

ZERTIFIZIERUNG  
NIS Expert



## VORWORT

# Certified NIS Expert

Diese nach ISO 17024 autorisierte Personenzertifizierung entspricht den international gültigen Standards und genießt weltweite Anerkennung.

Inzwischen reicht es für Unternehmen und andere Organisationen nicht mehr aus, in Security-Infrastruktur und -Produkte zu investieren. Security-Spezialist:innen müssen heute über umfangreiche Kompetenzen im Bereich Sicherheitsprozesse sowie über Kenntnisse technischer und organisatorischer Maßnahmen und der rechtlichen Rahmenbedingungen verfügen. Zertifizierungen stehen für eindeutige und hochwertige Kompetenzen. Sie gewinnen immer mehr an Bedeutung, da Auftraggeber:innen klare Kriterien für ihre Entscheidungen benötigen. Der Bedarf an Expert:innen mit entsprechendem Know-how im Bereich der Informationssicherheit wächst ständig, bedingt durch den technologischen Wandel, die zunehmende Abhängigkeit von digitalisierten Prozessen und das dadurch immer größer werdende Bedrohungspotenzial.

Mit dem NISG 2026 (Netz- und Informationssystemsicherheitsgesetz 2026) zur Umsetzung der Cybersicherheits-Richtlinie NIS-2 werden rund 4.000 Unternehmen und Einrichtungen aus gesellschaftlich relevanten Sektoren („wesentliche und wichtige Einrichtungen“) zu umfassenden Risikomanagementmaßnahmen und Meldepflichten bei Sicherheitsvorfällen verpflichtet. Auch deren Dienstleister und Lieferanten müssen entsprechende Maßnahmen treffen. Die Leitungsorgane wesentlicher und wichtiger Einrichtungen sind für die Aufsicht und Umsetzung der Vorgaben verantwortlich. Es gelten strenge Aufsichts- und Durchsetzungsmaßnahmen, im Extremfall bis hin zum Entzug von Genehmigungen zur Ausübung der Dienste bei wesentlichen Einrichtungen. Bei Nichterfüllung drohen Sanktionen von bis zu 10 Millionen Euro oder 2 % des Gesamtjahresumsatzes des Konzerns bei wesentlichen Einrichtungen bzw. von bis zu 7 Millionen Euro oder 1,4 % des Gesamtjahresumsatzes des Konzerns bei wichtigen Einrichtungen.

Das NISG 2026 gilt ab 1. Oktober 2026, weshalb sich betroffene Unternehmen rechtzeitig vorbereiten müssen. Mit der Zertifizierung „Certified NIS Expert“ und Ihrer bisherigen Berufserfahrung sind Sie in der Lage, die von Ihnen betreuten Unternehmen und Organisationen auf die gesetzlichen Anforderungen vorzubereiten und das Risiko von Schäden durch Cyberangriffe und andere Cybersicherheitsvorfälle zu verringern.



DAFÜR BRAUCHT ES MEHR EXPERTINNEN UND EXPERTEN,  
SOWIE BERATERINNEN UND BERATER!

# INHALT

1. Bedeutung	3
2. Basiswissen	5
3. Beurteilung	7
4. Unterlagen	9
5. Begutachtung	14
6. Rezertifizierung	18
7. Kosten	19
8. Kontakt	20

## NIS EXPERT ZERTIFIKAT

# 1. Bedeutung

Das Zertifikat „Certified NIS Expert“ wird vom zertifizierungsberechtigten Institut an Beraterinnen und Berater sowie Expertinnen und Experten mit relevanten Erfahrungen, Kenntnissen und Fähigkeiten im Bereich Informationssicherheit verliehen.

incite – Ihre Anlaufstelle für die Zertifizierung



## Vergabe

Die Zertifizierung wird exklusiv von incite verliehen, der Qualitätsakademie des Fachverbandes Unternehmensberatung, Buchhaltung und IT (UBIT).



## Anerkennung

incite ist nach ISO 17024 autorisiert und garantiert einen objektiven Prüfungs-, Entscheidungs- und Zertifizierungsprozess.



## Zielgruppe

Die Zertifizierung richtet sich ausschließlich an natürliche Personen, also nicht an Unternehmen, Institutionen oder Produkte.



## Organisationen

Unternehmen und Institutionen können jedoch qualifizierte Mitarbeiterinnen und Mitarbeiter zur Zertifizierung anmelden, sofern die Voraussetzungen erfüllt sind.



