Open C3S
Open Competence Center for Cyber Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16OH12021 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor/bei der Autorin.

Technische Universität Darmstadt

Verbundprojekt

Open C³S

Open Competence Center for Cyber Security

Studiengang

Zertifikatsangebot "Open C³S"

Ergebnisse der Profilpotenzialanalyse (PPA) für das

Weiterbildungsprofil

Certified in Risk and Information Systems Control (CRISC)

Mapping & Deckungsfaktoren

Anrechnungsempfehlungen des externen Experten

1. Anrechnungsempfehlungen auf der Grundlage der EQR-Bewertungen der Studiengangmodule durch die Hochschulen

EQR-Bewertung der beruflichen Prozesse, Mapping & Deckungsfaktoren: externer Experte

Das Mapping wurde in Bezug auf die für Anrechnung erforderliche Niveauäquivalenz *hinsichtlich der EQR-Bewertungen der Studiengangmodule durch die externen Experten (Konsens)* durchgeführt, so dass im Kontext der *EQR-Bewertungen der Studiengangmodule durch die Hochschulen* hinsichtlich des Niveaus Diskrepanzen auftreten. Weitere Information hierzu sind dem Abschlussbericht von Teilprojekt 2 im Projekt Open C³S zu entnehmen.

Anrechnungsempfehlungen (Niveauäquivalenz* & Deckungsfaktor ≥ 70%) sind farblich hervorgehoben.

2. Anrechnungsempfehlungen auf der Grundlage der EQR-Bewertungen der Studiengangmodule durch die externen Experten (Konsens)

EQR-Bewertung der beruflichen Prozesse, Mapping & Deckungsfaktoren: externer Experte

Die EQR-Bewertungen der Studiengangmodule der externen Experten (Konsens) basieren ausschließlich auf den *Angaben und Formulierungen* im Modulhandbuch des entsprechenden Studiengangs, das im Rahmen des Forschungs- und Entwicklungsprojektes Open C³S veröffentlich wurde. Weitere Information hierzu sind dem Abschlussbericht von Teilprojekt 2 im Projekt Open C³S zu entnehmen.

Anrechnungsempfehlungen (Niveauäquivalenz* & Deckungsfaktor ≥ 70%) sind farblich hervorgehoben.

* Im Rahmen der Profilpotenzialanalysen wurde bei der Zuordnung von beruflichen Prozessen zu einem Studiengangmodul eine negative Abweichung von einer EQR-Niveaustufe als Toleranzbereich für eine noch gegebene Niveauäquivalenz festgelegt. Weitere Information hierzu sind dem Abschlussbericht von Teilprojekt 2 im Projekt Open C³S zu entnehmen.

Forschungsgruppe Brinkmann/Seger
seger@ifs.tu-darmstadt.de

Studiengang

Zertifikatsangebot "Open C³S"

Ergebnisse der Profilpotenzialanalyse (PPA) für das

Weiterbildungsprofil

Certified in Risk and Information Systems Control (CRISC)

Mapping & Deckungsfaktoren

1. Anrechnungsempfehlungen auf der Grundlage der EQR-Bewertungen der Studiengangmodule durch die Hochschulen

EQR-Bewertung der beruflichen Prozesse, Mapping & Deckungsfaktoren: externer Experte

Anrechnungsempfehlungen (Niveauäquivalenz & Deckungsfaktor ≥ 70%) sind farblich hervorgehoben.

Modul Studiengang	EQR-Niveau Median	Deckungs-faktor %	Prozess berufliches Bildungsprofil	EQR-Niveau Median
Methoden digitaler Forensik	6			
Systemnahe Programmierung	6			
Reverse Engineering	7			
Mobilfunkforensik	7			
Applied Computer Systems	**6**	**80**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	**6**
Python 1 – Programmieren im IT-Security-Umfeld	6			
Python 2 – Programmieren im IT-Security-Umfeld	6			
Datenträgerforensik 1	7			
Datenträgerforensik 2	7			
Windows-Forensik	6			
Internettechnologien	**6**	**80**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	**6**
Netzsicherheit 1	**6**	**15**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	**6**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
Netzsicherheit 2	**6**	**15**	**Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner**	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
Netzsicherheit 3	**6**	**10**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
SPAM	6			
Sicherheit mobiler Systeme	7			
Computerstrafrecht	**6**	**15**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.5 The IT Risk Strategy of the Business	**6**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 2: IT Risk Assessment: 2.2 Analyzing Risk Scenarios	**5**
Computerstrafprozessrecht	6			
Europäisierung & Internationalisierung des Strafrechts	6			

Studiengang

Zertifikatsangebot "Open C³S"

Ergebnisse der Profilpotenzialanalyse (PPA) für das

Weiterbildungsprofil

Certified in Risk and Information Systems Control (CRISC)

Mapping & Deckungsfaktoren

2. Anrechnungsempfehlungen auf der Grundlage der EQR-Bewertungen der Studiengangmodule durch die externen Experten (Konsens)

EQR-Bewertung der beruflichen Prozesse, Mapping & Deckungsfaktoren: externer Experte

Anrechnungsempfehlungen (Niveauäquivalenz & Deckungsfaktor ≥ 70%) sind farblich hervorgehoben.

Modul Studiengang	EQR-Niveau Median	Deckungs-faktor %	Prozess berufliches Bildungsprofil	EQR-Niveau Median
Methoden digitaler Forensik	5			
Systemnahe Programmierung	5			
Reverse Engineering	5			
Mobilfunkforensik	5			
Applied Computer Systems	**4**	**80**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	**6**
Python 1 – Programmieren im IT-Security-Umfeld	4			
Python 2 – Programmieren im IT-Security-Umfeld	5			
Datenträgerforensik 1	4			
Datenträgerforensik 2	5			
Windows-Forensik	5			
Internettechnologien	**4**	**80**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	**6**
Netzsicherheit 1	**4**	**15**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	**6**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
Netzsicherheit 2	**4**	**15**	**Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner**	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
Netzsicherheit 3	**4**	**10**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
SPAM	4			
Sicherheit mobiler Systeme	4			
Computerstrafrecht	**4**	**15**	**Chapter 1: IT Risk Identification: 1.3 Elements of Risk**	**7**
			Chapter 1: IT Risk Identification: 1.5 The IT Risk Strategy of the Business	**6**
			Chapter 1: IT Risk Identification: 1.6 IT Concepts and Areas of Concern for the Risk Practitioner	**6**
			Chapter 2: IT Risk Assessment: 2.2 Analyzing Risk Scenarios	**5**
Computerstrafprozessrecht	4			
Europäisierung & Internationalisierung des Strafrechts	4			