



Energiemanagement

BAFA aktualisiert Merkblatt zur EEW-Förderung

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) hat das Merkblatt zur Energie- und Ressourceneffizienz in der Wirtschaft (EEW)-Förderung aktualisiert.

Die aktualisierte Version (7.4 vom 22.04.2026) des Merkblatts „Bundesförderung für Energie- und Ressourceneffizienz in der Wirtschaft (EEW) – Zuschuss“ enthält gegenüber der Vorgängerversion (7.3 vom 20.05.2025) **textliche Änderungen zur Antragsstellung**.

Die Antragstellung ist ausschließlich elektronisch über das Portal der **Förderzentrale Deutschland** zu stellen.

Es wird zudem darauf hingewiesen, dass die Nutzung des Portals Förderzentrale Deutschland eine Authentifizierung via **ELSTER-Zertifikat** oder **bundID** erfordert.

Beim BAFA finde Sie **weitere Nutzungshinweise zum Portal** der Förderzentrale Deutschland und das **aktualisierte Merkblatt zur EEW-Förderung**.

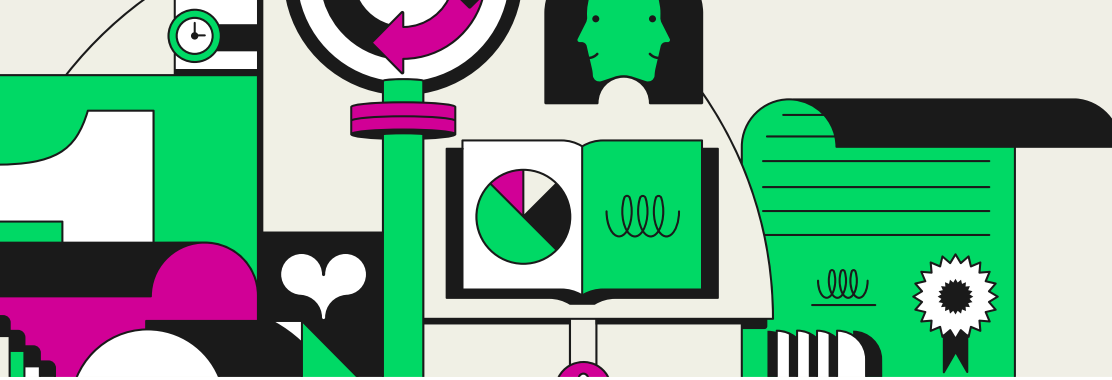
Haben Sie Fragen oder Hinweise zum Thema **Energieeffizienz**? Wenden Sie sich gerne an **Jochen Buser**.

EnEFG – BAFA aktualisiert Merkblatt

Kurz vor der finalen Änderung des Energieeffizienzgesetz (EnEFG) veröffentlicht das BAFA ein aktualisiertes Merkblatt.

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) hat heute eine aktualisierte Version seines **Merkblattes für das Energieeffizienzgesetz (EnEFG)** veröffentlicht (Stand 30.04.2026).

In der aktuellen Version 7 wurde eine Klarstellung des Standortbezugs im Rahmen der 90 %-Regelung ergänzt, sowie eine Klarstellung und Reduzierung der Inhalte der zu veröffentlichen Umsetzungspläne (für wirtschaftliche Maßnahmen).



90%-Regelung (Kapitel 4)

Das vollständig eingerichtete **EnMS nach DIN EN ISO 50001** oder **UMS nach EMAS nach § 8 EnEFG** muss analog zu den verpflichtenden Energieaudits (DIN EN 16247-1, Ausgabe November 2022) nach **§ 8a Abs. 1 Nr. 5 EDL-G** mindestens 90 % des gesamten Endenergieverbrauchs des Unternehmens abdecken.

Wichtige Ergänzung des BAFA: das Zertifikat sowie der Anhang zum Zertifikat muss alle Standorte des Unternehmens erfassen, die in Summe 90 % des Gesamtendenergieverbrauchs abdecken.

Hierbei ist zu beachten, dass der Gesamtenergieverbrauch im Sinne der ISO 50001 nicht mit dem Gesamt**end**energieverbrauch des BAFA gleichzusetzen ist:

- **ISO 50001** „normativ“: Energieverbrauch = Menge der eingesetzten Energie, Energieeinsatz = Art oder Weise, wie Energie verwendet wird und dem Anwendungsbereich des Energiemanagementsystems
- **Gesamtendenergieverbrauch** (weitergeleitete Energien dürfen zum Abzug gebracht werden)

Jedoch werden die 90%-Regel oder andere Schwellenwerte des EnEFG anhand der „BAFA-Methode“ bilanziert. Die GUTcert wird zu diesem Thema im Laufe des Sommers eine Hilfestellung veröffentlichen.

Umsetzungspläne (Kapitel 5)

Die ursprünglichen Vorgaben zu den Inhalten der veröffentlichten Umsetzungspläne wurden nun von sieben auf fünf Mindestvorgaben reduziert. Für die als wirtschaftlich identifizierten Maßnahmen müssen folgende Angaben veröffentlicht werden:

- Priorisierung der Maßnahmen,
- Bezeichnung der identifizierten und wirtschaftlich bewerteten Maßnahmen,
- Kalkuliertes Investitionsvolumen,
- Zeitrahmen für die Umsetzung und
- Angaben zum Umsetzungsfortschritt.

Alle Beschreibungen und weitere Details finden Sie im aktuellen Merkblatt hier.

Da sich das EnEFG aktuell noch in der Abstimmung befindet, kann es durchaus zu weiteren Änderungen in naher Zukunft kommen, daher sind alle Angaben auf den Stand 30.04.2026 des BAFA-Merkblatt zurückzuführen.



Mehr zur Novellierung des EnEFG erfahren Sie in [unserem Webinar am 02.06.](#)

Haben Sie Fragen oder Hinweise zum Thema Energieeffizienz? Wenden Sie sich gerne an [Jochen Buser](#).

DEHSt veröffentlicht eine vorläufige SPK-Billigkeitsrichtlinie und Antragsfrist 2026

Am 27.05.2026 veröffentlichte die DEHSt wichtige und langerwartete Neuigkeiten im Bereich der Strompreiskompensation (SPK).

Die neue Antragsfrist für diesjährige Anträge auf Strompreiskompensation (SPK) steht fest: 17. August 2026, wie in einer [kurzen News](#) verkündet wurde. Es handelt sich um eine materielle Ausschlussfrist. Die Leitfäden sollen in den nächsten Tagen aktualisiert werden.

Zusätzlich wurde eine [\(vorläufige\) Billigkeitsrichtlinie](#) zur SPK auf der Website der DEHSt veröffentlicht. Diese Fassung wurde der Europäischen Kommission zur Genehmigung vorgelegt. Die finale Fassung wird nach Genehmigung in den nächsten Wochen im Bundesanzeiger veröffentlicht.

Alle Unternehmen, die planen, einen SPK-Antrag noch in diesem Jahr zu stellen, sollten schnellstmöglich die Billigkeitsrichtlinie prüfen und mit dem Befüllen der FMS-Anträge beginnen. Diese sind ebenfalls seit dem 27.05. [online](#).

Unternehmen, die bereits bei uns eine SPK-Prüfung beauftragt haben, werden wir in den kommenden Tagen noch einmal gesondert und detaillierter informieren.

Ansprechperson

Haben Sie Fragen oder Hinweise zum Thema [ökologische Gegenleistungen](#) (SPK, BECV, EnFG)? Wenden Sie sich gerne an [Linda Finkenzeller](#).



DEHSt veröffentlicht angekündigtes Excel-Tool: Investitionsüberschuss für BECV

Das neue verpflichtende Excel-Tool soll bei Antragsstellern, prüfungsbefugten Stellen und der DEHSt für mehr Klarheit und Sicherheit bei der Anrechnung von Investitionsüberschüssen sorgen.

Mitte Mai veröffentlichte die DEHSt das lang erwartete Excel-Tool zur Erfassung von Investitionsüberschüssen für die Anrechnung bei Anträgen der Carbon-Leakage-Verordnung (BECV).

Das Tool ist verpflichtend zu nutzen, wenn Überschüsse aus den letzten Jahren mitgetragen und angerechnet werden sollen. Ebenso, wenn im laufenden Jahr Überschüsse durch eine Übererfüllung der Investitionsverpflichtung über 100% der Vorjahresbeihilfe hinaus entstehen. Das Tool muss separat vom Formular-Managementsystem (FMS) des BECV-Antrags durch eine prüfungsbefugte Stelle (pbSt) bestätigt werden. Aus diesem Grund soll es auch nicht im FMS selbst angehängt werden, sondern wird als separate Datei an die pbSt geschickt.

Mit der Einführung dieses Verfahrens antwortet die DEHSt auf das Anliegen von prüfungsbefugten Stellen und Antragstellern, eine übersichtlichere Erfassung von Investitionsüberschüssen bereitzustellen. Da Überschüsse vier Jahre lang mitgetragen werden können und Investitionssummen auch anteilig auf die verschiedenen Beihilfeverfahren nach BECV, Strompreiskompensation (SPK) und der Besonderen Ausgleichsregelung (BesAR) nach dem Energiefinanzierungsgesetz (EnFG) aufgeteilt werden können, ist das aus Sicht der GUTcert eine sinnvolle Ergänzung zur Antragsstellung.

Das Excel-Tool kann auf der [Website der DEHSt](#) heruntergeladen werden.

Das Tool ist ebenso verpflichtend für Anträge bei der SPK in diesem Jahr sein. Die FMS-Anwendungen für diesjährige SPK-Anträge stehen seit dem 27.05.2026 über die Seite des FMS zur Bearbeitung bereit. Das Excel-Tool wurde im Zuge dessen nicht erneut mit einem expliziten Bezug auf die SPK-Anträge veröffentlicht, daher sollte beim Befüllen sorgfältig geprüft werden, ob alle Angaben korrekt übernommen werden. Möglichweise erfolgt hier noch ein Update.

Haben Sie Fragen oder Hinweise zum Thema **ökologische Gegenleistungen** (SPK, BECV, EnFG)?
Wenden Sie sich gerne an [Linda Finkenzeller](#).



