MACS H6013: Business Continuity Management

Short Title:	Business Continuity Management APPROVED
Full Title:	Business Continuity Management

Module Code:	MACS H6013

ECTS credits:	10

NFQ Level:	9

Module Delivered in	2 programme(s)

Module Contributor:	Christina Thorpe

Module Description:	The purpose of this module is twofold: Firstly, to help the students to acquire an extremely thorough understanding of a globally recognised methodology for implementation and maintenance of Business Continuity Management (BCM) programs. On completion of the course, students should have acquired the skills and understanding to be able to participate in BCM programs and BC projects for an organisation. This module will introduce the essential steps of developing BC and Disaster Recovery (DR) strategies, design and implementation of BC plans, preparing and conducting awareness and training programmes. Students will acquire the essential skills and knowledge of project management, risk analysis and review, Business Impact Analysis (BIA), recovery strategy, plan development, and testing and exercising. Secondly, given the significant penetration of Cloud computing in recent years, this module will help the students gain an awareness of the security threats and best practices for securing the Cloud. The concept of Cloud computing continues to evolve, this module provides students with the latest information on new areas of focus in the changing Cloud security landscape. Amazon AWS will be used as a case study to demonstrate the important role the Cloud will have in the future of business continuity and disaster recovery. For example, students will investigate how S3 and Glacier can be used as backup solutions.

Learning Outcomes:

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

1. Identify and appraise the risks and their potential impact using appropriate data gathering methods.
2. Evaluate the benefits of BCM and construct an argument for implementing BCM in an organisation i.e., to obtain 'Executive Buy-in'.
3. Analyse a business and develop efficient plans for business continuity and disaster recovery to meet business needs.
4. Design and implement strategies and systems for protecting critical information assets in the Cloud.

Module Content & Assessment

Indicative Content
Introduction Introduction to business continuity and disaster recovery in IT environments. Scanning the risk horizon to investigate the changing nature and impact of risk and how it impacts on business continuity.
Understanding the Standards Why standards are necessary. A historical view and the evolution of the standards. Examining the key standards in the area of business continuity and disaster recovery. Comparing the various standards. Considerations when using standards.
Risk Evaluation and Control Understanding risk. The risk assessment process. Options for risk management. Risk identification and measurement. Risk standards. A detailed look at risk assessment in different industries, e.g., Health and safety, finance, health care, etc. Critical component failure analysis. Operational risk management. Output approach to risk. Site and security risk areas. Suppliers risk areas.
Business Impact Analysis Why and how to conduct a BIA. Data collection methods. Critical Success factors. Key performance indicators. SLAs. Desk review of documentation. Questionnaires. Interviews. Workshops. Impact matrix. RTO and RPO.
Developing Continuity Strategies Why it is necessary. Options: backups, alternative sites, quick resupply, offsite storage, buying in or outsourcing. Option comparison. ICT recovery strategies: continuous processing, virtualisation, Cloud. Contractual arrangements.
Emergency Response and Operations Define 'Emergency Response'. Incident management. Emergency services. Public authorities. Roles. Combined response. Salvage and restoration. Public relations and crisis communication.
Developing and Implementing the Plan Defining the scope. Developing the plan. Procedure driven planning. Decision driven planning. Planning considerations. BC terms. Tasks actions and functions. Roles and responsibilities. Alternative locations. Contact details. Vital documents and materials. Resource requirements. Reporting process. Audit trail. Software tools and formats.
Auditing, Maintaining, and Exercising the Plan Plan audit. Difference between testing and exercising. Why exercises are necessary. Exercise strategy and methods. Reporting. Plan review and maintenance. Tools.
BCDR in the Cloud Case study of AWS to demonstrate the important role the Cloud will play in the future of BCDR. Practical exercises with S3 and Glacier for backup. Investigate AWS Elastic Block Store for creating snapshots of data volumes. AWS import/export for rapid migration of large data sets into and out of the Cloud. AWS storage gateway.
Cloud Architecture Definition of Cloud Computing (Essential Characteristics, Cloud Service Models, Cloud Deployment Models), Multi-Tenancy, CSA Cloud Reference Model, Jericho Cloud Cube Model, Cloud Security Reference Model, Cloud Service Brokers, Service Level Agreements
Legal Issues: Contracts and Electronic Discovery Consideration of cloud-related issues in three dimensions, eDiscovery considerations, Jurisdictions and data locations, Liability for activities of subcontractors, Due diligence responsibility, Federal Rules of Civil Procedure and electronically stored information.
The Future of BCM Research the current state of the art in BCM and Cloud and propose a likely direction or trend that may be seen in the near future. Take a deep dive into a selection of recently published papers to aid discussion.

Indicative Assessment Breakdown	%
Course Work Assessment %	100.00%

Course Work Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Presentation	Preplanning Activities: Give a 10min presentation to the executive management committee to convince them to invest in BCM. Conduct a Business Impact Analysis and present the results.	2	30.00	Week 5
Project	Business Continuity & Disaster Recovery Plan and Presentation.	1,3	35.00	Week 9
Project	Develop and secure a Cloud application.	4	35.00	Sem 1 End

No Final Exam Assessment %

Indicative Reassessment Requirement
Coursework Only *This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.*

ITB reserves the right to alter the nature and timings of assessment

Indicative Module Workload & Resources

Indicative Workload: Full Time	
Frequency	**Indicative Average Weekly Learner Workload**
Every Week	30.00
Every Week	30.00
Every Week	140.00

Resources

Recommended Book Resources

Andrew N. Hiles (Author), Kristen Noakes-Fry (Editor) 2014, *Business Continuity Management: Global Best Practices*, 4th Ed.

j Samani (Author), Jim Reavis (Contributor), Brian Honan (Contributor) 2014, *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security*

This module does not have any article/paper resources

Other Resources

Internet based resource: *Disaster recovery 1*
http://www.disaster-recovery-guide.com/

Internet based resource: *Disaster recovery 2*
http://en.wikipedia.org/wiki/Seven_tiers_of_disaster_recovery

Whitepaper: AWS 2014, *AWS Disaster Recovery*, Amazon
http://media.amazonwebservices.com/AWS_D isaster_Recovery.pdf

Module Delivered in

Programme Code	Programme	Semester	Delivery
BN_KMACS_R	Master of Science in Computing in Applied Cyber Security	2	Elective
BN_KMACS_M	Master of Science in Computing in Applied Cyber Security (Research)	1	Group Elective 3