# ICT772 CYBERSECURITY GOVERNANCE, RISK AND COMPLIANCE MANAGEMENT T325 BRIEF

All information in the Subject Outline is correct at the time of approval. KOI reserves the right to make changes to the Subject Outline if they become necessary. Any changes require the approval of the KOI Academic Board and will be formally advised to those students who may be affected by email and via Moodle.
Information contained within this Subject Outline applies to students enrolled in the trimester as indicated

# 1. General Information

## 1.1 Administrative Details

| Associated HE Award(s) | Duration | Level | Subject Coordinator |
|---|---|---|---|
| Master of Information Systems (MIS) | 1 trimester | Postgraduate | Dr Fazla RABBY<br>fazla.rabby@koi.edu.au<br>P: +61 (2) 9283 3583<br>L: Level 7-11, 11 York St.<br>Consultation: via Moodle or by appointment. |

## 1.2 Core/Elective

This subject is an elective subject for MIS.

## 1.3 Subject Weighting

Indicated below is the weighting of this subject and the total course points

| Subject Credit Points | Total Course Credit Points |
|---|---|
| 4 | Master of Information Systems (64) |

## 1.4 Student Workload

Indicated below is the expected student workload per week for this subject

| No. Timetabled Hours/Week* | No. Personal Study Hours/Week** | Total Workload Hours/Week*** |
|---|---|---|
| 3 hours/week plus supplementary online material | 7 hours/week | 10 hours/week |

* Total time spent per week at lectures and tutorials
** Total time students are expected to spend per week in studying, completing assignments, etc.
*** Combination of timetable hours and personal study

**1.5 Mode of Delivery** Classes will be face-to-face or hybrid. Certain classes will be online (e.g., special arrangements).

**1.6 Pre-requisites** ICT722 Information Security, and
Completion of 8 subjects

## 1.7 General Study and Resource Requirements

- Students are expected to attend classes with the weekly worksheets and subject support material provided in Moodle. Students should read this material before coming to class to improve their ability to participate in the weekly activities.
- Students will require access to the internet and their KOI email and should have basic skills in word processing software such as MS Word, spreadsheet software such as MS Excel and visual presentation software such as MS PowerPoint.
- Computers and WIFI facilities are extensively available for student use throughout KOI. Students are encouraged to make use of the campus Library for reference materials.

*Software resource requirements specific to this subject:* Office 365, MS Imagine, MS Excel, Python, Spyder and Jupyter Notebook, RapidMiner.

### 1.8 Academic Advising

Academic advising is available to students throughout teaching periods including the exam weeks. As well as requesting help during scheduled class times, students have the following options:

- Consultation times: A list of consultation hours is provided on the homepage of Moodle where appointments can be booked.
- Subject coordinator: Subject coordinators are available for contact via email. The email address of the subject coordinator is provided at the top of this subject outline.
- Academic staff: Lecturers and Tutors provide their contact details in Moodle for the specific subject. In most cases, this will be via email. Some subjects may also provide a discussion forum where questions can be raised.
- Head of Program: The Head of Program is available to all students in the program if they need advice about their studies and KOI procedures.
- Vice President (Academic): The Vice President (Academic) will assist students to resolve complex issues (but may refer students to the relevant lecturers for detailed academic advice).

# 2. Academic Details

### 2.1 Overview of the Subject

Data breaches in information systems can be extremely damaging to businesses. This subject introduces students to cybersecurity risk management, cognitive risk, and international cybersecurity standards. The subject explores cybersecurity governance requirements and key legal, regulatory and compliance frameworks. Through authentic case studies, students will comprehensively evaluate, analyse, and apply one of the risk management approaches. On completion of this subject, students will be able to critically evaluate current governance structures and arrangements, in both public and private organisations, with reference to international best practice standards. They will be able to apply these skills to • assess and respond to an organisation's cybersecurity exposure • develop risk mitigation strategies • develop cybersecurity policies, standards, and procedures and effectively manage and monitor compliance obligations

### 2.2 Graduate Attributes for Postgraduate Courses

Graduates of postgraduate courses from King's Own Institute will gain the graduate attributes expected from successful completion of a postgraduate degree under the Australian Qualifications Framework (2nd edition, January 2013). Graduates at this level will be able to apply advanced body of knowledge from their major area of study in a range of contexts for professional practice or scholarship and as a pathway for further learning.