## Nutzen des Zertifikats

- **Qualitätsdarstellung:**  
Dokumentation des State of the Art in den relevanten Themenbereichen
- **Stärkung Ihrer Marktposition:**  
Qualitative Sichtbarkeit und Profilierung nach außen
- **Unterstützung bei der Kundengewinnung:**  
Der Fachverband UBIT bewirbt das Zertifikat aktiv. Ein spezieller Online-Service erleichtert potenziellen Auftraggeberinnen und Auftraggebern die Suche nach zertifizierten Expertinnen und Experten.

Für wen ist die Zertifizierung gedacht?

Die Zertifizierung wendet sich an Personen, die in folgenden Bereichen tätig sind:

- Netz- und Informationssicherheit sowie IT- und Informationssicherheitsmanagement
- Planung, Gestaltung und Umsetzung von Informationssicherheitskonzepten unter Berücksichtigung der NIS-2-Gesetzgebung (insbesondere NISG 2026 und zugehörige Verordnungen, NIS-2-Richtlinie und Durchführungsverordnung (EU) 2024/2690)
- Bewertung von Netz- und Informationssicherheit und Bestimmung des Reifegrads der Umsetzung in Organisationen
- Beratung und Unterstützung von Geschäftsleitungen, Beschäftigten, Kunden sowie Lieferanten in Fragen der Netz- und Informationssicherheit

 Sensibilisierung und Kommunikation der Bedeutung von Netz- und Informationssicherheit innerhalb von Unternehmen und Organisationen.

## Ihr Kompetenzprofil nach der Zertifizierung

Die zertifizierten Personen

- sind mit den technischen, organisatorischen und juristischen Grundlagen vertraut, die für Netz- und Informationssicherheit unverzichtbar sind,
- sind sich der Bedeutung von Netz- und Informationssicherheit für Menschen und Unternehmen bzw. Organisationen und der Konsequenzen bewusst,
- wissen über die Rahmenbedingungen der NIS-2-Gesetzgebung, insbesondere NISG 2026, NIS-2-Richtlinie und Durchführungsverordnung (EU) 2024/2690 Bescheid und können darauf aufbauend entsprechende Informationssicherheitskonzepte planen, gestalten und umsetzen,
- sind in der Lage, Netz- und Informationssicherheit zu evaluieren und den Reifegrad der Umsetzung zu bestimmen,
- verfügen über die notwendigen Kompetenzen anderen, insbesondere der Geschäftsleitung und den Mitarbeiter:innen, Kunden und Lieferanten die Bedeutung von Netz- und Informationssicherheit zu vermitteln.



## GRUNDLAGEN DER NETZ- UND INFORMATIONSSICHERHEIT (NIS)

# 2. Basiswissen

Um Netz- und Informationssicherheit wirksam umzusetzen, ist es unerlässlich, die technischen, organisatorischen und rechtlichen Grundlagen zu verstehen sowie deren Bedeutung für Unternehmen, Organisationen und Gesellschaft einordnen zu können. Die folgenden Punkte bilden das Fundament für ein systematisches und praxisorientiertes Verständnis der NIS-2-Anforderungen.



## Wissen, warum!

1. Netz- und Informationssicherheit
  - Bedeutung von Netz- und Informationssicherheit für Unternehmen und Organisationen
  - Risiken durch Digitalisierung, Vernetzung sowie Abhängigkeit von IT- und OT-Systemen
  - Auswirkungen von Sicherheitsvorfällen auf Menschen, Geschäftsprozesse und Gesellschaft
2. Sozial- und betriebswirtschaftliche Bedeutung und Chancen von NIS
  - Schutz kritischer Dienstleistungen und Wertschöpfungsketten
  - Resilienz, Vertrauen und Reputation
  - Wettbewerbsvorteile durch systematisches Sicherheits- und Risikomanagement
3. Gesetze und rechtliche Rahmenbedingungen, Auszug
  - NIS-2-Richtlinie
  - Netz- und Informationssystemsystemsicherheitsgesetz 2026 (NISG 2026)
  - Durchführungsverordnung (EU) 2024/2690
4. Mehrfachnutzen von Netz- und Informationssicherheit
  - Compliance und Rechtssicherheit
  - Business Continuity und Notfallvorsorge
  - Integration in Governance, Risiko- und Qualitätsmanagement

## Wissen, was!

5. Anforderungen der NIS-2-Gesetzgebung
  - Anwendungsbereich und betroffene Einrichtungen
  - Governance und Verantwortung der Leitungsorgane
  - Pflichten der Einrichtungen
  - Risikomanagement inklusive Sicherheit der Lieferkette
  - Technische und organisatorische Maßnahmen
  - Nachweis der Wirksamkeit
  - Meldepflichten

