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

Master IT GRC Management

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

Master IT GRC Management

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
Nationaler und internationaler Rechtsrahmen für Unternehmen	6-7			
Grundlagen IT Governance, Risk and Compliance Management	**6-7**	**85**	**Chapter 1: IT Risk Identification: 1.1 Risk Capacity, Risk Appetite and Risk Tolerance**	**6**
			Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	**6**
			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: 1.5 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 1: IT Risk Identification: 1.7 Methods of Risk Identification	**6**
			Chapter 1: IT Risk Identification: 1.8 IT Risk Scenarios	**7**
			Chapter 1: IT Risk Identification: 1.9 Ownership and Accountability	**6**
			Chapter 1: IT Risk Identification: 1.10 The IT Risk Register	**7**
			Chapter 1: IT Risk Identification: 1.11 Risk Awareness	**6**
			Chapter 2: IT Risk Assessment: 2.1 Risk Assessment Techniques	**7**
			Chapter 2: IT Risk Assessment: 2.2 Analyzing Risk Scenarios	**5**
			Chapter 2: IT Risk Assessment: 2.3 Current State of Controls	**6**
			Chapter 2: IT Risk Assessment: 2.4 Changes in the Risk Environment	**7**
			Chapter 2: IT Risk Assessment: 2.5 Project and Program Management	**5**
			Chapter 2: IT Risk Assessment: 2.6 Risk and Control Analysis	**6**
			Chapter 2: IT Risk Assessment: 2.7 Risk Analysis Methodologies	**6**
			Chapter 2: IT Risk Assessment: 2.8 Risk Ranking	**6**
			Chapter 2: IT Risk Assessment: 2.9 Documenting Risk Assessments	**6**
			Chapter 3: Risk Response and Mitigation: 3.1 Aligning Risk Response With Business Objectives	**7**
			Chapter 3: Risk Response and Mitigation: 3.2 Risk Response Options	**6**
			Chapter 3: Risk Response and Mitigation: 3.3 Analysis Techniques	**7**
			Chapter 3: Risk Response and Mitigation: 3.4 Vulnerabilities Associated With New Controls	**6**
			Chapter 3: Risk Response and Mitigation: 3.5 Developing a Risk Action Plan	**6**
			Chapter 3: Risk Response and Mitigation: 3.6 Business Process Review Tools and Techniques	**5**
			Chapter 3: Risk Response and Mitigation: 3.7 Control Design and Implementation	**5**
			Chapter 3: Risk Response and Mitigation: 3.8 Control Monitoring and Effectiveness	**6**
			Chapter 3: Risk Response and Mitigation: 3.9 Types of Risk	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 3: Risk Response and Mitigation: 3.11 Systems Control Design and Implementation	**6**
			Chapter 3: Risk Response and Mitigation: 3.12 Impact of Emerging Technologies on Design and Implementation of Controls	**6**
			Chapter 3: Risk Response and Mitigation: 3.13 Control Ownership	**6**
			Chapter 3: Risk Response and Mitigation: 3.14 Risk Management Procedures and Documentation	**6**

