EC-Council | Academia



EC-Council Disaster Recovery Professional Version 4

Lesson Plan

Comprehensive Disaster Recovery & Business Continuity Certification

EC-Council | Disaster Recovery Professional

OFFICIAL **EC-COUNCIL** CERTIFICATION GUIDE

(Certification Exam: 312-76)

EC-Council | Academia

EC-Council Academia

Student Course Syllabus

EC-Council Disaster Recovery Professional (EDRP) v4

Instructor Contact Information

Instructor Name:		**Office Location:**	
Email:		**Phone:**	
Office Hours:			

1. Purpose of the Class

This course is designed to equip learners with the knowledge and practical skills required to build resilient organizations through effective Business Continuity and Disaster Recovery (BCDR) planning. Participants will learn the concept of Business Continuity Management (BCM), Business Impact Analysis (BIA), risk assessment, disaster recovery planning, crisis management, governance, compliance, and operational resilience. The course also explores modern technologies such as cloud computing, virtualization, automation, and AI in disaster recovery. By the end of the course, learners will be able to develop, implement, and continuously improve BCDR strategies that minimize business disruption and ensure organizational resilience.

2. Course Objectives

Upon successful completion of this course, the students will be able to:

1. Understand Business Continuity and Disaster Recovery (BCDR) concepts, regulatory influences, and strategic importance, while evaluating best practices and the role of emerging technologies, including AI, in enhancing organizational resilience.
2. Understand Business Continuity Management (BCM), including its lifecycle, core elements, governance, and regulatory requirements, while evaluating the role of AI, Zero Trust, and organizational integration in strengthening operational resilience.
3. Understand the concepts, categories, and lifecycle of risk assessment, including its relationship to BCM and IT disaster recovery, to identify, evaluate, and prioritize business and technology risks effectively.

4. Understand risk treatment, dependency mapping, cascading risks, and risk prioritization methods to support informed continuity, recovery, and resilience decisions across the organization.
5. Understand the scope, purpose, assumptions, and analytical foundations of Business Impact Analysis (BIA), including how AI-enhanced techniques support the identification and prioritization of critical business functions, dependencies, and recovery requirements.
6. Understand how to conduct, validate, and communicate a defensible BIA using qualitative and quantitative methods to translate business impact findings into actionable recovery and resilience decisions.
7. Understand the purpose, structure, and development of a Business Continuity Plan, including continuity strategies, incident response, communication, recovery planning, and the use of AI to support resilience in AI-dependent operations.
8. Understand the foundational concepts, inputs, risks, and strategies of IT Disaster Recovery Planning, including the role of AI in supporting recovery, data protection, and operational resilience.
9. Understand the principles and mechanisms of data backup and system recovery, including recovery types, technologies, and AI-enabled validation.
10. Understand the recovery best practices, governance, and cost-aware decision-making to improve operational readiness across diverse infrastructure environments.
11. Understand how to design and maintain an effective disaster recovery plan that aligns recovery priorities, roles, procedures, and AI-supported automation to minimize disruption and strengthen resilience.
12. Understand the criteria, activation process, coordination structure, and crisis communication requirements for business continuity and disaster recovery plan activation to enable timely and controlled response during disruptive events.
13. Understand the methods, metrics, and maturity practices used to test, train, and exercise business continuity and disaster recovery plans so that readiness can be validated, improved, and sustained in changing operational environments.

3. EDRP Grading Policy

The academic credit used in EDRP is based on twelve-week courses that constitute 3 credits per course. Each course entails approximately 100 hours of work (reading, Online Discussion Forum postings, assignments, papers, and supplementary requirements).

Point-grade breakdown:

The EDRP course grading structure follows the academic grading symbols and quality points earned.

Percentage	Points	Grade	Comments	Quality Points Earned
90–100%	360–400	A	Superior Attainment of Course Outcomes	4.0
80–89%	320–359	B	Good Attainment of Course Outcomes	3.0
70–79%	280–319	C	Acceptable Attainment of Course Outcomes	2.0
60–69%	240–279	D	Poor Attainment of Course Outcomes	1.0
0–59%	000–239	F	Non-Attainment of Course Outcomes	0.0

4. EDRP Grading Structure

S. No.	Assessment	Details	Points
1	**Course Discussion Threads**	There are 17 discussion threads (each worth 4 pts.)	**68**
2	**Assignments from Reading**	There are 17 assignments from reading (each assignment is worth 6 pts.)	**102**
3	**Lab Assignments**	There are 6 lab assignments (each worth 4 pts.)	**24**
4	**Course Quizzes**	There are 56 quiz questions (each worth 1 pt.)	**56**
5	**Research Project**	There is 1 research project (worth 50 pts.)	**50**
6	**Final Exam**	There is 1 final exam (worth 100 pts.)	**100**
Total Points:			**400**

NOTE: Each week, you will have assessments that you must complete for class credit.

5. EDRP Program Objectives

1. Application of business continuity and disaster recovery principles, strategies, and best practices to ensure organizational resilience and operational continuity.
2. Ability to identify, assess, and mitigate risks through effective risk assessment and business impact analysis.
3. Development, implementation, and maintenance of Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) aligned with industry standards and regulatory requirements.
4. Application of critical thinking and structured decision-making to prepare for, respond to, and recover from disruptive incidents while minimizing business impact.
5. Understanding and application of emerging technologies, including Artificial Intelligence

(AI), to enhance continuity planning, disaster recovery, and organizational resilience.

6. Learning Standards

Four Standards of Performance

Always use these standards of performance when writing a research paper, responding to a case study, or responding in a discussion thread.

These four standards of performance, when used properly, will produce an excellent paper.

1. **Depth of reflection**: Demonstrate a conscious and thorough understanding of the writing prompt and subject matter. Analyze the evidence from several perspectives, draw conclusions based on evidence, research, and/or experience.
2. **Sequence your information:** Your work must have a clear and appropriate beginning, development, and conclusion. Most information should be organized in a clear and logical manner, with a beginning and a conclusion. Paragraphing and transitions should be adequate.
3. **Conclusions:** Draw conclusions based on evidence, research, or experience. Use the context of your reading and the assumptions the author makes.
4. **Language use**: Use sophisticated language that is precise and interesting. Sentences must be grammatically correct.

7. Additional Notes and Expectations

Attendance

Documenting Attendance in Distance Education Courses

Changes to federal regulations in recent years have highlighted the importance of accurate reporting on student attendance and participation in all courses, including distance education courses (online and hybrid/blended courses).

For compliance, we provide the following procedural guidance to faculty when filling out non-participation rosters. A student attends an online course (or the online portion of a hybrid/blended course) by participating in class or otherwise engaging in an academically related activity. Examples of such activity include but are not limited to the following:

1. Contributing to an online discussion or text chat session
2. Submitting an assignment or working draft; working through exercises
3. Taking a quiz or exam
4. Viewing and/or completing a tutorial
5. Initiating contact with a faculty member to ask a course-related question

Such academically related activities are readily tracked and documented through the University learning management system; email system; and in some cases, publisher websites. Documenting that a student has logged into an online class or website is not sufficient, by itself, to demonstrate academic attendance by the student. For example, if a student simply logs into

an online course on September 15 and logs out without any further activity, the student did not attend the online class on that day.

