

Security & Safety Engineering Bachelor

Ausgewählte Projekte aus dem Bereich Informationssicherheit					
Kennnummer	Workload	Credits	Studien-semester	Häufigkeit des Angebots	Dauer
WPV 28926	90 h	3	Bel.	Jedes Semester	1 Semester
WPV 18926					
1	Lehrveranstaltungen	Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	Ausgew. Proj. InfoSec	deutsch	2 SWS / 22,50 h	67,50 h	10 Studierende
2	Lernergebnisse (learning outcomes) / Kompetenzen Nach erfolgreiche Teilnahme an der Lehrveranstaltung können die Studierenden: Anwendung (3): <ul style="list-style-type: none"> ... in einer Ausarbeitung zu einem zum Semesterbeginn abgesprochenen Projekts die gewählte Lösung darstellen. ... das Abschlussergebnis der Bearbeitung eines zu Semesterbeginn abgesprochenen Projekts einem Fachpublikum präsentieren. Analyse (4): <ul style="list-style-type: none"> ... ein zu Semesterbeginn abgesprochenes Projekts in einer vorgegebenen Zeitspanne lösen. 				
3	Inhalte Das Projektthema wird im Vorfeld der Belegung zwischen dem/der Studierenden und dem Dozenten vereinbart.				
4	Lehrformen Seminar				
5	Teilnahmevoraussetzungen Inhaltlich: Informationssicherheit (SSB4) oder vergleichbare Kenntnisse				
6	Prüfungsformen 1 H (Hausarbeit) 50%, 1 PN (Präsentation) 50%				
7	Verwendung des Moduls Wahlpflichtmodul für SSB, SSM und bei Bedarf andere Studiengänge.				

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.2	kod		01.10.2013

Security & Safety Engineering Bachelor

8	Modulbeauftragte/r und hauptamtlich Lehrende Prof. Dr. Dirk Koschützki
9	Literatur Abhängig vom gewählten Thema.

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.2	kod		01.10.2013

Risikoingenieurwesen Master

Wahlpflichtvorlesung						
Kennnummer	Workload	Credits	Studien-semester	Häufigkeit des Angebots	Dauer	
RIW 18001	90 h	3	1.-2. Sem.	Jedes Semester	1 Semester	
1	Lehrveranstaltungen Interkulturelle Kompetenz für Ingenieure im Auslandseinsatz		Sprache deutsch	Kontakt-zeit 2 SWS / 22,5 h	Selbst-studium 67,5 h	geplante Gruppengröße 12 Studierende
2	<p>Lernergebnisse (learning outcomes) / Kompetenzen</p> <p>Deutschland ist nicht nur export-orientiert, sondern viele Firmen haben auch Niederlassungen in der ganzen Welt. Deshalb müssen / dürfen auch alle Studierende damit rechnen, dass sie in anderen Ländern berufliche Aufgaben zu erledigen haben.</p> <p>Die Studierenden erwerben in dieser Vorlesung die Kompetenz, sich auch im Umfeld anderer Kulturkreise sicher zu bewegen. Hierzu gehört</p> <ul style="list-style-type: none"> - andere Länder, deren Menschen, Kulturen und Gebräuche zu verstehen, - die Kenntnis, welchen ungewohnten Probleme man begegnen kann, - sich zurechtzufinden, wie man Problemstellungen erfolgreich meistert, - die Bereitschaft, durch eigenes Verhalten kritische Situationen zu vermeiden, - für die eigene Sicherheit bestmöglichst zu sorgen, - die Fähigkeit, auf Berufs- und Arbeitsebene mit den Counterparts zu kooperieren und auf diese Weise auch den maximalen Erkenntnisgewinn und Nutzen aus dem Auslandseinsatz zu ziehen. <p>Nach erfolgreicher Teilnahme an der Vorlesung können die Studierenden folgendes:</p> <p>Wissen (1):</p> <ul style="list-style-type: none"> • Sie besitzen ein Grundwissen über ausgewählte Länder und Kulturen. <p>Verständnis (2):</p> <ul style="list-style-type: none"> • Sie erkennen die wesentlichen Unterschiede zwischen dem eigenen und einem anderen Kulturkreis. <p>Anwendung (3):</p> <ul style="list-style-type: none"> • Sie können ihr Wissen inhaltlich und methodisch bei beruflichen Aufenthalten in fremden Regionen / Ländern / Kulturkreisen anzuwenden. <p>Analyse (4):</p>					

