Unit 5: Security

Unit code	**K/615/1623**
Unit type	**Core**
Unit level	**4**
Credit value	**15**

Introduction

Security is one of the most important challenges modern organisations face. Security is about protecting organisational assets, including personnel, data, equipment and networks from attack through the use of prevention techniques in the form of vulnerability testing/security policies and detection techniques, exposing breaches in security and implementing effective responses.

The aim of this unit is to provide students with knowledge of security, associated risks and how security breaches impact on business continuity. Students will examine security measures involving access authorisation, regulation of use, implementing contingency plans and devising security policies and procedures.

This unit introduces students to the detection of threats and vulnerabilities in physical and IT security, and how to manage risks relating to organisational security.

Among the topics included in this unit are Network Security design and operational topics, including address translation, DMZ, VPN, firewalls, AV and intrusion detection systems. Remote access will be covered, as will the need for frequent vulnerability testing as part of organisational and security audit compliance.

Students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

LO3 Review mechanisms to control organisational IT security.

LO4 Manage organisational security.

Essential Content

LO1 Assess risks to IT security

IT security risks:

Risks: unauthorised use of a system; unauthorised removal or copying of data or code from a system; damage to or destruction of physical system assets and environment; damage to or destruction of data or code inside or outside the system; naturally occurring risks.

Organisational security: business continuance; backup/restoration of data; audits; testing procedures e.g. data, network, systems, operational impact of security breaches, WANs, intranets, wireless access systems.

LO2 Describe IT security solutions

IT security solution evaluation:

Network Security infrastructure: evaluation of NAT, DMZ, FWs.

Network performance: RAID, Main/Standby, Dual LAN, web server balancing.

Data security: explain asset management, image differential/incremental backups, SAN servers.

Data centre: replica data centres, virtualisation, secure transport protocol, secure MPLS routing and remote access methods/procedures for third-party access.

Security vulnerability: logs, traces, honeypots, data mining algorithms, vulnerability testing.

LO3 Review mechanisms to control organisational IT security

Mechanisms to control organisational IT security:

Risk assessment and integrated enterprise risk management: network change management, audit control, business continuance/disaster recovery plans, potential loss of data/business, intellectual property, hardware and software; probability of occurrence e.g. disaster, theft; staff responsibilities; Data Protection Act; Computer Misuse Act; ISO 31000 standards.

Company regulations: site or system access criteria for personnel; physical security types e.g. biometrics, swipe cards, theft prevention.

LO4 **Manage organisational security**

Manage organisational security:

Organisational security: policies e.g. system access, access to internet email, access to internet browser, development/use of software, physical access and protection, 3rd party access, business continuity, responsibility matrix.

Controlling security risk assessments and compliance with security procedures and standards e.g. ISO/IEC 17799:2005 Information Technology (Security Techniques – code of practice for information security management); informing colleagues of their security responsibilities and confirming their understanding at suitable intervals; using enterprise risk management for identifying, evaluating, implementing and follow up of security risks according to ISO 31000 standards.

Security: tools e.g. user log-on profiles to limit user access to resources; online software to train and update staff; auditing tools to monitor resource access; security audits; penetration testing; ethical hacking; gathering and recording information on security; initiating suitable actions for remediation.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Assess risks to IT security		**LO1 & 2** **D1** Evaluate a minimum of three of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
P1 Identify types of security risks to organisations. **P2** Describe organisational security procedures.	**M1** Propose a method to assess and treat IT security risks.	
LO2 Describe IT security solutions		
P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs. **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.	**M2** Discuss three benefits to implement network monitoring systems with supporting reasons.	
LO3 Review mechanisms to control organisational IT security		**D2** Consider how IT security can be aligned with organisational policy, detailing the security impact of any misalignment.
P5 Discuss risk assessment procedures. **P6** Explain data protection processes and regulations as applicable to an organisation.	**M3** Summarise the ISO 31000 risk management methodology and its application in IT security. **M4** Discuss possible impacts to organisational security resulting from an IT security audit.	
LO4 Manage organisational security		**D3** Evaluate the suitability of the tools used in an organisational policy.
P7 Design and implement a security policy for an organisation. **P8** List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.	**M5** Discuss the roles of stakeholders in the organisation to implement security audit recommendations.	

Recommended Resources

Textbooks

Alexander, D. et al. (2008) *Information Security Management Principles*. BSC.

Steinberg, R. (2011) *Governance, Risk Management, and Compliance: It Can't Happen to Us – Avoiding Corporate Disaster While Driving Success*. Wiley.

Tipton, H. (2010) *Information Security Management Handbook*. 4th Ed. Auerbach Pubs.

Websites

www.bcs.org	British Computer Society (General Reference)
www.bsa.org.uk	Business Software Alliance (General Reference)
www.fast.org.uk	Federation Against Software Theft (General Reference)
www.ico.gov.uk	Information Commissioners Office (General Reference)

Links

This unit links to the following related units:

Unit 17: Network Security

Unit 23: Cryptography

Unit 24: Forensics

Unit 25: Information Security Management