Late Assignments Late assignments are not in the student's best interest. In this regard, if you face a problem that will prevent you from completing assignments in a timely manner, please send the instructor a deadline extension requests immediately with an explanation. The instructor can accept or reject the student's request based on their discretion. Continued requests will not be accepted, and the student may be dropped from the course at the instructor's request.

Writing Skills If your writing skills require improvement, there are some modules under "Student Orientation" in the learning management system (LMS) that can help you prepare for your writing process. Alternatively, you may purchase a basic writing skills book.

ACADEMIC HONESTY POLICY

Course Policies on Cheating and Plagiarism

As a model of the highest ethical standards and as an institution of higher learning, the University expects its students to conduct themselves with an unquestionable level of honesty and integrity. The University will not tolerate academic cheating or plagiarism in any form. Learning to think and work independently is not only a part of the educational process; it is the educational process. Cheating or plagiarism in any form is considered a serious violation of University policy, which each student agreed to when accepted into the program. Academic behaviors that violate the University policy will result in disciplinary action, without exception.

Some examples of cheating and plagiarism include but are not limited to the following:

Cheating	Use of material, information, or study aids not permitted by the faculty
Plagiarism	Use of another's words or ideas without acknowledging the source of the information
Falsification or Fabrication	Changing or altering data, quotes, citations, grades, or academic records
Unauthorized Collaboration	Intentional sharing of information when the faculty does not approve of such collaboration

The University will take action in all cases of academic dishonesty. The first instance will result in a failing grade for the assignment. The second instance will result in a failing grade in the course. The third instance will result in dismissal from the University. A record of all instances of academic dishonesty at the University, as well as a record of the action taken, will be kept in the individual student file and Dean's file.

1. The following steps will be taken in the event of academic dishonesty. The faculty/staff will inform the student of the allegation and provide evidence, offering the student the opportunity to respond and/or rectify the issue depending on the nature of the dishonesty and the particular assignment.
2. Once the student has had a chance to respond, the faculty/staff will determine whether academic dishonesty has occurred. If the faculty/staff concludes that academic dishonesty has occurred and has proof, they will report the student's name, class and assignment, nature of the academic dishonesty, and proof to the Dean. The type of disciplinary action to be taken will be determined by the student's record of instances identified above, and the disciplinary action will be taken by the faculty and/or the Dean.

Citing Sources

In academic communities, the ethics of research demand that writers be credited for their work. To not do so is to plagiarize, i.e., to appropriate the ideas, language, or work of another intentionally or unintentionally without sufficient acknowledgement that such material is not one's own. Whenever a student quotes, paraphrases, summarizes, or otherwise refers to the work of another, the student must cite their source either by way of a parenthetical citation or footnote. Unfortunately, this is the most common form of academic dishonesty. Regardless, it will be responded to with failing grades or dismissal, as detailed above.

Original Content

The majority of discussion topics, assignments, and essays created by students are expected to stem from their own personal thoughts and ideas. A minimum of 75% of all work must be original. Any submitted work that contains more than 25% unoriginal work, regardless of whether the sources are cited properly, may be considered a violation of the academic honesty policy, depending on the nature of the assignment and the opinion of the assigned instructor.

Timeline

A violation of the academic honesty policy can be discovered at any time. The issuance of a grade, or even a degree, can be changed if a violation is discovered. *The bottom line is this: it is just not worth it.*

Student Identity Verification

- The university takes measures to verify the identity of students who are applying to the university, completing courses, and taking proctored exams.
- Students access their courses and reference materials through our secure online learning management system, where they are required to enter their username and password. Students are responsible for safeguarding their individual credentials.
- The University implements student identity verification in several ways to ensure proper identification.

  1. A valid government-issued ID is required for admissions application.
  2. Login credentials are required for the online LMS portal.

8. Texts Required Throughout This Course

The following texts are required for this course:

- EC-Council Disaster Recovery Professional (EDRP) v4 Academia Series

These are embedded in the General Section of your course. The corresponding chapters for each week are embedded in your weekly reading material.

9. Scheduled Outline of Course Topics

WEEK ONE:

MODULES COVERED:

- Module 01 - Foundations of Business Continuity and Disaster Recovery

WEEK 1 - WEEKLY OBJECTIVES:

- Understand Business Continuity and Disaster Recovery (BCDR) concepts, regulatory influences, and strategic importance, while evaluating best practices and the role of emerging technologies, including AI, in enhancing organizational resilience.

WEEK 1 - ASSESSMENTS:

The course includes the following assessments under Week One.

- Discussion Threads: 1 discussion thread (each worth 4 pts.)
- Assignments from Reading: 1 reading assignments (each worth 6 pts.)
- Quizzes: 5 quiz questions (each worth 1 pt.)

WEEK 1 - DISCUSSION THREAD:

- Discuss the differences between BC and DR, and how regulations, best practices, and AI technologies are strengthening organizational resilience and modern continuity planning.

WEEK 1 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 01 - Foundations of Business Continuity and Disaster Recovery

WEEK 1 - ASSIGNMENTS FROM READING:

- Analyze how Business Continuity and Disaster Recovery improve organizational resilience.

WEEK 1 - QUIZ:

1. Which process identifies critical business functions and the impact of a disruption on them?
    a. Crisis Management
    b. Risk Assessment
    c. Business Impact Analysis
    d. Business Continuity Management

2. Which regulation specifically focuses on mitigating ICT risk to ensure operational resilience in the EU financial sector?
    a. SOX
    b. HIPAA
    c. PCI DSS
    d. DORA
3. Which AIOps capability identifies the source of a failure by correlating operational data?
    a. Predictive impact analysis
    b. Automated dependency discovery
    c. Root cause analysis
    d. Recovery analytics
4. Which emerging technology provides a safe environment for testing recovery plans and performing scenario analysis?
    a. Predictive Risk Analytics
    b. AI-Powered Monitoring
    c. Autonomous Recovery
    d. Digital Twins
5. Which technology combines AI, Machine Learning, automation, and operational analytics to automate IT and recovery operations?
    a. AIOps
    b. Generative AI
    c. AI-Powered Monitoring
    d. Digital Twins

WEEK 1 - ADDITIONAL RESOURCES:

White Papers:

- Sharpening Your Business Resilience Strategy: https://www.protect.airbus.com/wp-content/uploads/2025/10/15-10-2025_whitepaper_cyberresilience.pdf
- An Essential Guide to Backup Disaster Recovery and Preparation from an IT Perspective: https://www.scalecomputing.com/documents/White-Papers/Business-Resilience-Best-Practices.pdf

Videos:

- What are Business Continuity Plans and Disaster Recovery Plans?: https://www.youtube.com/watch?v=B4APySh4JL0
- Standard vs Framework vs Laws vs Regulations | TrustTalks - Ep 22 | Security and GRC Podcast: https://www.youtube.com/watch?v=gP776qsa4EU
- Operational resilience: https://www.youtube.com/watch?v=M0lFgFHLtlg
- Microsoft Sovereign Cloud Core Customer Scenarios: Business Continuity: https://www.youtube.com/watch?v=zQHKnpsutZU

WEEK TWO:

MODULES COVERED:

- Module 02 - Business Continuity Management

WEEK 2 - WEEKLY OBJECTIVES:

- Understand Business Continuity Management (BCM), including its lifecycle, core elements, governance, and regulatory requirements, while evaluating the role of AI, Zero Trust, and organizational integration in strengthening operational resilience.

