ICT742 CLOUD PRIVACY AND SECURITY T326 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 Technology (MIT)	1 trimester	Postgraduate	Dr MD Monir Hossain monir.hossain@koi.edu.au P: +61 (2) 9283 3583 L: 7-11, 11 York Street. Consultation: via Moodle or by appointment.

1.2 Core/Elective

This subject is
- a core subject for the Master of Information Technology (MIT) Cybersecurity
- an elective subject for the Master of Information Technology (MIT) General

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	MIT (64 Credit Points)

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

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: MS Imagine, Office 365, Amazon Web Services (AWS).

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

There are many businesses, government agencies, and other organisations that have adopted cloud computing to provide cost effective, highly available and reliable services to their users. However, the use of cloud-based solutions in organisations raises significant risks related to security and privacy. In this subject, students will become familiar with the fundamentals of security, privacy and trust within cloud systems. Students will develop a security solution for a business application using cloud services. They will develop the practical and research skills necessary to evaluate and implement trustworthy and secure applications.

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 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) Characterise different cloud technologies and related architectures	

b) Identify cybersecurity threats, privacy and ethical issues in cloud computing	
c) Explain infrastructure and platform security, application security, data security, and privacy in cloud systems	
d) Analyse regulations and compliance related to cloud security and privacy	
e) Develop cloud security solutions for business applications	

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 26 October	Introduction	Ch. 1 [Dotson]	Introduction to tutorial structure, group project, AWS, and registration on AWS Tutorial is not-graded
Week 2 02 November	Cloud computing architectures Security, privacy and ethical issues	Ch. 1 [Chen] Additional reading provided on Moodle	Introduction to Virtual Machine and create an EC2 instance on AWS Tutorial is graded
Week 3 09 November	Infrastructure security	Ch. 2 [Chen]	Setup and config AWS S3 bucket with encryption Tutorial is graded
Week 4 16 November	Data security in cloud	Ch.3 [Chen]	Setup and config AWS Security Group and Network ACL Tutorial is graded
Week 5 23 November	Network security in cloud	Ch.6 [Dotson]	Setup and config a VPC on AWS Group Project Meeting Tutorial is graded **Assessment 2 due: Quiz**
Week 6	Identity and access management in cloud	Ch. 4 [Chen] Ch. 4 [Dotson]	Setup and config AWS Identity and Access Management

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
30 November			Tutorial is graded
Week 7 07 December	Security management in cloud	Ch. 5 [Chen]	Group Project Meeting Setup and config AWS Key Management Service (KMS) Tutorial is graded
Week 8 14 December	Disaster recovery in cloud	Ch. 7 [Chen]	Group Project Meeting Setup and config AWS CloudTrial and AWS CloudWatch Tutorial is graded
Week 9 04 January	Audit and compliance in cloud	Ch. 8 [Chen]	Group project meeting Setup and configure AWS firewall Manager Tutorial is graded **Assessment 3 due: Research Individual Report**
Week 10 11 January	Security as a service (SaaS)	Ch. 9 [Chen]	Group Project Meeting Setup and configure AWS Artifact and Amazon Inspector Tutorial is graded
Week 11 18 January	IoTs security and privacy in the cloud environment	Resources will be provided on Moodle	Group Project Meeting Discussion and reflection Tutorial is graded
Week 12 25 January	Revision & preparation for the final exam		All Chapters
Week 13 01 February	Study review week and Final Exam Week		
Week 14 08 February	- Final Exam Week - Continuing students - enrolments for T127 open		Please see the exam timetable for the exam date, time and location
Week 15 15 February	- Student Vacation begins - New students - enrolments for T127 open		
Week 16 22 February	2. Results Released 3. Review of Grade Day for T326 – see Sections 2.6 and 3.2 below for relevant information. 4. Certification of Grades		

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
	NOTE: More information about the dates will be provided at a later date through Moodle/KOI email.		
T127 01 March 2027			
Week 1 01 March	Week 1 of classes for T127		

2.5 Teaching Methods/Strategies

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

- *Lectures* (1 hours/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: Weekly Tutorial	Week 2 to Week 11	15% (1.5% each week)	a,b,c,d
Assessment 2: Quiz (In-class)	Week 5	20%	a,b
Assessment 3: Individual Research Report (3000 words report)	Week 9	30%	a, b, c
Assessment 4: Final Examination on Campus: 2 hours + 10 mins reading time	Final Exam Period	35%	a,b,c, d, e

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 Texts:

Chen, L., Takabi, H. & Le-Khac, N., 2019. Security, Privacy, and Digital Forensics in the Cloud. Wiley. ISBN: 9781119053286.

Recommended Readings:

Dotson, C., 2023. Practical Cloud Security (2nd Edition). O'Reilly Media. ISBN: 9781098148164.

Amaithi Rajan, A. and V, V., 2023. Systematic Survey: Secure and Privacy-Preserving Big Data Analytics in Cloud. *Journal of Computer Information Systems*, pp.1-21. DOI: https://doi.org/10.1080/08874417.2023.2176946.

