

EC-Council



EC-COUNCIL DISASTER RECOVERY PROFESSIONAL

Lead recovery, strengthen resilience,
and master business continuity with
AI-powered insights.



EC-Council Disaster Recovery Professional

THE INDUSTRY PROBLEM

Downtime Is a Business Survival Problem

Disruption is now constant and expensive, yet most organizations are not prepared. The cost of a single hour offline has climbed into the millions for large enterprises.

90%

of organizations say one hour of downtime costs more than \$300,000

41%

of enterprises report \$1M-\$5M+ per hour of downtime

\$15k

average cost of downtime per minute

\$300M

lost per year, on average, from unplanned outages

Source: ITIC 2024 Hourly Cost of Downtime Survey; Cisco Newsroom; Splunk, The Hidden Costs of Downtime (2026).

Disruption Is Constant and Ransomware Makes It Worse

Outages are no longer rare events, and when ransomware is involved, recovery now takes weeks rather than hours.

86

outages per year on average (2025)

100%

of firms lost revenue to outages

40%

of organizations suffered a major outage caused by human error in the past 3 years. Of these human-error incidents, **85%** stem from staff failing to follow procedures or from flaws in the procedures themselves. (Uptime Institute, 2025)

Source: ITIC 2024 Hourly Cost of Downtime Survey; Cisco Newsroom; Splunk, The Hidden Costs of Downtime (2026).

They Believe They're Ready. The Data Says Otherwise.

94%

believe they are ready to handle disasters

26%

actually have a disaster plan in place

20%

describe themselves as fully prepared for outages

Sources: U.S. Chamber of Commerce Foundation; Cockroach Labs, State of Resilience 2025; Keiser University.

Regulation Is Closing In and Teams Aren't Ready

65%

of European financial institutions were not fully prepared for DORA

44%

worry about fines that can reach €5,000,000 (US\$5.5M) per outage

No.3

DR & business continuity jumped from outside the top 10 (2024) to a top-3 CISO priority in 2025

Sources: PwC Luxembourg; Apex Assembly, State of Resilience 2025; CSO Online

THE INDUSTRY SOLUTION

The Market Is Already Pivoting From Reactive Backup to Tested, Strategic Resilience

89%

of leaders name disaster recovery a key focus for their cloud environments

57%

of financial institutions include ICT third parties in DR testing for DORA

48%

faster recovery when backups are tested quarterly vs. annually

Sources: Cutover, Annual IT Disaster & Cyber Recovery Trends 2025; Total Assure

Modern Backup & Recovery: Immutable + Cloud

83%

faster restoration times are achieved with instant recovery technologies, while 76% of enterprises use automated scheduling and policy-based management.

38%

faster recovery times and 44% fewer outages compared to legacy or complex distributed IT setups

31 days to 14 days days: immutable + automated recovery halves recovery time

Sources: Market Reports World; Influxbox; Total Assure

AI & AIOps: The Resilience Force Multiplier

AIOps incident detection is increased by 35%, improves problem-solving accuracy by 25%, and reduces MTTR by 40% across multiple services and systems.

76%

accuracy in root cause analysis was achieved by organizations implementing AIOps, compared to just 34% among organizations without AIOps.

Sources: researchsquare, marketsandmarkets

THE MISSING LINK

Why Traditional BC/DR Training Falls Short and What EDRP v4 Delivers

Hands-On Resilience Skills. Risk-to-Recovery Planning. AI-Enabled BC/DR. Real Leadership Outcomes.

WHY RESILIENCE TRAINING FALLS SHORT

DR Without Business Continuity

Focuses on restoring systems, not sustaining critical operations and enterprise recovery.

Planning Without Risk & Business Impact

Overlooks BIA, dependencies, cascading risks, and recovery priorities.

Legacy-Focused Recovery Skills

Fails to address cloud, hybrid, virtualization, containers, SaaS, and modern recovery environments.

Plans That Aren't Proven

Limited focus on activation, testing, exercises, measurement, and continuous improvement.

Recovery Without Crisis Leadership

Misses escalation, crisis communication, stakeholder coordination, and decision-making skills.

No AI-Enabled Resilience Skills

Lacks AI, automation, analytics, and AIOps for risk analysis, early warning, and recovery decisions.