WEEK 2 - ASSESSMENTS:

The course includes the following assessments under Week Two.

- Discussion Threads: 2 discussion threads (each worth 4 pts.)
- Assignments from Reading: 2 reading assignments (each worth 6 pts.)
- Quizzes: 6 quiz questions (each worth 1 pt.)

WEEK 2 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 02 - Business Continuity Management

WEEK 2 - DISCUSSION THREAD:

- Discuss the purpose of BCM, its core components and lifecycle, and how AI governance supports organizational resilience and continuity operations.
- Discuss the importance of Zero Trust, legal and regulatory compliance, organizational roles, documentation, and integrating BCM into daily operations to establish a resilient business culture.

WEEK 2 - ASSIGNMENTS FROM READING:

- Explain how Business Continuity Management enables organizations to prepare for and recover from disruptions.
- Evaluate the importance of governance and continuous improvement in sustaining Business Continuity Management programs.

WEEK 2 - QUIZ:

1. Which BCM function focuses on satisfying regulatory, contractual, and audit expectations?
    a. Protective Function
    b. Enabling Function
    c. Strategic Function
    d. Compliance Function

2. Which threat modeling technique estimates cascading effects across the business over time?
    a. Scenario Modeling
    b. Impact Modeling
    c. Probability and Severity Modeling
    d. Stress Testing and "What-if" Analysis
3. Which phase of the PDCA cycle establishes recovery objectives such as RTO, RPO, and MTPD?
    a. Do
    b. Check
    c. Act
    d. Plan
4. Which AI governance framework emphasizes governance, risk management, reliability, security, and resilience?
    a. EU AI Act
    b. DORA
    c. GDPR
    d. NIST AI RMF
5. Which recovery component is restored before business applications to establish authentication and access control?
    a. Business applications
    b. Backup repositories
    c. Network services
    d. Identity services
6. Which Zero Trust principle limits the ability of attackers to move across systems and networks?
    a. Explicit Verification
    b. Least Privilege Access
    c. Micro-Segmentation
    d. Assume Breach

WEEK 2 - ADDITIONAL RESOURCES:

White Papers:

- Business Continuity Management: https://www.sas.com/content/dam/sasdam/documents/20250124/business-continuity-management.pdf
- Achieving IT Resilience: https://gtnwebsitestagingstorage.blob.core.windows.net/cms-assets-staging/Media/PDF-Files/Getronics_BusinessContinuity_Whitepaper.pdf?v=1781793055

Videos:

- What is Business Continuity Management (BCM)? | Complete Guide for Auditors & Risk Professionals: https://www.youtube.com/watch?v=1_KuRuPcPJ8&t=13s
- Securing Digital Trust: How AI is Redefining Organizational Resilience - Ajay Gupta: https://www.youtube.com/watch?v=cGs9wlQj5eM
- How to Conduct a Business Impact Analysis to Reduce Your Risk of Operational Disruptions: https://www.youtube.com/watch?v=jkUCL9tdPXw
- ISO 22301 Business Continuity Management Systems: https://www.youtube.com/watch?v=fDzIgKYjpUA&t=10s

WEEK THREE:

MODULES COVERED:

- Module 03 - Risk Assessment

WEEK 3 - WEEKLY OBJECTIVES:

- Understand the concepts, categories, and lifecycle of risk assessment, including its relationship to BCM and IT disaster recovery, to identify, evaluate, and prioritize business and technology risks effectively.
- Understand risk treatment, dependency mapping, cascading risks, and risk prioritization methods to support informed continuity, recovery, and resilience decisions across the organization.

WEEK 3 - ASSESSMENTS:

- The course includes the following assessments under Week Three.
- Discussion Threads: 3 discussion threads (each worth 4 pts.)
- Assignments from Reading: 3 assignments from reading (each worth 6 pts.)
- Lab Assignments: 1 lab assignment (each worth 4 pts.)
- Quizzes: 7 quiz questions (each worth 1 pt.)

WEEK 3 - DISCUSSION THREAD:

- Discuss the role of risk assessment in BCM and IT DR, including risk categories, recovery objectives (MTD, RTO, and RPO), and AI-specific risk considerations.
- Discuss the risk assessment lifecycle, the responsibilities of stakeholders, risk identification techniques, dependency mapping, and the importance of maintaining risk documentation.
- Discuss risk treatment strategies, mitigation approaches, and methods for prioritizing risks based on likelihood, impact, and time to support effective BC/DR decisions.

WEEK 3 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 03 - Risk Assessment

WEEK 3 - ASSIGNMENTS FROM READING:

- Analyze how risk management supports business continuity and disaster recovery planning.
- Evaluate the importance of understanding dependencies, risk impacts, and organizational interconnections in strengthening resilience and recovery capabilities.
- Discuss how risk treatment, prioritization, and continuous monitoring support informed continuity and disaster recovery decision-making.

WEEK 3 - LAB ASSIGNMENTS:

Week 3 Lab Assignment 1: Qualitative Risk Assessment Using MONARC

Lab Scenario

An organization is preparing to assess information security risks across a business unit that handles sensitive operational data. The security team wants to identify key assets, evaluate likely threats and vulnerabilities, and estimate the potential business impact of risk scenarios in a structured way.

Lab Objective

In this lab, you will perform a qualitative risk assessment using MONARC by creating or opening a risk analysis, defining the scope and business context, identifying assets and associated scenarios, evaluating likelihood and impact qualitatively, reviewing the resulting risk levels, and documenting the assessment output for further treatment planning. This aligns with MONARC training objectives that focus on learning the tool's main functions and conducting risk analysis based on the method

WEEK 3 - QUIZ:

1. Which AI-specific risk results from becoming dependent on proprietary AI platforms or services, making migration to an alternative provider difficult?
    a. AI Service Availability Risk
    b. AI Governance Risk
    c. AI Model Risk
    d. Vendor Lock-In
2. Which recovery objective defines the maximum acceptable amount of data loss following a disruption?
    a. Maximum Tolerable Period of Disruption (MTPD)
    b. Recovery Time Objective (RTO)
    c. Business Impact Analysis (BIA)
    d. Recovery Point Objective (RPO)
3. Which step of the risk assessment lifecycle defines continuity strategies, IT disaster recovery solutions, and recovery capabilities?
    a. Analyze Risks
    b. Evaluate and Prioritize Risks
    c. Treat Risks
    d. Monitor and Review Risks

4. Which executive responsibility establishes the amount and type of risk an organization is willing to pursue or retain?
    a. Risk acceptance
    b. Risk tolerance
    c. Risk appetite
    d. Residual risk
5. Which risk identification technique relies on cross-functional participation to identify enterprise-wide risks?
    a. Incident and Near-Miss Analysis
    b. Architecture and Dependency Review
    c. Scenario-Based Analysis
    d. Facilitated Workshops
6. Which risk identification error most commonly prevents organizations from recognizing cascading failures across business services?
    a. Treating risks as isolated events
    b. Underestimating speed and non-linear impacts
    c. Ignoring data and integrity cascades
    d. Relying on static dependency models
7. Which visual tool plots risks using likelihood and impact to communicate an organization's risk posture?
    a. Risk Register
    b. Risk appetite
    c. Risk Scoring
    d. Risk Heat Map

