Session 11 – Chapter 18 (pg. 869-917)

2025 CISSP Mentor Program

CHAPTER 18

Evan Francen

FRSecure

2025 CISSP MENTOR PROGRAM

AGENDA – SESSION 11

Chapter 18 (from the book)

Disaster Recovery Planning

- The Nature of Disaster
- Understand System Resilience, High Availability, and Fault Tolerance
- Recovery Strategy
- Recovery Plan Development
- Training, Awareness, and Documentation
- Testing and Maintenance

After we're done with this, we'll roll into Chapter 19.


RESILIENT CORP
Oh SNAP!
Wait a second…
It’s time for a dad joke!
DISASTER RECOVERY SYSTEM ONLINE
DISASTER RECOVERY SYSEM ONLINE
DISASTER RECOVERY SYSTM ONLINE
DISASTER RECOVERY SYSTEM ONLIE


Why don’t hackers ever take vacations?
Because they can’t stop phishing—even on the weekend.
VACATION MODE

CHAPTER 18

The Nature of Disaster

Disasters aren't just hurricanes and house fires—in information security, a disaster is **any event that disrupts normal operations and exceeds an organization's ability to quickly respond using standard procedures**.

These can be **natural** (earthquakes, floods), **technical** (hardware failure, data corruption), or **human-made** (cyberattacks, sabotage, even clumsy Carl tripping over the server cable).

The key characteristic? They cause **significant business impact** and require a **coordinated recovery effort**.

In CISSP terms, understanding the nature of disaster means recognizing:

- **Disruption magnitude** – when it overwhelms day-to-day continuity controls.
- **Scope of impact** – from data loss and downtime to reputational damage.
- **Unpredictability** – timing and nature of disasters vary wildly, so planning must be flexible and comprehensive.

CHAPTER 18

The Nature of Disaster

Natural Disasters

- Natural disasters are **uncontrollable environmental events** that can cause significant disruption to business operations.
- You need to understand **how these events threaten information systems**, and **how disaster recovery plans must account for them**.

Earthquakes

- Can destroy buildings, power grids, and telecommunications.
- Risk includes physical destruction of data centers, server farms, and infrastructure.
- Impacts may include complete loss of facilities, data, and long recovery times.

Mitigation: Seismic-resistant construction, offsite backups, geographically diverse data centers.

CH

The

Natu

- Na
  sig
- Yo
  ho

Ear

- C
- R
  a
- I
  r

https://www.usgs.gov/programs/earthquake-hazards/earthquakes

An official website of the United States government Here's how you know

USGS science for a changing world

SCIENCE PRODUCTS NEWS CONNECT ABOUT

Latest Earthquakes

EARTHQUAKE HAZARDS PROGRAM

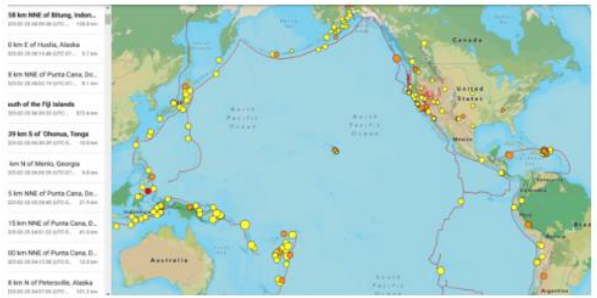
Earthquakes

By Earthquake Hazards Program

- HOME
- EARTHQUAKES
  - Latest Earthquakes
  - Lists, Maps, and Statistics
  - Special Earthquakes, Earthquake Sequences, and Fault Zones
  - Earthquake Photo Collections
  - Search Earthquake Catalog
  - Real-time Notifications
  - Information by Region
- HAZARDS
- SCIENCE

Find recent or historic earthquakes, lists, information on selected significant earthquakes, earthquake resources by state, or find webservices.

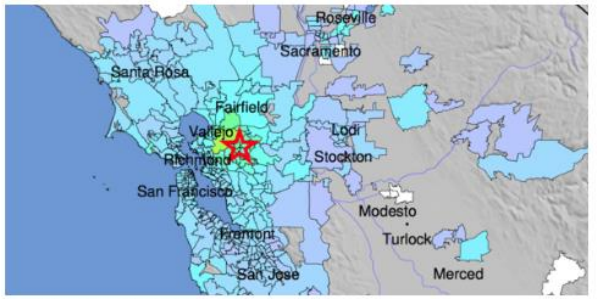
Latest Earthquakes



Latest earthquakes map and list for U.S. and worldwide. Tap/click on "gear icon" for options and settings.

