

CCY4401 Cybersecurity Risk Management**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001	4	8	2	2	--	3

COURSE AIM

To get the students to:

- Get an inside look at how cybersecurity and information technology (IT) managers determine which projects they will support with funding, and which they won't, based on a preliminary risk analysis.
- Learn techniques to be explicitly applied to cybersecurity
- Learn how to assess and articulate risk options and how to treat them.
- Learn the set of tools and techniques to build and maintain a risk management framework

COURSE WEEKLY CONTENTS

- 1 Course Aim and Course outline. What is cybersecurity and why learn cybersecurity
- 2 What Are Controls and Why Are They Important?
- 3 What is cyber risk?
- 4 Risk management principles and frameworks.
- 5 Quantitative versus Qualitative Risk Assessment
- 6 Identify, assess, and articulate risks and options available for treating risk
- 7 7th week Assessment.
- 8 Defining Information Security Metrics.
- 9 Analysis Techniques
- 10 Automating Metrics Calculations and Tools
- 11 Samples and techniques to implement risk management framework
- 12 12th week Assessment
- 13 Tools needed to successfully maintain a risk management framework
- 14 Industry case studies
- 15 Inspection reports, Feasibility reports, Research/laboratory reports, Foundational risk management techniques and Third-party security measures

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook	Cynthia Brumfield and Brian Haugli, Cybersecurity Risk Management, Wiley
	Gerardus Blokdyk, Cybersecurity Risk Management A Complete Guide, 5STARCook