Qualitätsmanagement

Unabhängigkeit als Wettbewerbsfaktor für Zertifizierungsstellen

Digitalisierung, künstliche Intelligenz, Cybersecurity, regulatorische Anforderungen und globaler Wettbewerbsdruck: Die Zertifizierungsbranche verändert sich.

Investoren treiben die Konsolidierung des Marktes voran und verändern damit Strukturen, Prozesse und Erwartungen an moderne Zertifizierungsdienstleistungen. Der Markt entwickelt sich daher zunehmend hin zu standardisierten und skalierbaren Auditmodellen. Große internationale Anbieter setzen verstärkt auf Effizienz, zentrale Steuerung und technologiegestützte Prozesse. Dadurch steigen Wettbewerbs- und Preisdruck – gleichzeitig nimmt jedoch häufig der individuelle Gestaltungsspielraum in Audits ab. So entwickelt sich Zertifizierung vielerorts vom persönlichen Vertrauensgeschäft hin zu einem standardisierten Serviceprodukt.

Gerade in diesem Umfeld gewinnt Unabhängigkeit an Bedeutung. Als Teil der **AFNOR-Gruppe** profitiert die GUTcert von einer langfristig ausgerichteten Eigentümerstruktur: Die Mutterorganisation AFNOR ist eine **französische Non-Profit-Organisation** mit öffentlichem Auftrag (association reconnue d'utilité publique). Dadurch stehen fachliche Qualität, faire Preise, nachhaltige Entwicklung und langfristige Kundenbeziehungen stärker im Fokus als kurzfristige Renditeziele.

Was bedeutet das für unsere Kundinnen und Kunden? Vor allem eine persönliche Betreuung, Kontinuität und echte Partnerschaft. Wir setzen auf feste Ansprechpersonen in der Zertifizierungsstelle, langfristig eingesetzte Auditorinnen und Auditoren sowie individuell ausgerichtete, fachlich fundierte Prüfungen. So möchten wir Transparenz, Vertrauen und Verlässlichkeit schaffen – anstatt Standardprozessen oder KI-gesteuerter Telefonhotlines. Gerade in einem zunehmend konsolidierten Markt wird diese Kombination aus Nähe, Transparenz und fachlicher Tiefe zu einem echten Differenzierungsmerkmal.

Erfahren Sie mehr über die GUTcert als Unternehmen in unserem **Firmenportrait**.

Ansprechpersonen

Haben Sie Fragen zum Artikel? Dann wenden Sie sich gerne an **Lea Graf** oder **Amelie Mandel**.



Emissionshandel

EU-ETS 1: Neue Benchmarks für den Zeitraum 2026–2030

Die EU-KOM hat einen Entwurf für die neuen Benchmarks im EU-ETS 1 veröffentlicht. Die Benchmarks sind wesentlicher Bestandteil für die Berechnung der kostenfreien Zuteilung.

Die EU-KOM hat am 11. Mai einen Entwurf veröffentlicht, in dem die neuen Benchmarks für die zweite Hälfte der 4. Handelsperiode (2026-2030) im Europäischen Emissionshandel (**EU-ETS 1**) angepasst werden.

Die neuen Benchmarks basieren auf den Effizienzdaten von 2021 und 2022. Für die Wärme und Brennstoffbenchmarks wird künftig auch Wärme berücksichtigt, die aus Strom erzeugt wird. Die deutlichsten Senkungen finden sich bei

- Brennstoff-Benchmarks (42,6 auf 38,1 Zertifikate/TJ) und
- Wärme-Benchmarks (47,3 auf 31,2 Zertifikate/ TJ)

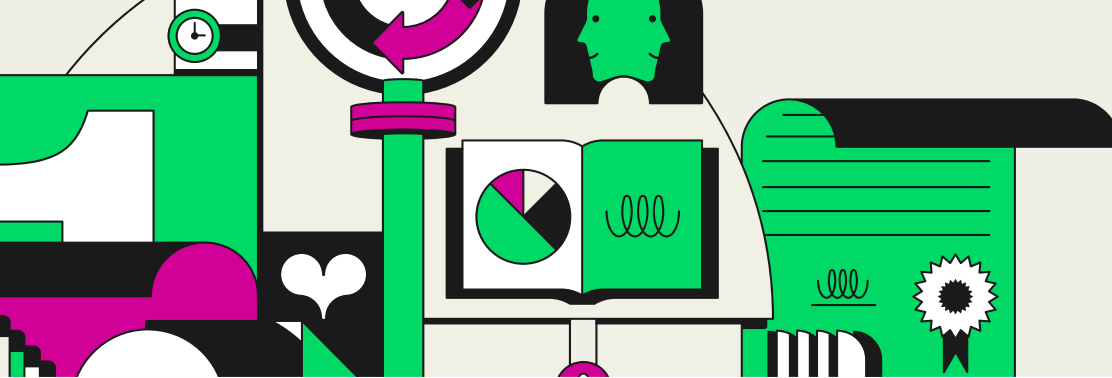
Darüber hinaus gibt es u.a. Senkungen bei Kalk, Mineralwolle, Zeitungsdruckpapier und gestrichenem Karton. Bei Wasserstoff steigt der Benchmark von 6,84 auf 7,98 Zertifikate/TJ.

Rückmeldungen zum Entwurf können noch bis zum 8. Juni 2026 gegeben werden. Verabschiedet wird er voraussichtlich Ende Juni 2026.

Die Entwürfe der EU-KOM mit allen Benchmark-Werten finden Sie hier unter ec.europa.eu.

Ansprechperson

Haben Sie Fragen oder Hinweise zum Thema Emissionshandel? Wenden Sie sich gerne an **Jannik Steinborn**.



Carbon Footprint

Der Low Emission Steel Standard (LESS): jetzt auch im Portfolio der GUTcert

LESS hat das Ziel, die Dekarbonisierung in der Stahlindustrie in Europa voranzubringen. Das zertifizierte Label informiert transparent über Emissionsstärken von Stahl.

Die Stahlproduktion in Europa trägt eine besondere Verantwortung zum Erreichen der europäischen Klimaziele. Mit 5 % der Gesamtemissionen der EU trägt sie erheblich zur weiteren Anreicherung von CO₂ in der Atmosphäre bei. Mit LESS aisbl wurde 2024 eine gemeinnützige Organisation ins Leben gerufen, die sowohl die Dekarbonisierung in der Stahlindustrie voranbringen möchte als auch das Label-System **LESS** beaufsichtigt.

Das LESS-System

Das besondere an LESS ist, dass es einem Klassifizierungssystem folgt und damit die Emissionsstärke des Stahls schnell erfassbar macht. Level D zeigt höhere Emissionen an, wobei das Erreichen dieses Levels heute schon den Einsatz der bestverfügbaren Technik erfordert. Level A bedeutet, dass die Emissionen nahe bei 0 sind. Um mit den Klimazielen von Paris konform zu sein, muss Level A erreicht werden. Bei der Klassifizierung werden der Prozess „hot-rolling“ und die vorgelagerten Emissionen wie eingekaufte Waren berücksichtigt. Ebenso wird die Verwendung von Stahlschrott als „sliding scale“ angegeben, wobei die Emissionen entlang einer Skala, die den Schrottanteil berücksichtigt, ausgewiesen werden. Mit diesem umfassenden Ansatz soll die Transformation des Industriezweigs erfolgen.

Zertifizierung nach LESS

Die Zertifizierung bei LESS und die Nutzung des LESS-Labels werden von externen Stellen geprüft, um Transparenz, Vergleichbarkeit und Glaubwürdigkeit zu gewährleisten. Die GUTcert befindetet sich aktuell im Prozess der Registrierung als Prüfstelle bei LESS aisbl.

Ob neu dabei oder bereits in der Rezertifizierung: Gerne prüfen wir auch Ihren Stahl nach LESS – sprechen Sie uns einfach an!

Ansprechperson

Haben Sie Fragen oder Hinweise zum Thema LESS? Wenden Sie sich gerne an **Johanna Sitter**.



ISCC/REDcert/SURE

THG-Quote: Bundestag beschließt strengere Regeln für Kraftstoffe

Der Bundestag hat die THG-Quoten-Novelle verabschiedet. Was sich für Kraftstoffanbieter und Lieferketten ab 2026 ändert, lesen Sie hier.

Was ist die THG-Quote?

Am 23. April 2026 hat der Bundestag auf Basis der europäischen **RED-III-Richtlinie** eine wichtige Weichenstellung für die Energiewende im Verkehr beschlossen: die **Novelle zur Treibhausgasminderungs-Quote (THG-Quote)**. Die THG-Quote verpflichtet Kraftstoffanbieter, die CO₂-Emissionen ihrer Kraftstoffe schrittweise zu senken. Wer Benzin oder Diesel verkauft, muss nachweisen, dass ein wachsender Anteil davon klimafreundlicher ist als fossile Alternativen, zum Beispiel durch Biokraftstoffe, grünen Wasserstoff oder Ladestrom. Für Unternehmen entlang der Lieferkette steigen damit die Anforderungen an Nachhaltigkeitsnachweise und Rückverfolgbarkeit.

Höhere Gesamtquote, neue Kraftstoffkategorien

Das Herzstück der Novelle: Die Gesamtquote steigt von aktuell 10,6 % auf 65 % bis 2040. Das ist ambitionierter als der ursprüngliche Regierungsentwurf, der 59 % vorsah.

Erstmals wird eine Unterquote für erneuerbare Kraftstoffe nicht-biogenen Ursprungs (RFNBO) eingeführt, also für grünen Wasserstoff und synthetische e-Fuels aus Ökostrom. Diese Unterquote steigt bis 2040 schrittweise auf 10 %. Das ist politisch bedeutsam, weil diese Kraftstoffe bislang kaum eine Rolle spielen und nun gezielt gefördert werden sollen. Nun werden also klare Investitionsanreize für neue Technologien und Lieferstrukturen gesetzt.

