Exam Cram Notes: Resilience and Recovery

1. Overview

Resilience and recovery involve strategies to **maintain operations** during disruptions and **restore systems** after failures, cyberattacks, or natural disasters. This includes **fault tolerance, redundancy, backups, and disaster recovery (DR) plans.**

---

2. Fault Tolerance & Redundancy

A. Fault Tolerance

✅ **Ensures continuous operation** even if a component fails.
✅ Uses **redundant systems** to take over in case of failure.

B. Redundancy Strategies

✅ **Server Redundancy –** Load balancing, clustering, or failover servers.
✅ **Power Redundancy –** Uninterruptible Power Supplies (UPS) & backup generators.
✅ **Network Redundancy –** Multiple ISPs, redundant routers, and SD-WAN.
✅ **Data Redundancy –** RAID configurations for fault-tolerant storage.

C. RAID (Redundant Array of Independent Disks)

✅ **RAID 0 (Striping) –** No redundancy, high performance.
✅ **RAID 1 (Mirroring) –** Data duplicated across disks for fault tolerance.
✅ **RAID 5 (Striping with Parity) –** Balanced redundancy & performance.
✅ **RAID 10 (Striping + Mirroring) –** High fault tolerance & performance.

---

3. Disaster Recovery (DR) Strategies

A. Disaster Recovery Sites

✅ **Cold Site –** Basic infrastructure, long setup time.
✅ **Warm Site –** Partial setup with some pre-configured systems.
✅ **Hot Site –** Fully operational backup site, instant failover.

B. Recovery Metrics

✅ **RTO (Recovery Time Objective) –** Maximum downtime allowed before services are restored.
✅ **RPO (Recovery Point Objective) –** Maximum acceptable data loss (e.g., last backup time).
✅ **MTTR (Mean Time to Repair) –** Average time to fix a system after failure.
✅ **MTBF (Mean Time Between Failures) –** Expected system uptime before failure.

C. Disaster Recovery Plan (DRP)

✅ **Business Impact Analysis (BIA)** – Identifies critical systems & potential impacts.
✅ **Tabletop Exercises –** Simulated disaster scenarios to test response plans.
✅ **Runbooks & Playbooks –** Step-by-step recovery procedures.

---

4. Backup & Restore Strategies

A. Backup Types

✅ **Full Backup –** Complete copy of all data (slowest, requires most space).
✅ **Incremental Backup –** Backs up only changed files since the last backup.
✅ **Differential Backup –** Backs up all changes since the last full backup.
✅ **Snapshot Backup –** Captures system state at a point in time.

B. Backup Locations

✅ **On-Premises Backup –** Fast recovery but vulnerable to disasters.
✅ **Cloud Backup –** Remote storage with redundancy & accessibility.
✅ **Offsite Backup –** Secure storage in a different location.
✅ **Air-Gapped Backup –** Physically disconnected storage to prevent ransomware attacks.

C. Backup Retention Policies

✅ Define how long backups should be kept before deletion.
✅ Regulatory compliance (e.g., HIPAA, GDPR) may require long-term retention.

---

5. High Availability (HA) Solutions

A. Load Balancing

✅ **Distributes network traffic across multiple servers** to ensure availability.
✅ **Types**: Round-robin, Least Connections, Source IP Hash.

B. Failover Clustering

✅ **Clustered servers work together** to maintain availability.
✅ One server takes over if another fails.

C. Geographic Redundancy

✅ **Multi-region cloud deployments** ensure uptime.
✅ Protects against local disasters (e.g., hurricanes, fires).

---

6. Incident Response & Business Continuity

A. Incident Response Plan (IRP)

✅ **Detection –** Monitor logs & SIEM for security events.
✅ **Containment** – Isolate affected systems.
✅ **Eradication –** Remove threats (e.g., malware, compromised accounts).
✅ **Recovery –** Restore systems & validate integrity.
✅ **Lessons Learned –** Update policies to prevent recurrence.

B. Business Continuity Plan (BCP)

✅ **Ensures mission-critical operations continue during disruptions.**
✅ **Key Components:**

- Risk assessment
- Communication plans
- Contingency procedures
- Employee training

---

7. Cyber Resilience Strategies

A. Zero Trust Architecture (ZTA)

✅ "Never trust, always verify" **–** Strict access controls.
✅ **Micro-segmentation –** Limits access between network zones.

B. Security Automation

✅ **AI-driven SIEM –** Detects threats & anomalies automatically.
✅ **Automated Response –** Blocks malicious IPs, quarantines infected devices.

C. Supply Chain Resilience

✅ **Diverse suppliers** reduce dependency on a single source.
✅ **Third-party risk management** ensures vendor security.

---

8. Key Exam Takeaways

✅ **Redundancy (RAID, failover clusters, backup power) ensures high availability.**
✅ **Disaster Recovery (DR) plans define RTO/RPO to restore operations.**
✅ **Backups (Full, Incremental, Differential, Air-Gapped) ensure data recovery.**
✅ **Load balancing, failover clustering, and cloud replication prevent downtime.**
✅ **Incident response and business continuity ensure organizations survive cyber incidents.**
✅ **Zero Trust, automation, and supply chain security enhance cyber resilience.**