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Helmut Körber	khe/31.10.2018	WS 2018/19

Risikoingenieurwesen Master

	<ul style="list-style-type: none"> • Sie sind in der Lage, sich eigenständig in andere Kulturkreise einzuarbeiten, • können eventuell zu erwartende Problemstellungen beurteilen und daraus • geeignete Verhaltensregeln zur Vermeidung ggf. kritischer Situation ableiten. <p>Synthese (5):</p> <ul style="list-style-type: none"> • Sie können ihr Wissen über fremde Kulturkreise eigenständig vertiefen und • die Erkenntnisse anderen vermitteln.
3	<p>Inhalte</p> <p>In der Vorlesung wird eine Auswahl aus nachfolgenden Themen behandelt:</p> <ul style="list-style-type: none"> • Management der eigenen Sicherheit. • Sprachen: Einführung in relevante Sprachfamilien und adäquater Umgang mit der Landessprache in der Zielregion, die man nicht / kaum beherrscht. • Klimatische Randbedingen und Gesundheitsvorsorge. • Andere Länder, andere Mentalitäten, Sitten, Gebräuche und Zeitverständnisse. • Verpflegung und Ernährung, wie man isst, Hygienestandards. • Gewohnte Zivilisationsstandards (sichere Energie- und Wasserversorgung, Abfall- und Müll-Management, Überlandfahrten) können nicht immer erwartet werden - Ursachen, Auswirkungen und Abhilfe. • Vor dem Kadi im fremden Land: Recht haben oder Recht bekommen. • Wesentliche kulturelle Unterschiede verschiedener Weltregionen und Länder. • Religionen: Einführung in die Fragestellung, ob oder inwieweit Religionen und Religionsgegensätze im Zielland den eigenen Aufenthalt und die zu erledigenden Arbeiten beeinflussen können. • Bildung und Bildungsunterschiede. • Historisches Grundwissen zur besuchten Region als Quelle zum besseren interkulturellen Verstehen und verstanden werden. • Beispiele für Kulturschock, seine Auswirkungen, und welche Erkenntnisse sich daraus ziehen lassen. • Verträge mit ausländischen Partnern: Schriftliche Verträge und mündliche Zusagen, Fragen zur Einhaltung / Nichteinhaltung von Verträgen. • Problem Korruption: Wo und wie tritt Korruption in Erscheinung? Wie ernst ist das Problem? Wie damit umgehen? • Ingenieure unter sich: Verständigung im Ausland auf Arbeitsebene, ingenieurtechnisches Wissen (z.B. technische Zeichnung, Berechnungsgleichung, Effizienz-

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Helmut Körber	khe/31.10.2018	WS 2018/19

Risikoingenieurwesen Master

	<p>kenngroße, RuI) als Lingua Franca selbst bei Sprachproblemen.</p> <ul style="list-style-type: none"> • Psychologie: Auswirkungen eines Auslandseinsatzes auf einen selbst - während des Aufenthalts im Zielland und nach Rückkehr. <p>Regionen und Länder, die in ausgewählten Fällen vertieft behandelt werden:</p> <ul style="list-style-type: none"> • Europa / EU: Mittel- und Westeuropa, Italien, Spanien, Russland • Nah- und Mittel-Ost: Jordanien, Ägypten, Arabische Emirate. • Südasien: Pakistan, Pashtunengebiet, Indien, Bangladesch. • Südost-Asien, Pazifik: Thailand, Malaysia, Singapur, Indonesien, Philippinen, Australien. • Afrika: Sudan, Rwanda, Swaziland, Südafrika. • Amerika: Argentinien, Paraguay, Kolumbien, Honduras, Dom. Republik, USA.
4	Lehrform Seminar und seminaristischer Unterricht
5	Teilnahmevoraussetzungen: keine
6	Prüfungsformen: Semesterbegleitende Studienleistung, Präsentation (sb PN) oder Klausur (sb K)
7	<p>Verwendung des Moduls</p> <ul style="list-style-type: none"> • Masterstudiengang Security & Safety Engineering • Modul ist auch in benachbarten Studiengängen verwendbar. Die Anrechenbarkeit richtet sich nach den Vorgaben der jeweiligen Prüfungsordnung
8	Modulbeauftragte/r und hauptamtlich Lehrender Prof. Dr. Helmut Körber
9	<p>Literatur</p> <ul style="list-style-type: none"> • Alexander von Humboldt, „Die Reise nach Südamerika“, Lamuv-Verlag, 2002, ISBN-13: 978-3-88977-241-1 • Kathleen Jamie, „The Golden Peak - Travels in North Pakistan“, Virago Press Ltd., London, 1992 (reissued as „Among Muslims“ in, 2002), existiert auch in deutscher Übersetzung als Taschenbuch „Im Licht der Gipfel - Grenzgänge in Kaschmir“, Rowohlt –Taschenbuch Verlag GmbH, Reinbeck bei Hamburg, 1994, 1290-ISBN 3 499 12654 bitte recherchieren). • Sonstige Unterlagen und Hinweise werden als EDV-Files zur Verfügung gestellt. • Ein Skript wird nicht ausgegeben.