Interactive Map

Did You Feel It?



Did You Feel It? (DYFI) collects information from people who felt an earthquake and creates maps that show what people experienced and the extent of damage. If you felt an earthquake, let us know.

CHAPTER 18

The Nature of Disaster

Natural Disasters

- Natural disasters are **uncontrollable environmental events** that can cause significant disruption to business operations.
- You need to understand **how these events threaten information systems**, and **how disaster recovery plans must account for them**.

Floods

- Caused by storms, hurricanes, or rising water tables.
- Destroys electrical systems, storage media, and physical records.
- Often leads to short circuits, mold, and corrosion of hardware.

Mitigation: Build in non-flood zones, elevate critical equipment, use water detection systems.

CHA

The N

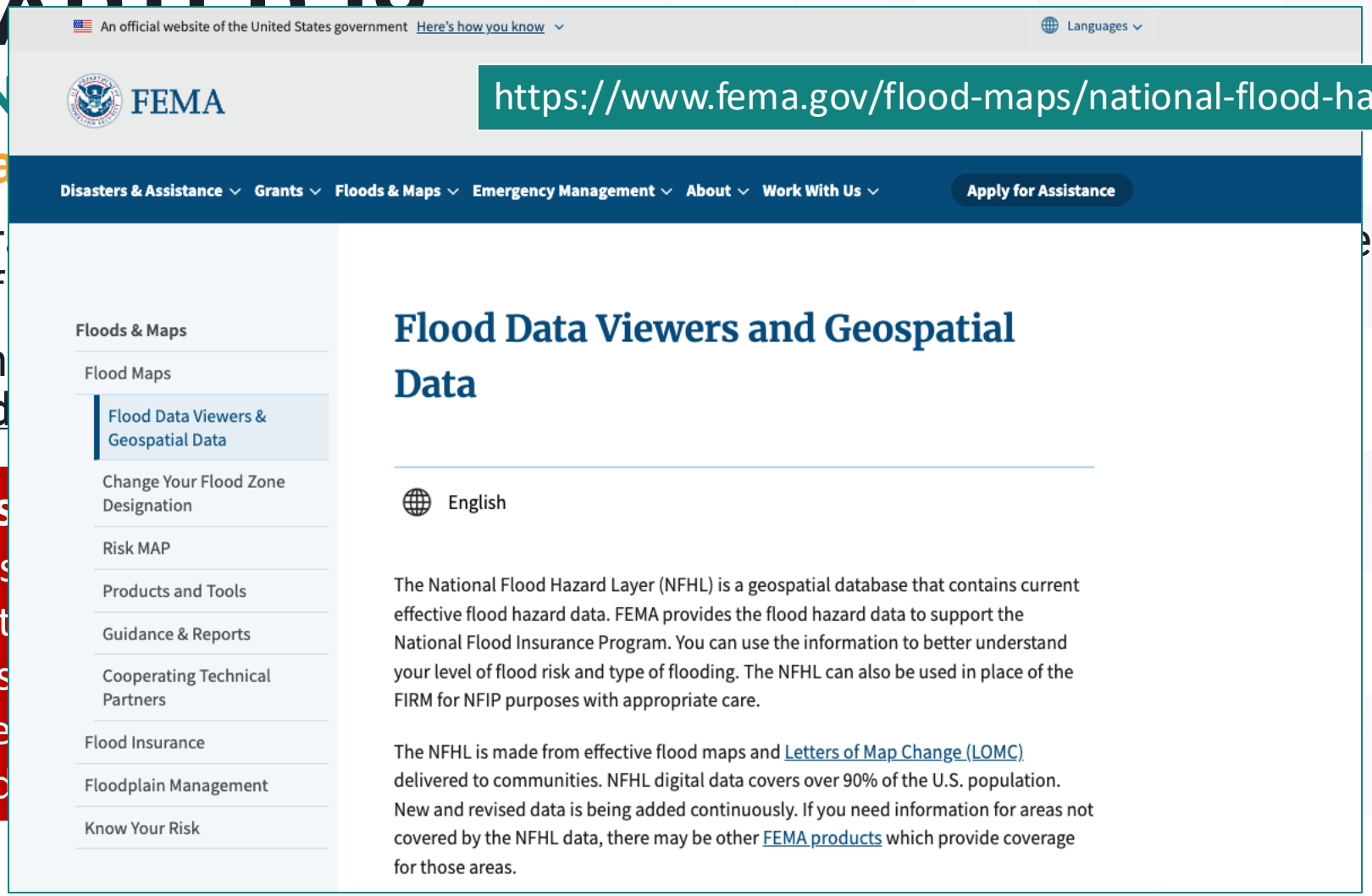
Natura

- Natur
  signif
- You n
  how d

Floods

- Caus
- Dest
  phys
- Ofte
  hard

https://www.fema.gov/flood-maps/national-flood-hazard-layer



CHAPTER 18

The Nature of Disaster

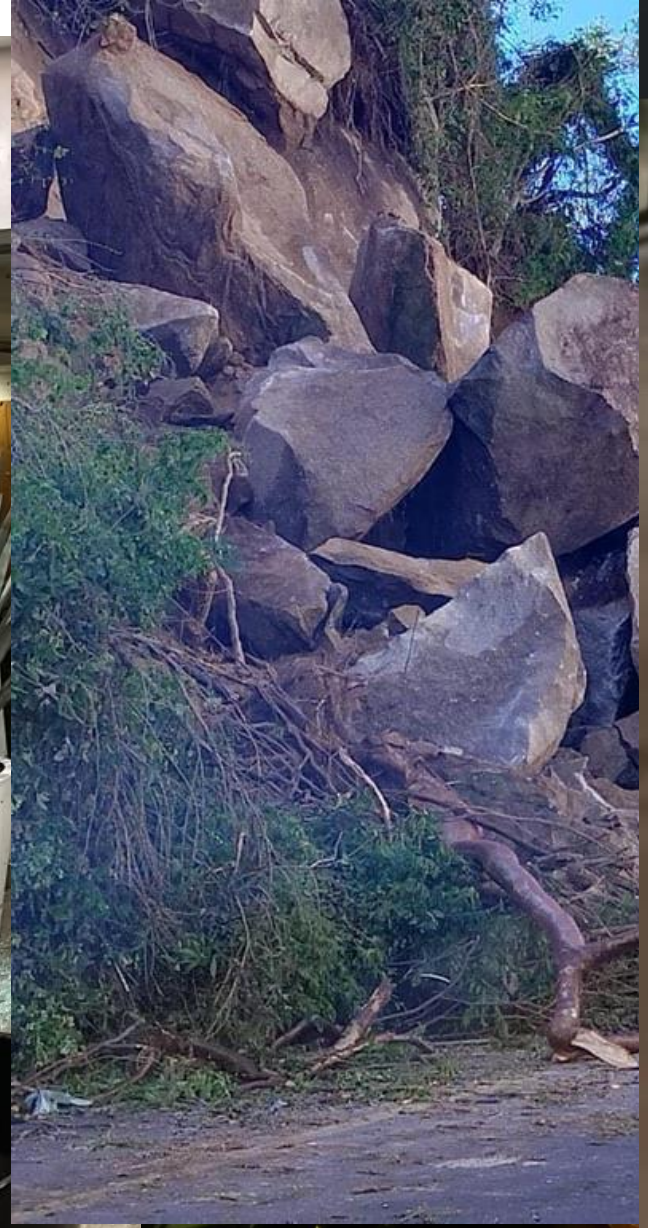
Natural Disasters

- Natural disasters are **uncontrollable environmental events** that can cause significant disruption to business operations.
- You need to understand **how these events threaten information systems**, and **how disaster recovery plans must account for them**.