King's Own Institute's generic graduate attributes for a master's level degree are summarised below:

| | KOI Postgraduate Degree Graduate Attributes | Detailed Description |
|---|---|---|
|  | Knowledge | Current, comprehensive and coherent knowledge, including recent developments and applied research methods |
|  | Critical Thinking | Critical thinking skills to identify and analyse current theories and developments and emerging trends in professional practice |
|  | Communication | Communication and technical skills to analyse and theorise, contribute to professional practice or scholarship, and present ideas to a variety of audiences |
|  | Research and Information Literacy | Cognitive and technical skills to access and evaluate information resources, justify research approaches and interpret theoretical propositions |
|  | Creative Problem Solving Skills | Cognitive, technical and creative skills to investigate, analyse and synthesise complex information, concepts and theories, solve complex problems and apply established theories to situations in professional practice |
|  | Ethical and Cultural Sensitivity | Appreciation and accountability for ethical principles, cultural sensitivity and social responsibility, both personally and professionally |
|  | Leadership and Strategy | Initiative, leadership skills and ability to work professionally and collaboratively to achieve team objectives across a range of team roles<br>Expertise in strategic thinking, developing and implementing business plans and decision making under uncertainty |
|  | Professional Skills | High level personal autonomy, judgement, decision-making and accountability required to begin professional practice |

Across the courses, these skills are developed progressively at three levels:

- **Level 1 Foundation –** Students learn the skills, theories and techniques of the subject and apply them in stand-alone contexts
- **Level 2 Intermediate –** Students further develop skills, theories and techniques of the subject and apply them in more complex contexts, beginning to integrate the application with other subjects
- **Level 3 Advanced** – Students have a demonstrated ability to plan, research and apply the skills, theories and techniques of the subject in complex situations, integrating the subject content with a range of other subject disciplines within the context of the course

Generally, skills gained from subjects in the Graduate Certificate and Graduate Diploma are at levels 1 and 2 while other subjects in the Master's degree are at level 3.

### 2.3 Subject Learning Outcomes

Listed below, are key knowledge and skills students are expected to attain by successfully completing this subject:

| Subject Learning Outcomes | Contribution to Course Graduate Attributes |
|---|---|
| a) Critically review the theoretical concepts and practical issues relating to governance, risk, and compliance management in a cybersecurity context. |  |
| b) Identify, evaluate, and formulate risk response strategies in order to develop and apply an appropriate risk management framework to manage cybersecurity. |  |
| c) Critically evaluate and effectively communicate risk mitigation strategies to both technical and nontechnical audiences. |  |
| d) Assess cybersecurity policies, standards, and procedures against key legal, regulatory and compliance frameworks to fulfil organisational compliance requirements. |  |

**2.4 Subject Content and Structure**

Below are details of the subject content and how it is structured, including specific topics covered in lectures and tutorials. Reading refers to the text unless otherwise indicated.

*Weekly Planner:*

| Week (beginning) | Topic covered in each week's lecture | Reading(s) | Expected work as listed in Moodle |
|---|---|---|---|
| Week 1<br>27 Oct | Introduction to cybersecurity management | Ch 1, Ch 2 Edwards and Weaver (2024) | Tutorial tasks from related topics on cybersecurity management fundamentals |
| Week 2<br>03 Nov | Cybersecurity measures in business and business appraisal for cybersecurity solutions | Extra resources from:<br>Ch 12, 26, and Ch 27 Edwards and Weaver (2024) | Tutorial tasks focusing on cybersecurity countermeasures |
| Week 3<br>10 Nov | Cybersecurity strategy, organisational strategic governance framework, governance and compliance decision making process | Ch 3, 4, 5, 6 and<br>Ch 12 Edwards and Weaver (2024) | Tutorial tasks on cybersecurity strategy, governance framework and compliance |
| Week 4<br>17 Nov | Compliant ICT security policies and procedures | Ch 1, 2, and<br>Ch 3 Johnson and Easttom (2020) | Tutorial tasks on security policies – case study-based exercises<br>**Assessment 1: due Draft proposal of Assessment 2** |