Certified Cloud Security Professional (CCSP) Study Guide by Ric Messier, 2026, O'Reilly Media. ISBN: 9781098179410.

Chakraborty, A., Kumar, M., Chaurasia, N. and Gill, S.S., 2023. Journey from cloud of things to fog of things: Survey, new trends, and research directions. Software: Practice and Experience, 53(2), pp.496-551. DOI:https://doi.org/10.1002/spe.3157.

Cloud Security Handbook, Second Edition by Eyal Estrin, 2025. ISBN: 9781836200017.

Ikegwu, Anayo Chukwu, et al, 2026, A survey of cyber threat intelligence in embedded system driven security for mobile health systems, Journal of Cloud Computing: Advances, Systems and Applications. DOI: https://doi.org/10.1186/s13677-025-00811-3.

ISC2 CCSP Certified Cloud Security Professional Official Study Guide, 3rd Edition by Mike Chapple, David Seidl. ISBN: 9781119909378.

Journal of Cloud Computing: Advances, Systems and Applications. DOI: https://doi.org/10.1186/s13677-025-00735-y.

M Dhinakaran,M Sundhari,S. Ambika,V. Balaji, R.Thalapathi Rajasekaran, 2024. Advanced Machine Learning Techniques for Enhancing Data Security in Cloud Computing Systems. IEEE International Conference on Computing, Power and Communication Technologies. DOI: 10.1109/IC2PCT60090.2024.10486559.

Mishra, P., Pilli, E.S. and Joshi, R.C., 2024. *Cloud Security: Attacks, Techniques, Tools, and Challenges*. CRC Press. ISBN: 9781032190266.

Mohammed Y. Shakor, Mustafa Ibrahim Khaleel, Mejdl Safran, Sultan Alfarhood, Michelle Zhu, 2024, Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security, IEEE Access. DOI: 10.1109/ACCESS.2024.3351119.

NIST Special Publication 800-190: Application Container Security Guide. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-190.pdf.

Oladunjoye, John Abiodun;Jessica, Egwom Onyinyechiln,2024, volume 12, issue 1, pages 8-16, Tools for A Comparative Assessment of Load Balancing Techniques in Cloud Computing: A Review, International Journal of Distributed & Cloud Computing. DOI: http://dx.doi.org/10.2139/ssrn.4869408.

Salman Manzoor, Antonios Gouglidis, Matthew Bradbury, Neeraj Suri, 2024, Enabling Multi-Layer Threat Analysis in Dynamic Cloud Environments. IEEE Transactions on Cloud Computing. **DOI:** 10.1109/TCC.2024.3365736

Sina Ahmadi, 2024, Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security, 15, 148-167. DOI: 10.4236/jis.2024.152010.

Wang, T., Liang, Y., Shen, X., Zheng, X., Mahmood, A. and Sheng, Q.Z., 2023. Edge Computing and Sensor-Cloud: Overview, Solutions, and Directions. *ACM Computing Surveys*. DOI:https://doi.org/10.1145/3582270.

Younus, Muhammad; Purnomo, Eko Priyo; Nurmandi, Achmad; Khairunnisa, Tiara, 2025, Analyzing the trend of government support for cloud computing usage in e-government architecture, p. 14,

Vacca, J.R. ed., 2020. *Cloud computing security: foundations and challenges*. CRC Press. ISBN: 978-0367151164.

Useful Websites:

- Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/
- NIST Cloud Computing: https://www.nist.gov/topics/cloud-computing
- Center for Internet Security (CIS) - Cloud Security: https://www.cisecurity.org/controls/cloud/
- OWASP Cloud Security: https://owasp.org/www-project-cloud-security/
- European Union Agency for Cybersecurity (ENISA) - Cloud Security: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-computing/cloud-security
- Australian Cyber Security Centre: https://www.acsc.gov.au/infosec/cloudsecurity.htm
- AWS Cloud Security Best Practices:https://www.rapid7.com/fundamentals/aws-cloud-security/
- AWS Cloud Security: https://www.w3schools.com/aws/aws_cloudessentials_sec_securityintroduction.php
- Amazon:

- https://aws.amazon.com/education/awseducate/
- https://aws.amazon.com/getting-started/tutorials/
- https://aws.amazon.com/security/introduction-to-cloud-security/

Suggested Periodicals:

- ACM Digital Library: https://dl.acm.org/
- IEEE Transactions on Cloud Computing: https://www.computer.org/web/tcc
- Journal of Computers and Security: https://www.journals.elsevier.com/computers-and-security/
- Springer Open Journals: https://www.springeropen.com/journals
- Transactions on Dependable and Secure Computing: https://www.computer.org/web/tdsc

Conference/ Journal Articles:

Students are encouraged to read peer reviewed journal articles and conference papers. Google Scholar provides a simple way to broadly search for scholarly literature. From one place, you can search across many disciplines and sources: articles, theses, books, abstracts and court opinions, from academic publishers, professional societies, online repositories, universities and other web sites.

*AUSTRALIAN INSTITUTE OF BUSINESS AND MANAGEMENT PTY LTD © ABN: 72 132 629 979 CRICOS 03171A