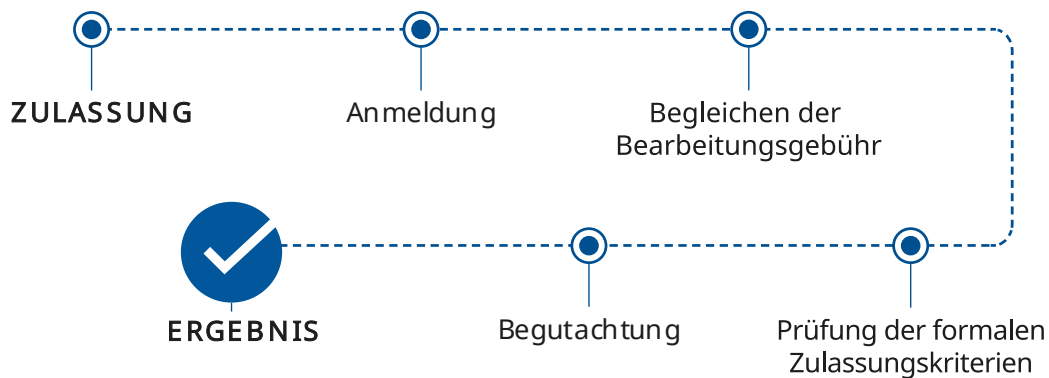
## Wissen, wie!

6. Planung und Umsetzung von Informationssicherheitskonzepten
  - Ableitung von Sicherheitsmaßnahmen aus gesetzlichen Anforderungen
  - Integration von IT- und OT-Sicherheit
  - Aufbau und Weiterentwicklung von Informationssicherheitsmanagement (ISMS) in Einrichtungen
7. Risikomanagement, Testen und Evaluation
  - Identifikation, Analyse und Bewertung von Risiken
  - Einsatz geeigneter Methoden und Werkzeuge
  - Dokumentation, Berichterstattung und Management-Reviews
  - Reifegradanalysen und Wirksamkeitsprüfungen
8. Technische, organisatorische und strategische Umsetzung
  - Technische und organisatorische Maßnahmen
  - Incident Management und Meldeprozesse
  - Business Continuity Management und Notfallmanagement
  - Netz- und Informationssicherheit als Führungsaufgabe
  - Verankerung in Unternehmensstrategie, Leitbild und Governance
  - Integration in Prozesse, Workflows und Projektmanagement
  - Zusammenarbeit mit internen und externen Stakeholdern

## ABLAUF UND KRITERIEN DER BEURTEILUNG

# 3. Beurteilung


Nach Anmeldung und Zahlung der Bearbeitungsgebühr wird der Zugang zum Kundenportal freigeschaltet. Die erforderlichen Unterlagen sind über die vorgesehenen Formulare vollständig einzureichen. Anschließend werden sie durch Sachverständige begutachtet und beurteilt.



### 1. Anmeldung und Unterlagen für die Zulassung

- Motivationsschreiben
- Lebenslauf
- Praxisnachweis von zwei Projekten aus den letzten drei Jahren
- Projektarbeit
- Aus- und Weiterbildung
- Anmeldung zur Zertifizierung
- Formulare für die Erstzertifizierung

Die detaillierten Anforderungen an die Einreichung der Unterlagen finden Sie im **4. Kapitel „Unterlagen“** auf Seite 9.

 Die Antragsunterlagen müssen nach verbindlicher Anmeldung zur Zertifizierung im Kundenportal hochgeladen werden.

## 2. Begleichen der Rechnung für die Bearbeitungsgebühr

Nach dem Einlangen Ihrer Unterlagen erhalten Sie eine Rechnung über die Bearbeitungsgebühr. Nach der Zahlung wird Ihr Antrag bearbeitet.

## 3. Prüfung der formalen Zulassungskriterien

incite prüft die formalen Zulassungsvoraussetzungen und bewertet die Antragsunterlagen.

## 4. Begutachtung

Die inhaltliche Begutachtung der eingereichten Unterlagen auf fachlicher Ebene erfolgt durch unabhängige Sachverständige gemäß den festgelegten Kriterien.

## 5. Ergebnis

Für die Zertifizierung ist eine positive Beurteilung der Projektarbeit erforderlich. Diese kann sich auf eines der im Praxisnachweis dargestellten Projekte beziehen. Nähere Informationen zu Inhalt und Erstellung der Projektarbeit sind im Kapitel „Unterlagen“ zu finden.

## ANFORDERUNGEN IM DETAIL

# 4. Unterlagen

Damit Ihr Antrag vollständig und korrekt bearbeitet werden kann, ist die Einreichung spezifischer Unterlagen erforderlich. Die folgenden Punkte zeigen im Detail, welche Nachweise benötigt werden und welche inhaltlichen Anforderungen dabei zu beachten sind.