| Week (beginning) | Topic covered in each week's lecture | Reading(s) | Expected work as listed in Moodle |
|---|---|---|---|
| Week 5<br>24 Nov | Risk assessment policy and its strategic context | Chr 4 & Ch 5 Johnson and Easttom (2020) | Tutorial tasks on strategic context of risk assessment – case study-based questions |
| Week 6<br>01 Dec | Cybersecurity risk management frameworks – Part I | Ch 2 and 3 Hubbard et al.<br><br>Ch7 and 8 Edwards and Weaver (2024) | Tutorial tasks on cybersecurity risk management – case study-based exercises<br>**Assessment 2: Topical case study** |
| Week 7<br>08 Dec | Cybersecurity risk management frameworks – Part II | Ch 10, 11 and 12 Hubbard et al.<br><br>Ch 9 and 10 Edwards and Weaver (2024) | Tutorial tasks on cybersecurity risk management – case study- based exercises |
| Week 8<br>15 Dec | Business continuity management planning framework | Ch 30 Edwards and Weaver (2024) | Tutorial tasks – cases study-based exercise to understand the importance of business continuity plan and management |
| Week 9<br>05 Jan | Preparing for disasters and resilience policy and strategy mapping | Ch 30 and 31 Edwards and Weaver (2024) | Tutorial tasks on cases studies to understand the use of disaster recovery and resilience **Assessment 3: due Individual Report** |
| Week 10<br>12 Jan | Implementation of cybersecurity solutions and change management | Ch 4, 25 and 26 Edwards and Weaver (2024) | Tutorial task using case studies to understand the use of cybersecurity solutions |
| Week 11<br>19 Jan | International and domestic regulations on cybersecurity | Ch 17 and 18 Edwards and Weaver (2024) | Tutorial tasks using case studies to understand domestic and international regulations for cybersecurity |

| Week (beginning) | Topic covered in each week's lecture | Reading(s) | Expected work as listed in Moodle |
|---|---|---|---|
| | | | **Assessment 4: due Report** |
| Week 12<br>27Jan (Tue) | Cybersecurity strategic plans: Effect on emerging threats and the change in the technologies of an organisation | Ch 27, 28 and 29 Edwards and Weaver (2024) | Tutorial tasks using case studies to discuss and understand strategic plans for cybersecurity<br><br>**Assessment 4: due Presentation** |
| Week 13<br>02 Feb | Study review week and Final Exam Week | | |
| Week 14<br>09 Feb | Examinations<br>Continuing students - enrolments for T126 open | | Please see exam timetable for exam date, time and location |
| Week 15<br>16 Feb | Student Vacation begins<br>New students - enrolments for T126 open | | |
| Week 16<br>23 Feb | • Results Released<br>• Review of Grade Day for T325 – see Sections 2.6 and 3.2 below for relevant information.<br>• Certification of Grades<br><br>NOTE: More information about the dates will be provided at a later date through Moodle/KOI email. | | |
| **T126 2 Mar 2026** | | | |
| Week 1<br>02 Mar | Week 1 of classes for T126 | | |

### 2.5 Teaching Methods/Strategies

Briefly described below are the teaching methods/strategies used in this subject:

- *Lectures* (1 hour/week) are conducted in seminar style and address the subject content, provide motivation and context and draw on the students' experience and preparatory reading.
- *Tutorials* (2 hours/week) include class discussion of case studies and research papers, practice sets and problem-solving and syndicate work on group projects. Tutorials often include group exercises and so contribute to the development of teamwork skills and cultural understanding. Tutorial participation is an essential component of the subject and contributes to the development of many of the graduate attributes (see section 2.2 above). Tutorial participation contributes towards the assessment in many subjects (see details in Section 3.1 for this subject). Supplementary tutorial material such as case studies, recommended readings, review questions etc. will be made available each week in Moodle.
- *Online* teaching resources include class materials, readings, model answers to assignments and exercises and discussion boards. All online materials for this subject as provided by KOI will be found in the Moodle page for this subject. Students should access Moodle regularly as material may be updated at any time during the trimester
- *Other contact* - academic staff may also contact students either via Moodle messaging, or via email to the email address provided to KOI on enrolment.

### 2.6 Student Assessment

Assessment is designed to encourage effective student learning and enable students to develop and demonstrate the skills and knowledge identified in the subject learning outcomes. Assessment tasks during the first half of the study period are usually intended to maximise the developmental function of assessment (formative assessment). These assessment tasks include weekly tutorial exercises (as indicated in the weekly planner) and low stakes graded assessments (as shown in the graded assessment table). The major assessment tasks where students demonstrate their knowledge and skills (summative assessment) generally occur later in the study period. These are the major graded assessment items shown in the graded assessment table.

