Modulbeschrieb

IT Governance, Risk and Compliance

Modulcode	M6
Leitidee	GRC steht für Governance, Risiko und Compliance Management. GRC ist eine Kombination aufeinander bezugnehmende Konzepte, wobei jeder Begriff eine individuelle Bedeutung und Ausrichtung hat. Im Modul IT GRC wird differenziert zwischen IT-Governance, IT-Risiken und IT-Compliance, deren innerbetriebliche Bedeutung, sowie die zu berücksichtigenden externen Anforderungen. Auch damit verknüpften Themen wie IT-Audit und -Assurance werden diskutiert; je nach Kontext flankiert von relevanten internationalen Standards und Referenzmodellen (z.B. COSO, ISO/IEC 38500, 20000, COBIT 5, ITIL, etc.). Perspektivisch werden vorwiegend multinational agierende bzw. streng regulierte Unternehmen und Branchen betrachtet; GRC-bezogene Anforderungen und Lösungen sind besonders für Unternehmen/Branchen von Bedeutung, die im globalen bzw. internationalen Umfeld agieren oder eben strengen regulatorischen Anforderungen unterliegen, wie zum Beispiel Banken und Versicherungen.
Art der Ausbildung	Wirtschaftsinformatik
Studiengang	Master of Science
Modultyp	C (Kernmodul)
ECTS Dotation	6 Credits
Für Modul verantwortlich	Prof. Dr. Petra Maria Asprion, BFH Bern
Eingangskompetenzen	Die Studierenden bringen Kenntnisse aus den folgenden Modulen mit: • M1: IT-Management • M2: Trends in der Informatik • M3a: Strategisches Prozessmanagement • M4: Projekt- und Changemanagement • M3b: Operatives Prozessmanagement • M5: Wissens- und Informationsmanagement Die Studierenden verfügen über ausreichend Kenntnisse der englischen Sprache, so dass sie sowohl mühelos mit englischer Fachliteratur umgehen wie auch englischsprachigem Unterricht folgen können.
Anschlussmodule	-

Bemerkungen	Zur Zulassung der Abschlussprüfung müssen die Studierenden eine Gruppenarbeit durchführen und diese im Plenum präsentieren.

Ausgangskompetenzen / Grobziele

Die Studierenden sind ausgebildet, um im Umfeld von IT-Governance, Risiko-, und Compliance-Anforderungen von mittleren bis grossen (multinationalen) Unternehmen zu arbeiten. Sie kennen wesentliche regulierende Anforderungen, wie sie vor allem global agierende Unternehmen bewältigen müssen; sie sind in der Lage, global valide Regulierungen (z.B. SOX, GxP) zu interpretieren und die daraus resultierenden Massnahmen (für ein englischsprachiges Umfeld) zu designen. Hierfür können sie etablierte, global anerkannte Werkzeuge wie z.B. COSO; COBIT, ITIL, ISO/IEC 20000, 38500 anwenden.

Sie wissen um die Bedeutung der Unternehmenskultur und des „Tone at the Top“ als „critical driver“ in Bezug auf eine erfolgreiche und compliante Unternehmensführung.

Insbesondere sind sie auch mit ethischen Überlegungen in Kontext der Informatik/Wirtschaftsinformatik vertraut und können diese Kenntnisse als Vertreter ihres Berufsfeldes im Unternehmensalltag berücksichtigen bzw. einbringen.

Ziele

Fachkompetenz

Die Studierenden

- verstehen Ansätze einer wert- und ethikorientierten IT-Führung im globalen/internationalen Unternehmensumfeld.
- verstehen relevante IT-GRC-orientierte Konzepte und Modelle, wie sie heute insbesondere in global agierenden Unternehmen zum Einsatz kommen.
- kennen und verstehen mindestens ein GRC-relevantes Rahmenwerk im Detail und können dieses konzeptionell anwenden.
- können Anforderungen in Zusammenhang mit IT-Compliance, -Governance und Risiko Management analysieren und Handlungsempfehlungen resp. Lösungen entwickeln.
- können Anforderungen und Massnahmen in Zusammenhang mit IT-Audit/Assurance-Aktivitäten evaluieren, konzipieren und umsetzen – und dies mit dem Fokus auf global/international agierende Unternehmen und Branchen.