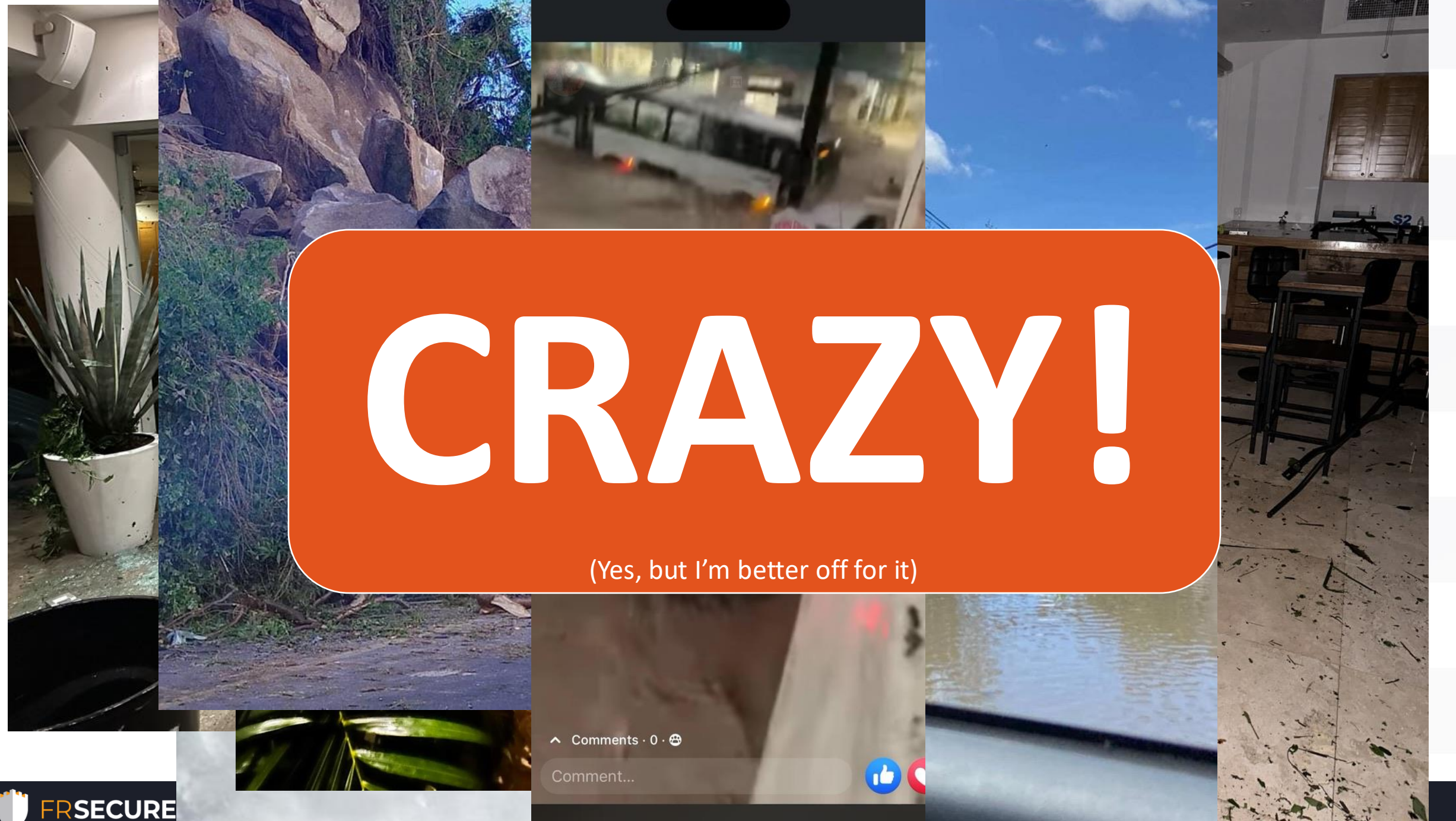
Storms (Hurricanes, Tornadoes, Blizzards)

- High winds and flying debris can cause structural damage and long-term power outages.
- Hurricanes can combine flooding and wind damage.
- Snowstorms can impact accessibility and cause roof collapses.

Mitigation: Reinforced buildings, uninterruptible power supplies (UPS), backup generators.




Comments · 0 ·
Comment...


CRAZY!
(Yes, but I’m better off for it)
Comments · 0 ·
Comment...

