ablauf- und Terminplans
- 2.8. Erstellen der Kostenplanung
- 2.9. Präsentieren der Projektplanung bei Entscheider
- 2.10. Aufsetzen des Berichtswesens
- 3. Durchführen des Projekts**
- 3.1. Einrichten des Projektcontrollings
- 3.2. Verteilen von Arbeitsaufträgen
- 3.3. Betreuen der Projektmitarbeiter und -mitarbeiterinnen
- 3.4. Steuern und Absichern der Projektdurchführung
- 3.5. Feststellen der Projektkosten
- 3.6. Prüfen der Risikosituation
- 3.7. Ermitteln der Projektfortschritte
- 3.8. Bewerten der Projektsituation
- 3.9. Prüfen der Zielerreichungskriterien
- 3.10. Festlegen von Steuerungsmaßnahmen
- 3.11. Erstellen und Pflegen der relevanten Dokumente
- 4. Abschließen des Projekts**
- 4.1. Begleiten der Übergabe und Abnahme
- 4.2. Auswerten des Projekts
- 4.3. Auflösen von Projektteam und Projektinfrastruktur
- 4.4. Vervollständigen der Dokumentation
- 4.5. Erstellen des Projektabschlussberichts
- 4.6. Übergeben des Abschlussberichts an den Auftraggeber

Anlage 3 - Profildarstellung IT Security Coordinator

IT Security Coordinator

Kurzbeschreibung:

IT Security Coordinator sorgen für die Aufrechterhaltung der IT-Sicherheit im Unternehmen, setzen IT Sicherheitskonzepte entsprechend geltender technischer Standards, Gesetze und Vorschriften um und passen Konzepte wie Maßnahmen laufend den aktuellen Gegebenheiten an.

Arbeitsgebiete und Aufgaben:

IT Security Coordinator beraten und unterstützen Unternehmensleitung, Partner und Kunden hinsichtlich der IT-Sicherheit von kritischen Geschäftsprozessen. Sie arbeiten an der Erstellung der IT-Sicherheitspolicy mit und konzipieren angemessene Sicherheitslösungen entsprechend den geltenden technischen Standards, Gesetzen und anderen Vorschriften. IT Security Coordinator analysieren IT-Risiken und Schwachstellen, erstellen organisatorische und technische Sicherheitskonzepte gemeinsam mit den zuständigen Fachkräften und erarbeiten Richtlinien und Vorschriften zur Informationssicherheit. Sie realisieren IT-Sicherheitsmaßnahmen und entwickeln unter Berücksichtigung neuer Produkte und Verfahren sowie der wirtschaftlichen Gegebenheiten risikomindernde Maßnahmen und Sicherheitsverfahren und führen sie ein. Sie sorgen für die Schulung und Sensibilisierung der Mitarbeiter.

Kompetenzen:

Gemeinsame Kompetenzen aller IT-Spezialisten

- Lernbereitschaft
- Eigenverantwortung
- Selbstmanagement

Profilspezifische Kompetenzen

- Analytische Fähigkeiten
- Folgebewusstsein
- Konfliktlösungsfähigkeit
- Planungsverhalten
- Sprachgewandtheit
- Systematisch-methodisches Vorgehen

Prozessspezifische Kompetenzen

- Kommunikationsfähigkeit
- Beurteilungsvermögen
- Systematisch-methodisches Vorgehen
- Ergebnisorientiertes Handeln
- Gewissenhaftigkeit
- Teamfähigkeit
- Eigenverantwortung
- Lernbereitschaft
- Selbstmanagement

Hauptprozesse und Tätigkeiten:

1. Aufrechterhalten der IT-Sicherheit

- 1.1. Erstellen regelmäßiger Managementreports zur aktuellen Sicherheitslage
- 1.2. Überprüfen von Funktionalität und Aktualität von Sicherheitsprozessen und -maßnahmen
- 1.3. Mitwirken bei der Planung und Einrichtung neuer IT-Services
- 1.4. Untersuchen von Sicherheitsvorfällen
- 1.5. Durchführen der Risikobewertung
- 1.6. Erstellen von Sofortinformationen an das Management
- 1.7. Anpassen von Aufgaben, Arbeitsabläufen, Hilfsmitteln, Regeln
- 1.8. Durchführen von Funktionsprüfungen