Methodenkompetenz

Die Studierenden

- sind in der Lage mit Hilfe von Referenzmodellen systematisch Fragestellungen und Aufgaben aus dem Themenbereich GRC zu beantworten resp. Lösungsvorschläge, insbesondere für globale bzw. international agierende Unternehmen, zu entwickeln.
- können Methoden zum Managen von IT-Risiken für einen vorgegebenen Unternehmens-/Organisationskontext auswählen, verknüpfen und anwenden.

Sozial-/Selbstkompetenz

Die Studierenden

- sind in der Lage, zu ethisch relevanten Themen der Wirtschaftsinformatik (z.B. Verantwortlichkeiten von Entscheidungsträgern, Asymmetrien in Informationssystemen, Datenspeicherung und Datenschutz) selbständig einen Standpunkt zu beziehen und daraus ableitbare Konsequenzen zu realisieren.
- können analysieren, welche personenbezogenen Einflussfaktoren im Kontext von (IT-)GRC in Unternehmen/-Organisationen sowie über die Unternehmens-/Organisationsgrenzen hinaus bestehen.
- verstehen es, in Gruppen und mit ihren je unterschiedlichen Herkunftsperspektiven, an Fallstudien/-Praxiskontexten GRC-Aspekte zielorientiert und methodenbasiert zu diskutieren.
- Vermögen es, sich im Berufsfeld IT-Audit / IT-GRC zu bewegen und verstehen es, aus unterschiedlichen Perspektiven eigenständig zu argumentieren.

Lerninhalte
Einführung in GRC

- GRC – auch eine Frage der Ethik im Kontext der Wirtschaftsinformatik
- GRC – Bedeutung für Unternehmen und Organisationen die global/international agieren
- GRC – relevante internationale Rahmenwerke – eine Übersicht

Themengebiet 1: IT-Compliance

- Fallstudien – Non-compliance in Unternehmen/Organisationen
- IT-Compliance – Anforderungen im die internationalen Umfeld und daraus resultierende Konsequenzen
- Interne Kontrollsysteme – Ausgestaltung, sowie Fallbeispiel (Orientierung an Anforderungen des US-amerikanischen Sarbanes-Oxley Act)
- IT-Audit und -Assurance – Akteure, Programme und Konsequenzen

Themengebiet 2: IT-Governance

- IT-Governance –wichtiges Führungsinstrument
- (Strategic) Business/IT-Alignment – die (COBIT) Zielkaskade
- COBIT 5 – Einführung und ausgewählte Prozesse
- Flankierend: Fallstudien (“Theory transformed in Practice”) basierend auf COBIT5

Themengebiet 3: IT-Risiko Management

- IT-Risiko Management – Prinzipien – Modelle – Prozesse
- Exkurs: Information Security Management Systems (ISMS)

Lehr- und Lernformen

Kontaktstudium	Dialogorientierter Unterricht mit integrierten Übungen/Fallstudien Ggf. Vorträge zu ausgewählten Themen durch externe Referenten (die mehrheitlich in internationalen Kontexten tätig sind)
Selbststudium	Einzel- und Gruppenarbeiten Übungen zur Vertiefung und Anwendung der erlernten Theorie Selbstständiges Erarbeiten von ausgewählten Themen mit Hilfe von ausgewählten Artikeln

Studienzeit pro Semester	ECTS-Credits	Kontaktstudium (Lektionen)	Kontaktstudium (Stunden)	Begleitetes Selbststudium (Lektionen)	Begleitetes Selbststudium (Stunden)	Autonomes Selbststudium (Stunden)	**Total (Stunden)**
Aufwand	6	56	42.0	95	71.0	67.0	**180**
Anteil			23.3%		39.4%	37.2%	**100%**

Unterrichtssprache Deutsch und Englisch

Leistungsnachweis/e Zur Zulassung zur Abschlussprüfung muss eine Gruppenarbeit bearbeitet werden.

Anzahl	Art des Leistungsnachweises	Gewichtung	Dauer	Hilfsmittel
1	Gruppenarbeit als Voraussetzung zur Zulassung der Modulschlussprüfung	40%		
2	Modulschlussprüfung	60%	90 Min.	Closed Book

Präsenzpflicht

Für Referate mit externen Referenten sowie für notenrelevante Präsentationen besteht Präsenzpflicht. Die entsprechenden Daten werden zu Semesterbeginn schriftlich bekannt gegeben. Absenz von präsenzpflichtigen Lektionen aus unwichtigen Gründen hat die Nichtzulassung zur Modulschlussprüfung zur Folge.