CHAPTER 18

The Nature of Disaster

Natural Disasters

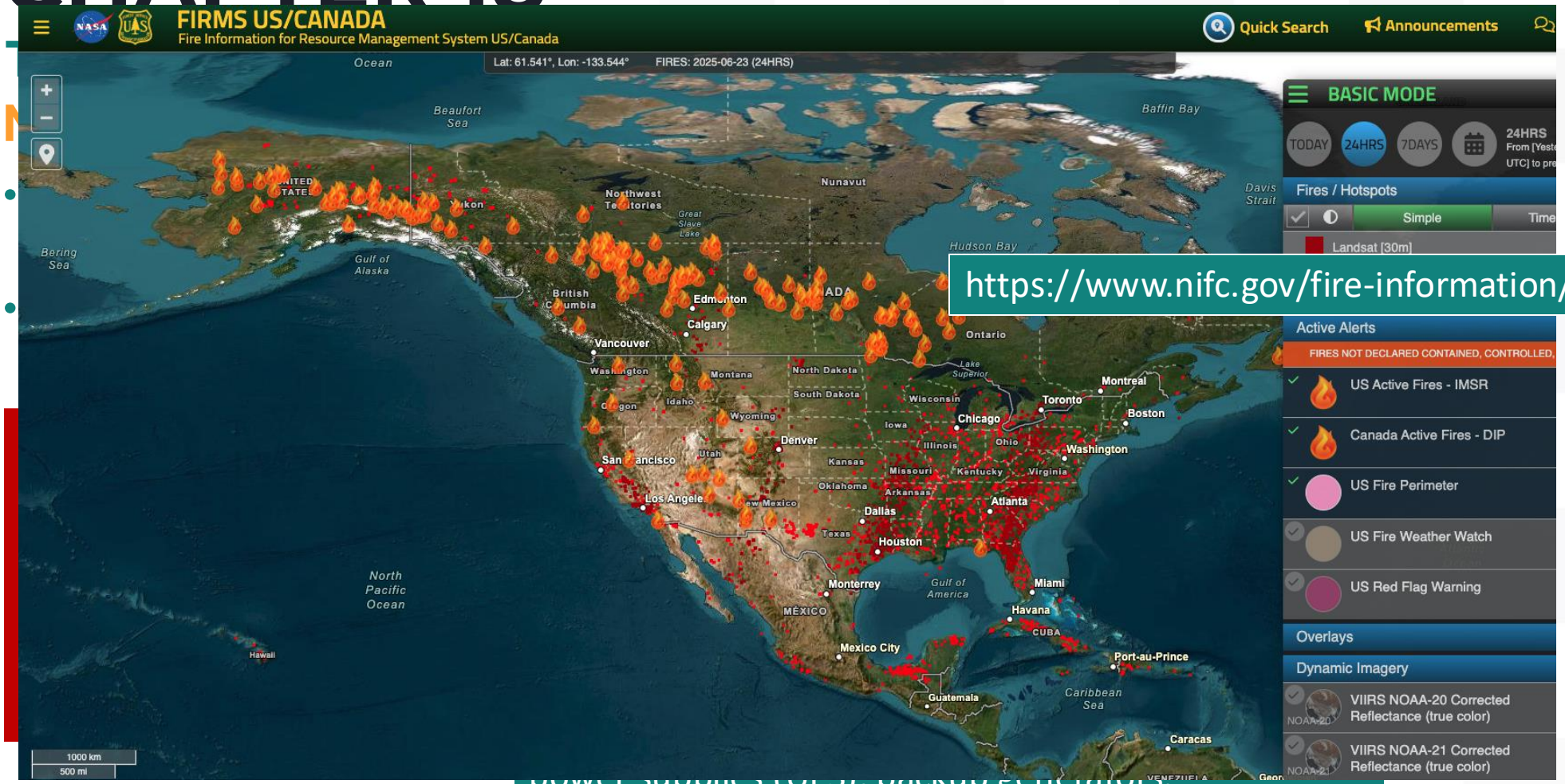
- Natural disasters are **uncontrollable environmental events** that can cause significant disruption to business operations.
- You need to understand **how these events threaten information systems**, and **how disaster recovery plans must account for them**.

Fires and Wildfires

- Common and extremely destructive.
- Damage includes heat, smoke, water damage from suppression systems, and total destruction.
- Often triggered by electrical faults, human error, or nearby wildfires.

Mitigation: Reinforced buildings, uninterruptible power supplies (UPS), backup generators.

CHAPTER 18



https://www.nifc.gov/fire-information/maps

power supplies (UPS), backup generators.

CHAPTER 18

The Nature of Disaster

Natural Disasters

- Natural disasters are **uncontrollable environmental events** that can cause significant disruption to business operations.
- You need to understand **how these events threaten information systems**, and **how disaster recovery plans must account for them**.