WHAT EDRP v4 DELIVERS

End-to-End Organizational Resilience

Integrates business continuity, disaster recovery, operational resilience, risk management, and crisis management.

Risk-to-Recovery Planning

Covers risk assessment, BIA, dependencies, RTO/RPO/MTD, and recovery prioritization.

Modern Disaster Recovery

Builds recovery skills across systems, data, cloud, hybrid, virtualization, containers, and automation.

Tested & Continuously Improved Plans

Covers activation, testing, exercises, KPIs, compliance monitoring, audits, and the PDCA model.

Crisis Management & Resilience Leadership

Develops crisis coordination, communication, stakeholder management, and recovery leadership.

AI-Enabled BC/DR

Applies AI, ML, GenAI, analytics, automation, and AIOps to strengthen resilience and recovery.

EDRP: A COMPREHENSIVE BUSINESS RESILIENCE CERTIFICATION

What Is EDRP?

The Comprehensive Business Continuity & Disaster Recovery Certification

The EC-Council Disaster Recovery Professional (EDRP) is a comprehensive, managerial-level business resilience certification designed to equip professionals to lead, plan, strategize, and manage BC/DR activities before, during, and after incidents.

An EDRP-certified professional helps organizations prepare against unwanted incidents that can cause significant financial loss, reputational damage, and operational disruption. EDRP covers the complete business resilience lifecycle, including business continuity management, disaster recovery, risk assessment, business impact analysis (BIA), crisis management and communication, data backup and recovery, compliance, governance, plan activation, testing, and continuous improvement.

Built for today's AI-enabled and cloud-driven environments, EDRP explores how AI, ML, generative AI, AIOps, automation, and emerging technologies enhance risk analysis, continuity planning, disruption detection, decision-making, and recovery.

The program also covers ISO 22301, regulatory and legal requirements, Zero Trust principles, and AI governance, aligning BC/DR practice with global standards using the PDCA (Plan-Do-Check-Act) model.

Training Highlight

- The certification program for professionals leading BC/DR, risk, and resilience programs
- Recommended 2–4 years of prior experience in IT infrastructure, network security operations, risk management, incident response, or related fields
- Learn insights on AI, ML, GenAI, and AIOps throughout the business continuity and disaster recovery lifecycle
- Aligned with ISO 22301, regulatory requirements, and the PDCA continuous-improvement model
- Delivered via Instructor-Led Training (ILT), iWeek live online, and iLearn self-paced online modes
- 1 year e-courseware & training video access · 6 months lab access · 1-year proctored exam voucher

Lead Your Organization Through Disruption

Start with EDRP v4

UNIQUE BENEFITS THAT MAKE EDRP DIFFERENT

Why EDRP Gives You a Unique Career Advantage

EDRP is not another IT-recovery checklist. It is the only BC/DR certification that simultaneously builds end-to-end resilience strategy, AI-enabled recovery fluency, and real crisis-leadership skill. Here are the six features that make EDRP v4 uniquely powerful:

1. End-to-End Organizational Resilience

Integrates business continuity, disaster recovery, operational resilience, risk management, crisis management, governance, and compliance, with a strong focus on strategic responsibilities.

BC · DR · RISK · CRISIS

2. Risk-to-Recovery Planning

Covers risk assessment, BIA, dependency mapping, cascading risks, risk treatment, RTO/RPO/MTD, and recovery prioritization.

RISK ⇒ BIA ⇒ RECOVERY

3. Modern Cloud & Hybrid Disaster Recovery

Develops recovery strategies across cloud, hybrid, virtualization, containers, applications, data, backup technologies, and automated recovery environments.

CLOUD · HYBRID · DRAAS

4. Scenario-Based Testing & Continuous Improvement

Strengthens preparedness through scenario-based testing, exercises, plan activation, KPIs, compliance monitoring, audits, and the PDCA model.

TESTING · KPIS · PDCA

5. Practical Crisis Management & Resilience Leadership

Builds capability in crisis communication, escalation, stakeholder coordination, governance, and decision-making, reinforced with real-world case studies.

