SBM4304 IS Security and Risk Management

Unit description

Security is a vital responsibility for organisations and it is critical to IT applications and business success. This unit explores the concept and specialised applications of information security and risks associated with information systems, and the implications that these risks have in a larger business context. Topics covered include cryptography fundamentals, computer security, network security, data security, web security, social issues of security and implementation. This unit provides students with advanced knowledge and skills for IT security industry. Students will develop the ability to identify different types of risks and learn how organisations employ various methods to manage those risks. Students will come to understand the importance of information security and risk management through a variety of case studies, developing both a theoretical and practical grasp of the role information system risk management plays in modern business.
This unit is a core unit in the BBIS program.

Learning outcomes

On successful completion of this unit, students will be able to:

[ULO1] Demonstrate why IS are vulnerable to destruction, error, abuse, and system quality problems.

[ULO2] Identify and manage organizational level IS-related security and risks.

[ULO3] Compare general management controls and application controls for IS.

[ULO4] Develop and document IS/IT risk and security management plans.

[ULO5] Evaluate the IS-related security and risk management techniques required to ensure the reliability, confidentiality, availability, integrity and security of digital business processes.

[ULO6] Critique the importance of auditing IS and safeguarding data quality.

[ULO7] Appraise the general impact of human factors and organizational issues on IS-related security and risk management.

Summary

Credit Points	6
Courses	BBIS
Total Credit Points	BBIS: 144 credit points
Pre-Requisites	N/A
Co-Requisites	N/A
Other Requirements	N/A
Unit Level	Core
Duration	14 weeks (12 teaching weeks; 1 study week; 1 final assessment week)
Mode of Delivery	On-campus
Assessment	Quiz: 10%; Case Study: 20%; Applied project: 20%; Laboratory Submission: 10%; Examination: 40%
Prescribed Textbook	Ciampa, M. 2017, CompTIA Security+ Guide to Network Security Fundamentals. 6th edn. Cengage, Australia
Expected student workload	Students should expect to spend approximately 8.5 hours per week over 14 weeks on learning activities for this unit. This includes time spent attending scheduled classes, undertaking private study, preparing assessments, and completing examinations.