Pandemics

- Not a physical disaster but impacts workforce availability and logistics.
- COVID-19 made this real—supply chains, remote access, and telework infrastructure were key.
- Focus on business continuity, not just system recovery.

Mitigation: Robust remote access policies, cloud services, redundancy in staffing and suppliers.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

The Nature of Disaster

Human Made Disasters

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

Acts of Terrorism / Bombings / Explosions

- Targets may include infrastructure, personnel, or public symbols.
- Effects range from physical damage and casualties to psychological impact and long-term downtime.
- Bombings and explosions may sever power, damage comms, or destroy facilities.

DR Planning: Evacuation procedures, alternate sites, remote work capability, coordination with law enforcement

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

Power Outages

- Often caused by grid failure, accidents, or severe weather, but also susceptible to sabotage.
- Downtime impacts data centers, HVAC systems, communication systems, etc.
- Prolonged outages can lead to data corruption, hardware failure, or environmental hazards.

DR Planning: UPS systems, generators, redundant power feeds, energy storage solutions.

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

Network/Utility/Infrastructure Failures

- Includes internet blackouts, ISP outages, water/gas failures, or backbone network collapses.
- May stem from misconfiguration, cyberattack, supply chain failure, or third-party issues.
- Can prevent access to cloud services, VoIP systems, or collaboration tools.

DR Planning: Multiple ISPs, SLAs with providers, offline contingencies, failover systems.

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

Hardware/Software Failures

- Covers server crashes, storage device failure, software bugs, patch issues, and application errors.
- Can result from aging hardware, poor QA, or zero-day exploitation.
- Risk of data loss, service interruption, or unplanned downtime.

DR Planning: Hardware redundancy, clustering, backups, version control, rollback plans.

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

Strikes / Labor Disputes / Picketing

- Can delay physical access, interrupt services, or block supply chains.
- Particularly relevant in transportation, manufacturing, and public sector.

DR Planning: Contingency staffing, vendor diversity, remote work support.

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- **Non-natural**, **often preventable** events that result from **human actions**—malicious **OR** accidental
- Understanding these risks helps build a more robust disaster recovery (DR) and business continuity (BC) posture.

Theft / Vandalism / Insider Threats

- Physical theft of hardware, documents, devices or deliberate damage to property/systems.
- Vandalism may target buildings, cabling, or signage, while insiders might sabotage systems or leak data.

DR Planning: Access controls, surveillance, incident response playbooks, forensic readiness.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

The Nature of Disaster

Human Made Disasters

- N
  m
- U
  bu

Th
- leak data.

DR Plannin
response p

CISSP Critical Takeaways

- Human-made disasters often involve malicious intent or negligence and are usually unpredictable in scope or timing.
- DR must plan for people-based contingencies as much as system-based ones.
- Training, detection, and layered defense are crucial in mitigation.
- Ensure incident response and business continuity teams are aligned and equipped to handle diverse threats.

Human Nature

- VERY short memories.
- Rarely think it’s going to happen to “us”.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Single Point of Failure (SPOF)

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Single Point of Failure (SPOF)

- Any **individual component**—hardware, software, or process—whose failure would cause the entire system or service to go down.

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Single Point of Failure (SPOF)

- Any **individual component**—hardware, software, or process—whose failure would cause the entire system or service to go down.
- In simpler terms: **if this one thing breaks, everything breaks**.

Examples:

- A server with no backup or failover.
- A single internet connection for a data center.
- One IT admin who knows all the passwords (and then quits).

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Single Point of Failure (S

- Any **individual component**— cause the entire system or s
- In simpler terms: **if this one**

Why it matters in CISSP:

- SPOFs (should) represent unacceptable risk in critical systems.
- Good architecture uses redundancy (load balancers, clusters, backup links) to eliminate SPOFs.
- Addressing SPOFs improves availability and resilience, two pillars of CIA (Confidentiality, Integrity, Availability).

Examples:

- A server with no backup or failover.
- A single internet connection for a data center.
- One IT admin who knows all the passwords (and then quits).

You want systems that fail gracefully, not catastrophically. Spotting and fixing SPOFs is a core disaster recovery and risk management skill.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

System Resilience

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

System Resilience

- The ability of a system to **continue operating during and after a disruption**, and to recover quickly from failures.