2. Erstellen eines IT-Sicherheitskonzeptes

- 2.1. Ableiten der Schutzziele
- 2.2. Abstimmen der Schutzziele mit Entscheidern
- 2.3. Prüfen des Erreichens der Schutzziele
- 2.4. Planen von Schutzmaßnahmen für nicht erreichte Schutzziele
- 2.5. Ermitteln der Umsetzungsgrade der Schutzmaßnahmen
- 2.6. Dokumentieren von Schutzzielen, Prüfergebnissen und Maßnahmenplan
- 2.7. Präsentieren des Maßnahmenplans bei Entscheidern

3. Umsetzen des IT-Sicherheitskonzeptes

- 3.1. Planen der Umsetzung des Sicherheitskonzeptes
- 3.2. Schätzen der Aufwände für die Umsetzung
- 3.3. Erarbeiten notwendiger konkreter Maßnahmen und Änderungen

- 3.4. Aufstellen von Regeln und Verhaltensempfehlungen
- 3.5. Erstellen von Hilfsmitteln
- 3.6. Begleiten der Umsetzung der konkreten Maßnahmen und Änderungen
- 3.7. Planen und Durchführen von Sensibilisierungsmaßnahmen für die Mitarbeiter
- 3.8. Planen und Organisieren von Schulungen für die Mitarbeiter
- 3.9. Überprüfen der korrekten Umsetzung der Maßnahmen
- 3.10. Dokumentieren der Umsetzung
- 3.11. Durchführen von Funktions- und Wirksamkeitsprüfungen
- 3.12. Erstellen eines Managementreports zur IT-Sicherheit
- 4. Mitwirken bei der Aktualisierung der IT-Sicherheitspolicy**
- 4.1. Dokumentieren der Hintergrundinformationen für den Änderungsvorschlag
- 4.2. Mitwirken beim Identifizieren kritischer Geschäftsprozesse und zugehöriger Unternehmenswerte
- 4.3. Mitwirken beim Identifizieren und Bewerten der Risiken
- 4.4. Mitwirken beim Erstellen des Änderungsvorschlags für die IT-Sicherheitspolicy
- 4.5. Mitwirken beim Abstimmen des Änderungsvorschlags mit den Entscheidern

Anlage 4 - Profildarstellung IT Solution Developer

IT Solution Developer

Kurzbeschreibung:

IT Solution Developer realisieren informationstechnische Lösungen an der Schnittstelle zwischen Informationstechnologie und spezifischen Anwendungsgebieten wie z. B. Wissensmanagement, Logistik, Medizintechnik.

Arbeitsgebiete und Aufgaben:

IT Solution Developer sind in der Lage die spezifischen Anforderungen aus den jeweiligen Anwendungsgebieten und die Besonderheiten zur Umsetzung der Anforderungen miteinander zu verknüpfen und können durch Informationstechnologie eine Lösung erarbeiten. Sie realisieren IT-Lösungen oder begleiten die vollständige Realisierung von IT-Lösungen, beginnend mit dem Ermitteln der fachlichen Anforderungen bis zur Übergabe an den Auftraggeber. Die Realisierung einer IT-Lösung kann ebenfalls das Erneuern oder Erweitern einer vorhandenen IT-Infrastruktur beinhalten. IT Solution Developer entwickeln die Lösung soweit als möglich mit dem Kunden gemeinsam, um dessen Anforderungen und Bedürfnissen technisch und sachlich angemessen gerecht zu werden. IT Solution Developer realisieren eine IT-Lösung ergebnisorientiert in definierten Schritten von der Anforderungsabstimmung über die Entwicklung bis zu deren Einführung. Unabhängig von der gewählten Vorgehensweise ist es immer notwendig, die Anforderungen (für den jeweiligen Schritt) abzustimmen, das Vorgehen zu strukturieren und die Ergebnisse zu kontrollieren.

Kompetenzen:

Gemeinsame Kompetenzen aller IT-Spezialisten

- Lernbereitschaft
- Eigenverantwortung
- Selbstmanagement

Profilspezifische Kompetenzen

- Ergebnisorientiertes Handeln
- Gewissenhaftigkeit
- Kommunikationsfähigkeit
- Kooperationsfähigkeit
- Teamfähigkeit
- Eigenverantwortung
- Lernbereitschaft
- Selbstmanagement

Prozessspezifische Kompetenzen

- Analytische Fähigkeiten
- Beurteilungsvermögen
- Fachübergreifende Kenntnisse
- Folgebewusstsein
- Konzeptionsstärke
- Systematisch-methodisches Vorgehen
- Entscheidungsfähigkeit
- Akquisitionsstärke
- Dialogfähigkeit/Kundenorientierung
- Problemlösungsfähigkeit
- Sprachgewandtheit
- Marktkenntnisse
- Projektmanagement
- Konfliktlösungsfähigkeit
- Belastbarkeit
- Lernfähigkeit