Regeln der Novelle im Überblick

- Gesamtquote: steigt bis 2040 auf 65 %
- RFNBO-Unterquote (grüner Wasserstoff, e-Fuels): Anhebung bis 2040 auf 10 %
- Herkömmliche Biokraftstoffe (z. B. Raps, Getreide): Anhebung bis 2033 auf 5,8 %
- Fortschrittliche Biokraftstoffe (z. B. Altfette, Reststoffe): Anhebung bis 2040 auf 9 %
- Strom für Elektro-Lkw und -Busse: ab 2027 anrechenbar mit Faktor 4
- Doppelanrechnung fortschrittlicher Biokraftstoffe: entfällt rückwirkend ab 01.01.2026
- Palmöl-Reststoffe: ab 2027 nicht mehr anrechenbar



Biokraftstoffe – weniger Fehlanreize, mehr Differenzierung

Bisher konnten fortschrittliche Biokraftstoffe doppelt auf die Quote angerechnet werden. Das führte zu einem künstlichen Überangebot an Zertifikaten. Dieser Mechanismus entfällt rückwirkend ab 1. Januar 2026.

Palmöl-Reststoffe scheiden ab 2027 vollständig aus der Anrechnung aus. Das betrifft direkt alle Lieferketten mit Bezug zu Palmölprodukten und macht eine Überprüfung bestehender Lieferbeziehungen sinnvoll.

Elektromobilität – Anreize für schwere Nutzfahrzeuge

Wer Ökostrom nachweislich für elektrische Lkw oder Busse bereitstellt, kann diesen ab 2027 mit dem Faktor 4 auf die THG-Quote anrechnen. Das macht die Elektrifizierung schwerer Flotten wirtschaftlich attraktiver und schafft neue Chancen für Logistik und Spedition.

Was das für Ihr Unternehmen bedeutet

Die Novelle verschärft die Anforderungen an Zertifizierungen, Nachweise und die Rückverfolgbarkeit in der Lieferkette. Wer Kraftstoffe liefert, verarbeitet oder als Rohstoff bezieht, sollte jetzt prüfen, ob die eigenen Prozesse den neuen gesetzlichen Vorgaben entsprechen.

Ansprechperson

Bei Fragen oder Anmerkungen rund um die Thematik **Nachhaltigkeitszertifizierungen** wenden Sie sich gerne an **Frieda Becker**.

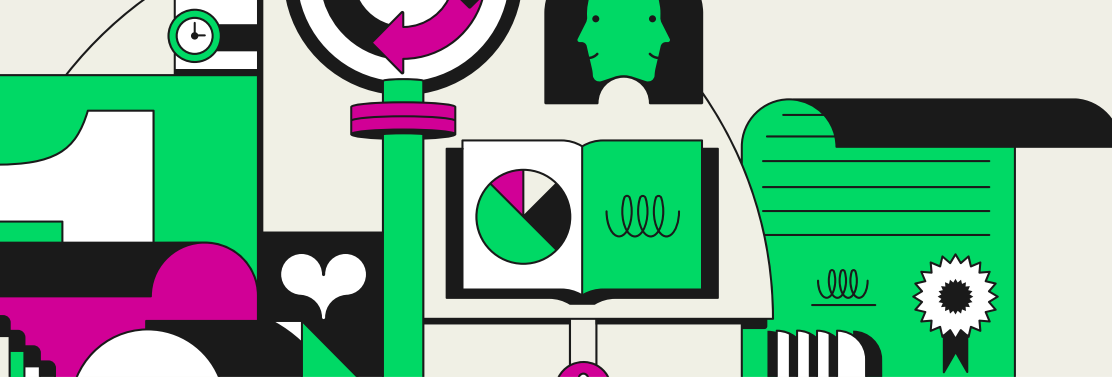
Neue Erweiterungen und Funktionen im FLIK-Tool

Das REDcert-System informiert über umfassende Updates im Onlinetool zur FLIK-Suche.

Mit dem **FLIK-Onlinetool** lassen sich interaktiv relevante Eigenschaften von Anbauflächen für Biomasse in Deutschland anzeigen. Es soll Anbaubetrieben und Auditierenden als Hilfe für landwirtschaftliche Audits im Rahmen der **Nachhaltigkeitszertifizierungen** gemäß **Erneuerbare Energien Richtlinie (RED III)** dienen. Welche Aktualisierungen hat es gegeben?

1. Aufnahme FLIK-Informationen für Baden-Württemberg

Es wurden FLIK-Statusinformationen für Baden-Württemberg aufgenommen, die in Abgleich mit den vom zuständigen Ministerium bereitgestellten Daten erfasst wurden.



2. Anzeige der relevanten NUTS2-Gebiete

Ein Info-Fenster für jede Fläche zeigt die Informationen zum zugehörigen NUTS2-Gebiet an. Für NUTS2-Gebiete, die sowohl einen Wert für mineralische Böden als auch organische Böden ausweisen, kann nun über den Layer „Organische Böden“ die aktuelle Moorkulisse des **Thünen-Instituts** eingeblendet werden. So können Biomasse-Erzeugerbetriebe für einzelne FLIK den Nachweis zum jeweils relevanten NUTS2-Wert führen. Eine pauschalisierte Erfassung – wie bereits in einem **früheren Artikel** erläutert – ist alternativ aber weiterhin möglich.

3. Neues Farbschema für die FLIK-Darstellung

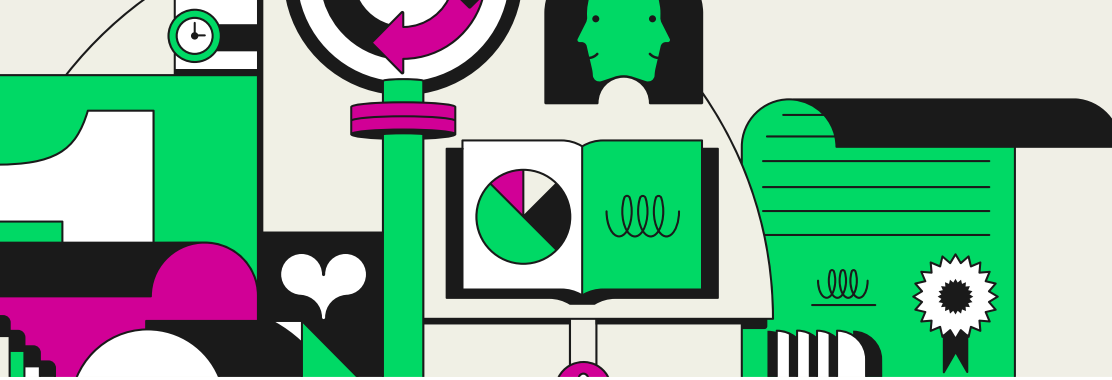
Mit einigen optischen Anpassungen des Flik-Tools werden folgende Unterscheidungen laut **REDcert** farblich neu dargestellt:

- „Blau kennzeichnet uneingeschränkt nutzbare Flächen (Status „Ackerland“ zum 01.01.2008)“
- „Rot steht für Flächen, die nicht für den nachhaltigen Biomasseanbau zugelassen sind (z. B. Sonderkulturen)“
- „Orange markiert Flächen, die unter Umständen mit zusätzlichen Auflagen oder Nachweisen für den Biomasseanbau genutzt werden können (z. B. nach dem 01.01.2008 umgebrochenes, nicht biologisch hochwertiges Grünland, bei dem eine Landnutzungsänderung in der Treibhausgasbilanz zu berücksichtigen ist)“

4. Technischer Support

Sollten Sie konkrete Fragen oder auch Ideen und Anregungen zum FLIK-Tool haben, können Sie unter der folgenden E-Mailadresse das Entwicklungsteam kontaktieren: <mailto:support@flik-suche.de>.

Bei Fragen oder Anmerkungen rund um die Thematik **Nachhaltigkeitszertifizierungen** wenden Sie sich gerne an **Frieda Becker**.



Informationssicherheit

EU-Maschinenverordnung: Mit Managementsystemen effizient zur Compliance

Die neue **EU-Maschinenverordnung** verschärft ab 2027 die Anforderungen an Sicherheit und Cybersecurity. Gleichzeitig gewinnen strukturierte Managementsysteme wie ISO 9001 und ISO 27001 an Bedeutung, um Compliance effizient und nachvollziehbar umzusetzen.

EU-Maschinenverordnung ab 2027: Das ändert sich

Die neue EU-Maschinenverordnung (EU) 2023/1230 tritt ab dem 20. Januar 2027 in Kraft und ersetzt die bisherige Maschinenrichtlinie, wie die IHK Lippe zu Detmold in einem [Artikel auf ihrer Webseite](#) informiert. Ziel ist es, die Anforderungen an die Maschinensicherheit an aktuelle technologische Entwicklungen anzupassen – insbesondere im Bereich Digitalisierung, vernetzter Systeme, Software und KI.

Neu bzw. stärker geregelt sind insbesondere:

- Anforderungen zu Sicherheit und Gesundheit bei der Bedienung von Maschinen
- Berücksichtigung von Digitalisierung, KI und vernetzten Systemen
- Erstmals verbindliche Anforderungen an Cybersecurity
- Klare Pflichten für Hersteller, Importeure und Händler.

Unternehmen müssen die Anforderungen spätestens ab dem 20. Januar 2027 vollständig anwenden. Für Maschinen, die ab diesem Datum in Verkehr gebracht werden, gilt ausschließlich die neue Verordnung.

Wichtig: Die Maschinenverordnung ist unmittelbar geltendes Gesetzesrecht und damit verpflichtend einzuhalten. Bisher galt die Maschinenrichtlinie, die erst in nationales Recht umgesetzt werden musste.

NIS-2: Gesetzliche Anforderungen an Cybersicherheit

Die **NIS-2-Richtlinie** betrifft Unternehmen mit kritischer oder wichtiger Infrastruktur und verpflichtet sie zu:

- Systematischem Risikomanagement in der IT
- Meldung von Sicherheitsvorfällen
- Technischen und organisatorischen Schutzmaßnahmen



Abgrenzung zur Maschinenverordnung:

- NIS-2 = allgemeine Cybersicherheits- und Organisationspflicht
- Maschinenverordnung = produktspezifische Sicherheitsanforderungen für Maschinen

Beide Regelwerke überschneiden sich im Bereich Cybersecurity, gelten aber unabhängig voneinander. **Finden Sie hier heraus, ob Sie von NIS-2 betroffen sind.**

ISO 9001 & ISO 27001: Zertifizierungen, kein Gesetz

ISO-Normen sind freiwillige, international anerkannte Managementsystemnormen. Sie ersetzen keine gesetzlichen Anforderungen, helfen Unternehmen jedoch dabei, diese strukturiert und nachvollziehbar umzusetzen.