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Helmut Körber	khe/31.10.2018	WS 2018/19

Risikoingenieurwesen Master

Wahlpflichtveranstaltung RIW Risikobeurteilung an ausgewählten Projekten					
Kennnummer	Workload	Credits	Studien-semester	Häufigkeit des Angebots	Dauer
RIW 28003	90 h	3	1./2. Sem.	Jedes Semester	1 Semester
1	Lehrveranstaltungen Projekte Risikobeurteilung	Sprache deutsch	Kontaktzeit 1 SWS / 1,25 h	Selbst- studium 78,75 h	geplante Gruppengröße 5
2	<p>Lernergebnisse (learning outcomes) / Kompetenzen</p> <p>Ziel des Moduls ist es, im Rahmen einer weitgehend selbständigen Bearbeitung eines Projektes spezielles Fachwissen aus dem Themenfeld Risikobeurteilung zu erarbeiten. Dabei werden auch Fertigkeiten im Projektmanagement in der Praxis eingesetzt. Die Studenten innen sollen ein Thema selbstständig bearbeiten können. Dazu ist die vorhandene Grundlageninformation zu sichten, zu strukturieren, zu hinterfragen und zu bewerten. Darauf aufbauend soll ein Plan zur Erreichung des gesetzten Zieles entwickelt werden. Nach dem erfolgreichen Abschluss des Projekts sollen die Studenten innen das gewählte Thema durchdrungen haben. In der Abschlussbesprechung wird eine Analyse des Projektes durchgeführt, an Hand der die Studenten innen ihre eigne Leistung und Defizite kritisch analysieren und weiteres Entwicklungspotential und –bedarf erkennen sollen</p> <p>Nach Abschluss der Veranstaltung können Studierende:</p> <p>Wissen / Kenntnisse (1): Die Studenten innen kennen einschlägigen Grundlagen des Themas.</p> <p>Verstehen (2): Die Studenten innen Verstehen die Zusammenhänge des bearbeiteten Fachgebiets.</p> <p>Anwenden (3): Die Studenten innen sind in der Lage, ihr Wissen inhaltlich und methodisch auf ein konkretes Problem anzuwenden.</p> <p>Analyse (4): Die Studenten innen sind in der Lage, Fachliteratur oder Laborergebnisse zu analysieren und zu prüfen.</p> <p>Synthese (5): Die Studenten innen können Ihre Ergebnisse begründen und auf andere Sachverhalte übertragen.</p>				

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	wbr		SoSe19

Risikoingenieurwesen Master

	Evaluation und Bewertung (6): Die Studenten innen können ihre eigene Leistung sowie die erreichten Ergebnisse bewerten.
3	Inhalte: Das Thema ist mit dem Dozenten im Vorfeld abzustimmen. Es ist grundsätzlich möglich, das Semesterprojekt weiterzuentwickeln oder Vorarbeiten zu einer Thesis zu leisten.
4	Lehrformen Seminar
5	Teilnahmevoraussetzungen Inhaltlich: Abschluss der Fächer, die für die Bearbeitung des Themas erforderlich sind. Die Feststellung erfolgt durch den Dozenten.
6	Prüfungsformen Prüfungsleistung: Studienbegleitung 1 Bericht oder 1 Laborarbeit je nach Vereinbarung. sbB oder sbL, 1 LP
7	Verwendung des Moduls Wahlpflichtfach RIW; für andere Studiengänge im Rahmen der SPO nach Freigabe durch den jeweiligen Studiendekan
8	Modulbeauftragte/r und hauptamtlich Lehrende Prof. Dr. Ulrich Weber
9	Literatur Literaturhinweise erfolgen durch den Dozenten.