### Motivationsschreiben

Das Motivationsschreiben im Umfang von ein bis maximal zwei A4-Seiten soll zu folgenden Punkten Aussagen treffen:

- Zu Ihrer Person: Was motiviert Sie, die Zertifizierung zu beantragen?
- Über welche Qualifikationen, Kenntnisse und Kernkompetenzen verfügen Sie, die dem Profil der Zertifizierung entsprechen?

### Lebenslauf

Der Lebenslauf dient einerseits als Basis zur Beurteilung der Ausbildung und der bisherigen Tätigkeiten. Als Nachweis ist ein umfassender Lebenslauf beizulegen, der die folgenden Punkte aufweist:

- aktueller persönlicher Status
- Aus- und Weiterbildung
- beruflicher Werdegang

### Praxisnachweis

Es muss eine mindestens dreijährige Tätigkeit als Informationssicherheitsexperte/in (selbständige oder unselbständige Tätigkeit) nachgewiesen werden.

Dieser Nachweis ist durch eine Auflistung von zwei Projekten aus den letzten drei Jahren im Bereich Informationssicherheit, idealerweise im Bereich der Umsetzung der NIS-Gesetzgebung (NISG 2026 oder NISG 2018), zu ergänzen. Dabei ist insbesondere auf die NIS-Anforderungen im IT und auch OT-Bereich, Risikomanagement, Business Continuity und Notfallmanagement einzugehen.

Die Projekte sollen unter Berücksichtigung der nachfolgend angeführten Punkte skizziert und nachvollziehbar dargestellt werden:

- Ausgangssituation und Zielsetzung
- Konzept und Umsetzung
- kritische Faktoren/Herausforderungen
- Erfolgsfaktoren und Ergebnis/Kundennutzen

Diese zwei Projekte werden anhand von Kundinnen-/Kunden- bzw. Dienstgeber-/Dienstgeberinnenreferenzen belegt (siehe Formular Kundenreferenz). Sollten die Anwärter/innen in den vergangenen drei Jahren z.B. ausschließlich an einem Großprojekt gearbeitet haben, so ist ggf. alternativ für einzelne Projektabschnitte je eine entsprechende Referenz vorzuweisen.

## Kundenreferenzen

Diese zwei Projekte (siehe Punkt Praxisnachweise) werden anhand von Kundenreferenzen belegt.



Bitte lassen Sie dieses Formular von einer Kundin oder einem Kunden oder Ihrem Dienstgeber (bei unternehmensinternem Projekt) ausfüllen und fügen Sie es Ihren Antragsunterlagen bei.

[Zum Formular Kundenreferenzen \[PDF\]](#)

## Laufende Aus- und Weiterbildungen

Es ist ein Nachweis über eine facheinschlägige Aus- oder kontinuierliche Weiterbildung mit Schwerpunkten in den unten angeführten Wissensgebieten zu erbringen. Ergänzend fügen Sie bitte eine aussagekräftige Selbstdarstellung bei, in der Sie detailliert auf absolvierte Fachvorträge, Seminare, Schulungen, Konferenzen, Kongresse oder Eigenstudien (Fachliteratur, Webseiten, Lehrmaterialien) eingehen, sofern diese nicht bereits eindeutig und vollständig aus Ihrem Lebenslauf hervorgehen.

Zum Nachweis sind entsprechende Belege wie Teilnahmebestätigungen, Zeugnisse o. Ä. beizulegen.

Wissenschwerpunkte in der Aus- und Weiterbildung zur NIS-2-Gesetzgebung sind:

- Rechtliche Grundlagen der NIS-2-Gesetzgebung, insbesondere NISG 2026
- Anwendungsbereich
- Governance und Verantwortung der Leitungsorgane
- Pflichten der betroffenen Einrichtungen:
- Registrierung
- Risikomanagement
- Technische und organisatorische Maßnahmen
- Nachweis der Wirksamkeit der Risikomanagementmaßnahmen
- Meldepflichten
- Durchsetzung, Aufsicht und Sanktionen

Zum Ausbildungsnachweis werden beispielsweise anerkannt:

- abgeschlossenes Universitätsstudium in Wirtschaftsinformatik, Telematik und Informatik oder ähnlichen Studienrichtungen
- äquivalente Master- oder Fachhochschulstudien bzw. entsprechend andere facheinschlägige Lehrgänge
- abgeschlossene AHS oder BHS Fachrichtung Elektrotechnik oder Informatik (oder vergleichbar)
- zusätzlich ist auf Weiterbildung speziell zu NIS-2 nachzuweisen (z.B.: Kurs, Selbststudium von Unterlagen).