WEEK 3 - ADDITIONAL RESOURCES:

White Papers:

- RISK MANAGEMENT STRATEGY: https://cdn.who.int/media/docs/default-source/documents/ethics/who-risk-management-strategy.pdf
- Recovery Point Objective (RPO) and Recovery Time Objective (RTO): https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/eb-rto-rpo-quick-guide.pdf

Videos:

- How to Conduct a Risk Assessment: https://www.youtube.com/watch?v=eObdoQtWw9M
- RTO and RPO explain | RTO and RPO in Disaster Recovery: https://www.youtube.com/watch?v=SQPTygQOV8Q
- Webinar: Business Continuity Management: Impact Analysis and Risk Assessment: https://www.youtube.com/watch?v=awLn7yZDKXs&t=147s
- Risk Mitigation Strategies in Disaster Recovery (DR) Planning: https://www.youtube.com/watch?v=-drcrCeQsHw

WEEK FOUR:

MODULES COVERED:

- Module 04 - Business Impact Analysis

WEEK 4 - WEEKLY OBJECTIVES:

- Understand the scope, purpose, assumptions, and analytical foundations of Business Impact Analysis (BIA), including how AI-enhanced techniques support the identification and prioritization of critical business functions, dependencies, and recovery requirements.
- Understand how to conduct, validate, and communicate a defensible BIA using qualitative and quantitative methods to translate business impact findings into actionable recovery and resilience decisions.

WEEK 4 - ASSESSMENTS:

- The course includes the following assessments under Week Four.
- Discussion Threads: 2 discussion threads (each worth 4 pts.)
- Assignments from Reading: 2 assignments from reading (each worth 6 pts.)
- Quizzes: 7 quiz questions (each worth 1 pt.)

WEEK 4 - DISCUSSION THREAD:

- Discuss the purpose and scope of BIA, its relationship with risk assessment, and how AI helps identify critical business functions, dependencies, and recovery requirements.
- Discuss the BIA process, evaluation techniques, recovery objectives, and how BIA findings support recovery planning and organizational resilience.

WEEK 4 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 04 - Business Impact Analysis

WEEK 4 - ASSIGNMENTS FROM READING:

- Analyze how Business Impact Analysis supports the identification of critical functions and recovery requirements.
- Evaluate the importance of Business Impact Analysis findings in supporting recovery and resilience decisions.

WEEK 4 - QUIZ:

1. Which core element of BIA scope defines the business functions, processes, and services included in the analysis?
    a. Organizational coverage
    b. Geographic and operational boundaries
    c. Supporting resources and dependencies
    d. Subject of analysis
2. Which BIA process step ensures that impact ratings are applied consistently across different business units before recovery requirements are finalized?
    a. Planning and Preparation
    b. Definition of Recovery Requirements
    c. Resource and Dependency Analysis
    d. Normalization and Validation
3. Which AI-related consideration recognizes that business processes may become less effective even when supporting systems remain operational?
    a. AI infrastructure and residency
    b. AI output integrity and trustworthiness
    c. Third-party AI resilience
    d. AI-augmented process dependency
4. Which recovery objective is most likely to be over-engineered if business impact tolerance is not established before technical recovery planning begins?
    a. MTPD
    b. MASL
    c. RPO
    d. RTO
5. Which BIA consideration may elevate an otherwise moderate business function to a critical recovery priority despite having limited financial impact?
    a. Mission-critical services and customer commitments
    b. Organizational size, structure, and complexity
    c. Risk appetite and tolerance for disruption
    d. Industry, regulatory, and contractual obligations

6. Which evaluation technique is specifically intended to reduce false precision when reliable impact data is unavailable?
    a. Proxy metrics
    b. Scenario bounding
    c. Subject matter expert judgment
    d. Ranges instead of point estimates
7. Which Business Impact Analysis activity provides the information needed to identify prerequisite services before recovery priorities are finalized?
    a. Risk assessment
    b. Business process mapping
    c. Predictive impact analysis
    d. Dependency analysis

WEEK 4 - ADDITIONAL RESOURCES:

White Papers:

- BCDR FOR BUSINESS: THE 7-STEP PATH TO CONDUCTING A BUSINESS IMPACT ANALYSIS (BIA): https://www.tpx.com/wp-content/uploads/2023/08/Backup-Whitepaper-Business-Impact-Analysis-BIA.pdf
- Enhancing Operational Resilience in a Dynamic World: https://www.opscentre.com/wp-content/uploads/2025/07/Whitepaper-Operational-Resilience-OpsCentre-vFINAL.pdf

Videos:

- Business Impact Analysis Explained: Ultimate Business Check-Up: https://www.youtube.com/watch?v=yuknjw7NBP4
- How to Conduct a BIA (Business Impact Analysis): https://www.youtube.com/watch?v=Dd6D5ijabdA
- What Is The Role Of Business Impact Analysis (BIA) In Disaster Recovery? - Admin Career Guide: https://www.youtube.com/watch?v=51TZBxzh8gQ
- What is a Business Impact Analysis?: https://www.youtube.com/watch?v=hY31GhZBga8

WEEK FIVE:

MODULES COVERED:

- Module 05 - Business Continuity Plan

WEEK 5 - WEEKLY OBJECTIVES:

- Understand the purpose, structure, and development of a Business Continuity Plan, including continuity strategies, incident response, communication, recovery planning, and the use of AI to support resilience in AI-dependent operations.

WEEK 5 - ASSESSMENTS:

The course includes the following assessments under Week Five.

- Discussion Threads: 1 discussion thread (each worth 4 pts.)
- Assignments from Reading: 1 assignment from reading (each worth 6 pts.)
- Quizzes: 5 quiz questions (each worth 1 pt.)

WEEK 5 - DISCUSSION THREAD:

- Discuss how a Business Continuity Plan helps organizations maintain critical operations through continuity strategies, incident response, communication planning, and AI-enabled support.

WEEK 5 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 05 - Business Continuity Plan

WEEK 5 - ASSIGNMENTS FROM READING:

- Analyze how Business Continuity Planning supports organizational resilience during operational disruptions.

WEEK 5 - QUIZ:

1. What is the primary purpose of a Business Continuity Plan (BCP) during a disruption?
    a. To restore IT systems and applications
    b. To continue delivering critical business functions during and after a disruption
    c. To eliminate all business risks
    d. To replace the Disaster Recovery Plan

2. Which characteristic of a high-quality Business Continuity Plan enables it to remain effective across technology failures, workforce shortages, and facility disruptions?
    a. Actionable Under Pressure
    b. Clearly Communicate in Plain Language
    c. Scalable to Different Incident Types
    d. Tested Through Exercises and Reviews
3. Which operational strategy allows organizations to continue critical business operations by modifying how work is performed during disruptions?
    a. Workforce Cross-Training
    b. Alternate Workflows
    c. Succession Planning
    d. Remote Operations
4. Which personnel strategy helps prevent leadership bottlenecks during a disruptive event?
    a. Minimum Staffing Requirements
    b. Workforce Cross-Training
    c. Succession Planning
    d. Remote Work Enablement
5. Which AI decision support capability helps organizations compare recovery strategies and predict likely outcomes during business continuity planning?
    a. Situation Analysis
    b. Recovery Prioritization
    c. Scenario Modeling
    d. Impact Assessment