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	wbr		SoSe19

Risikoingenieurwesen Master

Titel des Moduls: Wahlpflichtmodul					
Kennnummer	Workload	Credits	Studien- semester	Häufigkeit des Angebots	Dauer
RIW 28005	90 h	3	2. Sem.	Wintersemester	1 Semester
1	Lehrveranstaltungen Risikobewertung von 12.BImSchV- Industrieanlagen	Kontaktzeit 2 SWS / 22,5 h	Selbststudium 67,5 h	geplante Gruppengröße 12 Studierende	
2	<p>Lernergebnisse (learning outcomes) / Kompetenzen</p> <p>Die Studierenden erlernen, wie Risikoanalysen in der Praxis durchgeführt werden. Aufbauend auf den theoretischen Grundlagen der Bestimmung technischer Risiken werden Beispiele aus unterschiedlichen Ingenieur- und Wirtschaftsbereichen vorgestellt, in denen Risikobewertungen seit vielen Jahren durchgeführt werden und als Stand der Technik anzusehen sind.</p> <p>Ausgehend von realen Problemstellungen erarbeiten die Studierenden, wie eine quantitative Risikobestimmung durchzuführen ist. Sie lernen dabei, sowohl das Zusammenwirken und die Verknüpfung von Einzelereignissen und deren Behandlung bei der Risikoberechnung als auch die Problemstellungen bei der Beschaffung von Eintrittswahrscheinlichkeiten kennen. Weiterhin erarbeiten sie, auf welche Art und Weise das Schadensausmaß eines Ereignisses oder Störfalls festgelegt bzw. definiert werden kann.</p> <p>Bei Betriebsbereichen / Anlagen, die den erweiterten Pflichten der Störfall-Verordnung (12.BImSchV) unterliegen, ist eine Ermittlung und Bewertung von Risiken erforderlich. Da die Durchführung quantitativer Risikoanalysen äußerst aufwendig ist, erlernen die Studierenden auch, wie sich mittels eines systematischen Näherungsverfahrens das Risiko, das von einer technischen Anlage ausgeht, in vergleichsweise geringem Zeitaufwand, jedoch mit einer Genauigkeit, die den Anforderungen der 12.BImSchV entspricht, ermitteln lässt.</p> <p>Nach erfolgreicher Teilnahme an der Lehrveranstaltung können die Absolventen eine quantitative Risikoanalyse durchführen. Sie sind darüber hinaus in der Lage, auch Risiken systematisch und in guter Näherung zu ermitteln und so zu bestimmen, dass die Anforderungen der Störfall-Verordnung erfüllt und Bewertungen unter Risikogesichtspunkten möglich sind.</p>				