Whether caused by hardware faults, cyberattacks, natural disasters, or human error.

Think of it as:

- Not just preventing failure but bouncing back fast.
- Built on redundancy, fault tolerance, failover mechanisms, and robust incident response.

Key elements:

- Redundant systems (e.g., RAID, clustered servers)
- Automated recovery processes
- Graceful degradation (system stays partially functional under strain)
- Regular testing and adaptation

CHA

Unders
Fault T

- System resilience strengthens the **availability** aspect of the CIA triad and is central to disaster recovery, business continuity, and risk management.
- Basically, resilience is your system's version of *"fall down seven times, get up eight."*

System Resilience

- The ability of a system to **continue operating during and after a disruption**, and to recover quickly from failures.

Whether caused by hardware faults, cyberattacks, natural disasters, or human error.

Think of it as:

- Not just preventing failure but bouncing back fast.
- Built on redundancy, fault tolerance, failover mechanisms, and robust incident response.

Key elements:

- Redundant systems (e.g., RAID, clustered servers)
- Automated recovery processes
- Graceful degradation (system stays partially functional under strain)
- Regular testing and adaptation

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Fault Tolerance

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Fault Tolerance

- A system's ability to **continue functioning properly** even when one or more of its components fail.

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Fault Tolerance

- A system's ability to **continue functioning properly** even when one or more of its components fail.
- It doesn't just recover - **it absorbs the hit and keeps going** without interrupting service.

How it works:

- Uses redundant hardware, software, or processes.
- **Examples**: RAID storage, dual power supplies, server clustering.

Bottom line: Fault tolerance is like flying a plane with two engines—if one dies, you're still in the air.

CISSP Context:

- Supports high availability and resilience.
- Essential in critical systems where downtime isn't an option (e.g., hospitals, financial systems).

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

High Availability

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

High Availability

It's all about maximizing uptime—even when things go sideways.

- **High Availability (HA)** means a system is **designed to stay operational and accessible as much of the time as possible**, typically with **minimal downtime**.

Core Concepts:

- Achieved through redundancy, failover, and load balancing.
- Often measured in "nines" (e.g., 99.999% uptime = ~5 minutes of downtime per year).

CISSP Relevance:

- Supports availability in the CIA triad.
- Critical for business continuity and disaster recovery planning.
- HA is proactive, while disaster recovery is reactive—but both are essential.

Think of HA like a 24/7 diner—it never closes, even when the grill breaks.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Protecting Hard Drives

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

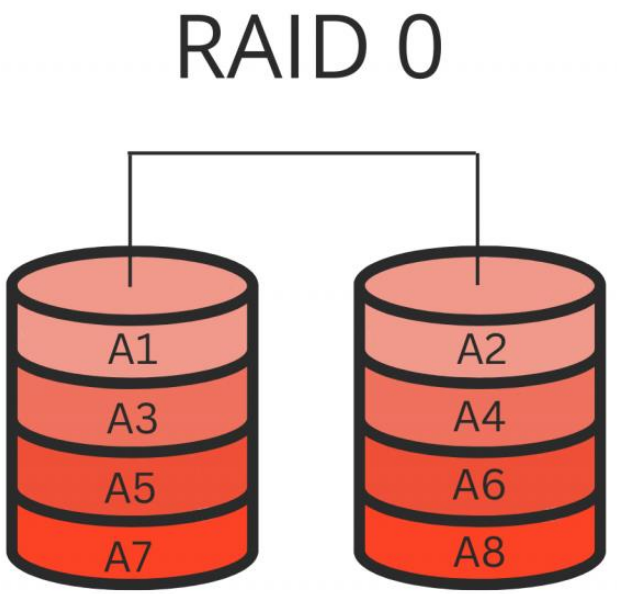
Protecting Hard Drives

RAID-0 (Striping) splits data evenly across two or more disks, with no redundancy. It's designed purely for speed, not safety.

Key Points:

- Performance boost: Reads/writes are faster because operations are split.
- No fault tolerance: If one disk fails, all data is lost.
- Minimum of two disks required.

CISSP Takeaway: RAID-0 is not fault tolerant and offers zero data protection. It's used in scenarios where performance is the only priority—not availability or resilience.



RAID-0 is like a race car: fast as hell, but one crash and it’s toast.