Modul Studiengang	EQR-Niveau Median	Deckungs-faktor %	Prozess berufliches Bildungsprofil	EQR-Niveau Median
			Chapter 4: Risk and Control Monitoring and Reporting: 4.1 Key Risk Indicators	7
			Chapter 4: Risk and Control Monitoring and Reporting: 4.2 Key Performance Indicators	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.3 Data Collection and Extraction Tools and Techniques	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.4 Monitoring Controls	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.6 Results of Control Assessments	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.7 Changes to the IT Risk Profile	6
Datenmanagement und Datenorganisation	6-7	20	Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	6
			Chapter 1: IT Risk Identification: 1.9 Ownership and Accountability	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
IT-Grundlagen	6-7			
Wirtschafts- und Internetkriminalität	6-7			
Informations- und IT-Management	6-7			
IT-GRC Standards und Frameworks	6-7	60	Chapter 1: IT Risk Identification: 1.5 The IT Risk Strategy of the Business	6
			Chapter 1: IT Risk Identification: 1.7 Methods of Risk Identification	6
IT-Sicherheit und Kryptografie	6-7	85	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: 1.5 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 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
Rechtsstreitigkeiten und eDiscovery	6-7			
Anforderungsmanagement IT-GRC	6-7	65	Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 3: Risk Response and Mitigation: 3.11 Systems Control Design and Implementation	6
Geschäftsprozess-Management im GRC-Kontext	6-7	50	Chapter 1: IT Risk Identification: 1.3 Elements of Risk	7
			Chapter 3: Risk Response and Mitigation: 3.6 Business Process Review Tools and Techniques	5
			Chapter 3: Risk Response and Mitigation: 3.7 Control Design and Implementation	5
			Chapter 3: Risk Response and Mitigation: 3.8 Control Monitoring and Effectiveness	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 3: Risk Response and Mitigation: 3.13 Control Ownership	6
Cloud Technologies & Cloud Security Architectures	6-7	65	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: 1.5 The IT Risk Strategy of the Business	6
			Chapter 1: IT Risk Identification: 1.7 Methods of Risk Identification	6
			Chapter 2: IT Risk Assessment: 2.4 Changes in the Risk Environment	7
			Chapter 3: Risk Response and Mitigation: 3.12 Impact of Emerging Technologies on Design and Implementation of Controls	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6
Case Study IT-Projektmanagement	6-7			
Case Study Wahlprojektmodul	6-7			
Nationales, europäisches und internationales Strafprozessrecht	6-7			
IT-Revision / IT-Prüfung	6-7	40	Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	6
			Chapter 1: IT Risk Identification: 1.3 Elements of Risk	7
			Chapter 2: IT Risk Assessment: 2.3 Current State of Controls	6
			Chapter 3: Risk Response and Mitigation: 3.11 Systems Control Design and Implementation	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6
IT – GRC für mobile Systeme und Architekturen	6-7			
Grundlagen der digitalen Forensik	6-7			
Compliance aus zivil- und strafrechtlicher Sicht	6-7			
IT-Governance & IT-Compliance	6-7	40	Chapter 1: IT Risk Identification: 1.1 Risk Capacity, Risk Appetite and Risk Tolerance	6
			Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	6
			Chapter 1: IT Risk Identification: 1.5 The IT Risk Strategy of the Business	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6

Modul Studiengang	EQR-Niveau Median	Deckungs-faktor %	Prozess berufliches Bildungsprofil	EQR-Niveau Median
IT-Risikomanagement	**6-7**	**90**	**Chapter 1: IT Risk Identification: 1.1 Risk Capacity, Risk Appetite and Risk Tolerance**	**6**
			Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	**6**
			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: 1.5 The IT Risk Strategy of the Business	**6**
			Chapter 1: IT Risk Identification: 1.7 Methods of Risk Identification	**6**
			Chapter 1: IT Risk Identification: 1.8 IT Risk Scenarios	**7**
			Chapter 1: IT Risk Identification: 1.9 Ownership and Accountability	**6**
			Chapter 1: IT Risk Identification: 1.10 The IT Risk Register	**7**
			Chapter 1: IT Risk Identification: 1.11 Risk Awareness	**6**
			Chapter 2: IT Risk Assessment: 2.1 Risk Assessment Techniques	**7**
			Chapter 2: IT Risk Assessment: 2.4 Changes in the Risk Environment	**7**
			Chapter 2: IT Risk Assessment: 2.5 Project and Program Management	**5**
			Chapter 2: IT Risk Assessment: 2.6 Risk and Control Analysis	**6**
			Chapter 2: IT Risk Assessment: 2.7 Risk Analysis Methodologies	**6**
			Chapter 2: IT Risk Assessment: 2.8 Risk Ranking	**6**
			Chapter 2: IT Risk Assessment: 2.9 Documenting Risk Assessments	**6**
			Chapter 3: Risk Response and Mitigation: 3.1 Aligning Risk Response With Business Objectives	**7**
			Chapter 3: Risk Response and Mitigation: 3.2 Risk Response Options	**6**
			Chapter 3: Risk Response and Mitigation: 3.3 Analysis Techniques	**7**
			Chapter 3: Risk Response and Mitigation: 3.4 Vulnerabilities Associated With New Controls	**6**
			Chapter 3: Risk Response and Mitigation: 3.5 Developing a Risk Action Plan	**6**
			Chapter 3: Risk Response and Mitigation: 3.7 Control Design and Implementation	**5**
			Chapter 3: Risk Response and Mitigation: 3.8 Control Monitoring and Effectiveness	**6**
			Chapter 3: Risk Response and Mitigation: 3.9 Types of Risk	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 3: Risk Response and Mitigation: 3.12 Impact of Emerging Technologies on Design and Implementation of Controls	**6**
			Chapter 3: Risk Response and Mitigation: 3.13 Control Ownership	**6**
			Chapter 3: Risk Response and Mitigation: 3.14 Risk Management Procedures and Documentation	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.1 Key Risk Indicators	**7**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.2 Key Performance Indicators	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.4 Monitoring Controls	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.6 Results of Control Assessments	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.7 Changes to the IT Risk Profile	**6**
Knowledge Discovery	6-7			