- incite behält sich die Anerkennung von Aus- und Weiterbildungen zu den o.a. Schwerpunkten vor.



Die Weiterbildungsangebote Webinar und Workshop Cybersicherheitsrichtlinie NIS 2 für Führungskräfte, Workshop NISG 2026, Workshop NISG 2026 für Führungskräfte, Lehrgang Data & IT Security Expert erfüllt die Weiterbildungsanforderungen zur Zertifizierung. Die Anerkennung anderer Aus- und Weiterbildungen erfolgt durch incite.

## Projektarbeit

Die Zertifizierung setzt eine positive Beurteilung der Projektarbeit voraus. Details regelt die „Anleitung zur Projektarbeit für die Zertifizierung als NIS Expert.“

Ziele der Projektarbeit:

Mit der Projektarbeit soll der Autor/die Autorin seine/ihre Kenntnisse und Fähigkeiten bei der Umsetzung von Vorgaben zur Implementierung von Netz- und Informationssicherheit (NIS) in einem Unternehmen oder einer anderen Organisation darstellen. Dabei soll es sich um ein konkretes NIS-Projekt handeln, das selbst umgesetzt, geleitet oder (mit)gestaltet wurde. Es sollen eigene Erfahrungen bei der Umsetzung des Projekts beschrieben werden. Es wird empfohlen, ein reales Projekt in einem Unternehmen oder in einer anderen Organisation heranzuziehen. Es können Annahmen getroffen werden (z.B. bezüglich Unsicherheiten aufgrund noch ausstehender Rechtsakte), diese müssen jedoch sinnvoll und nachvollziehbar sein.

Die Projektarbeit wird nach folgenden Bewertungskriterien beurteilt:

- Aufbau und Struktur
- Inhalt und Einhaltung der inhaltlichen Vorgaben
- Bezug zum Thema, Richtigkeit und Relevanz des Inhalts, Kompaktheit
- Fachkompetenz: Niveau, Schwierigkeitsgrad
- Praxisbezug
- Qualität der Lösung
- Bedeutung der Arbeit (z.B. Nutzen für die beratene Organisation)
- Kreativität und Eigenständigkeit
- Gesamtbild

Detaillierter Aufbau der Projektarbeit:

- Titel der Projektarbeit
- Inhaltsverzeichnis
- Einleitung [ca. 1 Seite; 1.800 Zeichen inkl. Leerzeichen; max. 3.600 Zeichen]
  - Kurze Beschreibung der eigenen Rolle des Autors/der Autorin im Projekt
  - Kurze Beschreibung der Einrichtung (Unternehmens oder der Organisation), in der Maßnahmen zur Netz- und Informationssicherheit implementiert wurden (Geschäftsbereiche, Struktur, usw.). Hinweis: Aus datenschutzrechtlichen Gründen empfehlen wir die Organisation nicht namentlich zu nennen, eine kurze Beschreibung mit für die Projektarbeit relevanten Daten wie Branche, Mitarbeiterzahl, etc., ist

ausreichend. Es ist auch zulässig eine fiktive Organisation heranzuziehen, wobei darauf ausdrücklich hinzuweisen ist.

