



## **ISC2 führt neue Express-Kurse mit kompaktem, zielgerichtetem Lernen für vielbeschäftigte Cybersecurity-Fachkräfte ein**

*On-Demand-Kurse in den Bereichen Governance, Risk and Compliance (GRC), Cloud-Sicherheit, Benutzerschulung zur Sensibilisierung und Datenschutz statten Cybersecurity-Fachkräfte mit den notwendigen Fähigkeiten aus und stärken ihre Security-Programme.*

**Alexandria, Va., 26. August 2025** – [ISC2](#), die weltweit führende gemeinnützige Mitgliederorganisation für Cybersecurity-Fachkräfte, stellt heute vierzehn neue [Express-Kurse](#) vor. Die Kurse behandeln aktuelle Themen und Trends der Cyber-Security-Branche in einem ein- bis zweistündigen, selbstbestimmten Format. Die Express-Kurse erleichtern Experten den Erwerb von Cybersecurity-Kenntnissen durch fundierte Lernerfahrungen, die sich an ihre anspruchsvollen Zeitpläne anpassen.

Eine aktuelle [Studie von ISC2](#) zeigt, dass Fähigkeiten in Cloud-Computing-Sicherheit und Risikobewertung, -analyse und -management zu den gefragtesten technischen Kompetenzen im Cybersecurity-Umfeld gehören. Die Express-Kurse decken diesen Bedarf an neuen Fähigkeiten konzentriert ab und unterstützen Cyber-Security-Profis beim Auf- und Ausbau ihrer Expertise.

„Die Express-Kurse sind Teil unseres Engagements und befähigen unsere Mitglieder, den aktuellen Themen immer einen Schritt voraus zu sein und ihre eigene berufliche Weiterentwicklung voranzutreiben“, sagt Casey Marks, Chief Operating Officer von ISC2. „Die Flexibilität dieser Kurse ermöglicht es Cybersecurity-Experten, ihre berufliche Entwicklung fortzusetzen, indem sie neue Technologien und Praktiken kennenlernen und Bereiche identifizieren, in denen sie zusätzliche Ausbildung benötigen.“



## Die neuen Express-Kurse umfassen:

### Sicherheitsbildung, -schulung und -bewusstsein (SETA)

- [Grundlagen eines engagierten SETA](#): Fähigkeiten zur Entwicklung einer starken Sicherheitskultur innerhalb des Teams einer Organisation über das Bewusstsein hinaus hin zu aktivem Lernen.
- [Planung eines SETA-Programms](#): Erforderliche Überlegungen, Ressourcen und Support-Strukturen, um eine starke Sicherheitskultur in einer Organisation zu fördern.
- [Implementierung und Überprüfung von SETA-Programmen](#): Möglichkeiten zur Gestaltung, Umsetzung und Bewertung der Wirksamkeit von Sicherheitsprogrammen einer Organisation.

### Cloud- und Softwaresicherheit

- [Virtualisierungs- und Container-Technologien in der Cloud-Sicherheit](#): Ein Grundlagenkurs zur Cloud-Sicherheit, der für alle Ebenen von Cyber-Fachkräften konzipiert ist.
- [Bewertung von Cloud-Service-Provider-Vereinbarungen und Service Level Agreements \(SLAs\)](#): Die Erkundung, wie Cloud-Service-Vereinbarungen bewertet werden können, um sicherzustellen, dass sie strategische Ziele unterstützen.
- [Stakeholder-Management und Einbindung von Entwicklungsteams](#): Ein Kurs auf mittlerem Niveau über das Management von Software-Security-Entwicklern oder die Entwicklung einer Cybersecurity-Strategie.