Studiengang

Master IT GRC Management

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
Nationaler und internationaler Rechtsrahmen für Unternehmen	4			
Grundlagen IT Governance, Risk and Compliance Management	4	85	Chapter 1: IT Risk Identification: 1.1 Risk Capacity, Risk Appetite and Risk Tolerance	6
			Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	6
			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: 1.5 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 1: IT Risk Identification: 1.7 Methods of Risk Identification	6
			Chapter 1: IT Risk Identification: 1.8 IT Risk Scenarios	7
			Chapter 1: IT Risk Identification: 1.9 Ownership and Accountability	6
			Chapter 1: IT Risk Identification: 1.10 The IT Risk Register	7
			Chapter 1: IT Risk Identification: 1.11 Risk Awareness	6
			Chapter 2: IT Risk Assessment: 2.1 Risk Assessment Techniques	7
			Chapter 2: IT Risk Assessment: 2.2 Analyzing Risk Scenarios	5
			Chapter 2: IT Risk Assessment: 2.3 Current State of Controls	6
			Chapter 2: IT Risk Assessment: 2.4 Changes in the Risk Environment	7
			Chapter 2: IT Risk Assessment: 2.5 Project and Program Management	5
			Chapter 2: IT Risk Assessment: 2.6 Risk and Control Analysis	6
			Chapter 2: IT Risk Assessment: 2.7 Risk Analysis Methodologies	6
			Chapter 2: IT Risk Assessment: 2.8 Risk Ranking	6
			Chapter 2: IT Risk Assessment: 2.9 Documenting Risk Assessments	6
			Chapter 3: Risk Response and Mitigation: 3.1 Aligning Risk Response With Business Objectives	7
			Chapter 3: Risk Response and Mitigation: 3.2 Risk Response Options	6
			Chapter 3: Risk Response and Mitigation: 3.3 Analysis Techniques	7
			Chapter 3: Risk Response and Mitigation: 3.4 Vulnerabilities Associated With New Controls	6
			Chapter 3: Risk Response and Mitigation: 3.5 Developing a Risk Action Plan	6
			Chapter 3: Risk Response and Mitigation: 3.6 Business Process Review Tools and Techniques	5
			Chapter 3: Risk Response and Mitigation: 3.7 Control Design and Implementation	5
			Chapter 3: Risk Response and Mitigation: 3.8 Control Monitoring and Effectiveness	6
			Chapter 3: Risk Response and Mitigation: 3.9 Types of Risk	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 3: Risk Response and Mitigation: 3.11 Systems Control Design and Implementation	6
			Chapter 3: Risk Response and Mitigation: 3.12 Impact of Emerging Technologies on Design and Implementation of Controls	6
			Chapter 3: Risk Response and Mitigation: 3.13 Control Ownership	6
			Chapter 3: Risk Response and Mitigation: 3.14 Risk Management Procedures and Documentation	6

Modul Studiengang	EQR-Niveau Median	Deckungs-faktor %	Prozess berufliches Bildungsprofil	EQR-Niveau Median
			Chapter 4: Risk and Control Monitoring and Reporting: 4.1 Key Risk Indicators	7
			Chapter 4: Risk and Control Monitoring and Reporting: 4.2 Key Performance Indicators	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.3 Data Collection and Extraction Tools and Techniques	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.4 Monitoring Controls	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.6 Results of Control Assessments	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.7 Changes to the IT Risk Profile	6
Datenmanagement und Datenorganisation	4	20	Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	6
			Chapter 1: IT Risk Identification: 1.9 Ownership and Accountability	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
IT-Grundlagen	4			
Wirtschafts- und Internetkriminalität	4			
Informations- und IT-Management	4			
IT-GRC Standards und Frameworks	4	60	Chapter 1: IT Risk Identification: 1.5 The IT Risk Strategy of the Business	6
			Chapter 1: IT Risk Identification: 1.7 Methods of Risk Identification	6
IT-Sicherheit und Kryptografie	4	85	Chapter 1: IT Risk Identification: 1.3 Elements of Risk	7
			Chapter 1: IT Risk Identification: 1.4 Information Security Risk Concepts and Principles	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 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
Rechtsstreitigkeiten und eDiscovery	4			
Anforderungsmanagement IT-GRC	5	65	Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 3: Risk Response and Mitigation: 3.11 Systems Control Design and Implementation	6
Geschäftsprozess-Management im GRC-Kontext	5	50	Chapter 1: IT Risk Identification: 1.3 Elements of Risk	7
			Chapter 3: Risk Response and Mitigation: 3.6 Business Process Review Tools and Techniques	5
			Chapter 3: Risk Response and Mitigation: 3.7 Control Design and Implementation	5
			Chapter 3: Risk Response and Mitigation: 3.8 Control Monitoring and Effectiveness	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 3: Risk Response and Mitigation: 3.13 Control Ownership	6
Cloud Technologies & Cloud Security Architectures	5	65	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: 1.5 The IT Risk Strategy of the Business	6
			Chapter 1: IT Risk Identification: 1.7 Methods of Risk Identification	6
			Chapter 2: IT Risk Assessment: 2.4 Changes in the Risk Environment	7
			Chapter 3: Risk Response and Mitigation: 3.12 Impact of Emerging Technologies on Design and Implementation of Controls	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6
Case Study IT-Projektmanagement	5			
Case Study Wahlprojektmodul	5			
Nationales, europäisches und internationales Strafprozessrecht	4			
IT-Revision / IT-Prüfung	5	40	Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	6
			Chapter 1: IT Risk Identification: 1.3 Elements of Risk	7
			Chapter 2: IT Risk Assessment: 2.3 Current State of Controls	6
			Chapter 3: Risk Response and Mitigation: 3.11 Systems Control Design and Implementation	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6
IT – GRC für mobile Systeme und Architekturen	4			
Grundlagen der digitalen Forensik	5			
Compliance aus zivil- und strafrechtlicher Sicht	4			
IT-Governance & IT-Compliance	5	40	Chapter 1: IT Risk Identification: 1.1 Risk Capacity, Risk Appetite and Risk Tolerance	6
			Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	6
			Chapter 1: IT Risk Identification: 1.5 The IT Risk Strategy of the Business	6
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	6
			Chapter 4: Risk and Control Monitoring and Reporting: 4.5 Control Assessment Types	6

