Amrita School of Business

Amrita Vishwa Vidyapeetham

Coimbatore

Term V (03 Oct 2018 – 23 Dec 2018)

Course Title:	Cybersecurity Governance, Risk and Compliance
Course Code:	CGRC
Credits:	**3**
Total Sessions:	24
Course Instructor:	Prof. Pradeep Menon.
Contact Information:	pradeep.pkd@gmail.com
Course Link:	
Office:	
Office hours:	Monday, Wednesday & Friday 2:00 – 4:00 pm
Course contributes mostly to:	**Employability/ Entrepreneurship**/ Skill Development/ Value-add

Course Description

The proliferation of Information Technology tools in organizations has not only created new opportunities, but also poses new challenges for organizations. A major challenge that affects organizational value to the extent of survival is Cybersecurity. As organizations continue to embrace new technologies, devices and ways of working, it is also exposing itself to cyber adversaries more than in the past. Cybersecurity as a field is of growing importance due to the increasing reliance on computer systems and the Internet, wireless networks such as Bluetooth and Wi-Fi, the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things. Governance, Risk Management, and Compliance (GRC) are three related facets that help assure an organization reliably achieves objectives, addresses uncertainty and acts with integrity.

Cybersecurity GRC enable managers to leverage the use of new technology and provide innovative offerings securely and continually to their customers. By following an effective Cybersecurity GRC strategy managers would be able to effectively balance security and business needs.

Course Objectives

The course gives an introduction to the topics of Cybersecurity, IT Service Management, and Business Continuity. It discusses in detail the People, Process and Technology elements that underpin the various management systems.

The International Standards Management Systems such as the ISO 27001, ISO 22301 and ISO 20000 are discussed to understand how these makes up an effective Cybersecurity GRC framework for enterprises. The students are also taken through the ethical hacking steps and requisite counter measure while considering risk assessment. At the end of the course, the students will be able to:

1. Appreciate the concept of management systems and components
2. Align cybersecurity goals to Strategic Business Goals
3. Write high level cybersecurity policy objectives
4. Assess cybersecurity risks and recommend risk treatment options in line with organizational risk appetite
5. Recommend appropriate risk mitigation techniques and control measures
6. Review organizational compliance to cybersecurity standards and related frameworks

Alignment of course objectives (CO) with learning goals (LG) of Assurance of Learning

Derived from its mission, ASB has adopted five learning goals, (apart from the discipline competency) - the management-specific attributes, knowledge and skills that its graduates are expected to possess when they complete the programme. The six outcomes of this course are mapped to the '*Critical and integrative Thinking*' learning goal. The assessments, written report for the field visit and the writing exercise would reinforce the second learning goal, *'Effective written and oral communication'*.

LG CO	Critical and integrative Thinking	Effective written and oral communication	Societal and Environmental Awareness	Ethical Reasoning	Leadership
CO1	3	0	2	0	1
CO2	2	3	1	0	2
CO3	2	3	0	0	0
CO4	3	1	2	0	1
CO5	3	2	2	0	0

CO6	3	0	1	0	1

Key: 3 – Highly relevant; 2 –Moderately relevant; 1 – Low relevance; 0- No relevance

Unit-wise scope for outcomes and Bloom’s taxonomy

Production and Operations Management I and II, being the first core courses in the function, are designed focusing primarily on the Bloom’s learning levels of applying, analyzing and evaluating levels of learning.

CO **Bloom’s Levels of Learning**	**CO 1**	**CO 2**	**CO 3**	**CO 4**	**CO 5**	**CO 6**
Creating			X			
Evaluating			X	X		X
Analyzing			X	X	X	X
Applying	X	X	X	X	X	X
Understanding	X	X	X	X	X	X
Remembering	X	X				

Structure of the course

The Cybersecurity Governance, Risk and Compliance course is an introductory course that provides an overview of Cybersecurity management in organizations. As Cybersecurity has raised to Board Level attention and has become a prominent element for survival of organizations, this is necessary for any business graduate across specialization areas. The course structure includes introduction of concepts, case study discussions, field visits and interviews and mini project.