Bibliographie

Relevante Literatur:
Hinweis: U.s. Liste ist eine Auswahl und wird ggf. zu Semesterbeginn aktualisiert; es gilt die in der Vorlesung abgegebene oder auf der Lernplattform bereitgestellte (relevante und ergänzende) Literatur!

Die (relevante) Literatur ist vorwiegend in englischer Sprache und wird auf Moodle bereitgestellt.

- Asprion, P.M.; Knolmayer, G. (2012): Assimilation of Compliance Software in Highly Regulated Industries: An Empirical Multitheoretical Investigation. HICCS 2013.

- Babb, S. (2013): Using COBIT 5 for Risk Management. ISACA COBIT Focus, Volume 4, October 2013.
- Boultwood, B. (2013): GRC Value Proposition. Global Association of risk Professionals (GARP).
- Bruinsma, C. (2009): Tone at the Top Is Vital! A Delphi Study. ISACA JOURNAL VOLUME 3, 2009.
- Bulgurcu, B., Cavusoglu, H. und Benbasat, I. 2010. "INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS", MIS Quarterly (34:3), S. 523-A527.
- IIA (2013): The three lines of defence in effective risk management and control The Institute of Internal Auditors. Position paper.
- Knolmayer, G. and Asprion, P.M., (2011): Assuring Compliance in IT Outsourcing Relationships: Frameworks and Selected Applications, in: The Fifth Global Sourcing Workshop, Courchevel, France.
- Miyagi, I; Monden, H.; Kimura, R.; Aramaki, M.; Hara, K.; Ishijima, T. (2014): Align Business Initiatives and IT Solutions. Collaboration Is Critical for Effective IT Governance. ISACA JOURNAL Vol 4, 2014.
- N.N. (2010) What GRC Could Mean to Your Organization. Tone at the top. Institute of Internal Auditors.
- Pozza, G. (2014): Social Approach to IT Governance. Incorporating Boundary Objects. ISACA JOURNAL Vol 4, 2014.
- Pozza, G. (2014): Communicating IT Governance - Does It Matter? ISACA JOURNAL Vol 2, 2014.
- Rittenberg, L.; Martens, F. (2012): Enterprise Risk Management. Understanding and Communicating Risk Appetite. COSO - Committee of Sponsoring Organizations of the Treadway Commission.
- Short, J.; Gerrard, M. (2010): IT Governance Must Be Driven by Corporate Governance. Gartner Research. ID Number: G00172463.
- Vaidya, A. (2013): Doing Business in India Requires Digital Compliance. ISACA JOURNAL Vol 6, 2013.
- Weill, P.; Ross, L. (2004): IT Governance at One Page. CISR WP No. 349 and Sloan WP No. 4516-05. MIT Sloan Management.

Ergänzende Literatur:

- Bashiri, I. et al. (2010): Informatik im Fokus - Strategic Alignment, Springer, Berlin et al.
- Holtschke, B. et al. (2009): Quo vadis CIO?, Springer, Berlin et al.
- ISACA (2012): COBIT 5 – A Business Framework for the Governance and Management of Enterprise IT. www.isaca.org/cobit.
- ISACA (2012): COBIT 5 – Enabling Processes. www.isaca.org/cobit.
- Johannsen, W.; Goeken, M. (2011): Referenzmodelle für IT-Governance – Methodische Unterstützung der Unternehmen-IT mit COBIT, ITIL & Co. dpunkt-Verlag, Heidelberg.
- Pfaff, D.; Ruud, F. (2013): Schweitzer Leitfaden zum InternenKontrollsystem (IKS), orell füssli, Zürich.
- Rüter, A.; Schröder, J.; Göldner, A. (Hrsg.) (2010): IT-Governance in der Praxis – Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen. Springer, Berlin et al.

- Weill, P.; Ross, J.W. (2004): How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, Boston/Massachussetts.

Sowie fallweise im Unterricht abgegebene oder auf der Lernplattform bereitgestellte Literatur.