Modul Studiengang	EQR-Niveau Median	Deckungs-faktor %	Prozess berufliches Bildungsprofil	EQR-Niveau Median
IT-Risikomanagement	**5**	**90**	**Chapter 1: IT Risk Identification: 1.1 Risk Capacity, Risk Appetite and Risk Tolerance**	**6**
			Chapter 1: IT Risk Identification: 1.2 Risk Culture and Communication	**6**
			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: 1.5 The IT Risk Strategy of the Business	**6**
			Chapter 1: IT Risk Identification: 1.7 Methods of Risk Identification	**6**
			Chapter 1: IT Risk Identification: 1.8 IT Risk Scenarios	**7**
			Chapter 1: IT Risk Identification: 1.9 Ownership and Accountability	**6**
			Chapter 1: IT Risk Identification: 1.10 The IT Risk Register	**7**
			Chapter 1: IT Risk Identification: 1.11 Risk Awareness	**6**
			Chapter 2: IT Risk Assessment: 2.1 Risk Assessment Techniques	**7**
			Chapter 2: IT Risk Assessment: 2.4 Changes in the Risk Environment	**7**
			Chapter 2: IT Risk Assessment: 2.5 Project and Program Management	**5**
			Chapter 2: IT Risk Assessment: 2.6 Risk and Control Analysis	**6**
			Chapter 2: IT Risk Assessment: 2.7 Risk Analysis Methodologies	**6**
			Chapter 2: IT Risk Assessment: 2.8 Risk Ranking	**6**
			Chapter 2: IT Risk Assessment: 2.9 Documenting Risk Assessments	**6**
			Chapter 3: Risk Response and Mitigation: 3.1 Aligning Risk Response With Business Objectives	**7**
			Chapter 3: Risk Response and Mitigation: 3.2 Risk Response Options	**6**
			Chapter 3: Risk Response and Mitigation: 3.3 Analysis Techniques	**7**
			Chapter 3: Risk Response and Mitigation: 3.4 Vulnerabilities Associated With New Controls	**6**
			Chapter 3: Risk Response and Mitigation: 3.5 Developing a Risk Action Plan	**6**
			Chapter 3: Risk Response and Mitigation: 3.7 Control Design and Implementation	**5**
			Chapter 3: Risk Response and Mitigation: 3.8 Control Monitoring and Effectiveness	**6**
			Chapter 3: Risk Response and Mitigation: 3.9 Types of Risk	**6**
			Chapter 3: Risk Response and Mitigation: 3.10 Control Activities, Objectives, Practices and Metrics	**6**
			Chapter 3: Risk Response and Mitigation: 3.12 Impact of Emerging Technologies on Design and Implementation of Controls	**6**
			Chapter 3: Risk Response and Mitigation: 3.13 Control Ownership	**6**
			Chapter 3: Risk Response and Mitigation: 3.14 Risk Management Procedures and Documentation	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.1 Key Risk Indicators	**7**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.2 Key Performance Indicators	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.4 Monitoring Controls	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.6 Results of Control Assessments	**6**
			Chapter 4: Risk and Control Monitoring and Reporting: 4.7 Changes to the IT Risk Profile	**6**
Knowledge Discovery	5			