CRISIS LEADERSHIP · 5 CASE STUDIES · 12 EXERCISES · 10 LABS

6. AI-Driven Business Continuity & Disaster Recovery

Applies AI, ML, generative AI, automation, analytics, and AIOps to risk analysis, early warning, disruption detection, continuity planning, and recovery decisions.

AI · GENAI · AIOPS

EDRP V4 COURSE CURRICULUM

10 Modules. Complete Resilience Lifecycle Coverage.

From foundational BC/DR concepts to AI-enabled recovery decisions, EDRP v4 covers every phase of the business resilience lifecycle, from risk identification through recovery and continuous improvement.

Module 01

Foundations of Business Continuity and Disaster Recovery

Learn the fundamental concepts of business continuity and disaster recovery and understand how organizations build operational resilience against disruptions, disasters, and emerging technology risks.

BCDR Case Study Analysis:

1. 2013 Target Data Breach
2. Maersk and the NotPetya Cyberattack (2017)
3. Southwest Airlines Operational Collapse (December 2022)
4. TSMC Manufacturing Disruption (2018)
5. Toyota Supply Chain Disruption After the 2011 Earthquake and Tsunami

Key topics covered:

Organizational Resilience, Business Continuity, Disaster Recovery, BC vs. DR, BC/DR Evolution, BC/DR Standards and Regulations, BC/DR Best Practices, AI, Machine Learning, Generative AI, AIOps, AI-Assisted Continuity Monitoring, Emerging Technologies.

Module 02

Business Continuity Management

Learn how to establish and manage a business continuity management program that strengthens organizational resilience through risk assessment, business impact analysis, continuity strategies, crisis management, testing, and continuous improvement.

BCDR Exercise Walkthrough:

- Business Continuity Assessment for an AI-dependent Organization

Key topics covered:

Business Continuity Management (BCM), BCM Lifecycle, Business Impact Analysis (BIA), Risk Assessment, Threat Modeling, Continuity Strategies, Disaster Recovery Planning, Crisis Management, Crisis Communication, Training and Awareness, Testing and Exercises, Maintenance and Continuous Improvement, ISO 22301, AI Governance, Zero Trust, BCM Roles and Responsibilities, BCM Documentation.

Module 03

Risk Assessment

Learn how to identify, analyze, prioritize, and treat risks that can disrupt business operations, IT infrastructure, applications, data, and AI-enabled services.

BCDR Exercise Walkthrough:

- Risk Assessment

Hands-on Labs:

- Qualitative Risk Assessment Using MONARC

Key topics covered:

Risk Management, Risk Categories, Threats, Vulnerabilities, Impact, IT Disaster Recovery Risks, AI Risks, Risk Assessment Lifecycle, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Monitoring, Risk Register, Risk Matrix, Dependency Mapping, Cascading Risks, Shared-Service Risks, Risk Prioritization, Risk Scoring, Risk Heat Maps, Risk Mitigation, Redundancy, Resilience, Backup, Replication, Clean-Room Recovery, Third-Party Risk.

Module 04

Business Impact Analysis

Learn how to conduct a Business Impact Analysis (BIA) to identify critical business functions, assess operational impacts, establish recovery requirements, and translate business needs into actionable resilience and recovery strategies.

BCDR Exercise Walkthrough:

- Business Impact Analysis
- AI-generated Impact Models, RTO, and RPO Determination

Key topics covered:

Business Impact Analysis, AI-Enhanced BIA, BIA Scope, BIA Planning, Business Functions and Processes, Criticality Assessment, Business and IT Dependencies, Third-Party Dependencies, Minimum Acceptable Service Levels, Impact Categories, Time-Based Impact Analysis, Recovery Time Objective (RTO), Recovery Point Objective (RPO), Qualitative Analysis, Quantitative Analysis, BIA Data Collection, BIA Execution, BIA Results Analysis, Recovery Requirements, BIA Reporting and Communication.

Module 05**Business Continuity Plan**

Learn how to develop a comprehensive Business Continuity Plan (BCP) that enables organizations to maintain critical operations, manage disruptions, communicate effectively, and recover essential business functions.