- Motivation der Einrichtung für das Projekt (z.B. Eigeninteresse, gesetzliche Anforderungen, Aufforderung durch Kunden)
- Hauptteil [ca. 4,5 Seiten; 8.100 Zeichen inkl. Leerzeichen]
  - Ausgangssituation
  - Prüfung, ob die Einrichtung in den Anwendungsbereich des NISG 2026 fällt, ggf. unter genauer Angabe des entsprechenden (Teil-)Sektors laut Anlage 1 oder 2 NISG 2026, oder ob die Einrichtung in die Lieferkettenregelung fällt.
  - Vorteile und Nutzen der Umsetzung der Maßnahmen
  - Herausforderungen
  - Ziele des Projekts (z.B. Implementierung der gesetzlichen Vorgaben im Unternehmen, Vorbereitung auf eine Zertifizierung oder Prüfung durch eine unabhängige Stelle, Verbesserung der Cyberresilienz in Bezug auf...) und Nicht-Ziele
  - Umsetzungsplan mit Zeitplan
  - grobe Kostenschätzung (kann auch fiktiv sein)
  - Realisierung des Projekts (Projektphasen)
- Reflexion und Learnings [ca. 1,5 Seiten; 2.700 Zeichen inkl. Leerzeichen]
- Anhang und Anlagen  
Es ist möglich ergänzende Unterlagen (Skizzen, Diagramme, Pläne, statistische Auswertungen, etc.) anzufügen. Diese zählen zum Umfang (maximale Seitenanzahl) der Projektarbeit und sind im Text zu erläutern, sofern, sie nicht selbsterklärend sind.
- Allfällige Quellennachweise und Literaturverzeichnis  
Allfällige Zitate sind anzugeben (z.B. mit fortlaufender Kopfnote und im Literaturverzeichnis).
- Erklärung des Verfassers  
Die Erklärung der eigenständigen Erstellung der Projektarbeit bzw. die Kennzeichnung von KI-generierten Passagen erfolgt durch die ausdrückliche Bestätigung der entsprechenden Checkbox im Kundenportal.
- Form  
Die Projektarbeit soll so gestaltet sein, dass sie den Anforderungen im Geschäftsleben (z.B. Vorlage der Projektarbeit durch eine/n externe/n Berater/in bei einem Kunden) entspricht. Bullet points und stichwortartige Angaben sind zulässig, sofern sie sinnvoll sind und die Aussage nachvollziehbar ist.
- Umfang  
Der Umfang der Projektarbeit (ohne Inhaltsverzeichnis, Quellenangabe und Anhang) soll 7 bis 10 A4-Seiten (12.600 bis 18.000 Zeichen inkl. Leerzeichen) maximal aber 14 A4-Seiten (25.200 Zeichen inkl. Leerzeichen) inklusive aller Dokumente (Anlagen, etc.) umfassen.

## Selbstauskunft und Zustimmungserklärung



[Zum Formular Selbstauskunft \[PDF\]](#)

## BEURTEILUNG IM DETAIL

# 5. Begutachtung

Die Projektarbeit bildet den zentralen Bestandteil des Qualifikationsverfahrens und entscheidet u.a. über die Vergabe des Zertifikats. Um Fairness, Objektivität und Qualität zu gewährleisten, gelten klare Rahmenbedingungen, Abläufe und Beurteilungskriterien.

### Verfahren im Überblick

Um sicherzustellen, dass die Vergabe der Zertifizierung tatsächlich nur an hoch qualifizierte, und erfahrene Anwärterinnen und Anwärter erfolgt, müssen diese neben der Erfüllung der formalen Zulassungsvoraussetzungen ihre Erfahrungen im Rahmen einer Projektarbeit darstellen.

In der Projektarbeit wird die Arbeitsweise der Anwärterin oder dem Anwärter durch Sachverständige überprüft.


### Beurteilung

Die Beurteilung erfolgt mit „Projektarbeit positiv beurteilt“ oder „Projektarbeit nicht positiv beurteilt“. Ein Rechtsmittel dagegen nicht zulässig.

Negative Beurteilung:

Im Falle einer nicht positiv beurteilten Projektarbeit ist eine einmalige Neuabgabe in den Kosten der Zertifizierung inkludiert.

Die endgültige Freigabe der Zertifizierung erfolgt nach positiver Beurteilung aller Voraussetzungen durch incite.

 **Es wird darauf hingewiesen, dass alle Informationen und Daten vertraulich behandelt werden und eine Verschwiegenheitspflicht besteht.** Den Sachverständigen liegen alle notwendigen Unterlagen der Anwärterin oder des Anwärters vor. Bitte achten Sie darauf in der Projektarbeit keine Informationen wie personenbezogene Daten, sensiblen Daten, Geschäfts- und Betriebsgeheimnisse preiszugeben. Es ist möglich für die Projektarbeit ein fiktives Unternehmen heranzuziehen. Bei realen Unternehmen empfehlen wir allfällige Informationen über diese Unternehmen oder Personen zu anonymisieren. Ist dies nicht möglich, gehen Sie von fiktiven Annahmen aus bzw. ändern Sie den Sachverhalt entsprechend ab.

## Sachverständige

Im Rahmen des Zertifizierungsverfahrens wird der jeweilige Zertifizierungsantrag von einer unabhängigen sachverständigen Person innerhalb von vier Wochen nach vollständiger Einreichung aller erforderlichen Unterlagen begutachtet. Die Anonymität der sachverständigen Person ist dabei jederzeit gewährleistet. Die gesamte Kommunikation zwischen Antragsteller/in und sachverständiger Person erfolgt ausschließlich über incite.

Die eingesetzten Sachverständigen verfügen über fundierte Kenntnisse des Sachgebiets.

## Laufzeit und Rezertifizierung

Das Zertifikat ist drei Jahre gültig. Bis zum Ende des dritten Geltungsjahres kann auf Antrag die Rezertifizierung für weitere drei Jahre erfolgen.