WEEK 5 - ADDITIONAL RESOURCES:

White Papers:

- Security White Paper Data security is serious business: https://www.alchemer.com/wp-content/uploads/2024/09/Alchemer_Security_Whitepaper_091824.pdf
- Business Continuity and Disaster Recovery Whitepaper: https://a.storyblok.com/f/157376/x/70db445270/aircall-business-continuity-whitepaper.pdf

Videos:

- Business Continuity Planning: Strategies to Minimize Business Disruptions: https://www.youtube.com/watch?v=pYCfHQk7538
- Artificial Intelligence in Business Continuity: https://www.youtube.com/watch?v=uSP-cT8ucLk
- Incident Response Lifecycle | IR Plan | NIST SP 800-61 Security Incident Handling| Cybersecurity: https://www.youtube.com/watch?v=IRSQEO0koYY&t=178s
- Business Continuity, Disaster Recovery, and Security Incident Response Plan - Sedara Whiteboard: https://www.youtube.com/watch?v=CzOsIe-hwWA

WEEK SIX:

MODULES COVERED:

- Module 06 - Disaster Recovery Planning

WEEK 6 - WEEKLY OBJECTIVES:

- Understand the foundational concepts, inputs, risks, and strategies of IT Disaster Recovery Planning, including the role of AI in supporting recovery, data protection, and operational resilience.

WEEK 6 - ASSESSMENTS:

The course includes the following assessments under Week Six.

- Discussion Threads: 2 discussion threads (each worth 4 pts.)
- Assignments from Reading: 2 assignments from reading (each worth 6 pts.)
- Quizzes: 5 quiz questions (each worth 1 pt.)

WEEK 6 - DISCUSSION THREAD:

- Discuss the role of IT DRP in supporting business continuity, including key planning inputs, risk analysis, data recovery objectives, and AI-assisted recovery capabilities.
- Discuss common disaster recovery strategies, data recovery within the disaster lifecycle and how AI supports risk identification and recovery prioritization.

WEEK 6 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 06 - Disaster Recovery Planning

WEEK 6 - ASSIGNMENTS FROM READING:

- Analyze how IT Disaster Recovery Planning enables organizations to protect critical operations and support business continuity during disruptive events.
- Evaluate how recovery strategies and emerging technologies enhance recovery readiness and organizational resilience.

WEEK 6 - QUIZ:

1. Which disaster recovery strategy provides the fastest recovery by maintaining a fully operational replica of the production environment?
    a. Cold site
    b. Warm site
    c. Hot site
    d. Backup and restore

2. Which disaster recovery strategy provides data replication with lower network overhead by allowing data to be written to the secondary system after it is committed to the primary system?
    a. Synchronous replication
    b. Backup and restore
    c. Asynchronous replication
    d. Hot site
3. Which disaster recovery approach keeps only critical core services running while allowing the remaining infrastructure to be started during a disaster?
    a. Active-passive replication
    b. Backup and restore
    c. Pilot light
    d. Hot site
4. What is the primary benefit of synchronous replication in disaster recovery strategies?
    a. Lowest implementation cost
    b. Near-zero data loss during recovery
    c. Simplified infrastructure management
    d. Elimination of backup requirements
5. What component of recovery management includes backup and restore solutions, replication technologies, monitoring systems, and automation tools?
    a. Governance and Ownership
    b. Technology Stack
    c. Policies and Standards
    d. Testing and Validation

WEEK 6 - ADDITIONAL RESOURCES:

White Papers:

- The State of Disaster Recovery and Cyber-Recovery, 2024–2025: Factoring in AI: https://www.cristie.com/wp-content/uploads/2024/09/IDC-White-Paper_State-of-DR-and-Cyber-Recovery-2025-2025_US52445524.pdf
- Disaster Recovery of Workloads on AWS: Recovery in the Cloud: https://docs.aws.amazon.com/pdfs/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-workloads-on-aws.pdf

Videos:

- How to write an IT Disaster Recovery Plan: https://www.youtube.com/watch?v=0DtzC94PZAk
- AWS Disaster Recovery | RTO | RPO | Business Continuity Plan | Simplified and Visualized: https://www.youtube.com/watch?v=WYCbczFIj3E
- Disaster Recovery 101: How to Choose Between Hot vs Warm vs Cold DR Sites: https://www.youtube.com/watch?v=9cKWR2-4RLI
- Disaster Recovery Strategies: https://www.youtube.com/watch?v=5ATF-eii6cQ

WEEK SEVEN:

MODULES COVERED:

- Module 07 - Data Backup and System Recovery

WEEK 7 - WEEKLY OBJECTIVES:

- Understand the principles and mechanisms of data backup and system recovery, including recovery types, technologies, and AI-enabled validation.
- Understand the recovery best practices, governance, and cost-aware decision-making to improve operational readiness across diverse infrastructure environments.

WEEK 7 - ASSESSMENTS:

The course includes the following assessments under Week Seven.

- Discussion Threads: 2 discussion threads (each worth 4 pts.)
- Assignments from Reading: 2 assignments from reading (each worth 6 pts.)
- Lab Assignments: 5 lab assignments (each worth 4 pts.)
- Quizzes: 6 quiz questions (each worth 1 pt.)

WEEK 7 - DISCUSSION THREAD:

- Discuss the core concepts, types, and models of data backup and recovery, including how AI is used to optimize backup validation and efficiency.
- Discuss the tools, technologies, and architectures used for data recovery, and the best practices organizations should follow when implementing recovery capabilities.

WEEK 7 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 07 - Data Backup and System Recovery

WEEK 7 - ASSIGNMENTS FROM READING:

- Analyze how data backup and recovery capabilities enable organizations to protect critical information and maintain operational resilience.
- Evaluate how modern backup technologies and recovery strategies improve data protection and recovery readiness.

WEEK 7 - LAB ASSIGNMENTS:

Week 7 Lab Assignment 1: File Backup and Recovery Using Windows Shadow Copy

Lab Scenario

Business-critical files stored on centralized file servers are frequently accessed and modified by employees, making them susceptible to accidental deletion, unauthorized modifications, file corruption, and application-related errors. To minimize data loss and maintain business continuity, organizations implement file-level recovery mechanisms that enable administrators and users to quickly restore previous versions of shared files and folders without recovering the entire server.

Lab Objective

In this lab, you will implement file-level backup and recovery in a Windows enterprise environment by enabling Shadow Copies on a file server, accessing shared resources from a domain-joined workstation, simulating accidental deletion, file overwrite, and corruption incidents, restoring previous versions of files and folders, and configuring scheduled recovery points to validate the effectiveness of file recovery mechanisms in maintaining business continuity and reducing data loss.

Week 7 Lab Assignment 2: File Recovery Using EaseUS Data Recovery Wizard

Lab Scenario

Organizations rely on centralized file servers to store and share critical business data across departments. Since these shared resources are accessed by multiple users, accidental file deletion remains one of the most common causes of data loss. Effective recovery procedures are essential to ensure business continuity and reduce downtime.

Lab Objective

In this lab, you will implement file recovery in an enterprise environment by creating and managing business-critical data, simulating accidental file deletion, performing storage scans using EaseUS Data Recovery Wizard, identifying recoverable data, restoring deleted files to a secure location, and validating the integrity of recovered information to demonstrate effective data recovery practices that support business continuity and minimize the impact of data loss incidents.