BCDR Exercise Walkthrough:

- Business Continuity Plan

Key topics covered:

Business Continuity Planning, BCP Purpose and Structure, BCP vs. DRP, Continuity Strategy Development, Operational Continuity, Personnel Strategies, Facilities and Workspace Strategies, IT and Data Strategies, AI-Enabled Continuity Planning, AI Fallback and Manual Override, Incident Response Planning, Crisis Communication, Communication Methods, AI-Assisted Crisis Communications, Third-Party AI Services, AI-Dependent Business Operations.

Module 06**Disaster Recovery Planning**

Learn how to develop disaster recovery strategies and plans that protect critical IT infrastructure, applications, data, and supporting services while enabling organizations to recover from disruptive events.

BCDR Exercise Walkthrough:

- Disaster Recovery Planning

Key topics covered:

IT Disaster Recovery, DR Planning, Infrastructure Recovery, Application Recovery, Data Recovery, Supporting Services, IT DR Inputs, IT Risk and Threat Landscape, Data Loss Scenarios, Recovery Objectives, Data Availability, System Uptime, Recovery and Resilience Planning, Disaster Recovery Strategies, Automated Recovery Orchestration, Cloud Disaster Recovery, Disaster Recovery as a Service (DRaaS), Clean-Room Recovery, Backup Scheduling, Data Retention, AI-Driven Recovery Prioritization, Self-Healing Infrastructure.

Module 07**Data Backup and System Recovery**

Learn how to design, implement, and evaluate data backup and recovery capabilities to protect critical information, support recovery objectives, and improve organizational resilience.

BCDR Exercise Walkthrough:

1. Cloud-based Data Recovery Using AWS
2. Disaster Recovery as a Service (DRaaS)
3. Technical Recovery Activities: Multi-system Disruption

Hands-on Labs:

- File Backup and Recovery Using Windows Shadow Copy
- File Recovery Using EaseUS Data Recovery Wizard
- File Backup and Recovery Using BorgBackup
- File Backup and Deduplication Using Windows Server Deduplication
- Full Disk Backup and Restore Using Windows Server Backup
- Image Backup and Recovery Using Windows Server Backup
- System Backup and Recovery Using Windows System Restore
- Hyper-V Snapshot-Based Virtual Machine Backup and Recovery
- Virtual Machine Snapshot Backup and Recovery Using VM Backup v9

Key topics covered:

Data Recovery, Data Backup, Data Restoration, File-Level Recovery, Application-Level Recovery, System-Level Recovery, Database Recovery, Virtual Machine Recovery, Full, Incremental and Differential Backups, Continuous Data Protection (CDP), Cloud Backup, Immutable Backups, Backup Optimization, Ransomware Recovery, Recovery Architectures, Backup and Recovery Technologies, Replication, Snapshots, Deduplication, Compression, Virtualization, Hyper-Converged Infrastructure, Cloud Recovery, Kubernetes, Docker, Cross-Region Recovery, Cross-Account Recovery, AI-Assisted Recovery.

Module 08

Disaster Recovery Plan Development

Learn how to develop a structured, practical, and adaptable Disaster Recovery Plan (DRP) that aligns recovery strategies with business requirements, risk considerations, and organizational resilience objectives.

Key topics covered:

Disaster Recovery Planning, DRP Purpose and Objectives, IT Disruption and Disaster Scenarios, DRP Structure and Components, Roles and Responsibilities, BCP Alignment, Risk and Impact Considerations, Recovery Objectives, Recovery Strategies, Recovery Resources, Personnel and Vendors, Recovery Procedures, Communication and Coordination, AI-Driven Recovery Workflows, Automated Runbook Generation, Plan Maintenance, Intelligent Recovery Documentation, AI Governance, DRP Best Practices.

Module 09

Business Continuity and Disaster Recovery Plan Activation

Learn how to activate and manage business continuity and disaster recovery plans during disruptive events through effective escalation, decision-making, incident command, coordination, and crisis communication.

BCDR Exercise Walkthrough:

- Crisis Communication Plan
- Analyze AI-Generated Activation Recommendations During a Complex Outage Scenario

Key topics covered:

BC/DR Plan Activation, Incident Response vs. BC/DR Activation, Activation Criteria, Crisis Communication, Activation Decision Support, Qualitative and Quantitative Activation Triggers, Partial and Full Plan Activation, Alerting and Escalation, Disaster Declaration, Incident Command Structure, Cross-Team Coordination, Situational Awareness, External Stakeholder Coordination, Crisis Communication, Media Response, Social Media and Misinformation Management, AI-Powered Crisis Communications, Plan Termination, Lessons Learned.

