What Do You Know?

- IS security overview
- Risk Management Strategy
  - Part 1: Risk analysis
  - Breaches, threats, vulnerabilities
  - Part 2: risk mitigation
  - access controls
  - Part 3: security management
  - Security policies and procedures
  - Business continuity plans (BCP) and disaster recovery
  - Part 4: Security Audit and feedback
- E-commerce - Internet security
- Holistic Security design
- Privacy, ethics, and the law
- Current issues and future Trends in IS Security

OVERVIEW

RISK MANAGEMENT

- Risk analysis/assessment
  - Determine critical assets
  - Analyse threats
  - Statistics
  - Current / future trends
  - Establish vulnerabilities

SECURITY FRAMEWORK

goals of IS security

- Confidentiality
- Availability
- Integrity
- Non-repudiation
- Authentication

RISK MANAGEMENT

- Risk mitigation
  - Assess current access controls
  - New access controls
- Security management
  - Security policies
  - Culture
- Business continuity plans (BCP)
- Security audit
  - Detect situations
  - Computer forensics
  - Preserve evidence
  - Re-evaluate access controls and policies
  - Business continuity plans (BCP)
  - Disaster recovery

PART A - COMPULSORY 25 marks

TOPIC:

- E-CRIME – Online Trading Practices
  - Research Conducted By The Australian Government
  - Three questions related to the above report
  - Succinct coherent well structured discussion
  - You must show you have read the report
  - Summarise the survey outcomes

Downloadable off the IMS3110 website

Part B - Short Answer 40 marks

- Answer any FOUR (10 marks each)
- Clarity and structure
- All main issues covered
- Diagrams if asked for will be apportioned marks
- Try to understand what I am looking for

How to get the most value from your short answer!!

- Discuss the statement ........
- Describe the issues ...
- Name and describe ..... 
- Describe the differences ...
- Provide a detailed description outlining...
- Provide reasons why ......
Short Answer Question From Past Exam Paper (10 Marks)

Provide at least five reasons why security threats and breaches to security systems have been increasing over the last 20 years.

Part C – Definitions – 15 marks

You are given 10 key terms - define ONLY 5
- Provide some key terms with which you are familiar
- What are some of the key points about these terms

Pass Requirements

The 40% rule applies to units and determines the final result for a student where the student’s performance in either the examination or assignment component of the unit is unsatisfactory. Students need to be aware of the 40% rule which is:

- In order to pass a unit, a student must gain all of the following:
  - at least 40% of the marks available for the examination component: i.e. the final examination and any tests performed under exam conditions, taken as a whole
  - at least 40% of the marks available for the assignment component: i.e. the assignments and any other assessment tasks (such as presentations) taken as a whole
  - at least 50% of the total marks for the unit
  - Where a student gains less than 40% for either the examination or assignment component, the final result for the unit will be no greater than ‘44’

Exam Preparation

- Analyse each week’s lecture
  - Address the learning objectives for each week
  - What do you think are the major IS security issues
- Think about the main issues I have discussed in lectures
- Mind map using the overview
- You MUST demonstrate higher knowledge by doing additional reading:
  - shown at the end of each set of lecture slides
  - In the reading list
  - In the online discussions
- Prepare model answers to last year’s exam questions
- WARNING:
  - Rewording MY lecture notes will not be sufficient to gain good marks – it could lead to a fail

GOOD LUCK!!

- Check to make sure you have the date and time and location of the exam correct.
- DO NOT TAKE ANY PAPER OR ANYTHING TO WRITE ON – a student was disqualified from the exam last year for cheating