Hauptprozesse und Tätigkeiten:

1. Konzipieren der fachlichen Lösung

- 1.1. Identifizieren und Beschreiben der betroffenen (Geschäfts-)Prozesse
- 1.2. Identifizieren und Beschreiben des Handlungsbedarfs
- 1.3. Identifizieren und Beschreiben von Rollen und Verantwortlichkeiten
- 1.4. Ermitteln der fachlichen Anforderungen
- 1.5. Ermitteln der Rahmenbedingungen
- 1.6. Ermitteln fachlicher Risiken
- 1.7. Gewichten und Bewerten der fachlichen Anforderungen
- 1.8. Erstellen fachlicher Lösungsansätze
- 1.9. Erstellen und Pflegen der relevanten Dokumente
- 1.10. Vorstellen und Diskutieren des Aufschlags für das Fachkonzept mit dem Auftraggeber

2. Konzipieren der technischen Lösung

- 2.1. Prüfen der funktionalen und technischen Machbarkeit
- 2.2. Prüfen und Einbeziehen von beachtenden Standards, Normen, Qualitätsanforderungen etc.
- 2.3. Überführen der fachlichen Anforderungen in technische Anforderungen
- 2.4. Bewerten der technischen Anforderungen auf technische Risiken
- 2.5. Prüfen möglicher technischer Lösungsvarianten
- 2.6. Prüfen von Standardlösungen und -komponenten auf Einsetzbarkeit
- 2.7. Schätzen von Aufwänden und Kosten für die Varianten
- 2.8. Planen des Projekts
- 2.9. Bewerten der Projektrisiken, Planen des Testens und der Validierung, einschließlich der Betaphase
- 2.10. Einholen, Bewerten und Bearbeiten von Angeboten
- 2.11. Bewerten der Funktionalität der Standardlösungen oder -komponenten bezogen auf das technische Konzept
- 2.12. Erstellen und Pflegen der relevanten Dokumente
- 2.13. Präsentieren der Varianten beim Entscheider

3. Realisieren der Lösung

- 3.1. Planen der technischen Umsetzung der Lösung im Detail
- 3.2. Definieren der organisatorischen und infrastrukturellen Anforderungen für die Umsetzung
- 3.3. Sicherstellen der Testbarkeit der Lösung
- 3.4. Planen des Änderungsmanagements, des Supports und der Wartung der Lösung
- 3.5. Mitwirken bei der detaillierten Projektplanung
- 3.6. Begleiten der technischen Umsetzung
- 3.7. Validieren der Lösung
- 3.8. Erstellen und Pflegen der relevanten Dokumente
- 3.9. Dokumentieren der Lösung

4. Ausliefern der Lösung

- 4.1. Mitwirken bei der Einweisung und Schulung der Nutzer
- 4.2. Integrieren der Lösung in die Zielumgebung
- 4.3. Durchführen der Betaphase in der Zielumgebung
- 4.4. Beheben von Mängeln und Optimieren der Lösung
- 4.5. Erstellen und Pflegen der relevanten Dokumente
- 4.6. Übergeben der Lösung an den Kunden/Auftraggeber

Anlage 5 - Profildarstellung IT Tester

IT Tester

Kurzbeschreibung:

IT Tester planen und organisieren die den Software- und Hardwareentwicklungsprozess begleitenden Tests auf den Stufen Komponenten-, Integrations-, System- und Abnahmetest und führen diese Tests durch. Sie stellen Testumgebungen bereit und sind für die Durchführung der Tests auf allen Stufen verantwortlich.

Arbeitsgebiete und Aufgaben:

IT Tester begleiten und unterstützen den Entwicklungsprozess in enger Zusammenarbeit mit Kunden und den Spezialisten aus den Bereichen Systemanalyse, Systementwicklung und Produktion. Zur Testgestaltung gehören der Entwurf und die Definition von Teststrategien, Testdaten, Testfällen und Testszenarien, die Planung und das Design von Testumgebungen, die Entwicklung von Tests sowie die Erstellung von automatisierten Testabläufen. Die Testdurchführung umfasst manuelle wie automatisierte Tests inklusive der entsprechenden Protokollierung. Dazu gehören Test- und Fehlerprotokolle, die Konfiguration, die Dokumentation und die Wartung von Testumgebungen.