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

Learn how to validate the effectiveness of business continuity and disaster recovery plans through structured testing, training, exercises, performance measurement, audits, and continuous improvement.

BCDR Exercise Walkthrough:

- BCDR Effectiveness and Continuous Improvement

Key topics covered:

BCDR Testing, Training and Exercises, Business Continuity Testing, IT Disaster Recovery Testing, Test Planning, Test Execution, Exercise Classification, Scenario Generation with AI, Progressive Testing Programs, BCDR KPIs and Metrics, Dashboards and Reporting, Recovery Confidence Scoring, Digital Twins, Virtualized Testing, Automation and Orchestration, BCDR Audits, Maturity Models, Corrective Action Management, Lessons Learned, Continuous Improvement, Readiness Programs.

BUILT FOR MODERN RESILIENCE TEAMS

What Skills You'll Gain

Complete Risk-to-Recovery Skillset

After completing the EDRP course, the student will be able to:

- Define and differentiate between Business Continuity (BC) and Disaster Recovery (DR) concepts in enterprise environments.
- Explain organizational resilience principles and their role in continuity planning.
- Identify key BC/DR standards, regulations, and legal requirements impacting organizations.
- Analyze strategic approaches for aligning BC and DR programs with business objectives.
- Apply best practices for designing and maintaining effective BC and DR frameworks.
- Assess emerging technologies and their impact on operational resilience strategies.
- Describe the Business Continuity Management (BCM) lifecycle and PDCA model.
- Conduct business impact analysis (BIA) and interpret its outputs for decision-making.
- Identify critical business functions, dependencies, and recovery priorities.
- Perform risk assessments and classify threats, vulnerabilities, and impacts.
- Develop risk treatment strategies aligned with organizational risk appetite.
- Map dependencies and analyze cascading risks across business and IT environments.
- Establish recovery objectives such as RTO, RPO, and MTD based on business needs.

- Develop and maintain a business continuity plan aligned with organizational requirements.
- Design crisis management and communication strategies during disruptions.
- Construct disaster recovery plans covering IT systems, applications, and data recovery.
- Evaluate disaster recovery strategies, including cloud, hybrid, and automated recovery models.
- Implement data backup and restoration strategies using modern technologies.
- Differentiate between backup models such as full, incremental, differential, and CDP.
- Assess and select appropriate recovery tools, platforms, and architectures.
- Understand cloud-based, virtualization, and container-based recovery approaches.
- Apply best practices for secure, reliable, and efficient data recovery operations.
- Determine conditions for activating BC/DR plans based on risk and impact thresholds.
- Execute plan activation procedures, including escalation, coordination, and communication.
- Coordinate incident response activities using structured command and control frameworks.
- Conduct BCDR testing, training, and exercises to validate readiness and effectiveness.
- Measure and improve organizational resilience using KPIs, audits, and continuous improvement models.

AI-Enabled Business Continuity & Disaster Recovery Skills You'll Gain

- Integrate AI-based tools to support risk analysis and decision-making in continuity planning.
- Utilize AI-enabled monitoring and early warning systems for disruption detection.
- Understand how AI, automation, and analytics enhance modern operational resilience.
- Evaluate the role of AI, ML, and AIOps in modern business continuity and disaster recovery operations.

JOB ROLES

EDRP Maps to Resilience, Risk & Recovery Leadership Roles

EDRP maps to strategic, operational, and advisory roles across business continuity, disaster recovery, IT resilience, and risk management, spanning leadership, technical operations, and consulting career tracks.