- **ISO 9001 (Qualitätsmanagement)**
 - Strukturiert Prozesse und Dokumentation
 - Unterstützt Produktqualität und Nachvollziehbarkeit
 - Hilft bei der Umsetzung von Konformitätsanforderungen
 - Berücksichtigt im Rahmen von Audits nach ISO 9001 auch die Einhaltung produktspezifischer gesetzlicher Anforderungen – dazu zählt selbstverständlich auch die EU-Maschinenverordnung
- **ISO 27001 (Informationssicherheit)**
 - Strukturiert den Umgang mit IT- und Cyberrisiken
 - Schützt Systeme vor Manipulation und Angriffen
 - Unterstützt technische Anforderungen aus Maschinenverordnung und NIS-2.

Wichtige Abgrenzung:

ISO-Zertifizierungen ersetzen keine gesetzlichen Anforderungen. Sie dienen als Nachweis für funktionierende Managementsysteme und unterstützen Unternehmen bei der Einhaltung von Prozessen und Standards.

Regelwerk	Typ	Zweck
EU-Maschinenverordnung	Gesetzliche Vorgabe	Verbindliche Anforderungen an die Sicherheit von Maschinen
NIS-2	Gesetzliche Vorgabe	Verbindliche Anforderungen an Cybersicherheit und Organisation
ISO 9001	Norm/Zertifizierung	Struktur für Qualitäts- und Prozessmanagement
ISO 27001	Norm/Zertifizierung	Struktur für Informationssicherheit

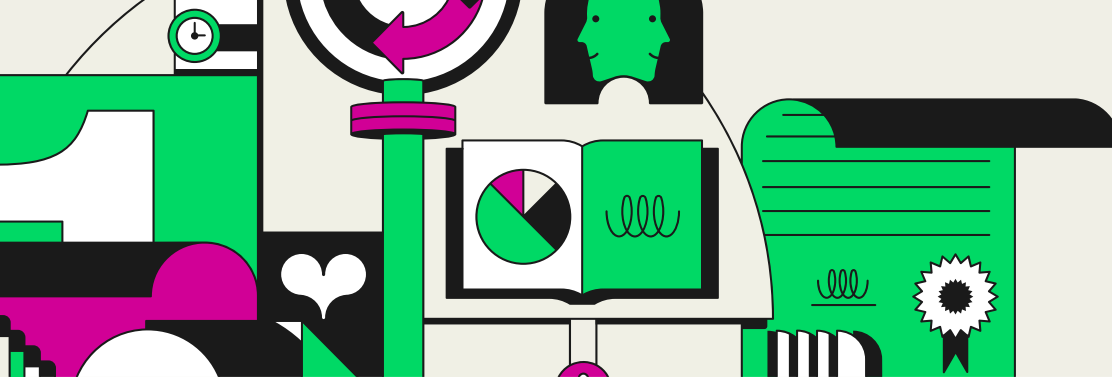


Tabelle 1: Gesetze definieren, was verpflichtend einzuhalten ist – ISO-Normen unterstützen Unternehmen dabei, diese Anforderungen strukturiert und nachvollziehbar umzusetzen.

Risiken und Sanktionen

Verstöße gegen die Maschinenverordnung können nicht nur Bußgelder verursachen, sondern auch erhebliche wirtschaftliche Folgen haben.

Mögliche Maßnahmen der Marktüberwachung sind unter anderem:

- Verbot des Inverkehrbringens
- Rückruf bereits ausgelieferter Maschinen
- Stilllegung von Maschinen oder Anlagen.

Zusätzlich können Verstöße gegen die EU-Maschinenverordnung (EU) 2023/1230 mit **Bußgeldern** von bis zu 100.000 Euro geahndet werden – beispielsweise bei fehlender CE-Kennzeichnung, unvollständiger Konformitätserklärung oder mangelhafter technischer Dokumentation.

Warum Zertifizierungen jetzt strategisch wichtig sind

Auch wenn ISO 9001 und ISO 27001 nicht verpflichtend sind, bieten sie klare Vorteile:

- Vereinfachte Umsetzung gesetzlicher Anforderungen und regulatorischer Produktvorgaben
- Bessere Nachweisbarkeit gegenüber Behörden
- Geringeres Risiko bei Audits und Marktüberwachung
- Strukturierte Integration von Cyber-, Qualitäts- und Compliance-Anforderungen.

Beide Normen tragen komplementär zur Umsetzung der Anforderungen bei: Während ISO 9001 die prozessuale und organisatorische Basis schafft, ergänzt ISO 27001 diese um die systematische Behandlung von Cyber- und Informationssicherheitsrisiken. Besonders im Zusammenspiel unterstützen beide Normen eine ganzheitliche Umsetzung der Anforderungen der Maschinenverordnung.

Fazit

Die EU-Maschinenverordnung und NIS-2 setzen den rechtlichen Rahmen. ISO 9001 und ISO 27001 liefern die organisatorische und methodische Grundlage, um diese Anforderungen effizient und nachvollziehbar umzusetzen.

Unternehmen, die frühzeitig zertifizierte Managementsysteme einsetzen, sind besser aufgestellt für die Umsetzung ab 2027.



Haben Sie Fragen oder Hinweise zum Thema Maschinenverordnung und Zertifizierung? Wenden Sie sich gerne an **Nils Gartmann**, **Lea Graf** und **Amelie Mandel**.

Claude Mythos: Auswirkungen auf modernes Penetration Testing

Claude Mythos automatisiert das Finden und Ausnutzen von Schwachstellen. Welche Folgen hat das für Pentests, Angriffsgeschwindigkeit und Security-Prozesse?

Was ist „Claude Mythos“?

„**Claude Mythos Preview**“ ist ein nicht öffentlich zugängliches Frontier-KI Modell von Anthropic mit Fokus auf IT-Sicherheit, das bisherige Systeme in einem Punkt deutlich übertrifft: Es kann Schwachstellen nicht nur finden, sondern diese auch praktisch ausnutzen.

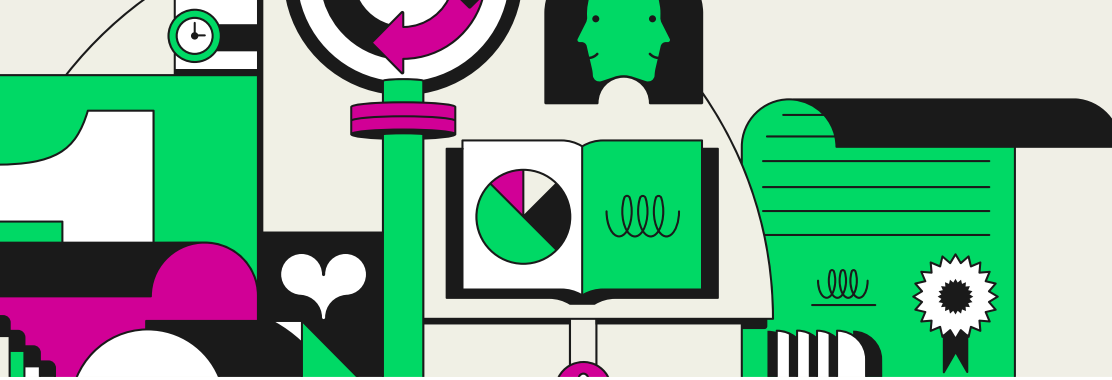
In internen Tests identifizierte das Modell tausende bislang unbekannte Sicherheitslücken, unter anderem in allen gängigen Browsern und Betriebssystemen und erzeugte daraus funktionierende Exploits – also Skripte oder Programme, die gezielt Schwachstellen in Software o. ä. ausnutzen.

Entscheidend ist hier vor allem die Fähigkeit, mehrere Schwachstellen zu einer funktionierenden Angriffskette zu verknüpfen. Gleichzeitig entwickelt das Modell Exploits iterativ weiter und testet sie, bis ein Angriff zuverlässig funktioniert. Neben Open-Source-Code analysiert Mythos auch geschlossene Software und leitet daraus Angriffsansätze ab. Im Unterschied zu klassischen Tools arbeitet das Modell dabei nicht signaturbasiert, sondern hypothesengetrieben, generiert aktiv neue Testszenarien und kann mehrstufige Angriffsschritte teilweise selbstständig verketteten.

Aufgrund dieser Fähigkeiten ist Mythos bislang nicht frei verfügbar, sondern wird im Rahmen von **Project Glasswing** eingesetzt, einer Kooperation mit ausgewählten Unternehmen, die damit gezielt kritische Software prüfen und absichern.

Was sich im Penetration Testing konkret verschiebt

Der größte Aufwand im **Penetration Testing** liegt selten im reinen Auffinden von Schwachstellen, sondern in deren praktischer Ausnutzung. Genau dieser Schritt wird durch Modelle wie Mythos stark beschleunigt. Anstatt Schwachstellen manuell zu prüfen und Exploits schrittweise zu entwickeln, liefert das Modell oft direkt nutzbare Ergebnisse, inklusive funktionierenden Exploits.



Damit verschiebt sich die Rollenverteilung im Pentesting: weniger technische Detailarbeit, mehr Bewertung und Einordnung. Zugleich verändert sich die Tiefe der Analyse. Angriffspfade, die bisher Erfahrung und Zeit erforderten, lassen sich zunehmend automatisiert ableiten und testen.

Auswirkungen auf Praxis und Bedrohungslage

Pentests in der Praxis werden schneller und effizienter, denn große Codebasen lassen sich in kurzer Zeit prüfen und Ergebnisse sind oft direkt nutzbar, weil bereits ein funktionierender Exploit vorliegt.

Der größere Effekt zeigt sich jedoch auf der Angreiferseite: Wenn Exploit-Entwicklung nicht mehr der limitierende Faktor ist, können deutlich mehr Angriffsvarianten parallel entwickelt und getestet werden. Eine einzelne Person kann damit eine Skalierung erreichen, die bisher nur in Teams möglich war.