Week 7 Lab Assignment 3: File Backup and Recovery Using BorgBackup

Lab Scenario

Business-critical files stored on Linux workstations are frequently accessed, modified, and shared by users, making them susceptible to accidental deletion, file corruption, ransomware attacks, hardware failures, and other disasters.

Lab Objective

In this lab, you will implement a centralized file backup and recovery solution using BorgBackup by configuring a remote backup repository hosted on a backup server, creating encrypted backups of critical files, simulating data loss scenarios such as accidental deletion and file corruption, and restoring the original files from the backup repository to validate the recovery process and maintain business continuity.

Week 7 Lab Assignment 4: File Backup and Deduplication Using Windows Server Deduplication

Lab Scenario

Organizations regularly back up business-critical data from client systems to centralized backup servers to support disaster recovery and business continuity. Over time, repeated backups of the same data create multiple redundant copies that consume significant storage on the backup repository.

Lab Objective

In this lab, you will create and share a backup target folder on a Windows Server 2025 Backup Server, install Data Deduplication, back up data from a Windows 11 client to the server using Robocopy, generate multiple backup copies to simulate redundant data, configure and run a deduplication job, and verify the storage savings achieved.

Week 7 Lab Assignment 5: Full Disk Backup and Restore Using Windows Server Backup

Lab Scenario

Organizations rely on business-critical data stored on servers to support daily operations and service delivery. Hardware failures, accidental deletions, ransomware incidents, and other disruptive events can result in data loss and operational downtime. To ensure business continuity and meet recovery objectives, organizations implement Disk-to-Disk (D2D) backup strategies that store backup data on secondary storage devices for rapid restoration.

Lab Objective

In this lab, you will implement a Disk-to-Disk (D2D) backup and recovery solution by installing and configuring Windows Server Backup, creating a backup of a business data volume, storing the backup on secondary storage, simulating a data loss incident, restoring the protected volume from the backup, and validating the recovered data to ensure business continuity and disaster recovery readiness.

WEEK 7 - QUIZ:

1. Which backup model captures only the data that has changed since the previous backup?
    a. Differential backup
    b. Full backup
    c. Continuous Data Protection (CDP)
    d. Incremental backup

2. Which recovery approach is commonly required after complete hardware failure or severe ransomware attacks?
    a. File-level recovery
    b. Database recovery
    c. System-level (Bare-Metal) recovery
    d. Application-level recovery
3. Which replication technology writes data to both the primary and secondary storage sites before a transaction is considered complete?
    a. Differential backup
    b. Asynchronous replication
    c. Synchronous replication
    d. Cloud backup
4. Which disaster recovery workload platform integrates compute, storage, and networking into a single software-defined architecture?
    a. SaaS / Application Platforms
    b. Hyperconverged Infrastructure (HCI)
    c. Container Platform
    d. Virtualization platforms
5. Which capability of VMware vSphere allows administrators to move running virtual machines between hosts with minimal disruption?
    a. API-based backup
    b. vMotion
    c. Bare-Metal Restore
    d. Changed Block Tracking
6. Which cost optimization strategy recommends storing recent backups on hot storage and long-term backups on archive storage?
    a. Backup Frequency Optimization
    b. Hybrid Backup Strategy
    c. Tiered Storage Strategy
    d. Retention Policy Optimization

WEEK 7 - ADDITIONAL RESOURCES:

White Papers:

- Contingency Planning Guide for Federal Information Systems: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
- Data Backup Options: https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf

Videos:

- Incremental vs Differential Backup, & Full – Explained: https://www.youtube.com/watch?v=o-83E6levzM
- Disaster Recovery vs. Backup: What's the difference?: https://www.youtube.com/watch?v=07EHsPuKXc0&t=147s
- Snapshots vs Backups vs Replications:

  https://www.youtube.com/watch?v=BcA13YbUv-4

WEEK EIGHT:

MODULES COVERED:

- Module 08 - Disaster Recovery Plan Development

WEEK 8 - WEEKLY OBJECTIVES:

- Understand how to design and maintain an effective disaster recovery plan that aligns recovery priorities, roles, procedures, and AI-supported automation to minimize disruption and strengthen resilience.

WEEK 8 - ASSESSMENTS:

The course includes the following assessments under Week Eight.

- Discussion Threads: 1 discussion thread (each worth 4 pts.)
- Assignments from Reading: 1 assignment from reading (each worth 6 pts.)
- Quizzes: 5 quiz questions (each worth 1 pt.)

WEEK 8 - DISCUSSION THREAD:

- Discuss the purpose, structure, and components of a disaster recovery plan, and the best practices, including AI-driven enhancements, for developing a clear plan.

WEEK 8 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 08 - Disaster Recovery Plan Development

WEEK 8 - ASSIGNMENTS FROM READING:

- Analyze how an effective Disaster Recovery Plan enables organizations to respond to disruptions and maintain operational resilience.

WEEK 8 - QUIZ:

1. Which type of disruption involves failures such as server crashes or network outages?
    a. Human-caused incidents
    b. Utility failures
    c. Hardware or infrastructure failures
    d. Third-party disruptions

2. Which Disaster Recovery Plan component establishes the maximum acceptable amount of data loss after a disruption?
    a. Recovery Time Objective (RTO)
    b. Business Impact Analysis (BIA)
    c. Recovery Point Objective (RPO)
    d. Risk Assessment
3. Which recovery approach specifies the use of cold sites, warm sites, hot sites, and cloud-based failover to restore IT services?
    a. Personnel and Vendor Considerations
    b. Infrastructure and Application Recovery Approaches
    c. Documentation Standards
    d. Communication Protocols
4. What is the primary purpose of AI-driven recovery workflows during disaster recovery?
    a. To eliminate the need for disaster recovery plans
    b. To dynamically analyze incidents and prioritize recovery actions in real time
    c. To replace business continuity policies
    d. To perform backup validation
5. Which Disaster Recovery Plan component documents the conditions required during a disaster, such as personnel availability and accessibility of alternate sites?
    a. Recovery Objectives
    b. Assumptions
    c. Communication Protocols
    d. Recovery Procedures

WEEK 8 - ADDITIONAL RESOURCES:

White Papers:

- IT Disaster Recovery Planning Guide: https://www.baculasystems.com/wp-content/uploads/2023/02/dr-guide.pdf
- Disaster Recovery Planning & Procedure: https://ficonsulting.com/wp-content/uploads/2022/12/FI_2022_DisasterRecovery_WP_F.pdf

Videos:

- What is the Difference Between Business Continuity and Disaster Recovery?: https://www.youtube.com/watch?v=USCaj46GDPc&t=15s

- Realized Solutions 7 Essential Components of a Successful Disaster Recovery Plan: https://www.youtube.com/watch?v=F_rNp2G3tQQ
- Disaster Recovery Plan (DRP): https://www.youtube.com/watch?v=U_GpytrH6R8

WEEK NINE:

MODULES COVERED:

- Module 09 - Business Continuity and Disaster Recovery Plan Activation

WEEK 9 - WEEKLY OBJECTIVES:

- Understand the criteria, activation process, coordination structure, and crisis communication requirements for business continuity and disaster recovery plan activation to enable timely and controlled response during disruptive events.

