BIS300 Unit Outline

Unit Code and Title: BIS300 INFORMATION AND CYBER SECURITY
Course(s): Bachelor of Professional Accounting
Core Unit: Elective
Credit Points: 10 credit points
Study Period: Year Three
AQF Level 7: One Quadmester
Study Load: Students should expect to spend approximately 130 hours on studying and completing assignments across the study period. This includes time spent attending scheduled weekly classes, Work Integrated Learning (WIL) activities (if any), undertaking private study, and preparing for assessments, and examinations.
Pre-Requisite: There is one prerequisite BIS100 Introduction to Business Information Systems
Mode(s) of Delivery: This unit will be delivered predominantly face-to-face and online via Learning Management System (Canvas)/Zoom with recordings available for later viewing. Where appropriate, assessments MUST be submitted to Turnitin for authentication checking

Unit Description:

In the information age, dependence on information systems and services exposes entities to security threats such as viruses, computer hacking and denial of service attacks. Managers, accountants, and auditors are expected to implement controls over integrity of information they produce and rely upon. This unit discusses the key objectives of authentication, confidentiality, integrity, non-repudiation and availability in security. The importance of Information Security policies, processes, standards and procedures and Business Continuity Planning including backup, disaster recovery and continuity of operations are addressed from a managerial perspective.

Prescribed Textbook:

Shoemaker, D., and Sigler, K., 2015. Cybersecurity: Engineering a Secure Information Technology Organisation Cengage.

Unit Learning Outcomes (ULOs): On successful completion of this unit, students will be able to:

[ULO1] Describe and apply the key concepts of information security and assurance that includes cyber security.
[ULO2] Apply and assess risk assessment and management methodologies in simple scenarios.
[ULO3] Articulate basic systems controls and demonstrate application in small businesses.

[ULO4] Describe and assess the key elements of business continuity planning and perform case analysis.		
[ULO5] Apply and discuss in an organizational setting the principles of information privacy that covers cyber security.		

Assessment Requirements:

Assessment Type	Due	Weighting (% of total marks)
Assessment 1: Discussion Forum – On-Campus and Online	Week 1 to 8	10%
Assessment 2: Mid Quadmester Test – On Campus or Online (Closed-book)	Week 5	15%
Assessment 3: Group Report on ICT Critical Appraisal Plan and Presentation: Part A: For a given organization prepare information and cyber security plan with an evaluation of the key concepts of information security and assurance that includes cyber security, risk assessment and management methodologies in simple scenarios, and basic systems controls and demonstrate application in small businesses (constraints and problems that might arise). Part B: Critically reflect, analyze, and report on the key elements of business continuity planning and perform case analysis in the given organizational setting in your proposed coherent, coordinated, and consistent information and cyber security plan. Part C: Presentation. Groups of three or four must provide a 6000-word written report with an individual reflective summary report of 1500 words from each group member. Variations of plus or minus 10% of word limitation are acceptable.	Week 8	25% (Report 20% plus presentation 5%)
Assessment 4: Final examination (Closed Book). The 3 hours invigilated examination is conducted in the week 10 following the week 9 of study break and exam revision	Week 10	50%

Note: It is your responsibility as a student to regularly check the academic policy documents available on the school website and unit materials available on the learning Management System (LMS). ***Failure to do so could lead to students taking a risk of failing to maintain satisfactory progress in the unit and completing the course on time**. ***A breach of academic integrity could lead to the imposition of penalties**.