Unterlässt ein Certified NIS Expert den Antrag auf Rezertifizierung und meldet sich auch nach einmaliger Erinnerung nicht, so erlischt die Zertifizierung mit Ablauf der gewährten Dauer und der Certified NIS Expert wird aus der Liste genommen.

Außerdem erfolgt die Streichung aus der öffentlichen Liste der Certified NIS Experts, wenn die Aktualisierung der persönlichen Stammdaten trotz Aufforderung nicht durchgeführt wird.

 incite weist ausdrücklich darauf hin, dass die Zertifizierung nur für physische Personen, nicht für Unternehmen und keinesfalls für Produkte vergeben wird.

## Verhaltens- und Nutzungsregeln

Teilnehmende am Zertifizierungsverfahren verpflichten sich, die nachstehenden Grundsätze einzuhalten:

- **Vertraulicher Zugang zum Kundenportal**  
Der persönliche Zugang zum Kundenportal ist vertraulich zu behandeln und darf nicht an Dritte weitergegeben oder gemeinsam genutzt werden. Die Verantwortung für sämtliche über das Kundenportal vorgenommenen Handlungen liegt bei der jeweiligen antragstellenden Person.
- **Eigenständigkeit der Leistungserbringung**  
Alle im Rahmen des Zertifizierungsverfahrens eingereichten Unterlagen, insbesondere die Projektarbeit, sind eigenständig zu erstellen. Die Eigenständigkeit der Arbeit stellt ein wesentliches Beurteilungskriterium dar.
- **Einsatz von Künstlicher Intelligenz (KI)**  
Der Einsatz von KI-gestützten Werkzeugen ist zulässig. Textpassagen oder Inhalte, die unter wesentlicher Mitwirkung von KI erstellt wurden, sind jedoch ausdrücklich und nachvollziehbar zu kennzeichnen.
- **Verantwortung und Transparenz**  
Die antragstellende Person trägt die volle Verantwortung für die Richtigkeit, Vollständigkeit und Nachvollziehbarkeit aller eingereichten Inhalte – unabhängig vom Einsatz unterstützender Werkzeuge.

## Entzug des Zertifikats

Ein Verstoß gegen die Auflagen für zertifizierte Personen führt zum sofortigen Entzug des Zertifikates ohne Anspruch auf Rückerstattung von Gebühren.



Alle für den Zertifikatserhalt relevanten und verbindlichen Bedingungen, einschließlich möglicher Entzugsgründe, sind im folgenden Dokument zusammengefasst:

[Bedingungen für Zertifikatsinhaberinnen und Zertifikatsinhaber \[PDF\]](#)

## Expertinnen- und Expertenverzeichnis



Zur Sichtbarmachung der Zertifikatsstandards führt und bewirbt incite ein Expertinnen- und Expertenverzeichnis.

[Expertinnen- und Expertenverzeichnis](#)

Der Nachweis erfolgt durch die schriftliche Zustimmung zur Aufnahme der Stamm- und Leistungsdaten der zu zertifizierenden Person im Verzeichnis mittels beigefügten Formulars.

Die Zustimmung kann jederzeit per E-Mail an [office@incite.at](mailto:office@incite.at) widerrufen werden.

## Rechtslage zur Titelführung

Zertifizierungsbezeichnungen sind keine akademischen Grade:

- Daher gibt es keine rechtliche Grundlage für deren Eintragung in Urkunden gemäß § 88 Abs. 1 des Universitätsgesetzes 2002 – UG, BGBl. I Nr. 120/2002.

Das Universitätsgesetz unterscheidet klar zwischen akademischen Graden, die durch den erfolgreichen Abschluss eines Hochschulstudiums erworben werden, und Zertifizierungsbezeichnungen, die im Rahmen von Fortbildungen oder speziellen Lehrgängen vergeben werden.

- Zertifizierungen besitzen nicht denselben rechtlichen Status wie akademische Grade, daher dürfen sie auch nicht in offiziellen Dokumenten wie beispielsweise Geburtsurkunden, Reisepässen oder amtlichen Schriftstücken aufgeführt werden.



**Ihr Ziel ist in  
greifbarer Nähe.**

Mit dem Fachgespräch beginnt Ihr Weg  
als zertifizierte Expertin bzw. zertifizierter  
Experte. Nutzen Sie die Chance!

## ANFORDERUNGEN IM DETAIL

# 6. Rezertifizierung

Bis zum Ende des jeweils dritten Geltungsjahres kann auf Antrag die Rezertifizierung für weitere drei Jahre erfolgen. Für die Rezertifizierung sind bestimmte Nachweise erforderlich.