Der eigentliche Game-Changer ist damit die Geschwindigkeit – die Zeit zwischen dem Auffinden einer Schwachstelle und ihrer praktischen Ausnutzung schrumpft enorm.

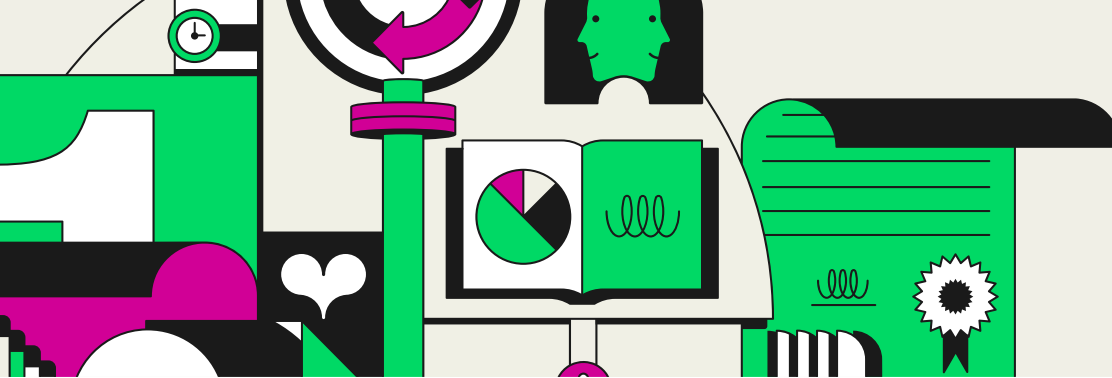
Klassische Sicherheitsprozesse, die auf längere Analyse- und Patchzyklen ausgelegt sind, kommen hier schnell an ihre Grenzen.

Mythos ist nicht grenzenlos – was weiterhin „menschlich“ bleibt

Trotz dieser Fähigkeiten ersetzt Mythos kein vollständiges Penetration Testing. Seine Stärken zeigt das Modell vor allem bei der technischen Analyse von Code und isolierten Systemen.

Gerade reale Umgebungen mit unklaren Abhängigkeiten und geschäftsspezifischer Logik lassen sich teils nicht vollständig abbilden. Auch klassische Black Box Tests, bei denen wenig über das Zielsystem bekannt ist, bleiben anspruchsvoll. Zudem fehlt Modellen wie Mythos die Fähigkeit, längere Angriffskampagnen konsistent zu planen und durchzuführen. Sie arbeiten punktuell sehr effektiv, aber nicht als vollständig orchestrierte Angreifer.

Ein weiterer Faktor ist die kontrollierte Nutzung solcher Systeme. Modelle wie Mythos reagieren sensibel auf Kontext und Formulierung von Anfragen. Wie auch in praktischen Tests (z. B. bei **Cloudflare**) zu sehen ist, können Antworten je nach Framing variieren oder eingeschränkt werden. Diese Mechanismen sind gewollt und einer der Gründe, warum das Modell aktuell nicht frei verfügbar ist. Gleichzeitig begrenzen sie in bestimmten Situationen die direkte Anwendbarkeit beim Penetration Testing.

**Fazit: Der Engpass verschiebt sich**

Claude Mythos verändert Penetration Testing vor allem dadurch, dass ein zentraler Engpass wegfällt – die Überführung von Schwachstellen in echte Angriffe. Für Unternehmen bedeutet das vor allem eins: Die Herausforderung liegt künftig weniger im Finden von Lücken als in deren Bewertung und schneller Reaktion.

Ansprechperson

Haben Sie Fragen oder Kommentare zum Thema Claude Mythos oder Penetration Testing? Wenden Sie sich gerne an **Luis Klein**.

Cybersicherheitsmonitor 2026 veröffentlicht**Die Befragung zur Cybersicherheit gibt Einblicke in den Online-Alltag der Deutschen.**

Jährlich veröffentlichen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) den **Cybersicherheitsmonitor**. Dafür werden über 3000 Menschen ab 16 Jahren zu ihrem digitalen Alltag befragt.

Zahlen, die aufhorchen lassen

Mehr als jeder Zehnte (11%) war im letzten Jahr von einer Straftat im Internet betroffen. Besonders häufig waren Betrug beim Onlineshopping (22%), Onlinebanking (13%) und Phishing (12%). Starke Passwörter und Antivirenprogramme sind die häufigsten Schutzmaßnahmen, doch nicht einmal jeder Zweite (40%) nutzt sie.

Fokusthema Onlinebetrug und künstliche Intelligenz

Da selbst die seit vielen Jahren etablierten Schutzmaßnahmen nur unzureichend eingesetzt werden, verwundern auch die Zahlen zu KI-generierten Inhalten kaum. Viele der Nutzerinnen und Nutzer sind wenig sensibilisiert dafür, dass Inhalte, die täglich beispielsweise auf Social-Media-Plattformen konsumiert werden, womöglich KI-generiert sein könnten: Unstimmigkeiten wie fehlerhafte Schatten oder Gliedmaßen auf KI-Bildern haben nur 28% der Befragten schon einmal gesucht oder bemerkt.

Außerdem halten es nur 38% für technisch möglich, ein KI-System so zu manipulieren, dass es sensible Daten weitergibt – was jedoch eine sehr reale Gefahr ist.



Vom Monitor zum Ernstfall

Bei unserem **Netzwerk Informationssicherheit** befassen wir uns mit solchen Bedrohungen und besprechen wirksame Schutzmaßnahmen. Unser Kollege **Nimrod Briller** der **Berlin Cert** wird etwa die Gefahren durch KI-Tools aufgreifen: Trotz verantwortungsvoller Nutzung entstehen z.B. durch Fehleinschätzungen Sicherheitsrisiken, die zu bewerten und zu minimieren sind.

Mit einem Einblick in den „Wilden Westen Cybercrime“ durch die Experten der Zentralen Ansprechstelle Cybercrime für die Wirtschaft (**ZAC**) im Landeskriminalamt Berlin wird das Programm des Netzwerktreffens mit Erfahrungsberichten aus dem Ernstfall ergänzt. Die Referenten Olaf Borries und Lars Huwald unterstützen in ihrer Rolle beim LKA Unternehmen, Behörden, Verbände und Vereine bei Cyberangriffen und Sicherheitsvorfällen.

Alle Themen finden Sie in unserem **Programm**.

Ansprechperson

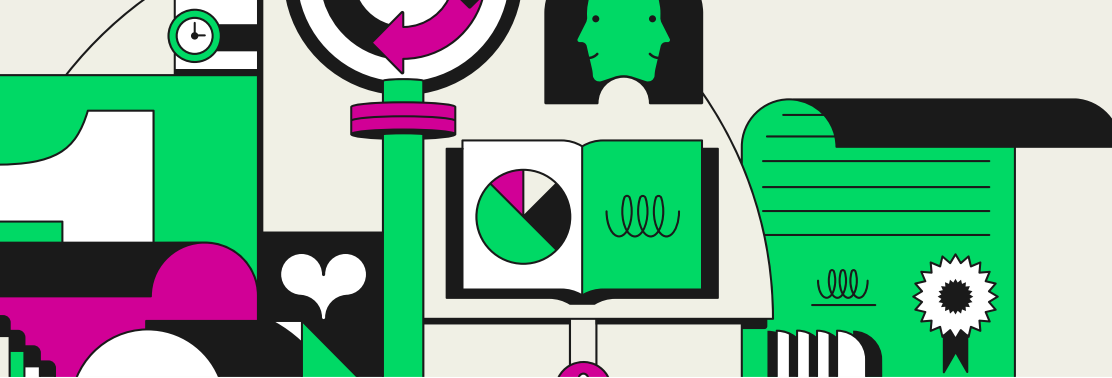
Bei Fragen oder Anmerkungen rund um die Thematik wenden Sie sich gerne an **Tim Stauffenberg**

NIS-2-Schulungspflicht: BSI aktualisiert Empfehlungen für Geschäftsleitungsschulungen

Das BSI hat nun eine aktualisierte Version seiner Empfehlungen zu Schulungen für Geschäftsleitungen nach dem **novellierten BSI-Gesetz (BSIG) veröffentlicht.**

Seit Dezember 2025 gilt eine ausdrückliche Schulungspflicht für Geschäftsleitungen „wichtiger“ und „besonders wichtiger“ Einrichtungen (**§ 38 BSIG**). Geschäftsleitungen sollen dadurch ausreichende Kenntnisse erwerben, um Cyberrisiken bewerten und Risikomanagementmaßnahmen überwachen und beurteilen zu können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu nun seine Handreichung zu Geschäftsleitungsschulungen überarbeitet und im April 2026 die **Version 1.0** veröffentlicht. Die Empfehlungen wurden dabei an mehreren Stellen konkretisiert und erweitert.



Was ist neu an der aktualisierten Handreichung?

1. Anpassung an das geltende BSI-Gesetz

Die vorherige Version basierte noch auf dem Gesetzentwurf (BSIG-E). Die neue Version 1.0 bezieht sich nun auf das tatsächlich in Kraft getretene BSIG und aktualisiert entsprechend die gesetzlichen Verweise und Anforderungen.

2. Erweiterter Adressatenkreis

Das BSI stellt klar, dass sich die Schulungspflicht nicht nur auf „klassische“ Geschäftsführungen oder Vorstände beschränkt. Erfasst werden alle Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Leitung und Vertretung der Einrichtung berufen sind – beispielsweise auch Vorstände, CEO, CIO oder CFO. Das BSI geht davon aus, dass die Schulungspflicht bei den meisten Einrichtungen mehrere Personen trifft.

