

---

# Global Information Security Society for Professionals of Pakistan



## **Certified Information System Auditor**

### **Information Systems Operations and Business Resilience**

This course is worth 27 percent of the CISA examination  
(about 41 questions)



# Instructor Introduction

## Muhammad Saquib Malik

EMBA (LUMS) – In progress  
MS Information Security  
Certified Information Security Manager (CISM)  
Certified Information Security Auditor (CISA)  
Project Management Professional (PMP)  
Certificate of Cloud Security Knowledge (CCSK)  
Certificate of Cloud Auditing Knowledge (CCAK)  
Privacy and Data Protection Foundation (GDPR)  
IRCA Certified ISO 27001 Lead Auditor (ISMS)  
Certified Information Technology Infrastructure Library (ITIL)  
Certified EC-Council Instructor (CEI)  
Certified Ethical Hacker (CEH)  
Certified Hacking Forensics Investigator (CHFI)  
Certified Secure Computer User (CSCU)  
Certified Administrator for IBM Qradar



Global Information Security Society for Professionals of Pakistan

## Part A: Information Systems Operations



- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-user Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release and Patch Management
- IT Service Level Management.
- Database Management

## Part B: Business Resilience

- Business Impact Analysis
- System Resiliency
- Data Backup, Storage and Restoration
- Business Continuity Plan
- Disaster Recovery Plans



## Part B: Business Resilience

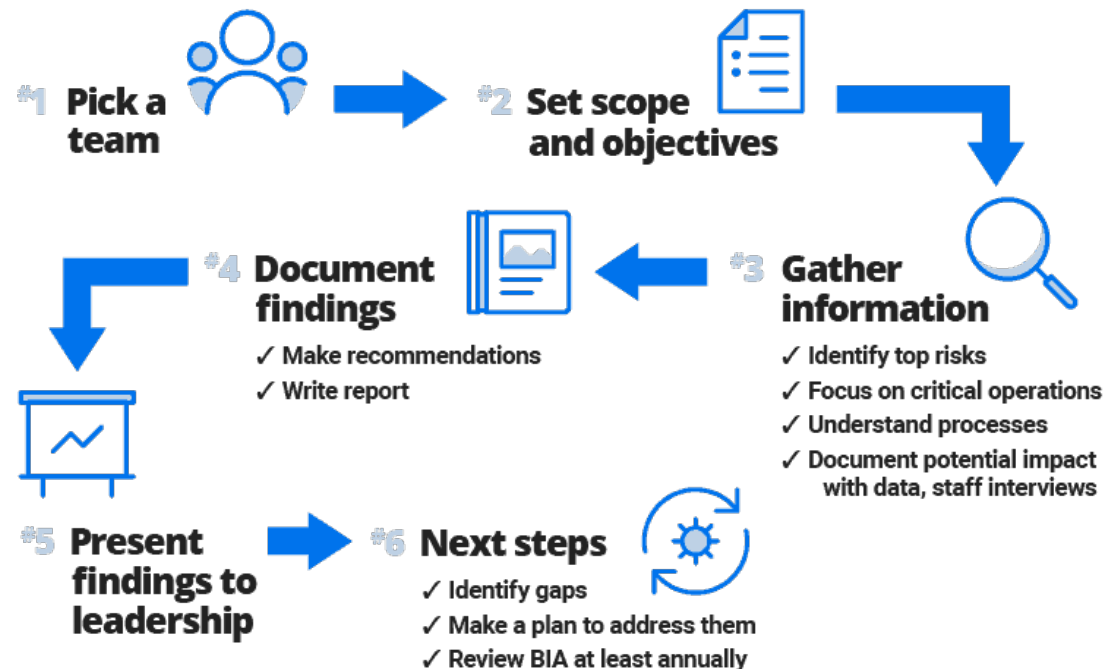


# Business Impact Analysis



A business impact analysis (BIA) **predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.**

## Key Steps in Business Impact Analysis



# Benefits of Business Impact Analysis



| Enhanced functionality                                                           | Reduced cost                                                                     | Increased compliance                                      |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------|
| Interdependencies between processes can be identified & documented               | Elimination of potential fines related to regulatory requirements                | Identification of potential gaps in regulatory compliance |
| Shadow IT functions, often with critical business dependencies can be identified | Removal of unnecessary redundancies – process, people                            |                                                           |
| Identification of new process or process changes to the existing ones            | Identification of potential changes to insurance, maintenance or licensing costs |                                                           |
| Better understanding on the actual impact                                        |                                                                                  |                                                           |