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.0	khe		WiSe20/21

Risikoingenieurwesen Master

3	<p>Inhalte</p> <p>Grundlagen für eine Risikoanalyse:</p> <ul style="list-style-type: none"> - Definition des technischen Risikos, - Problemstellungen bei der Bestimmung des Risikos, - Beispiele aus technischen und nicht-technischen Bereichen, in denen Risikoanalysen durchgeführt wurden und werden (Luft- und Raumfahrt, Kernenergie und Reaktortechnik, Versicherungswesen), - Rasmussen-Studie (USA), Deutsche Risikostudie Kernkraftwerke, probabilistische Risikoanalyse bei Genehmigungsverfahren für Kernkraftwerke in der Welt. <p>Risikobewertungen in der technischen Praxis:</p> <ul style="list-style-type: none"> - ATEX, Verhinderung von Explosionen, - Zuverlässigkeit der Mess-, Steuerungs- und Regelungstechnik technischer Anlagen, - Einstufungen nach VDE/VDI 2180 (sowie SIL). <p>Quantitative Risikoanalyse:</p> <ul style="list-style-type: none"> - Anlagenanalysen, Fehlerbaumanalyse, - Erfassung und Abschätzung des zu erwartenden Schadensausmaßes, - Fehlerhäufigkeiten und Eintrittswahrscheinlichkeiten für Ereignisse, die zu einem Störfall führen können, - Beschaffung von Eintrittswahrscheinlichkeiten, Genauigkeit der Werte, - Verknüpfung von Einzelwahrscheinlichkeiten, - Übungsbeispiel: Quantitative Bestimmung des Risikos einer Anlage, die den erweiterten Pflichten der Störfall-Verordnung unterliegt. <p>Rechtlicher Rahmen für Risikoanalysen und -bewertungen konventioneller Anlagen:</p> <ul style="list-style-type: none"> - Europäischer Rechtsrahmen / Seveso-Richtlinie, - allg. Ziele der EU bezüglich des von technischen Anlagen ausgehenden Risikos, - Umsetzung des europäischer Rechts in den Mitgliedsländern der EU, - Störfall-Verordnung (12.BImSchV) in Deutschland, - Praxis der Risikobewertung in anderen Ländern, z.B. Schweiz, Niederlande. <p>Der Risikobegriff in der Störfall-Verordnung:</p> <ul style="list-style-type: none"> - Deterministische und probabilistische Ansätze zur Untersuchung von nicht-bestimmungsgemäßen Ereignissen und potenziellen Störfällen, - 12.BImSchV: Betreiberpflichten, Fundgrube zur Risikoerfassung in den Anhängen der Störfall-Verordnung, - Grundpflichten und erweiterte Pflichten von Anlagenbetreibern in Deutschland,
----------	--

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.0	khe		WiSe20/21

Risikoingenieurwesen Master

	<p>- Anwendungsübung: Vorschriften in der 12.BImSchV, die sich mit der Bewertung des Risikos befassen.</p> <p>Praxisbewährtes Näherungsverfahren zur Bestimmung und Bewertung von Risiken:</p> <ul style="list-style-type: none"> - Denkbare Ereignisketten in Anlagen, die zu einem Störfall führen können, - Vorhandenen technischen Vorkehrungen und / oder organisatorische Maßnahmen, mit denen ein Störfall in der zu bewertenden Anlage verhindert und - sollte er dennoch eintreten - dessen Auswirkungen begrenzt werden sollen, - Schwachstellenanalyse und Feststellung der zu erwartenden Auswirkungen, - Einstufungen der „Schwere“ (12.BImSchV) der Auswirkungen eines Störfalls, Untersuchung und Definition, wie sich die Schwere eines Ereignisses festlegen lässt, - Einstufungen der zu erwartenden Eintrittswahrscheinlich eines Ereignisses, Hilfestellung bei der Beschaffung dieser Kenngröße, - Beispiele für Eintrittswahrscheinlichkeiten, - Abschätzung / Bestimmung des Risikos aus den vorgenannten Einzelkomponenten, - Übungsbeispiel: Näherungsweise Bestimmung des Risikos einer Anlage, die den erweiterten Pflichten der Störfall-Verordnung unterliegt (z.B. Ammoniaktanklager, Wasserstoff-Abfüllanlage o.ä.), - technische und wirtschaftliche Aspekte der Risikominimierung, - andere Näherungsverfahren zur Risikobestimmung, Risikomatrix.
4	<p>Lehrformen seminaristischer Unterricht</p>
5	<p>Teilnahmevoraussetzungen Inhaltlich: Grundstudium</p>
6	<p>Prüfungsformen Semesterbegleitende Klausur (sbK)</p>
7	<p>Verwendung des Moduls Studiengang Security & Safety Engineering Master Modul ist auch in benachbarten Studiengängen verwendbar. Die Anrechenbarkeit richtet sich nach den Vorgaben der jeweiligen Prüfungsordnung</p>
8	<p>Modulbeauftragte/r und hauptamtlich Lehrender Dr.-Ing. Helmut Körber</p>
9	<p>Literatur H. Körber: „Practicality of Risk Analyses of Establishments“, WIT Transactions on the</p>

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.0	khe		WiSe20/21

Risikoingenieurwesen Master

Built Environment, Volume 189, WIT Press, 2019, ISSN 1743-3509, p.131 -143.
zu finden unter

<https://www.witpress.com/elibrary/wit-transactions-on-the-built-environment/189>

Weitere Unterlagen, Hinweise und Arbeitshilfen werden als EDV-Files zur Verfügung gestellt. Ein Skript wird nicht ausgegeben.