## Praxisnachweise und Kundenreferenzen

Es muss ein Nachweis über die aktive Tätigkeit im Bereich Informationssicherheit, idealerweise im Bereich der Umsetzung der NIS-Gesetzgebung (NISG 2026 oder NISG2018) seit der letzten Zertifizierung erbracht werden:

- Dabei ist insbesondere auf die NIS-Anforderungen im IT und auch OT-Bereich, Risikomanagement, Business Continuity und Notfallmanagement einzugehen.
- Außerdem sind diese Referenzen anhand der im Praxisnachweis aus den letzten drei Jahren seit der Erstzertifizierung angeführten Kriterien (Auftragsklärung, Ausgangssituation, Konzept, Umsetzung, Erfolgsfaktoren und Ergebnis) durch drei Projektbeschreibungen darzustellen.

## Nachweis der Weiterbildung

Durch kontinuierliche Weiterbildung erfolgt die Sicherstellung, dass der Standard der fachlichen Eignung nicht nur gehalten, sondern auch laufend erweitert wurde.

Folgende Kriterien muss der Nachweis der Weiterbildung erfüllen:

- Ein Mindestausmaß von 24 Lehreinheiten, seit der letzten Zertifizierung, erfolgt durch die Vorlage detaillierter Angaben zur Absolvierung von Seminaren, Fachvorträgen, Fachpublikationen, Schulungen, Kongressen, Konferenzen, Leselisten, die Mitgliedschaft in Arbeitsgruppen zum Thema, o.ä.
- Beilegen von Besuchsbestätigungen, Zeugnissen und ähnlichen Nachweisdokumenten.



## FINANZIELLER ÜBERBLICK

# 7. Kosten

Das Zertifizierungsverfahren ist kostenpflichtig – hier finden Sie wichtige Angaben zu den Gebühren.

## Erstzertifizierung

Die Erstzertifizierung stellt die erstmalige, offizielle Bewertung und Zertifizierung einer Person nach definierten Qualitäts- und Kompetenzstandards dar. Sie dient dazu, die grundlegende Eignung und Qualifikation nachzuweisen.

**Kosten: EUR 650,- zzgl. 20 % USt. (Preisanpassungen vorbehalten)**

Zusätzlich fällt eine jährliche Identifikationsgebühr von EUR 150,- zzgl. 20 % USt. an, welche rückwirkend verrechnet wird. Danach besteht die Möglichkeit einer Rezertifizierung.



Informieren Sie sich regelmäßig auf unserer Website über aktuelle Fördermöglichkeiten für die Zertifizierung.

---

## Neuantritt

Bei einer nicht bestandenen Zertifizierung kann die Zertifizierung erneut gebucht werden.

**Kosten: EUR 120,- zzgl. 20 % USt. (Preisanpassungen vorbehalten)**

---

## Rezertifizierung

Die Rezertifizierung ist eine wiederkehrende Überprüfung, die nach Ablauf von drei Jahren erfolgt. Sie stellt sicher, dass die zertifizierte Person weiterhin die geforderten Standards erfüllt und ihre Qualifikation aufrechterhält. Die Kosten der Rezertifizierung sind mit der jährlich zu entrichtenden Identifikationsgebühr abgedeckt.

## 8. Kontakt

Bei Fragen zur Zertifizierung, zum Ablauf oder zu den Voraussetzungen wenden Sie sich bitte an die folgende Ansprechperson:



**Mag. Nadia Mürwald**



+43 5 90 900 3799



[nadia.muerwald@incite.at](mailto:nadia.muerwald@incite.at)



Es gelten unsere Allgemeinen Geschäftsbedingungen und die Datenschutzerklärung.  
[Allgemeine Geschäftsbedingungen](#)

Unser incite-Team ist gerne für Sie da

Montag bis Donnerstag von 9 bis 17 Uhr

Freitag von 9 bis 14 Uhr

Telefon: +43 5 90 900 3792

E-Mail: [office@incite.at](mailto:office@incite.at)

Web: [www.incite.at](http://www.incite.at)

know how. get incite.

**incite Ausbildungs- und Schulungsveranstaltungen GmbH**  
Wiedner Hauptstraße 57/ III EG  
1040 Wien

Tel.: +43 5 90 900 3792  
E-Mail: [office@incite.at](mailto:office@incite.at)

Firmenbuchnummer: 211159d  
Firmenbuchgericht: Handelsgericht Wien  
UID: ATU52682208  
DVR: 4006135

Kammerzugehörigkeit: Wirtschaftskammer Wien  
Stand: Juni 2025