3. Erweiterung der empfohlenen Schulungsformate

Neu aufgenommen wurden konkrete Empfehlungen für praxisnahe Schulungsformate. Neben klassischen „Frontalformaten“ nennt das BSI beispielsweise:

- Tabletop-Exercises und Planspiele
- Audit-Simulationen
- Szenarien und Case-Studies
- Live-Hacking-Demonstrationen

4. Konkretisierung der Schulungsinhalte

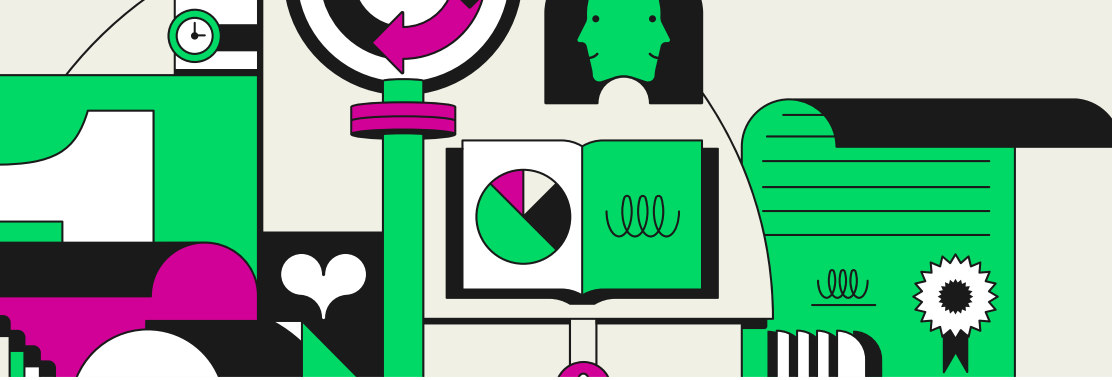
Die Handreichung strukturiert die Inhalte klarer in Kerninhalte und unterstützende Inhalte. Besonders hervorgehoben werden:

- Risikoanalyse
- Risikomanagementmaßnahmen
- Auswirkungen von Risiken auf Geschäftsprozesse
- Melde- und Registrierungspflichten
- Haftungs- und Überwachungspflichten

5. Präzisere Anforderungen an Schulungsdokumentation

Neu konkretisiert das BSI auch, wie Schulungen dokumentiert werden sollten. Empfohlen werden mindestens Angaben zu:

- Schulungsanbieter/interne Stelle
- den beschulten Teilnehmenden



- Datum, Uhrzeit, Dauer der Schulungseinheiten
- Bezüge zu den gesetzlichen Vorgaben aus § 38 Absatz 3 BSIg

Hintergrund ist insbesondere die mögliche Nachweisführung im Rahmen von Aufsichtsmaßnahmen und Prüfungen nach §§ 61 und 62 BSIg.

Damit wird deutlich: Nicht nur die Durchführung, sondern auch die nachvollziehbare Dokumentation der Schulungen gehört zu einer angemessenen Managementpraktik.

Empfehlungen statt verbindlicher Vorgaben

Wichtig ist dabei: Die Handreichung ist zwar keine rechtsverbindliche Vorgabe, zeigt aber deutlich, welche Erwartungen das BSI an Geschäftsleitungsschulungen hat.

Das BSI formuliert ausdrücklich Empfehlungen („SOLL“ bzw. „KANN“) zur Ausgestaltung entsprechender Schulungen. Unternehmen erhalten damit konkrete Hinweise darauf, welche Erwartungen künftig an angemessene Schulungskonzepte gestellt werden dürften.

Compliance sichern mit der NIS-2-Schulung der GUTcert Akademie

Für Unternehmen bedeutet dies: Geschäftsleitungen müssen sich deutlich intensiver mit Cyberrisiken, Risikomanagement und ihrer eigenen Verantwortung auseinandersetzen.

Die **NIS-2-Schulung der GUTcert Akademie** vermittelt die aktuellen Anforderungen aus NIS-2 und BSIg praxisnah und managementorientiert – einschließlich Governance, Risikomanagement und Umsetzung in der Unternehmenspraxis.

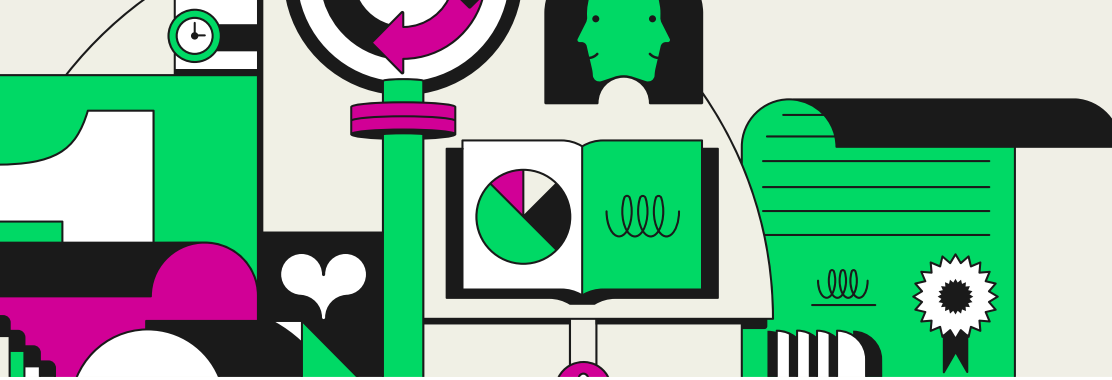
Bei Fragen oder Anmerkungen rund um die Thematik wenden Sie sich gerne an **Cedric Sell**.

GUTcert

Save the Date: Innovationstag Zertifizierung 2027

„Standards als Stabilitätsanker in einer KI-geprägten Welt“ – unser Thema am 15. Januar 2027 bei der alljährlichen Jahresauftaktveranstaltung der GUTcert in Berlin.

Künstliche Intelligenz, neue regulatorische Vorgaben, steigende Nachhaltigkeitsanforderungen und sich wandelnde Normen verändern die betriebliche Praxis: Fast täglich sehen sich Unternehmen mit neuen Herausforderungen konfrontiert. Umso wichtiger werden Standards als verlässlicher Orientierungsrahmen in dieser sehr dynamischen Arbeitswelt.



Herzliche Einladung zum Innovationstag Zertifizierung 2027

Freuen Sie sich auf aktuelle Impulse, fachlichen Austausch und praxisnahe Diskussionen rund um zentrale Zukunftsthemen der Zertifizierung und Unternehmensentwicklung. Auch wenn das Programm noch nicht zu 100% feststeht, stehen doch bereits folgende Themen stark im Fokus:

- EU AI Act und das verantwortungsvolle Nutzen von KI
- EmpCo und aktuelle regulatorische Anforderungen
- Revisionen/Transition von ISO 9001 und ISO 14001
- Managementsysteme, Klima- & Ressourcenschutz
- Entwicklungen im Bereich Medizinprodukte und AZAV

Nach gemeinsamen Keynotes bieten die vertiefenden Fachsessions am Nachmittag Raum für branchenspezifische Perspektiven, konkrete Praxisfragen und intensiven Austausch mit Expertinnen und Experten und GUTcert-Mitarbeitenden.

Neben dem fachlichen Input steht jedoch vor allem eines im Mittelpunkt: Herausforderungen frühzeitig einzuordnen und Chancen aktiv zu nutzen, um gemeinsam die Zukunft zu gestalten.

Jetzt Termin vormerken und Early-Bird-Rabatt sichern

Die Anmeldung ist bereits geöffnet – aktuell profitieren Teilnehmende von vergünstigten Early-Bird-Konditionen.

Selbstverständlich wird die Tagung auch wieder mit einem gemeinsamen Get-together am Vorabend eingeleitet – wir freuen uns, Sie auch dort zu begrüßen!

Weitere Informationen zu Veranstaltung und Anmeldung finden Sie [hier](#).

Ansprechperson

Haben Sie Fragen oder Hinweise zum Innovationstag? Wenden Sie sich gerne an das Team der [Akademie](#).



GUTcert Akademie

AI-Act-Omnibus: EU verschiebt Fristen und konkretisiert KI-Regeln

EU-Kommission, Parlament und Rat haben Anpassungen am EU AI Act beschlossen. Was Unternehmen jetzt über den AI-Act-Omnibus wissen sollten.

Der **EU AI Act** bleibt eines der wichtigsten Regulierungsinstrumente für Unternehmen, die Künstliche Intelligenz entwickeln, einsetzen oder integrieren. Mit dem jüngst ausgehandelten „AI-Act-Omnibus“ reagiert die EU nun auf einen zentralen Kritikpunkt aus Wirtschaft und Industrie: die praktische Umsetzbarkeit. EU-Kommission, Parlament und Rat haben sich im Trilog Anfang Mai politisch auf ein umfangreiches Anpassungspaket verständigt. Ziel ist es, den bürokratischen Aufwand zu reduzieren und die Anforderungen mit weiteren regulatorischen Vorgaben zu harmonisieren.

Der finale Gesetzestext wird derzeit noch juristisch und sprachlich finalisiert. Anschließend müssen Parlament und Rat den Kompromiss formell verabschieden. Mit einer Veröffentlichung im Amtsblatt der Europäischen Union wird derzeit voraussichtlich im Sommer 2026 gerechnet.

Die wichtigsten zu erwartenden Änderungen im Überblick

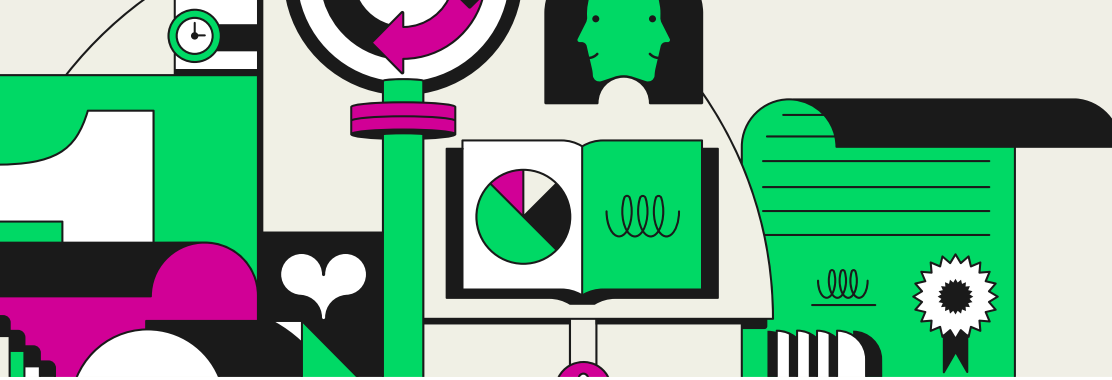
Auch nach dem Omnibus bleibt der risikobasierte Ansatz des **AI Act** bestehen: Besonders strenge Anforderungen gelten weiterhin für sogenannte Hochrisiko-KI-Systeme – also Anwendungen mit potenziellen Auswirkungen auf Sicherheit, Gesundheit oder Grundrechte.

