

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.

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung



# Technische Universität Darmstadt

## Verbundprojekt Open C<sup>3</sup>S Open Competence Center for Cyber Security

### Studiengang Bachelor Informatik / IT-Sicherheit

Ergebnisse der Profipotenzialanalyse (PPA) für das

### Weiterbildungsprofil ISO 27001 Lead Auditor

## 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 C<sup>3</sup>S zu entnehmen.

**Anrechnungsempfehlungen (Niveauäquivalenz\* & Deckungsfaktor  $\geq$  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 C<sup>3</sup>S veröffentlicht wurde. Weitere Information hierzu sind dem Abschlussbericht von Teilprojekt 2 im Projekt Open C<sup>3</sup>S zu entnehmen.

**Anrechnungsempfehlungen (Niveauäquivalenz\* & Deckungsfaktor  $\geq$  70%) sind farblich hervorgehoben.**

\* Im Rahmen der Profipotenzialanalysen 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 C<sup>3</sup>S zu entnehmen.



Bundesministerium  
für Bildung  
und Forschung



**Studiengang  
Bachelor Informatik / IT-Sicherheit**

Ergebnisse der Profilpotenzialanalyse (PPA) für das

**Weiterbildungsprofil  
ISO 27001 Lead Auditor**

**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  $\geq 70\%$ ) sind farblich hervorgehoben.**

Modul Studiengang	EQR- Niveau Median	Deckungs- faktor %	Prozess berufliches Bildungsprofil	EQR- Niveau Median
Mathematik 1	6			
Grundlagen der Programmierung	6			
Einführung in die IT-Sicherheit	6			
Konzeptionelle Modellierung	6			
Mathematik 2	6			
Rechnerstrukturen	6			
Theoretische Informatik	6			
Systemsicherheit 1	6			
Algorithmen und Datenstrukturen	6			
Kryptographie 1	6			
Systemnahe Programmierung	6			
Systemsicherheit 2	6			
Proseminar	6			
Einführung in die digitale Forensik	6			
Compilerbau	6			
Netzicherheit 1	6			
Kryptographie 2	6			
Realisierung von Softwareprojekten	6			
Netzicherheit 2	6			
Netzicherheit 3	6			
Weiterführende Themen der Computerforensik	6			
Kryptographische Protokolle	6			
Sicherheit mobiler Systeme	6			
<b>Sicherheitsmanagement</b>	<b>6</b>	<b>50</b>	<b>Context of the organization: 4.1 Understanding the organization and its context</b>	<b>5</b>
			<b>Context of the organization: 4.2 Understanding the needs and expectations of interested parties</b>	<b>5</b>
			<b>Context of the organization: 4.3 Determining the scope of the information security management system</b>	<b>5</b>
			<b>Context of the organization: 4.4 Information security management system</b>	<b>5</b>
			<b>Improvement: 10.1 Nonconformity and corrective action</b>	<b>5</b>
			<b>Improvement: 10.2 Continual improvement</b>	<b>5</b>
			<b>Leadership: 5.1 Leadership and commitment</b>	<b>5</b>
			<b>Leadership: 5.2 Policy</b>	<b>5</b>
			<b>Leadership: 5.3 Organizational roles, responsibilities and authorities</b>	<b>5</b>
			<b>Operation: 8.1 Operational planning and control</b>	<b>5</b>
			<b>Operation: 8.2 Information security risk assessment</b>	<b>5</b>
			<b>Operation: 8.3 Information security risk treatment</b>	<b>5</b>
			<b>Performance evaluation: 9.1 Monitoring, measurement, analysis and evaluation</b>	<b>5</b>
			<b>Performance evaluation: 9.2 Internal audit</b>	<b>5</b>
			<b>Performance evaluation: 9.3 Management review</b>	<b>5</b>
			<b>Planning: 6.1 Actions to address risks and opportunities</b>	<b>5</b>
			<b>Planning: 6.2. Information security objectives and planning to achieve them</b>	<b>5</b>
			<b>Support: 7.1 Resources</b>	<b>5</b>
			<b>Support: 7.2 Competence</b>	<b>5</b>
			<b>Support: 7.3 Awareness</b>	<b>5</b>
			<b>Support: 7.4 Communication</b>	<b>5</b>
			<b>Support: 7.5 Documented information</b>	<b>5</b>