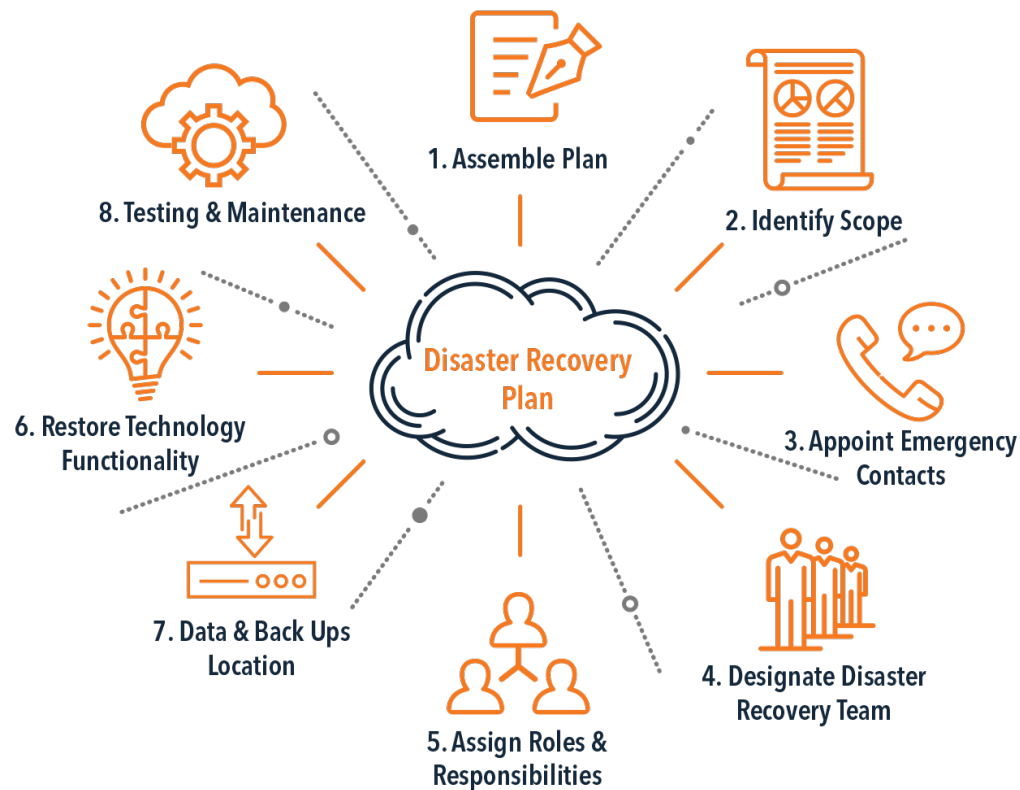
# Quality Assurance



- Verify that all changes have been
  - Authorized
  - Tested
- Implemented in a controlled manner



# Disaster Recovery Planning



- Support of critical business processes.
- Restoration of IT services.
- Cost-effective controls to prevent or recover from IT disruption.

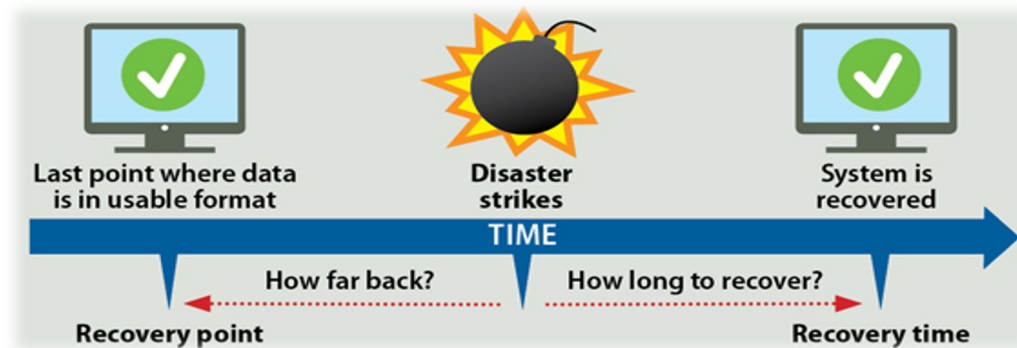
# Role of BIA & Risk Assessment



Determine urgency for recovery

Determine Recovery Point objective (RPO)