Gleichzeitig enthält das Omnibus-Paket mehrere wichtige Anpassungen:

- Fristen für Hochrisiko-KI-Systeme sollen verschoben werden
- Transparenzpflichten für generative KI werden teilweise später anwendbar
- Doppelregulierung mit bestehenden EU-Regelwerken soll reduziert werden
- Anforderungen zwischen verschiedenen Produktregelungen werden besser aufeinander abgestimmt
- Unternehmen sollen mehr Rechtssicherheit bei Compliance- und Konformitätsverfahren erhalten.

Mehr Zeit für Hochrisiko-KI und generative KI

Eine der wichtigsten Änderungen betrifft die Fristen für Hochrisiko-KI-Systeme: Die Anforderungen für **Systeme nach Anhang III** des AI Act sollen erst **ab Dezember 2027** gelten –



ursprünglich war der Beginn bereits für 2026 vorgesehen. Für bestimmte KI-Systeme im Zusammenhang mit regulierten Produkten **nach Anhang I** – etwa im Bereich Maschinen oder Industrieanlagen – ist derzeit sogar eine **Anwendung ab August 2028** vorgesehen.

Besonders relevant ist dies für Unternehmen aus Industrie, Maschinenbau, Automatisierung und Robotik. Im Zusammenhang mit der europäischen Maschinenverordnung soll die Anwendung der Hochrisikoregeln ebenfalls später starten. Ziel ist es, Überschneidungen zwischen AI Act und bestehenden Produktregelungen zu reduzieren und Unternehmen mehr Zeit für Compliance- und Konformitätsprozesse zu geben.

Auch für generative KI-Systeme sind Änderungen vorgesehen: **Die Transparenzpflichten nach Artikel 50 (2)** sollen voraussichtlich erst ab **Dezember 2026** gelten – und damit vier Monate später als ursprünglich geplant. Keine Änderungen sind dagegen derzeit für die Transparenzpflichten nach Artikel 50 (4) vorgesehen. Die Kennzeichnung künstlich erzeugter oder manipulierter Inhalte – etwa Deepfakes – bleibt damit weiterhin verpflichtend.

Warum Unternehmen sich trotzdem schon jetzt vorbereiten sollten

Auch wenn einzelne Fristen verschoben werden: Der regulatorische Rahmen des AI Act steht längst fest. Unternehmen gewinnen vor allem Zeit für die praktische Umsetzung – nicht jedoch einen Aufschub der grundlegenden Anforderungen.

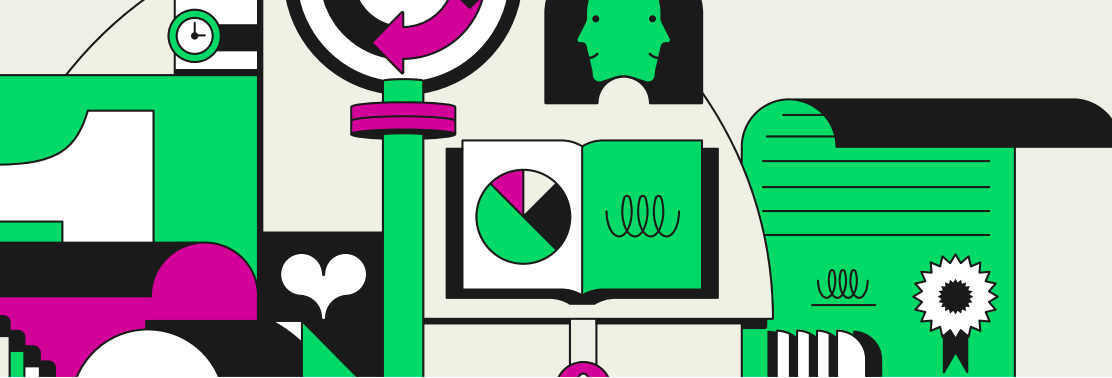
Gerade der Aufbau von AI-Compliance-Strukturen, Risikomanagementprozessen und internen Verantwortlichkeiten benötigt in vielen Unternehmen erhebliche Vorlaufzeit. Hinzu kommt, dass zurzeit auf EU-Ebene zahlreiche technische Standards zur Umsetzung der AI-Act-Anforderungen entwickelt werden – unter anderem zu **Cybersecurity (EN 18282)** oder **Qualitätsmanagement (DIN EN 18286)**.

Unternehmen, die KI-Systeme entwickeln, einsetzen oder integrieren, sollten die zusätzliche Zeit deshalb gezielt nutzen, um:

- eigene KI-Anwendungen zu bewerten
- Risikoklassen einzuordnen
- Governance- und Compliance-Strukturen aufzubauen
- Dokumentations- und Qualitätsprozesse vorzubereiten
- regulatorische Anforderungen frühzeitig in Projekte zu integrieren.

Kompetenzen aufbauen mit dem Seminar der GUTcert Akademie

In unserem Seminar „**EU AI Act: Anforderungen verstehen und praxisnah umsetzen**“



erhalten Sie einen kompakten und praxisnahen Überblick über die aktuellen Anforderungen des EU AI Act sowie die Entwicklungen rund um den AI-Act-Omnibus.

Sie erfahren unter anderem:

- Wie Hochrisiko-KI-Systeme eingeordnet werden
- Welche technischen und organisatorischen Anforderungen künftig gelten
- Wie Risikomanagement- und Qualitätsmanagementsysteme aufgebaut werden
- Welche Anforderungen an Transparenz, Monitoring und Human Oversight bestehen
- Welche Rolle harmonisierte europäische Standards künftig spielen werden

**Das Wichtigste
auf einen Blick**

- 1 Tag | 09:00–17:00 Uhr
- 699 € zzgl. MwSt.
- für **Bestandskunden** der GUTcert: **50 € Rabatt**
- Nächster Termin: **16.09.2026**

Weitere Informationen und Termine: [Seminar | EU AI Act](#)

Haben Sie Fragen oder Anmerkungen zum Thema? Wenden Sie sich gerne an [Cedric Sell](#).

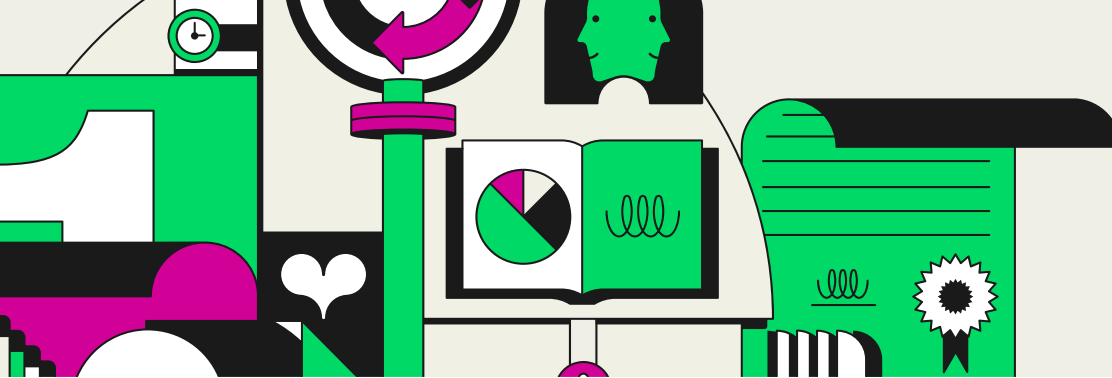
Neues Seminar: Grundlagen der Cybersicherheit

Mit unserem 2-tägigen Seminar zu Cybersicherheit lernen Sie, Sicherheitsrisiken frühzeitig zu erkennen und wirksame Schutzmaßnahmen praxisnah umzusetzen.

Laut [Allianz-Risk-Barometer](#) gehören Cyberangriffe 2026 weltweit zu den bedeutendsten Bedrohungen und damit größten Geschäftsrisiken für Unternehmen. Unternehmen stehen daher vor der Herausforderung, ihre Cybersicherheitsmaßnahmen kontinuierlich weiterzuentwickeln. Ein wirksamer Schutz vor Cyberbedrohungen erfordert das Zusammenspiel technologischer Lösungen, strukturierter Prozesse und eines ausgeprägten Sicherheitsbewusstseins der Mitarbeitenden.

Cybersicherheit ganzheitlich verstehen und umsetzen mit unserem Seminar

Cybersicherheit ist ein entscheidender Erfolgsfaktor für Unternehmen und gewinnt durch regulatorische Anforderungen wie [NIS-2-Richtlinie](#) zunehmend an Bedeutung. [Unser Seminar](#) vermittelt praxisnah die zentralen Grundlagen moderner Cybersicherheit und zeigt, wie



technische, organisatorische und regulatorische Anforderungen wirksam umgesetzt werden können. Teilnehmende lernen, typische Bedrohungen frühzeitig zu erkennen, Sicherheitsrisiken im Unternehmensalltag zu minimieren und geeignete Schutzmaßnahmen anzuwenden.

Inhalte der Cybersicherheitsschulung

- Threat Intelligence: Aktuelle Bedrohungen, Risiken und Angreifer-Methoden – von Social Engineering und Ransomware zur Cyber-Kill-Chain
- Netzwerk-Sicherheit: VLAN und Netz-Segmentierung, (Next-Gen-) Firewalls und VPN-Lösungen
- Identity Management: Authentifizierung, Zugriffskontrollen und Passwortsicherheit (z. B. SSO, MFA, OTP)
- Angewandte Kryptographie: Symmetrische und asymmetrische Verschlüsselung (AES, GPG), Integritätsprüfungen, Digitale Signaturen & Zertifikate
- Sicherheitsmanagement: Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen, anerkannte deutsche und internationale Sicherheitsstandards (**BSI, ISO/IEC 27001, NIS-2**)
- Security Audits: Penetration Tests, Bewertung von Sicherheitsmaßnahmen und Interne Sicherheitsaudits
- Incident Response: Erkennungsmethoden (SIEM/IDS/EDR) und Erstmaßnahmen bei Sicherheitsvorfällen

Zielgruppe & Voraussetzungen

Das Seminar richtet sich an Einsteigerinnen und Einsteiger mit grundlegenden IT-Kenntnissen.