### Governance, Risiko und Compliance

- [Cyberrisiken auf Business-Ebene für effektive Führung übertragen](#): Ein Überblick, wie man mit der Führungsebene einer Organisation, einschließlich des Vorstands, kommuniziert.
- [Navigation durch Cybersecurity-Frameworks](#): Ein Kurs zum Verständnis, welche [Cybersecurity-Frameworks](#) relevant sind, um die Sicherheitslage einer bestimmten Organisation aufrechtzuerhalten.
- [CNI- und OT-Standards](#): Ein definitionsbasierter Überblick über Kritische Nationale Infrastrukturen (CNI) und Operational Technology (OT) sowie die sicherheitsrelevanten Aspekte.



## Datenschutz

- [Einhaltung von Vorschriften, Gesetzen, Standards und Frameworks](#): Eine dynamische Übung zur Ermittlung bewährter Vorgehensweisen für die Einhaltung von Vorschriften.
- [Auswirkungen, Analyse und Management von Verstößen](#): Ein praxisnaher Blick auf ein fiktives Unternehmen, das die Auswirkungen eines Verstoßes gegen Datenschutz- oder -regelungen durchläuft.
- [Klassifizierung, Kategorisierung und Sicherheit von Daten](#): Best Practices zum Verständnis von Daten und deren Bedeutung für die Einhaltung von Vorschriften und Resilienz.
- [Überarbeitung von Richtlinien und Verfahren](#): Ein interaktives Szenario eines Cybersecurity-Teams, das Richtlinien, Verfahren und Dokumentationsanforderungen nach einem Vorfall überprüft.
- [Aufbau einer Organisationskultur](#): Möglichkeiten, die Unterstützung von Interessengruppen in der gesamten Organisation zu sichern, Datenschutzrisiken zu mindern und die fortlaufende Einhaltung zu gewährleisten.

Die Kurse sind für Mitglieder über [My Courses](#) vergünstigt erhältlich oder für Nichtmitglieder unter [www.isc2.org/development](http://www.isc2.org/development) verfügbar. Sie sind zwischen 0,5 – 1,0 CPE-Credits wert.

Weitere Informationen zum vollständigen Katalog der Express-Kurse finden Sie unter: <https://www.isc2.org/professional-development/courses#Express>



## Über ISC2

ISC2 ist die weltweit führende Nonprofit-Organisation für Cybersecurity-Experten. Mit über 265.000 zertifizierten Mitgliedern und Partnern setzen wir uns in einer immer stärker vernetzten Gesellschaft für eine sichere Cyberwelt ein. Unsere renommierten Zertifizierungen – darunter die branchenführende CISSP®-Zertifizierung – dienen Fachkräften als Nachweis ihrer Kenntnisse, Fähigkeiten und Kompetenzen in jeder Phase ihrer Karriere.

ISC2 setzt Cybersecurity auf die politische und gesellschaftliche Agenda. Wir fördern die Relevanz, Vielfalt und Dynamik der Cybersecurity-Branche durch engagierte Fürsprache, fundiertes Fachwissen und die Schulung und Zertifizierung von Fachkräften.

Mit unserer gemeinnützigen Stiftung, dem [Center for Cyber Safety and Education](#), vereinfachen wir den Zugang zu diesem Berufszweig für angehende Nachwuchskräfte.

Erfahren Sie mehr über [ISC2](#) und werden Sie Teil unserer Mission. Vergrößern Sie ihr Netzwerk und folgen Sie uns auf [X](#), [Facebook](#) und [LinkedIn](#).

© 2025 ISC2 Inc. | ISC2, CISSP®, SSCP®, CCSP®, CGRC®, CSSLP®, HCISPP®, ISSAP®, ISSEP®, ISSMP®, CC® und CBK® sind eingetragene Marken von ISC2, Inc.

## Pressekontakt:

ISC2

Kiri O'Leary, Corporate Communications Professional

[koleary@isc2.org](mailto:koleary@isc2.org)

TC Communications

Arno Lücht, +49 157 52443749

Thilo Christ, +49 171 6220610

Alexandra Schmidt, +49 170 3871064

[ISC2@tc-communications.de](mailto:ISC2@tc-communications.de)