Modul Studiengang	EQR- Niveau	Deckungs- faktor	Prozess berufliches Bildungsprofil	EQR- Niveau
	Median	%		Median
Spam	6			
Netzbasierter Angriffserkennung	6			
User-Centered Security	6			
Incident Management	6			
Elektronische Identitäten	6			
Ethisches Hacking	6			
Anonymität im Netz	6			
Internetforensik	6			
Seminar	6			
Projekt	6			
Bachelorarbeit	6			

**Studiengang  
Bachelor Informatik / IT-Sicherheit**

Ergebnisse der Profilpotenzialanalyse (PPA) für das

**Weiterbildungsprofil  
ISO 27001 Lead Auditor**

**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  $\geq 70\%$ ) sind farblich hervorgehoben.**

Modul Studiengang	EQR- Niveau	Deckungs- faktor	Prozess berufliches Bildungsprofil	EQR- Niveau
	Median	%		Median
Mathematik 1	5			
Grundlagen der Programmierung	5			
Einführung in die IT-Sicherheit	3			
Konzeptionelle Modellierung	4			
Mathematik 2	5			
Rechnerstrukturen	3			
Theoretische Informatik	4			
Systemsicherheit 1	3			
Algorithmen und Datenstrukturen	4			
Kryptographie 1	3			
Systemnahe Programmierung	4			
Systemsicherheit 2	4			
Proseminar	4			
Einführung in die digitale Forensik	4			
Compilerbau	5			
Netzicherheit 1	4			
Kryptographie 2	5			
Realisierung von Softwareprojekten	4			
Netzicherheit 2	5			
Netzicherheit 3	5			
Weiterführende Themen der Computerforensik	5			
Kryptographische Protokolle	5			
Sicherheit mobiler Systeme	4			
<b>Sicherheitsmanagement</b>	<b>4</b>	<b>50</b>	<b>Context of the organization: 4.1 Understanding the organization and its context</b>	<b>5</b>
			<b>Context of the organization: 4.2 Understanding the needs and expectations of interested parties</b>	<b>5</b>
			<b>Context of the organization: 4.3 Determining the scope of the information security management system</b>	<b>5</b>
			<b>Context of the organization: 4.4 Information security management system</b>	<b>5</b>
			<b>Improvement: 10.1 Nonconformity and corrective action</b>	<b>5</b>
			<b>Improvement: 10.2 Continual improvement</b>	<b>5</b>
			<b>Leadership: 5.1 Leadership and commitment</b>	<b>5</b>
			<b>Leadership: 5.2 Policy</b>	<b>5</b>
			<b>Leadership: 5.3 Organizational roles, responsibilities and authorities</b>	<b>5</b>
			<b>Operation: 8.1 Operational planning and control</b>	<b>5</b>
			<b>Operation: 8.2 Information security risk assessment</b>	<b>5</b>
			<b>Operation: 8.3 Information security risk treatment</b>	<b>5</b>
			<b>Performance evaluation: 9.1 Monitoring, measurement, analysis and evaluation</b>	<b>5</b>
			<b>Performance evaluation: 9.2 Internal audit</b>	<b>5</b>
			<b>Performance evaluation: 9.3 Management review</b>	<b>5</b>
			<b>Planning: 6.1 Actions to address risks and opportunities</b>	<b>5</b>
			<b>Planning: 6.2. Information security objectives and planning to achieve them</b>	<b>5</b>
			<b>Support: 7.1 Resources</b>	<b>5</b>
			<b>Support: 7.2 Competence</b>	<b>5</b>
			<b>Support: 7.3 Awareness</b>	<b>5</b>
			<b>Support: 7.4 Communication</b>	<b>5</b>
			<b>Support: 7.5 Documented information</b>	<b>5</b>

Modul Studiengang	EQR-Niveau	Deckungs-	Prozess berufliches Bildungsprofil	EQR-Niveau
	Median	faktor %		Median
Spam	4			
Netzbasierte Angriffserkennung	5			
User-Centered Security	4			
Incident Management	3			
Elektronische Identitäten	4			
Ethisches Hacking	5			
Anonymität im Netz	4			
Internetforensik	4			
Seminar	5			
Projekt	5			
Bachelorarbeit	5			