ENTERPRISE CYBER RISK MANAGEMENT, BUSINESS CONTINUITY AND DISASTER RECOVERY COURSE

Introduction

The Enterprise Cyber Risk Management, Business Continuity and Disaster Recovery programme is designed to equip senior managers, risk professionals, ICT leaders, business continuity coordinators and operational decision-makers with the capabilities required to identify cyber-related threats, protect critical business services and maintain organisational operations during disruptive events. Organisations face a wide range of disruptions, including ransomware attacks, system failures, data loss, cloud service outages, supplier incidents, infrastructure damage and interruptions to essential utilities. Such events can affect revenue, customer service, public service delivery, regulatory compliance and institutional reputation. Effective resilience therefore requires an integrated approach that connects cyber risk management with business impact analysis, continuity planning, disaster recovery and executive crisis management. The programme examines how organisations can identify critical assets and services, evaluate cyber and operational risks, establish risk treatment priorities and develop realistic recovery arrangements. Participants explore enterprise risk assessment, business impact analysis, recovery time objectives, recovery point objectives, backup strategies, alternate operating arrangements and disaster recovery testing. The course also considers ransomware preparedness, third-party dependencies, cloud resilience, crisis communication and the coordination of technical and business recovery activities. Particular attention is given to the relationship between business continuity plans and ICT disaster recovery plans, ensuring that technology recovery supports the actual priorities of the organisation.

Course Objectives

- Explain the relationship between enterprise cyber risk, business continuity and disaster recovery.

- Identify critical organisational assets, processes, systems and service dependencies.
- Conduct cyber risk assessments and develop risk treatment priorities.
- Undertake business impact analysis and determine recovery priorities.
- Define recovery time objectives (RTOs) and recovery point objectives (RPOs).
- Develop and maintain business continuity and ICT disaster recovery plans.
- Evaluate backup, restoration, redundancy and alternative operating arrangements.
- Coordinate cyber incident response, crisis management and business recovery.
- Design testing, simulation and continuous improvement programmes for resilience plans.
- Develop an integrated cyber risk management and organisational resilience roadmap.

Course Modules

> Module 1: Foundations of Enterprise Cyber Risk and Resilience
- Understanding enterprise risk management and cyber risk exposure.
- Relationships among cybersecurity, operational risk and organisational resilience.
- Identifying critical business services and technology dependencies.
- Establishing risk ownership, accountability and resilience objectives.

> Module 2: Cyber Risk Identification and Assessment
- Identifying threats, vulnerabilities and potential business consequences.
- Assessing ransomware, data loss, system failure and supplier disruption.
- Evaluating risk likelihood, impact and existing control effectiveness.
- Developing cyber risk registers, risk ratings and treatment prioriti

> Module 3: Risk Treatment and Resilience Controls
- Risk avoidance, reduction, transfer and acceptance.
- Selecting preventive, detective and recovery controls.
- Evaluating redundancy, system resilience and security safeguards.
- Monitoring residual risks, control gaps and corrective actions.

> Module 4: Business Impact Analysis and Recovery Priorities
- Identifying critical processes, products and services.
- Assessing financial, operational, legal and reputational impacts.
- Determining maximum tolerable disruption and recovery priorities.
- Establishing recovery time objectives and recovery point objectives.

> Module 5: Business Continuity Planning and Management
- Principles and components of a business continuity management system.
- Developing continuity strategies for critical functions.
- Alternative work arrangements, manual workarounds and resource planning.
- Defining roles, escalation arrangements and continuity plan activation criteria.

> Module 6: ICT Disaster Recovery and Data Protection
- Disaster recovery architecture and recovery environment design.
- Backup strategies, restoration procedures and data integrity verification.
- Cloud recovery, replication, redundancy and alternate infrastructure.
- Developing and documenting ICT disaster recovery procedures.

> Module 7: Cyber Incidents, Crisis Management and Communication
- Integrating cyber incident response with business continuity arrangements.
- Crisis leadership, incident escalation and emergency decision-making.
- Internal communication and coordination with customers, suppliers and regulators.
- Managing ransomware, data breaches and extended service outages.

> Module 8: Third-Party Risk and Operational Dependencies
- Identifying critical suppliers, outsourced services and technology dependencies.
- Assessing supplier continuity capabilities and recovery commitments.
- Business continuity requirements in contracts and service-level agreements.
- Developing contingency arrangements for supplier failure and service interruption.

> Module 9: Testing, Exercising and Continuous Improvement
- Tabletop exercises and scenario-based continuity simulations.
- Testing backups, restoration procedures and disaster recovery arrangements.
- Evaluating recovery performance against RTOs and RPOs.
- Documenting lessons learned and updating plans after exercises or incidents.

> Module 10: Cyber Risk and Organisational Resilience Capstone
- Conducting a preliminary cyber risk and business impact assessment.
- Identifying critical services and establishing recovery priorities.
- Preparing an integrated business continuity and disaster recovery action plan.
- Presenting a resilience roadmap with responsibilities, testing schedules and performance indicators.

P.O Box 7254- 01000
www.trustgatecorporateskills.co.ke
Location Thika & Nairobi