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.0	khe		WiSe20/21

Wahlpflichtvorlesung					
Kennnummer	Workload	Credits	Studien-semester	Häufigkeit des Angebots	Dauer
FH 27141 17141	90 h	3	4-7	WS und SS	1 Semester
1	Lehrveranstaltungen Experimentalvorlesung Kernreaktor I	Sprache Deutsch	Kontaktzeit 2 SWS / 20 h	Selbst- studium 70 h	geplante Gruppengröße 12
2	Lernergebnisse (learning outcomes) / Kompetenzen Grundkenntnisse in der Reaktorsicherheit, Reaktorphysik, Anfahrprozedur.				
3	Inhalte Theorie: <ul style="list-style-type: none"> • Reaktorsicherheitskonzepte • Kernspaltung • Moderation • Kritikalität I • Reaktivität Praxis: <ul style="list-style-type: none"> • Funktionsprüfungen am Reaktor SUR-100 • Anfahrübungen • Fahrübungen • Kritische Regelstabstellung • Regelplattenkalibrierung I 				
4	Lehrformen Vorlesung und praktische Übungen				
5	Teilnahmevoraussetzungen Physik 1 oder Naturwissenschaftliche Grundlagen 1				
6	Prüfungsformen Hausarbeit				
7	Verwendung des Moduls Wahlpflichtvorlesung				
8	Modulbeauftragte/r und hauptamtlich Lehrende Prof. Dr. Sabine Prys				

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Prys		WiSe17/18

9	<p>Literatur</p> <p>[1] Volkmer, M: Radioaktivität und Strahlenschutz; Informationskreis Kernenergie, 2012</p> <p>[2] Volkmer, M: Basiswissen Kernenergie; Informationskreis Kernenergie, 2013</p> <p>[3] Koelzer, W: Lexikon zur Kernenergie; Informationskreis Kernenergie, 2013</p> <p>[4] Prys, S.: Skripte</p>
----------	--

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Prys		WiSe17/18

Wahlpflichtvorlesung - Bachelor						
Kennnummer	Workload	Credits	Studien-semester	Häufigkeit des Angebots	Dauer	
FH 26161	90 h	3	3-7	gemäß Aushang	1 Semester	
1	Lehrveranstaltungen		Sprache	Kontaktzeit	Selbst-studium	geplante Gruppengröße
	IT-Governance / IT-Compliance		Deutsch	2 SWS / 22,50 h	67,50 h	15
2	Lernergebnisse (learning outcomes) / Kompetenzen					
	<p>Am ersten Tag der Vorlesung werden die Studierenden im Bereich der IT-Governance eingeführt und bekommen einen Überblick zur Thematik der gesetzlichen Grundlagen der IT-Compliance. Anschließend werden die Studierenden in die nationale und internationale ISO 27000 Standardisierung und Gremienarbeit eingeführt. Die effektive und effiziente Anwendung der Normen gibt tiefe Einblicke in die Aufgaben der IT-Revision und IS-Audits. Der Fachteil Datenschutz gibt Aufschluss über das Bundes/Landes-datenschutzgesetz und die Aufgabe eines Datenschutzbeauftragten. Im letzten Teil des ersten Tages der Vorlesung lernen die Studierenden noch einmal die Grundzüge der IT-Sicherheit, jedoch mit dem Fokus auf die technischen und organisatorischen Schutzmaßnahmen. <i>Zur Umsetzung der gelernten Inhalte erstellen die Studierenden in Gruppenarbeit (Case Study) eine Präsentation die 50% zur Note beiträgt. Der Dozent wird in der Vorlesungszeit anwesend sein und Fragen sowie Tipps für die Umsetzung geben.</i></p> <p>Am zweiten Tag liegt der Fokus auf der Entstehung und in die Einführung der ISO 27000 Reihe, sowie den wesentlichen Grundzügen von Management Systemen. Den Studierenden werden die ISO 27001:2015 Anforderungen der Kapitel und der Annex A Controls vermittelt. <i>Im Anschluss wird durch die Studierenden die erarbeitete Case Study vor ihren Kommilitonen präsentiert und Fragen dazu beantwortet.</i></p> <p>Ferner wird auf weitere IT-Governance Standards COBIT 5 und BSI IT Grundschutz eingegangen. Der dritte Teil des Vortrags geht auf Cyber- Kriminalität ein und zeigt anhand von Beispielen, was für Auswirkungen Industriespionage und Cyber War hat. Für die IT-Awareness wird den Studierenden eine Awareness-Kampagne aus der Praxis vorgeführt. <i>Im Anschluss an die Vorlesung werden die Rahmenbedingungen für die Hausarbeit festgelegt und die Themen der Hausarbeiten vergeben (Abgabetermin Tag 3 wird dann festgelegt). Mit den Hausarbeiten werden Aufgaben erarbeitet, wie sie in der beruflichen Realität auftreten können.</i></p>					

