



UNIVERSITI TEKNOLOGI MARA

ASM655: MANAGEMENT OF INFORMATION SECURITY

| | |
|---|--|
| Course Name (English) | MANAGEMENT OF INFORMATION SECURITY APPROVED |
| Course Code | ASM655 |
| MQF Credit | 4 |
| Course Description | The course focuses on the managerial aspects of information security, such as access control models, information security governance, and information security program assessment and metrics. Coverage on the foundational and technical components of information security is included to reinforce key concepts. This course offers a unique overview of information security from a management perspective while maintaining a finger on the pulse of industry changes and academic relevance. This course also reviews some of the recent issues in information security and how to secure information in modern organizations. |
| Transferable Skills | Students able to discuss the concepts of cyber and information security and the key practices and processes for managing security effectively. Students are also capable to apply the practice used in legal, ethical, and regulatory issues that shape policy development and the ways in which organizations implement and administer security. |
| Teaching Methodologies | Lectures, Blended Learning, Case Study, Small Group Sessions , Problem-based Learning |
| CLO | <p>CLO1 Discuss the concepts of cyber and information security and the key practices and processes for managing security effectively</p> <p>CLO2 Apply the access controls and authentication as they are used to secure systems and how they can be mitigated</p> <p>CLO3 Apply the practice used in legal, ethical, and regulatory issues that shape policy development and the ways in which organizations implement and administer security</p> |
| Pre-Requisite Courses | No course recommendations |
| Topics | |
| 1. Introduction To The Management of Information Security | |
| <ul style="list-style-type: none"> 1.1) Introduction To Security 1.2) Key Concepts of Information Security: Threats and Attacks 1.3) Management and Leadership 1.4) Principles of Information Security Management | |
| 2. Compliance: Law and Ethics | |
| <ul style="list-style-type: none"> 2.1) Introduction to Law and Ethics 2.2) Ethics in InfoSec 2.3) Professional Organizations and Their Codes of Conduct 2.4) Information Security and Law 2.5) Organizational Liability and The Management of Digital Forensics | |
| 3. Governance and Strategic Planning for Security | |
| <ul style="list-style-type: none"> 3.1) The Role of Planning 3.2) Strategic Planning 3.3) Information Security Governance 3.4) Planning for Information Security Implementation | |
| 4. Information Security Policy | |
| <ul style="list-style-type: none"> 4.1) Enterprise Information Security Policy 4.2) Issue-specific Security Policy 4.3) System-specific Security Policy 4.4) Guidelines for Effective Policy Development and Implementation | |

| |
|---|
| 5. Developing The Security Program 5.1) Organizing for Security 5.2) Placing Information Security Within an Organization 5.3) Components of The Security Program 5.4) Implementing Security Education, Training and Awareness (SETA) Programs 5.5) Project Management in Information Security |
| 6. Risk Management 6.1) Risk Management 6.2) Introduction to The Management of Risk in Information Security 6.3) The Risk Management Process 6.4) Introduction to Risk Treatment 6.5) Managing Risk 6.6) Alternative Risk Management Methodologies |
| 7. Security Management Models 7.1) Introduction to Blueprint, Framework and Security Models 7.2) Security Management Models 7.3) Security Architecture Models 7.4) Access Control Models 7.5) Academic Access Control Models |
| 8. Security Management Practices 8.1) Introduction to Security Practices 8.2) Security Employment Practices 8.3) Information Security Performance Measurement 8.4) Benchmarking |
| 9. Planning for Contingencies 9.1) Introduction to Contingency Planning 9.2) Incident Response 9.3) Disaster Recovery 9.4) Business Continuity 9.5) Crisis Management 9.6) Business Resumption 9.7) Testing Contingency Planning |
| 10. Security Maintenance 10.1) Introduction to Security Maintenance 10.2) Security Management Maintenance Models |

| | | | | |
|---|---|---|------------------------|------------|
| Assessment Breakdown | | % | | |
| Continuous Assessment | | 100.00% | | |
| Details of Continuous Assessment | Assessment Type | Assessment Description | % of Total Mark | CLO |
| | Assignment | Group Assignment | 20% | CLO2 |
| | Case Study | Individual Case Study | 20% | CLO2 |
| | Group Project | Group Project | 40% | CLO3 |
| | Test | Test | 20% | CLO1 |
| Reading List | Recommended Text | <ul style="list-style-type: none"> • Michael E. Whitman, Herbert J. Mattford 2018, <i>Management of Information Security</i>, 6th Edition Ed., Cengage Singapore [ISBN: 9789814834735] | | |
| | Reference Book Resources | <ul style="list-style-type: none"> • Michael E. Whitman, Herbert J. Mattford 2013, <i>Management of Information Security</i>, 4th Edition Ed., Cengage Learning [ISBN: 9781285062297] • Alan, C. and Steve, W. 2008, <i>IT Governance: A Manager's Guide to Data Security</i>, 3rd edition Ed. • William, S. and Lawrie, B. 2016, <i>Computer Security: Principles and Practice</i>, Pearson • David, B., Patrick, S., and Michael, S. 2011, <i>Applied Information Security: A Hands-on Approach</i> | | |
| Article/Paper List | This Course does not have any article/paper resources | | | |
| Other References | This Course does not have any other resources | | | |