Determine Recovery time objective (RTO)



# Disaster Recovery Planning

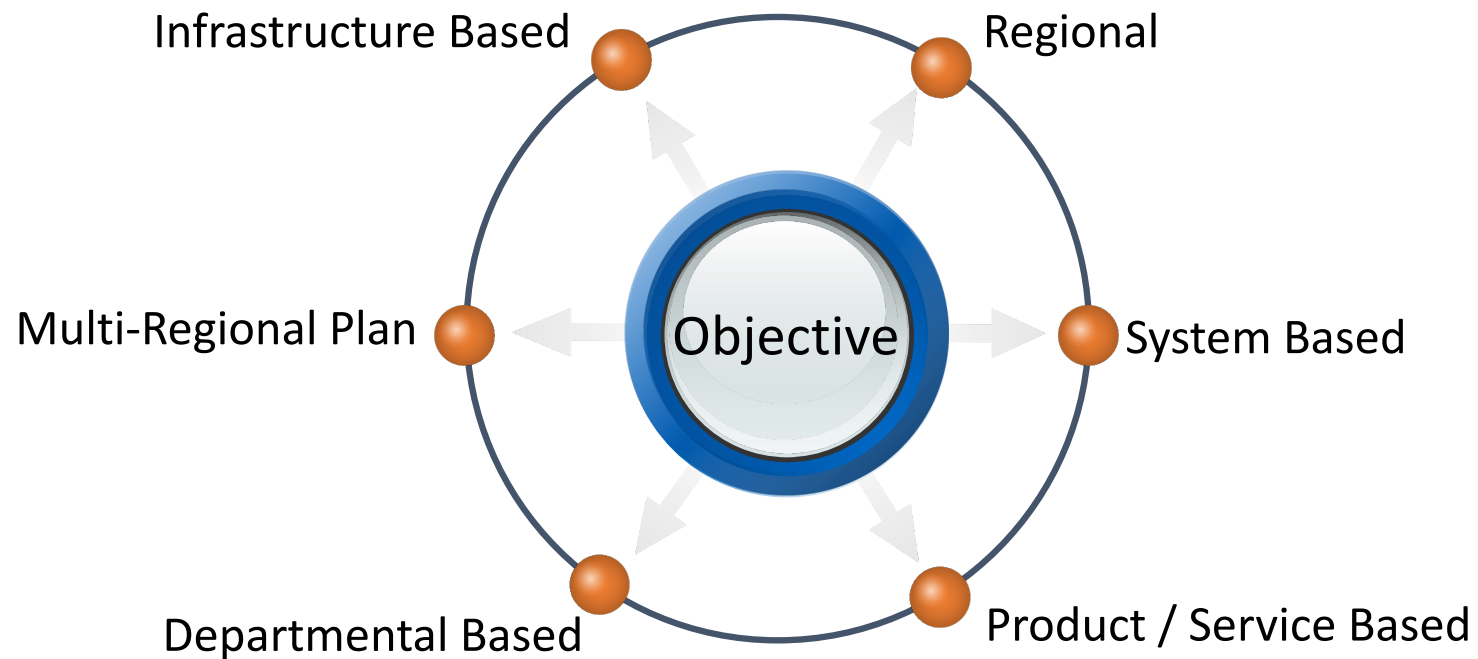


**Continuous process with periodic review**

**Adjust to changing business priorities and requirements**



# The DRP



# Ultimate Goal of DRP



Respond to incidents that may impact  
business and people

Comply with regulations and market demands

# Recovery Point Objective (RPO)



Amount of acceptable data loss

Determines frequency of backups

Depends on data volatility

Influences type of backup media to facilitate recovery

# Recovery Time Objective (RTO)



Acceptable downtime in case of failure

Point when business functions must recover

The shorter the recovery time,  
the higher the cost, normally

# Very Short RTO & RPO



Data Mirroring

Hot Site

Redundant Equipment

Real-time Replication

## Other Terminologies



Interruption window  
Time from business interruption to recovery

Service Delivery Objective (SDO)  
Level of services to be restored at an alternate site or alternate process