Strategic / Leadership Roles	
• BCDR Manager • Business Continuity Officer • Operational Resilience Manager	• BCDR Lead • Crisis Management Officer • Risk & Compliance Manager
IT / Security Operations Roles	
• IT Disaster Recovery Manager • Network Security Manager • IT Risk Manager	• IT Operations Manager • Incident Response Manager
Consulting / Advisory Roles	
• BCDR Consultant • Business Continuity Consultant	• Risk Management Consultant • IT Resilience Consultant

Avg. Salary in the US

Job Role	Average Salary (USD)
Business Continuity Manager	\$123,967
IT Operations Manager	\$117,510
Business Continuity Specialist	\$103,623
Risk Management Consultant	\$103,186
Risk & Compliance Manager	\$95,103
Disaster Recovery Manager	\$86,378

Sources: indeed, ziprecruiter,

WHO SHOULD ENROL IN EDRP?**Built for Resilience Leaders at Every Career Stage**

EDRP is ideal for professionals moving from technical or operational roles into strategic resilience leadership. A recommended 2–4 years of experience in IT infrastructure, network security operations, risk management, incident response, or related fields prepares learners for the program, no mandatory prerequisite is required.

IT & Security Managers

Move beyond protecting systems into building and leading resilient organizations, connecting cybersecurity operations with enterprise BCM and DR planning.

Business Continuity & DR Managers

Modernize legacy BC/DR expertise for cloud, hybrid, and AI-enabled resilience, and strengthen testing and continuous-improvement capability.

Enterprise Risk Managers

Turn risk assessments into actionable recovery priorities by connecting risk management with BIA, BCM, and DR strategy.

Incident Response Managers

Extend incident-response expertise beyond containment into business continuity, crisis coordination, and enterprise recovery leadership.

Aspiring Resilience Leaders

Build an end-to-end understanding of BCM, DR, risk, BIA, crisis management, and governance to move from individual contributor into strategic leadership.

Ideal Prospects

BC/DR professionals, IT & security managers, risk & resilience professionals, incident & crisis managers, and IT audit / GRC professionals.

PROGRAM DETAILS

EDRP Training & Exam Details

Training Information

Course Title	EC-Council Disaster Recovery Professional (EDRP) Version 4
Live Training Duration	5 days
Delivery Mode	Instructor-led training: live online, in-person, and self-paced video lectures
Course Access	1 year e-courseware and training videos
Lab Access	6 months access to hands-on lab environments
Exam Voucher	1-year validity proctored exam voucher
Prerequisites	Recommended 2–4 years of experience in IT infrastructure administration, network security operations, risk management, incident response, or related fields

Exam Information

Exam Code	312-76
Exam Title	EC-Council Disaster Recovery Professional
Number of Questions	150 Questions
Duration	4 Hours
Test Format	Multiple Choice
Passing Score	70%
Availability	ECC Exam Portal

About EC-Council



EC-Council's mission is to build and redefine the cybersecurity profession globally through education, certification, and workforce development, with an expanded focus on AI-enabled and AI-secure enterprises.

Through industry-recognized certifications and training, EC-Council prepares professionals to address challenges across cybersecurity, AI governance, and the secure adoption of AI technologies. Its certification portfolio includes programs such as Certified Ethical Hacker (CEH), Certified Penetration Testing Professional (CPENT), Computer Hacking Forensic Investigator (CHFI), Certified Network Defender (CND), Certified SOC Analyst (CSA), Certified Threat Intelligence Analyst (CTIA), Certified Incident Handler (ECIH), and the Certified Chief Information Security Officer (CCISO). EC-Council also provides cybersecurity

services to some of the largest businesses globally, trusted by 7 of the Fortune 10, 47 of the Fortune 100, the U.S. Department of Defense (DoD), the intelligence community, NATO, and more than 2,000 universities, colleges, and training companies in more than 140 countries.

EC-Council is an ANAB ISO/IEC 17024-accredited organization and has recognition under DoD Directive 8140/8570, as well as recognition in the U.K. by GCHQ and other bodies. Founded in 2001, EC-Council employs more than 400 individuals worldwide and operates 10 global offices in the U.S., U.K., Malaysia, Singapore, India, and Indonesia, including U.S. offices in Albuquerque, New Mexico, and Tampa, Florida.

Learn more at eccouncil.org.

LEAD RECOVERY. STRENGTHEN RESILIENCE.

Build organizational resilience.

Earn a globally recognized credential.

Master business continuity with AI-powered insights.



EC-Council Disaster Recovery Professional

 www.eccouncil.org/edrp