Pedagogy

The classes will use discussions predominantly, supported with lectures. Though the course is focused on strategy, techniques will also be practiced. Tutorials allow for problem solving practice. Every module will have assigned ‘take home’ exercises to practice critical thinking, where the students are expected ‘*to earn a ticket to class*’ with their 3 questions based on the assigned work. The students shall work in groups on the assigned topic to submit a mini project. This exercise is to give the students an opportunity to identify and use appropriate information and to practice writing skills.

Assessment (Grading Policy: Relative)

S. no	**Assessment exercise**	**Description**	**Weight**
Group assessment (25%)			
1	Class Presentations	*Students are assigned class presentation work for each module; They will present the topics assigned and raise pertinent challenges*	5%
2	Writing exercise	*A short term paper on a given topic is submitted in the given template based on information compiled from secondary research*	10%
3	Fieldwork report	*Each group identifies an organization involved in cybersecurity management . The learning is compiled into a poster which will be presented / displayed.*	10%
Individual Assessment (75%)			
1	Attendance	*Expected attendance, as per the rules*	5%
2	Glossary preparation & Quiz from Glossary	*Each group prepares a glossary of terms from the assigned module with a minimum of 25 terms. The group members will take a quiz individually on the terms that they have compiled*	10%
3	Mid-term examination	*A closed book exam with emphasis on the understanding and application of concepts*	20%

4	End-term examination	*A closed book comprehensive exam with emphasis on analyzing, evaluating and critiquing*	40%

Course Requirements

Throughout this course, the students are expected to demonstrate highest levels of involvement and commitment, in terms of efforts, quality of work, and conduct both at individual level and as groups. The potential of making learning interesting and effective lies primarily in the hands of the students and are expected to use the same for this course throughout the term. The course demands **study efforts of 6 hours/week outside classroom (3 hours for every one session of class). Preparation is mandatory for attending the classes.**

Course Text and Reference

- Cybersecurity for Beginners - Raef Meeuwisse
- Enterprise Cybersecurity by Scott Donaldson and Stanley Siegel
- How to Measure Anything in Cybersecurity Risk by Douglas W. Hubbard and Richard Seierse
- CSX Cybersecurity Fundamentals Study Guide by ISACA

Session Plan

Session numbers	Topics
1	Introduction to Cyber Security
2	Conceptual Description of Governance, Risk and Compliance
3 & 4	IT Governance Frameworks and Strategic Planning
5	Governance Models – MIT Sloan School of Management and ISO 38500
6	Discussion on Paper “IT Doesn’t Matter” by Nicholas Carr
7	IT Governance Case Study Discussion
8	3 Waves - Information Security and Cyber Security Contexts
9	Cyber Security Components
10	Introduction to ISO 27001
11 & 12	Ethical Hacking and Risk Management
13	Security Policy Management
14	Security Architecture Design
15	Security Awareness Program Design
16	Security Technologies
17	Case Study Discussion
18	Introduction to Service Management
19 & 20	Service Management Frameworks – ITIL and ISO 20000
20	Build of IT Service Management System
22	Introduction to Business Continuity Management
23	Building a Business Continuity Management system using ISO 22301
24	Case Study Discussion and Careers in Cyber Security

Contribution to Placements

The knowledge, readings, exercises and assignments for the course make explicit contributions to success during the placement process.

- Field work report: Resume, Interview (*for written communication practice*)
- Glossary of technical terms: Interview, Group Discussion (*for Domain knowledge ready reference*)
- Critical thinking Q & A : Group Discussion, Interview (*as critical thinking practice*)
- Modules mind maps: Group Discussion, Interview (*as a structured thinking tool*)
- Entry level operations positions and JD for these positions mapped with course objectives and discussed