# Recovery Strategies



Mirrored Sites



Hot site / Mobile site / Cloud



Warm Site



Cold Site



Reciprocal Agreement



Outsourcing



# Alternate Site Considerations



- Separation distance
- Cost
- Availability
- Cold Site
- Ease of Support. Access / Security



# Contracted Third Party Recovery Site



Configuration & Compatibility

Communication & Activation Process

Priority & Multiple Clients

Security of Site

Reliability of Vendor



# Alternate Hardware & Networks



- Spare equipment's
- Process to acquire necessary equipment
- Network redundancy, diverse routing, availability of bandwidth etc.
- Voice, data, internet service restoration
- Last mile circuit protection

# Application Recovery



Clustering Load Balancing

Redundant servers  
Active-passive

Cloud Services  
Virtual Machines SaaS



# Data Backup



 Electronic vaulting

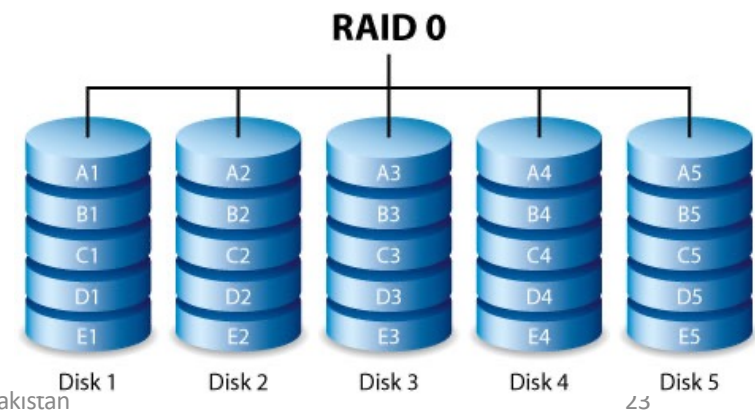
 Tape backups

 RAID - Redundant Array of Independent Disks

# RAID Levels



| RAID    | Configuration                  |
|---------|--------------------------------|
| RAID 0  | Stripping                      |
| RAID 1  | Mirroring                      |
| RAID 2  | Not Used                       |
| RAID 3  | Byte Level Parity              |
| RAID 4  | Block Level Parity             |
| RAID 5  | Interleaved Block Level Parity |
| RAID 10 | Stripping and Mirroring        |



## Type of Backups



Full Backup



Incremental Backup



Differential Backup

## Functionalities of Backups



Encryption



Compression



Rotation & Age of Media

# Writing a DR Plan



List of actions and activities, structured process and procedures required to make disaster recovery efforts effective, efficient, and realistic.

Should be action-based not wordy.

Written simply and clearly so that it could be used by a knowledgeable person that has not previously seen the plan.

# Parts of DR Plan



- Declaration of a disaster.
- Roles of teams and individuals.
- Links to other plans - BCP, Evacuation, etc.
- Contact lists (including internal and suppliers).
- Detailed recovery procedures for systems and applications.
- List of resources required for recovery.

# Disaster Recovery Teams



Application



Network & Communication



Data Storage



Incident Response



Restoration



Logistics & Support



# Reason of Testing DR Plans



Identify gaps

Verify timeframes

Train personnel

Check configuration & Compatibility



# DR Plans Steps



Obtain approval

Execute the test

Evaluate the test

Improve the plan

# Testing DR and Strategy



Checklist test

Structured walkthrough

Simulation

Start small

Parallel

Test with unavailability

Full interruption

Apply lesson learned

Report to management

DANKSCHEEN  
 SPASIBO  
 SHACHALHYA  
 HURUN  
 CHRLTY  
 YAQHANYELAY  
 TASHAKKUR ATU  
 WADEEJA  
 MAITEKA  
 HUI  
 YUSPAGANATAM  
 GRACIAS  
 SUKSAMA  
 EKHMET  
 ARIGATO  
 SHUKURIA  
 MERASTANHY  
 SANCO  
 GOZAIMASHITA  
 EFCHARISTO  
 AGUYJE  
 FAKARUE  
 KOMAPSUMNIDA  
 MAKE  
 LAH  
 GRAZIE  
 MEHRBANI  
 PALDIES  
 THANK  
 YOU  
 BOLZIN  
 MERCI  
 TINGKI  
 BIYAN  
 SHUKRIA  
 MINMONCHAR