Kompetenzen:

Gemeinsame Kompetenzen aller IT-Spezialisten

- Lernbereitschaft
- Eigenverantwortung
- Selbstmanagement

Profilspezifische Kompetenzen

- Systematisch-methodisches Vorgehen
- Kommunikationsfähigkeit
- Kooperationsfähigkeit
- Teamfähigkeit
- Eigenverantwortung
- Lernbereitschaft
- Selbstmanagement

Prozessspezifische Kompetenzen

- Analytische Fähigkeiten
- Belastbarkeit
- Beurteilungsvermögen
- Folgebewusstsein
- Gewissenhaftigkeit
- Problemlösungsfähigkeit

Hauptprozesse und Tätigkeiten:

1. Planen der Tests

- 1.1. Zusammenstellen der notwendigen Unterlagen
- 1.2. Mitwirken beim Festlegen von Umfang und Art der Testdokumentation
- 1.3. Erstellen und Pflegen der relevanten Dokumente
- 1.4. Festlegen der Testobjekte
- 1.5. Ableiten der Testziele
- 1.6. Mitwirken beim Festlegen der Teststrategie
- 1.7. Abschätzen von Testumfang und Testrisiken
- 1.8. Erstellen von Testphasenplan und Testterminplan
- 1.9. Planen der Ressourcen
- 1.10. Beschreiben der Testumgebung
- 1.11. Auswählen von Testwerkzeugen

2. Erstellen des Testdesigns

- 2.1. Erstellen und Pflegen der relevanten Dokumente
- 2.2. Analysieren der Testobjekte
- 2.3. Spezifizieren der Testfälle
- 2.4. Spezifizieren der Testdaten
- 2.5. Abstimmen des Testdesigns mit Verantwortlichen

3. Vorbereiten der Tests

- 3.1. Erstellen und Pflegen der relevanten Dokumente
- 3.2. Erstellen der Testumgebung
- 3.3. Beschaffen der Testdaten

- 3.4. Erstellen von Testszenarien
- 3.5. Vorbereiten von Testrahmen und Testskripten
- 3.6. Abstimmen der Testszenarien mit den Verantwortlichen
- 4. Durchführen der Tests**
 - 4.1. Erstellen und Pflegen der relevanten Dokumente
 - 4.2. Erfassen der Testobjekte
 - 4.3. Durchführen der Tests
 - 4.4. Auswerten der Testergebnisse
 - 4.5. Analysieren der Abweichungen
 - 4.6. Mitwirken bei der Entscheidung über das weitere Vorgehen
 - 4.7. Prüfen auf Erreichen der Testendekriterien
- 5. Abschließen der Tests**
 - 5.1. Mitwirken bei der Erstellung des Testberichts
 - 5.2. Vervollständigen der Dokumentation der Tests
 - 5.3. Übergeben der Testdokumentation an den Projektleiter
 - 5.4. Übergeben der Testmittel an die Wartung
 - 5.5. Analysieren und Dokumentieren der Erfahrungen aus dem Testprojekt

Anlage 6 - Profildarstellung Software Developer

Software Developer

Kurzbeschreibung:

Software Developer konzipieren und implementieren Komponenten für informationstechnische Systeme.

Arbeitsgebiete und Aufgaben:

Software Developer setzen einen Systementwurf in funktionsfähige, integrierbare Komponenten um. Dabei können Software Developer auf bestimmte Anwendungen, Funktionalitäten oder Bereiche spezialisiert sein. Software Developer spezifizieren Komponenten und definieren Schnittstellen. Sie entwerfen Algorithmen, definieren Datenstrukturen und setzen Programme in höheren Programmiersprachen, in der Regel mit Hilfe entsprechender Tools, um. Sie konzipieren und implementieren Datenbanken, erstellen auf der Ebene der Komponenten Testspezifikationen, Testdaten und Testumgebungen und führen die Tests durch.

Kompetenzen:

Gemeinsame Kompetenzen aller IT-Spezialisten

- Lernbereitschaft
- Eigenverantwortung
- Selbstmanagement

Profilspezifische Kompetenzen

- Analytische Fähigkeiten
- Belastbarkeit
- Dialogfähigkeit/Kundenorientierung
- Folgebewusstsein
- Gewissenhaftigkeit
- Konzeptionsstärke
- Problemlösungsfähigkeit

Prozessspezifische Kompetenzen

- Ergebnisorientiertes Handeln
- Systematisch-methodisches Vorgehen
- Kommunikationsfähigkeit
- Kooperationsfähigkeit
- Teamfähigkeit
- Eigenverantwortung
- Lernbereitschaft
- Selbstmanagement

Hauptprozesse und Tätigkeiten:

1. Überprüfen und Erweitern des Systementwurfs

- 1.1. Überprüfen und Abstimmen von Anforderungsdefinition und Systementwurf
- 1.2. Zerlegen des Systementwurfs in Komponenten
- 1.3. Präsentieren des Systementwurfs und Anforderungsdefinition beim Entscheider

2. Vorbereiten der technischen Umsetzung

- 2.1. Mitwirken bei der Projektplanung
- 2.2. Planen der technischen Umsetzung der Komponenten
- 2.3. Abstimmen mit Anforderungsmanagement und Qualitätssicherung
- 2.4. Mitwirken bei der Festlegung des Entwicklungsrahmens
- 2.5. Prüfen und Auswählen von Fertigprodukten
- 2.6. Bewerten und Auswählen existierender Standards

3. Festlegen der Schnittstellen

- 3.1. Konzipieren der erforderlichen Schnittstellen
- 3.2. Mitwirken bei der Konzeption der Systemintegration
- 3.3. Mitwirken bei der Konzeption der Systemtests
- 3.4. Abstimmen mit Anforderungsmanagement und Qualitätssicherung

4. Implementieren und Testen der Komponenten

- 4.1. Definieren von zu erstellenden Komponenten
- 4.2. Verfeinern der Entwürfe der Komponenten
- 4.3. Abstimmen der internen Schnittstellen und Datenformate
- 4.4. Ableiten von Testdaten und Testszenarien für Komponententests
- 4.5. Implementieren von Testprogrammen für Komponententests
- 4.6. Implementieren der Komponentenspezifikation
- 4.7. Durchführen von Komponententests
- 4.8. Dokumentieren der Entwicklung

Prüfungs- und Zertifizierungsordnung (PZO)

Standard IT-Spezialisten

Bereich Personenzertifizierung



4.9. Abstimmen mit Anforderungsmanagement und Qualitätssicherung

5. Vorbereiten der Integration

5.1. Vorbereiten der Integration

5.2. Mitwirken bei Systemintegration und Systemtests

5.3. Abstimmen mit Anforderungsmanagement und Qualitätssicherung

6. Übergeben und Einführen des Systems

6.1. Mitwirken bei der Vorbereitung der Installation in Betriebsumgebung

6.2. Mitarbeiten beim Erstellen von Dokumentation und Schulungsmaterialien

6.3. Begleiten der Installation und der Abnahmetests

6.4. Mitwirken bei technischen Einweisungen

Anlage 7 - Dokumentenmatrix

Dokument/Formblatt	Nr.	Teilnehmer			Prüfer			DEKRA Certification		
		EZ		RZ	EZ		RZ	EZ		RZ
Prüfungs- und Zertifizierungsordnung (PZO) IT-Spezialisten	D-03S-04	x		x	x		x	x		x
Allgemeine Zertifizierungsbedingungen (AZB) Personenzertifizierung	D-030-19	x		x	x		x	x		x
Allgemeine Geschäftsbedingungen (AGB) Personenzertifizierung	D-030-18	x		x	x		x	x		x
Ablauf des Zertifizierungsverfahrens Personenzertifizierung	V-09S-01				x		x	x		x
Antrag zur Zertifizierung IT-Spezialisten	F-03S-13	x						x		
Antrag zur Rezertifizierung	F-03S-17			x						x
Projektblatt RZ	F-03S-16			x			x			x
Dokumentationsvorlage IT Administrator	F-03S-19	x			x			x		
Dokumentationsvorlage IT Project Coordinator	F-03S-11	x			x			x		
Dokumentationsvorlage IT Security Coordinator	F-03S-29	x			x			x		
Dokumentationsvorlage IT Solution Developer	F-03S-20	x			x			x		
Dokumentationsvorlage IT Tester	F-03S-12	x			x			x		
Dokumentationsvorlage Software Developer	F-03S-10	x			x			x		
Profilmatrizen IT-Spezialisten	C-09S-22				x			x		
Prüfungsbericht IT-Spezialisten	F-09S-35				x		x	x		x
Antrag zur Wiederholungsprüfung	F-03S-09	o		o				o		o
Zertifikat*	-	x		x				x		x
Entscheid zum Zertifizierungsverfahren	-	x		x				x		x
Prüferbeauftragung	F-06S-03				x		o	x		o
Rechnung und Reisekostenbelege des Prüfers	-				x		x	x		x
DIN EN ISO 17024	-						x			x
Erklärungen:										
EZ = Erstzertifizierung RZ = Rezertifizierung o = bei Bedarf (optional) x = zwingend erforderlich *Zertifikat nur bei erfolgreicher Zertifizierung										