Das Wichtigste auf einen Blick

- Nächster Termin: 17.09.- 18.09.2026, 09:00 – 17:00 Uhr
- Anmeldung: Über diesen [Link](#)
- Kosten: 1.249 € zzgl. MwSt.
- Rabatt für Bestandskunden der GUTcert: 50 €

Bei Fragen oder Anmerkungen zu unseren Veranstaltungen wenden Sie sich gerne an das **Team der GUTcert Akademie**.



Das neue Gebäudemodernisierungsgesetz (GModG) löst das Gebäudeenergiegesetz (GEG) ab

Das GModG wurde im Bundeskabinett beschlossen. In unserem Webinar erfahren Sie, welche Anforderungen künftig gelten und wie Sie sich frühzeitig darauf vorbereiten können.

Mit dem **geplanten Gebäudemodernisierungsgesetz (GModG)** steht eine grundlegende Neuausrichtung der Regeln im Gebäudesektor bevor. Das GModG soll das bisherige **Gebäudeenergiegesetz (GEG)** ablösen und bestehende Regelungen stärker an die **EU-Gebäuderichtlinie (EPBD)** anpassen. Für Unternehmen und Energieberater ergeben sich daraus grundlegende Änderungen und konkreter Handlungsbedarf.

Die Hintergründe der Umstellung und die Verortung im GUTcert Webinar

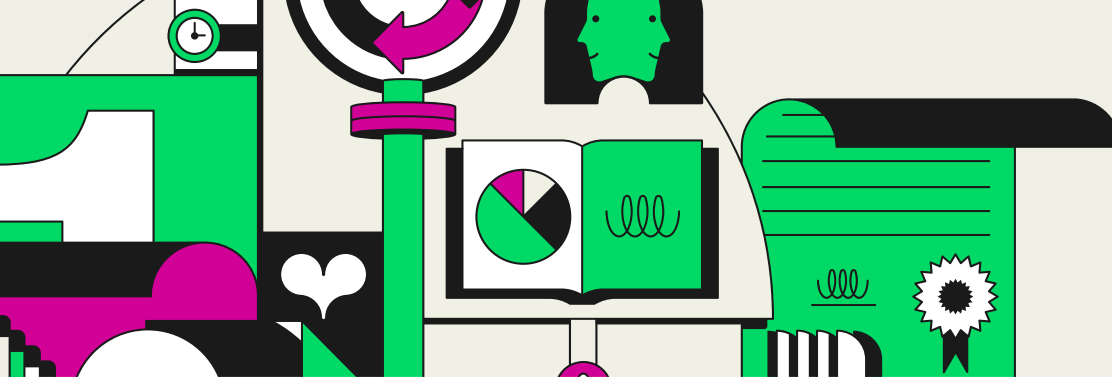
In **unserem Webinar** erfahren Sie, welche politischen Entwicklungen zur Einführung des GModG geführt haben und welche Systematik dem neuen Gesetz zugrunde liegt. Sie erhalten einen Überblick darüber, wie sich die Aufgaben, Nachweise und Anforderungen für die Energieberatung verändern und wie diese im Zusammenhang mit den Klimaschutzanforderungen im Gebäudesektor einzuordnen sind. Darüber hinaus gewinnen Sie Sicherheit im Umgang mit den neuen Rahmenbedingungen und können die zukünftigen Regelungen in Ihre berufliche Praxis integrieren.

Überblick der Fortschreibungen

- Umstellung auf den Gesamtprimärenergiebedarf
- Anforderungen an Heizsysteme
- Weiterentwicklung von Energieausweisen und Effizienzklassen
- Nutzungspflichten für erneuerbare Energien
- Berücksichtigung von Photovoltaik
- Neue Vorgaben für Nichtwohngebäude (NWG)
- Anpassung der Referenzgebäude
- Aktualisierung der DIN/TS 18599

Zielgruppe

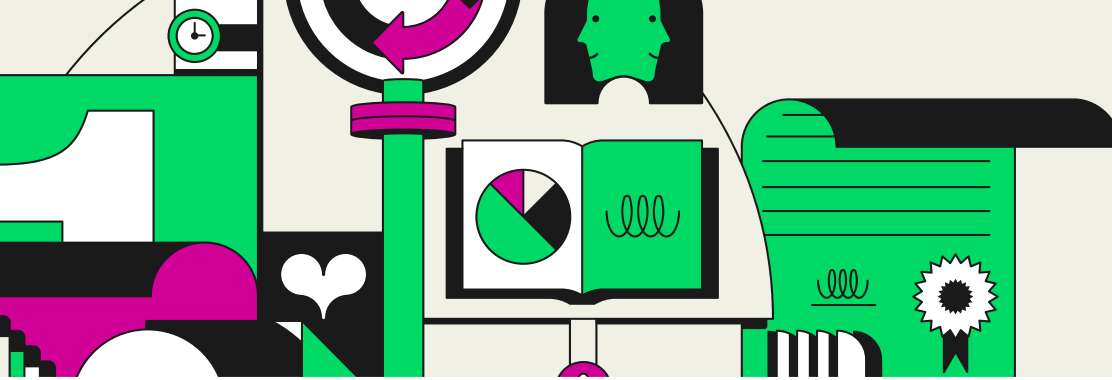
Das Webinar richtet sich an Fach- und Führungskräfte im Gebäudesektor und an Energieberater.



**Das Wichtigste
auf einen Blick**

- Nächster Termin: 01.07., 13:30 – 15:30 Uhr
- Anmeldung: Über diesen [Link](#)
- Kosten: 150 €

Bei Fragen oder Anmerkungen zu unseren Veranstaltungen wenden Sie sich gerne an das **Team** der **GUTcert Akademie**.



Veranstaltungstermine der GUTcert Akademie (Auszug)

08.06.–12.06.2026

Umweltbeauftragter/-auditor (gn) nach ISO 14001:2015 (GUTcert) [zum Seminar](#)

08.06.–10.06.2026

Qualitätsbeauftragter/-auditor (gn) nach ISO 9001:2015 (GUTcert) [zum Seminar](#)

09.06.–10.06.2026

AZAV: Grundlagen und aktuelle Themen [zum Seminar](#)

09.06.–11.06.2026

Beauftragter (gn) für Nachhaltiges Veranstaltungsmanagement nach ISO 20121 – Modul 2 [zum Seminar](#)

12.06.2026 und 26.06.2026

Klimarisiken und -folgen systematisch managen nach ISO 14090/91 [zum Seminar](#)

15.06.2026

KI in ISO-Managementsystemen: Von der Theorie zur praktischen Anwendung [zum Seminar](#)

16.06.–17.06.2026

Klimamanagementbeauftragter (gn) im Unternehmen: Vom Corporate Carbon Footprint bis zur Klimaneutralität – Modul 1 [zum Seminar](#)

16.06.–17.06.2026

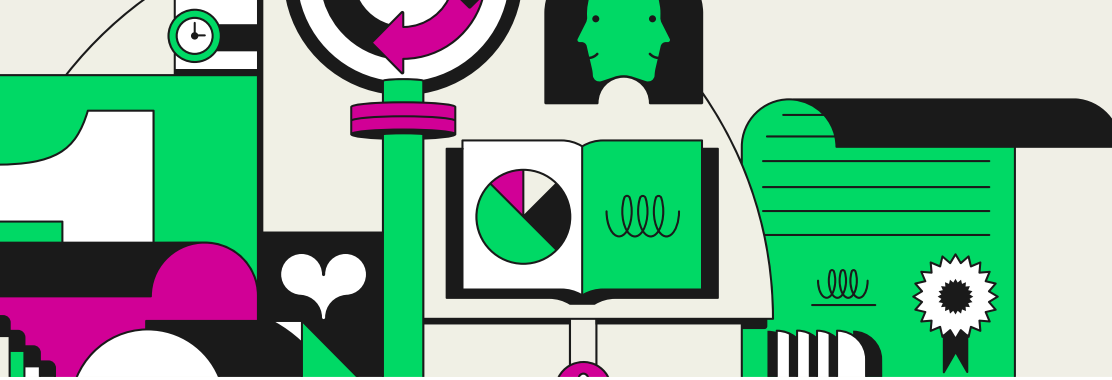
Umweltrecht: Grundlagen und aktuelle Themen [zum Seminar](#)

17.06.–18.06.2026

Energiekennzahlen und Einfluss-faktoren nach ISO 50001 i.V.m. ISO 50006 und ISO 50015 [zum Seminar](#)

17.06.2026

Netzwerk Informationssicherheit [zum Seminar](#)



18.06.2026

Wirtschaftlichkeitsanalyse im Energiemanagement nach VALERI (DIN EN 17463) [zum Seminar](#)

18.06.2026

Klimamanagementbeauftragter (gn) im Unternehmen: Product Carbon Footprint (PCF) – Modul 2 [zum Seminar](#)

18.06.2026

Webinar: Einführung in die RSPO-Zertifizierung [zum Seminar](#)

22.06.–26.06.2026

Beauftragter (gn) für integrierte Managementsysteme und Compliance-Sicherung (GUTcert) [zum Seminar](#)

Dieser Newsletter dient der allgemeinen Information. Für die Newsletter im Infobrief werden keine Gewähr und Haftung übernommen. Sollten Sie diesen Newsletter irrtümlich erhalten haben, bitten wir um Entschuldigung. Klicken Sie bitte [hier](#), dann wird Ihre Mailadresse aus dem Verteiler gelöscht.

GUT Zertifizierungsgesellschaft für Managementsysteme | Umweltgutachter
Eichenstraße 3b, 12435 Berlin, Germany | +49 30 2332021 - 0 | info@gut-cert.de
Geschäftsführer: Prof. Dr.-Ing. Jan Uwe Lieback | Amtsgericht Berlin-Charlottenburg, HRB 64544 | USt-ID-Nr. DE 190888348