Final grades are awarded by the Board of Examiners in accordance with KOI's Assessment and Assessment Appeals Policy. The definitions and guidelines for the awarding of final grades are:

- *HD High distinction* (85-100%): an outstanding level of achievement in relation to the assessment process.
- *D Distinction* (75-84%): a high level of achievement in relation to the assessment process.
- *C Credit* (65-74%): a better than satisfactory level of achievement in relation to the assessment process.
- *P Pass* (50-64%): a satisfactory level of achievement in relation to the assessment process.
- *F Fail* (0-49%): an unsatisfactory level of achievement in relation to the assessment process.
- *FW:* This grade will be assigned when a student did not submit any of the compulsory assessment items.

Provided below is a schedule of formal assessment tasks and major examinations for the subject.

| Assessment Type | When assessed | Weighting | Learning Outcomes Assessed |
|---|---|---|---|
| Assessment 1: Draft Proposal of Assessment 2 (750 words), critically review the case study and prepare a proposal | Week 4 | 10% | a |
| Assessment 2: Case Study: Cyber security measures and their effectiveness for organisations (1500 words) | Week 6 | 20% | a, b |

| | | | |
|---|---|---|---|
| Assessment 3: Individual report: Essay critique on cybersecurity policy (2000 words) | Week 9 | 35% | c, d |
| Assessment 4: Group report: Case study on cybersecurity risk management with individual reflection: Report and presentation (2000 words, group -1500 words, individual – 500 words) | Week 11: Report Week 12: Presentation | Report: 20% Weekly log: 5% Presentation: 10% | a, b, c |

*Requirements to Pass the Subject:*

To gain a pass or better in this subject, students must gain a *minimum of 50%* of the total available subject marks.

### 2.7 Prescribed and Recommended Readings

Provided below, in formal reference format, is a list of the prescribed and recommended readings.

**Prescribed Books**

The Cybersecurity Guide to Governance, Risk, and Compliance. Jason Edwards, Griffin Weaver, Wiley (2024)

How to Measure Anything in Cybersecurity Risk, 2nd Edition , By Douglas W. Hubbard, Richard Seiersen, Daniel E. Geer Jr., Stuart McClure, Wiley (2023)

Johnson, R. and Easttom, C., *Security policies and implementation issues*. 3rd ed. Burlington, MA: Jones & Bartlett Learning (2020).

**Recommended Books**

The Cybersecurity Guide to Governance, Risk, and Compliance. Jason Edwards, Griffin Weaver, Wiley (2024)

How to Measure Anything in Cybersecurity Risk, 2nd Edition , By Douglas W. Hubbard, Richard Seiersen, Daniel E. Geer Jr., Stuart McClure, Wiley

Andy Taylor, David Alexander, Amanda Finch, David Sutton, 2020, Information *Security Management Principles: Third edition.* BCS, The Chartered Institute for IT

Evans, A 2019, *Managing Cyber Risk*, Routledge 1st Edition.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC press.

Hodson, C 2019, *Cyber Risk Management Prioritize Threats, Identify Vulnerabilities and Apply Controls*, Kogan Page, 1st edition.

Hubbard, D. W & Seiersen, R 2016, *How to measure anything in cybersecurity risk*, John Wiley & Sons.

**Journals**
Journal of Cybersecurity and Privacy
Journal of Cybersecurity
Journal of Information Assurance and Cybersecurity
Journal of Information Security

**Recommended Research Articles**

Awang, N., Narayana Samy, G.N, and Hassan, N. H. 2022. Prioritizing Cybersecurity Management Guidelines using Analytical Hierarchy Process (AHP) Decision Technique. *Open International Journal of Informatics*, 10(Special Issue 1), pp.1–10.

Vinaja, R., 2022. Cybersecurity Management: An Organizational and Strategic Approach. *Journal of Global Information Technology Management*. Vol 25 (2). 2022

Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. 2016. Taxonomy of information security risk assessment (ISRA). *Computers & security*, 57, pp. 14-30.

Yeoh, W. Wang, S., Popovič, A. and Chowdhury, N. H., 2022. A systematic synthesis of critical success factors for cybersecurity, *Computers & Security*, Vol 118, 2022.

Zamfiroiu, A., & Sharma, R. C. 2022. Cybersecurity Management for Incident Response., *Romanian Cyber Security Journal* Vol. 4(1) 2022

**Useful Websites:**

The following industry websites are useful introductory sources covering a range of information useful for this subject.

- Guidelines to managing information security risks faced by organizations (https://www.iso.org/standard/80585.html)
- NIST Risk Management Framework (https://csrc.nist.gov/Projects/risk-management )
- NIST Cyber Security Framework (https://www.nist.gov/cyberframework)
- General Data Protection Regulation (https://gdpr-info.eu/)