H8BNS: Security Principles

Module Code:	H8BNS
Long Title	Security Principles APPROVED
Title	Business and Network Security
Module Level:	LEVEL 8
EQF Level:	6
EHEA Level:	First Cycle

Credits:	5

Module Coordinator:	Eugene McLaughlin

Module Author:	Eugene McLaughlin

Departments:	School of Computing

Specifications of the qualifications and experience required of staff	

Learning Outcomes

On successful completion of this module the learner will be able to:

#	Learning Outcome Description
LO1	Understand the architecture and environment in which E-Business operates.
LO2	Apply security principles to Application Development.
LO3	Assess Networks and computer systems for security weaknesses. Identify appropriate defense mechanisms in order to protect systems and data from data loss or malicious attack
LO4	Address different security issues when dealing with different server APIs when creating Web and Mobile applications.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	

H8BNS: Security Principles

Module Content & Assessment

Indicative Content
Introduction to E-Business (5%) E-Business: Definition and concepts E-Business Framework, Classification, and Content Digital revolution, its business environment, and organisational responses WWW Architecture E-Business Architectural framework The Role of the Information Architect Business Process Models
Access Control (10%) Identify the mechanisms that work together to to create architecture to protect the assests of an information system - Concepts / Methodologies / Techniques - Attacks - Effectiveness
Telecommunications and Network Security (10%) discusses network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality. Network architecture and design Communication channels Network components Network attacks
Cryptography (10%) the principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity. Secret Key Public Key Protocols Encryption algorithms Encryption concepts Digital signatures Cryptanalytic attacks Public Key Infrastructure (PKI) Information hiding alternatives
Information Security Governance and Risk Management (10%) the identification of an organization’s information assets and the development, documentation and implementation of policies, standards, procedures and guidelines. Security governance and policy Information classification/ownership Contractual agreements and procurement processes Risk management concepts Personnel security Security education, training and awareness Certification and accreditation
Software Development Security (10%) refers to the controls that are included within systems and applications software and the steps used in their development. Systems development life cycle(SDLC) Application environment and security controls Effectiveness of application security
Security Architecture and Design (10%) contains the concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability. Fundamental concepts of security models Capabilities of information systems (e.g. memory protection, virtualization) Countermeasure principles Vulnerabilities and threats (e.g. cloud computing, aggregation, data flow control)
Operations Security (10%) used to identify the controls over hardware, media and the operators with access privileges to any of these resources. Resource protection Incident response Attack prevention and response Patch and vulnerability management
Business Continuity and Disaster Recovery Planning (10%) addresses the preservation of the business in the face of major disruptions to normal business operations. Business impact analysis Recovery strategy Disaster recovery process
Legal, Regulations, Investigations and Compliance (5%) addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence.
Physical(Environmental)Security (5%) addresses the threats, vulnerabilities and countermeasures that can be utilized to physically protect an enterprise’s resources and sensitive information. Site/facility design considerations Perimeter security Internal security Facilities security
OWASP Top 10 Mobile and Security (5%) Current OWASP Top 10 for Mobile and Application Security

Assessment Breakdown	%
Coursework	30.00%
End of Module Assessment	70.00%

Assessments

Full Time

Coursework

Assessment Type:	Continuous Assessment (0200)	**% of total:**	30
Assessment Date:	Sem 1 End	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
Sample Assessment: Create a Business continuity and Disaster Recovery document for the organisation of your choice. Please include assessments of Risk in the following areas. The preservation of the business in the face of major disruptions to normal business operations. • Business impact analysis • Recovery strategy • Disaster recovery process

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	70
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2,3,4
Non-Marked:	No		

Assessment Description:
End-of-Semester Final Examination

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

H8BNS: Security Principles

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	2	Every Week	2.00
Tutorial	No Description	1	Every Week	1.00
Independent Learning	No Description	7.5	Every Week	7.50
			Total Weekly Contact Hours	3.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	No Description	2	Every Week	2.00
			Total Weekly Contact Hours	2.00

Module Resources

Recommended Book Resources

Shon Harris. (2012), CISSP All-in-One Exam Guide, 6th Edition, McGraw-Hill Osborne Media, p.1008, [ISBN: 0071781749].

Raymond R Panko, Julia Panko. (2012), Business Data Networks and Security, Prentice Hall, p.528, [ISBN: 0132742934].

Turban Effraim, King David et al. (2008), Electronic commerce, A managerial perspective,, Pearson International Edition..

Supplementary Book Resources

Chetan Damani, Ravi Damani. (2007), E-Business 2.0: The Evolution of E-Business:1,, Imano plc.

This module does not have any article/paper resources

This module does not have any other resources

Discussion Note:	