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Teuscher		SoSe14

	<p>Am dritten Tag wird die schriftliche Hausarbeit in gedruckter/gebundener Form (geheftet maximal 10-15 Seiten) und in elektronischer (Word oder Excel) dem Dozent übergeben, Sie trägt 30% zur Note bei.</p> <p>Ferner werden die Ergebnisse der Hausarbeiten den Kommilitonen in Präsentationen (20% der Note) vorgetragen und im Anschluss diskutiert.</p>
3	<p>Inhalte</p> <ul style="list-style-type: none"> • Einführung zur IT-Governance • Übersicht zur IT-Compliance • Die DS-GVO , Einblicke in die Tätigkeiten eines Datenschutzbeauftragten (inkl. Praxisbeispiele) • Aufgaben und Tätigkeit des Information-Security-Officer • Die ISO27000 Normenreihe, ISO 27001 Norm und das ISMS inkl. KRITIS Anforderungen • Erstellung eines Auditprogramms (inkl. Praxisbeispiele) • BSI IT-Grundschutz Vorgehen auf der Basis von ISO27001 • Einführung in COBIT 5 • Cyber Security Risk inkl. des Cyber Thrillers "World Wide War" • Anforderungen an eine Security Awareness Kampagne
4	<p>Lehrformen Seminar</p>
5	<p>Teilnahmevoraussetzungen Verständnis zur IT-Sicherheit, Informationssicherheit, Datenschutz</p>
6	<p>Prüfungsformen -Tag 1 Workshop, Gruppenarbeit zählt 50% der Note: In einer Präsentation stellt die Gruppe Ihre Lösungen zu den 7 Chase Study Fragen vor. -Tag 3: Gruppenarbeit die zu 20% aus einer Präsentation der Hausarbeit und zu 30% aus der Hausarbeit (maximal 15 Seiten) besteht.</p>
7	<p>Verwendung des Moduls Wahlpflichtvorlesung</p>
8	<p>Modulbeauftragte/r und hauptamtlich Lehrende Andreas Teuscher Leiter der Fachgruppe Cybersecurity des ISACA Germany Chapter e.V. (CISA, CGEIT, CRISC), ISO27001 LA, BSI ISO27001 LA auf Basis GS, IT-SiKat §11, §8a BSIG, Smart Meter Gateway Admin, ISO 9001 LA, Chief Industrial Security Officer bei der SICK AG.</p>
9	<p>Literatur Frei verfügbare Unterlagen für die Durchführung der Gruppen und Hausarbeit:</p>

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Teuscher		SoSe14

- [1] Bundesdatenschutz Gesetz (http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf)
- [2] Landesdatenschutz Gesetz BaWü (<http://www.baden-wuerttemberg.datenschutz.de/>)
- [3] Bitkom Leitfaden und Nachschlagewerk: Kompass der IT-Sicherheitsstandards (http://www.bitkom.org/de/publikationen/38337_31037.aspx)
- [4] Leitfaden für den Cyber Security Check (www.isaca.de)

Vom Dozenten für die Vorlesung zur Verfügung gestellte Unterlagen:

- [5] COBIT 5 (<http://www.isaca.org/COBIT/Pages/COBIT-5-german.aspx>)
- [6] Standard ISO/IEC 27000:2011, Informationstechnologie-Sicherheitsverfahren-Management-systeme für die Informationssicherheit-Überblick und Terminologie.
- [7] Standard ISO/IEC 27001: 2013, Information technology - Security techniques - Information security management systems - Requirements.
- [8] Standard ISO/IEC 27002: 2013, Information technology - Security techniques - Code of practice for information security controls

Version	Erstellt von	Freigabe (Datum/Kürzel)	Gültig ab
1.1	Teuscher		SoSe14