WEEK 9 - ASSESSMENTS:

The course includes the following assessments under Week Nine.

- Discussion Threads: 1 discussion thread (each worth 4 pts.)
- Assignments from Reading: 1 assignment from reading (each worth 6 pts.)
- Quizzes: 5 quiz questions (each worth 1 pt.)

WEEK 9 - DISCUSSION THREAD:

- Discuss how organizations determine when to activate BC/DR plans, and how roles and responsibilities, incident command structures, and crisis communication support an effective response.

WEEK 9 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 09 - Business Continuity and Disaster Recovery Plan Activation

WEEK 9 - ASSIGNMENTS FROM READING:

- Analyze how effective plan activation, communication, and coordination enable organizations to respond to disruptive events and maintain business continuity.

WEEK 9 - QUIZ:

1. Which type of disruption requires formal activation of business continuity and disaster recovery plans?
    a. Brief system outage
    b. Temporary staffing shortage
    c. Declared disaster
    d. Minor facility issue

2. What is the primary purpose of a crisis communication plan during a disruptive event?
    a. **Maintaining trust and confidence among employees, customers, and stakeholders**
    b. Restoring failed IT systems automatically
    c. Replacing incident response procedures
    d. Authorizing disaster recovery plan activation
3. Which component helps decision-makers evaluate response options and determine appropriate actions during business continuity or disaster recovery plan activation?
    a. Communication Plans
    b. **Decision Support Tools**
    c. Activation Criteria
    d. Recovery Objectives
4. Why is information sharing and situational awareness important during cross-team coordination in business continuity and disaster recovery plan activation?
    a. To eliminate regulatory reporting requirements
    b. **To provide a common operating picture across teams for informed decision-making**
    c. To reduce the number of recovery objectives
    d. To replace incident command structures
5. Which plan supports the Crisis Communication Plan by providing information about IT system outages, recovery timelines, and data integrity?
    a. Business Continuity Plan (BCP)
    b. **Disaster Recovery Plan (DRP)**
    c. Human Resources Plans
    d. Legal and Compliance Frameworks

WEEK 9 - ADDITIONAL RESOURCES:

White Papers:

- Disaster Recovery: A Guide for IT Professionals: https://www.wanstor.com/app/uploads/2025/03/whitepaper-wanstor-offsite-backup-disaster-recovery-a-guide-for-it-professionals.pdf
- Crisis Communications Planning Guide: https://www.communications.gov.uk/wp-content/uploads/2024/09/Crisis-Comms-STOP-guidance-2.pdf

Videos:

- What is BCDR? Business Continuity and Disaster Recovery Explained: https://www.youtube.com/watch?v=zn_u5_jNJ-M&t=17s
- BCDR Made Simple: Easy Steps to Safeguard Your Organization: https://www.youtube.com/watch?v=t6uIDhKEPX4

WEEK TEN:

MODULES COVERED:

- Module 10 - Business Continuity and Disaster Recovery Plan Activation Test, Training, and Exercise

WEEK 10 - WEEKLY OBJECTIVES:

- Understand the methods, metrics, and maturity practices used to test, train, and exercise business continuity and disaster recovery plans so that readiness can be validated, improved, and sustained in changing operational environments.

WEEK 10 - ASSESSMENTS:

The course includes the following assessments under Week Ten.

- Discussion Threads: 2 discussion threads (each worth 4 pts.)
- Assignments from Reading: 2 reading assignments (each worth 6 pts.)
- Quizzes: 5 quiz questions (each worth 1 pt.)

WEEK 10 - DISCUSSION THREAD:

- Discuss the purpose and types of BCDR testing, training, and exercises, and how they validate plan effectiveness before a real incident occurs.
- Discuss how metrics, KPIs, maturity models, audits, and lessons learned drive continuous improvement in BCDR testing programs.

WEEK 10 - REQUIRED READING MATERIAL:

Read the following chapters from the book:

- Module 10 - Business Continuity and Disaster Recovery Plan Activation Test, Training, and Exercise

WEEK 10 - ASSIGNMENTS FROM READING:

- Analyze how testing, training, and exercises improve organizational resilience and validate BC/DR capabilities.
- Evaluate the importance of continuous testing and program improvement in maintaining effective BC/DR capabilities.

WEEK 10 - QUIZ:

1. Which aspect of Business Continuity and Disaster Recovery plan testing identifies findings such as DNS failover failures?
    a. **Verification of technical recovery capability**
    b. Validation of governance and decision authority
    c. Reduction of false confidence
    d. Validation of Assumptions

2. What is the primary objective of General Awareness Training in a BCDR program?
    a. To execute failover and replication procedures
    b. To introduce continuity concepts and individual responsibilities to all employees
    c. To authorize disaster recovery plan activation
    d. To measure RTO and RPO compliance
3. Which BCDR testing methodology evaluates recovery capabilities in a non-production environment without affecting live business operations?
    a. Simulation-based Testing
    b. Full-scale DR testing
    c. Parallel testing
    d. Partial DR testing
4. Which IT Disaster Recovery Testing Method includes activities such as transaction log application?
    a. Backup and Restore Validation
    b. System Recovery and Failover Testing
    c. Application Dependency and Integration Testing
    d. Network, Identity, and Access Recovery Validation
5. Which AI-Enhanced Resilience Maturity Model level enables organizations to predict outcomes and recommend optimal actions for Business Continuity and Disaster Recovery testing and resilience improvement?
    a. Level 1: Manual
    b. Level 2: Assisted
    c. Level 3: Predictive
    d. Level 4: Autonomous

WEEK 10 - ADDITIONAL RESOURCES:

White Papers:

- Adobe Business Continuity and Disaster Recovery Program: https://www.adobe.com/cc-shared/assets/pdf/trust/adb-business-continuity-and-disaster-recovery-program-overview.pdf
- Designing a Business Continuity Training Program to Maximize Value & Minimize Cost: https://drj.com/wp-content/uploads/2019/07/Designing_a_Business_Continuity_Training_Program.pdf

Videos:

- Tip #5: Testing & Refining | Creating a BCDR Plan: https://www.youtube.com/watch?v=R07WWThMY4U
- Updated Strategies on Developing a BCDR Training Program: https://www.youtube.com/watch?v=eApxO07RTPU
- Key Performance Indicators (KPIs) with examples: https://www.youtube.com/watch?v=KJ1-X-vgcZs&list=PLskUGS0LFR3JCLxbkBlGM5BQiQMrrJHcl

WEEK ELEVEN:

WEEKLY OBJECTIVES:

- Understand Business Continuity and Disaster Recovery (BCDR) concepts, regulatory influences, and strategic importance, while evaluating best practices and the role of emerging technologies, including AI, in enhancing organizational resilience.
- Understand Business Continuity Management (BCM), including its lifecycle, core elements, governance, and regulatory requirements, while evaluating the role of AI, Zero Trust, and organizational integration in strengthening operational resilience.
- Understand the concepts, categories, and lifecycle of risk assessment, including its relationship to BCM and IT disaster recovery, to identify, evaluate, and prioritize business and technology risks effectively.
- Understand risk treatment, dependency mapping, cascading risks, and risk prioritization methods to support informed continuity, recovery, and resilience decisions across the organization.
- Understand the scope, purpose, assumptions, and analytical foundations of Business Impact Analysis (BIA), including how AI-enhanced techniques support the identification and prioritization of critical business functions, dependencies, and recovery requirements.
- Understand how to conduct, validate, and communicate a defensible BIA using qualitative and quantitative methods to translate business impact findings into actionable recovery and resilience decisions.
- Understand the purpose, structure, and development of a Business Continuity Plan, including continuity strategies, incident response, communication, recovery planning, and the use of AI to support resilience in AI-dependent operations.
- Understand the foundational concepts, inputs, risks, and strategies of IT Disaster Recovery Planning, including the role of AI in supporting recovery, data protection, and operational resilience.
- Understand the principles and mechanisms of data backup and system recovery, including recovery types, technologies, and AI-enabled validation.
- Understand the recovery best practices, governance, and cost-aware decision-making to improve operational readiness across diverse infrastructure environments.
- Understand how to design and maintain an effective disaster recovery plan that aligns recovery priorities, roles, procedures, and AI-supported automation to minimize disruption and strengthen resilience.
- Understand the criteria, activation process, coordination structure, and crisis communication requirements for business continuity and disaster recovery plan activation to enable timely and controlled response during disruptive events.

- Understand the methods, metrics, and maturity practices used to test, train, and exercise business continuity and disaster recovery plans so that readiness can be validated, improved, and sustained in changing operational environments.

WEEK 11 ASSESSMENTS:

Summative Assessment Research Project: 50 pts.

Directions on Project:

Guidelines on Graduate Project

Following are the guidelines for your graduate project.

Selecting a Topic

- Choose a project topic from one of your completed labs from the previous weeks. You may go back through the lab content to familiarize yourself with the information required to complete your project.
- Prepare a rough outline of project proposal you would like to submit. Discuss the topic and draft project proposal with instructor.
- Conduct further research on the topic. Make a detailed proposal.

Working on the Project

- You have to complete your project within the stipulated deadlines. Plan your project accordingly.
- While meeting the executives of a company in relation to your project, make sure you have appropriate approvals and request letters from the concerned university department or company.
- Make sure your instructor approves questionnaires designed for any survey in relation to the project.
- You must use any data collected in course of the research, only for the approved project. You must not share collected information with other students.
- Make notes of key points during the course of research. It would save lot of time in preparation of project report.
- Make sure all relevant journals, magazines, papers and books are available in the university library.
- Analysis is the most critical part of the project and forms basis for all findings. Make sure you make use of appropriate statistical tools in analysis.

Writing a Project Report

- Review the style guidelines for project report
- The project report should not exceed 7,000 words
- Abstract should be between 150-250 words

- Select A4 size; page orientation should be portrait. Specify “1” margin on all sides.
- Number all pages consecutively. Start every chapter on a new page.
- Provide double spacing
- You should use Times New Roman Font- “12” for text and “10” for footnotes. Use a larger font size for section headings.
- A project report must contain:

Content	Section
a. Title Page	Preliminaries
b. Table of Contents	
c. Abstract	
d. Introduction and background	Body of the report
e. Problem statement	
f. Objectives of the project	
g. Literature review	
h. Methodology adopted	
i. Results - project findings	
j. Recommendations	
k. Conclusion	
l. Bibliography	References
m. Appendix	
n. List of figures and tables	
o. Index words (if required)	

- Be clear and precise. Express your ideas in a logical way.
- Abstract should reflect the essence of the project
- The introduction should provide the overview of the topic and highlight its significance
- Clearly indicate the objectives of your project.
- Describe all the methods used such as interviews and questionnaires in the methodology section.
- Ensure that literature review is in your own words. Analyze other person’s contribution to the topic. Identify the gaps in the literature. Emphasize on the likely contribution of your project to the existing literature on the topic.
- Describe your findings from analysis in the results section. As this is the most critical part

of the project, ensure that there are no errors in analysis. Make proper inferences from analysis and findings.

- The conclusion section should summarize your objectives, findings and learning's from the project. Provide useful supplementary information in the Appendix.
- Avoid plagiarism. The project report should reflect your understanding of the topic. The majority of the paper should be in your own words and reflect your own ideas.
- Give credit for all referenced work. Provide appropriate citation and references for all quotations.
- Ensure that papers referenced are relevant and not outdated.
- Your paper should be reader friendly. Use footnotes to explain difficult terms.
- Don't use text from Wikipedia in footnotes
- All tables and figures must be suitably numbered and titled. Give appropriate credit.
- On completion, go through the entire project. Ensure there are no proofing errors and you have adhered to all guidelines related to the project.

Presentation – To be included as part of final project submission, but separate from project document word count. (This is a separate portion of the final project)

- The presentation should not exceed 20 minutes.
- Don't use more than 15 slides.
- Give a high level overview of report findings and suggestive mitigation strategies to eradicate or prevent future intrusions.
- Submit to the instructor for review and grading.

WEEK TWELVE:

WEEK'S OBJECTIVES USED:

- Understand Business Continuity and Disaster Recovery (BCDR) concepts, regulatory influences, and strategic importance, while evaluating best practices and the role of emerging technologies, including AI, in enhancing organizational resilience.
- Understand Business Continuity Management (BCM), including its lifecycle, core elements, governance, and regulatory requirements, while evaluating the role of AI, Zero Trust, and organizational integration in strengthening operational resilience.
- Understand the concepts, categories, and lifecycle of risk assessment, including its relationship to BCM and IT disaster recovery, to identify, evaluate, and prioritize business and technology risks effectively.
- Understand risk treatment, dependency mapping, cascading risks, and risk prioritization methods to support informed continuity, recovery, and resilience decisions across the organization.
- Understand the scope, purpose, assumptions, and analytical foundations of Business Impact Analysis (BIA), including how AI-enhanced techniques support the identification and prioritization of critical business functions, dependencies, and recovery requirements.
- Understand how to conduct, validate, and communicate a defensible BIA using qualitative and quantitative methods to translate business impact findings into actionable recovery and resilience decisions.
- Understand the purpose, structure, and development of a Business Continuity Plan, including continuity strategies, incident response, communication, recovery planning, and the use of AI to support resilience in AI-dependent operations.
- Understand the foundational concepts, inputs, risks, and strategies of IT Disaster Recovery Planning, including the role of AI in supporting recovery, data protection, and operational resilience.
- Understand the principles and mechanisms of data backup and system recovery, including recovery types, technologies, and AI-enabled validation.
- Understand the recovery best practices, governance, and cost-aware decision-making to improve operational readiness across diverse infrastructure environments.
- Understand how to design and maintain an effective disaster recovery plan that aligns recovery priorities, roles, procedures, and AI-supported automation to minimize disruption and strengthen resilience.
- Understand the criteria, activation process, coordination structure, and crisis communication requirements for business continuity and disaster recovery plan activation to enable timely and controlled response during disruptive events.

- Understand the methods, metrics, and maturity practices used to test, train, and exercise business continuity and disaster recovery plans so that readiness can be validated, improved, and sustained in changing operational environments.

WEEK 12 ASSESSMENTS:

Summative Assessment Final Exam: 100 pts.

During week twelve you will be required to complete a final exam that incorporates several areas of critical thinking and decision-making. The exam will include multiple choice, short answer, and essay questions covering all learning outcomes of the course. Contact your instructor for specific question related to this assessment.