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

RAID-1 is like having a twin—if one goes down, the other picks up the slack.

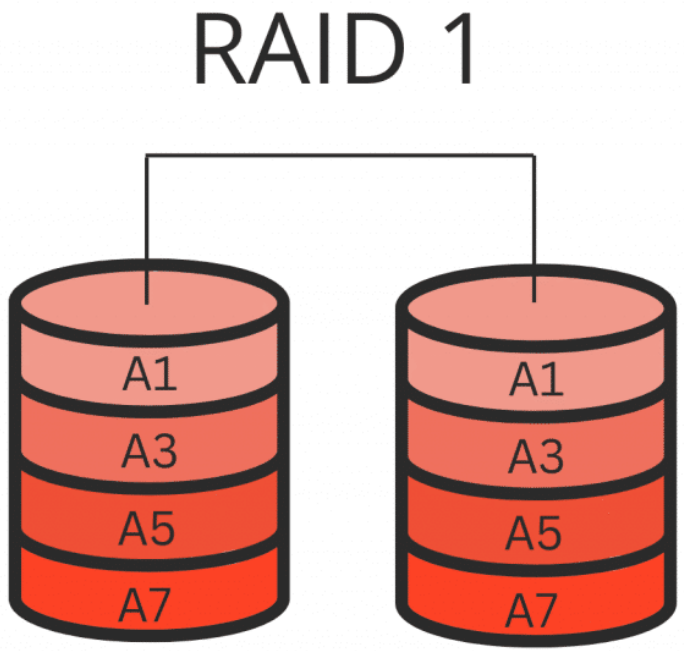
Protecting Hard Drives

RAID-1 (Mirroring) stores identical copies of data on two or more disks. If one fails, the system keeps running using the other(s).

Key Points:

- High fault tolerance: One disk can fail without data loss.
- No performance gain for writes; slight improvement for reads.
- Requires at least two disks.

CISSP Relevance: RAID-1 supports availability and data integrity, making it great for critical systems where uptime matters more than storage efficiency.



CHAPTER 18

Think of RAID-5 like a group project where one member keeps backup notes—if someone bails, the data's still covered.

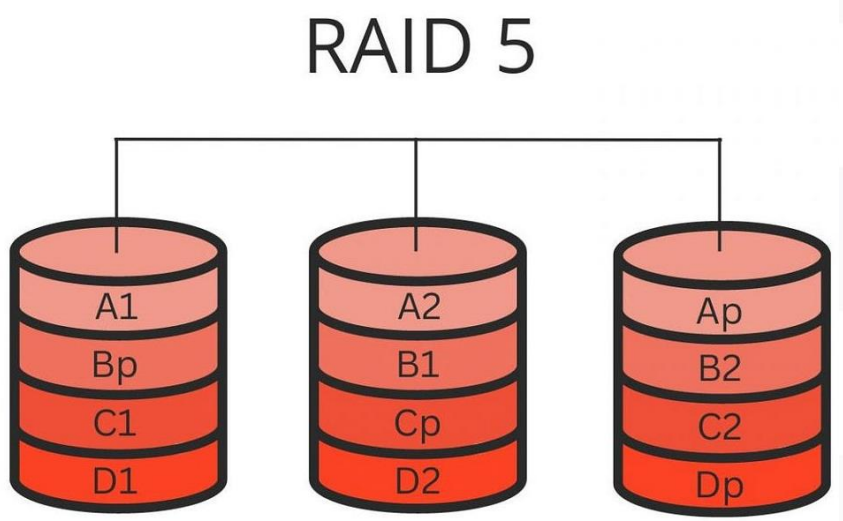
Understand System Resilience, High Availability, and Fault Tolerance

Protecting Hard Drives

RAID-5 (Striping with Parity) stripes data across **three or more disks** and adds **parity** data, which allows the system to recover if one disk fails.

Key Points:

- Fault tolerance: Survives the loss of one disk.
- Efficient use of space: Only one disk's worth used for parity.
- Good read performance, write performance is moderate due to parity calculations.
- Minimum of three disks required.



CISSP Relevance: RAID-5 balances performance, fault tolerance, and capacity—a common choice for systems needing resilience without sacrificing too much storage.

CHAPTER 18

RAID-10 is like a luxury SUV: fast, safe, and sturdy—but you're paying for it.

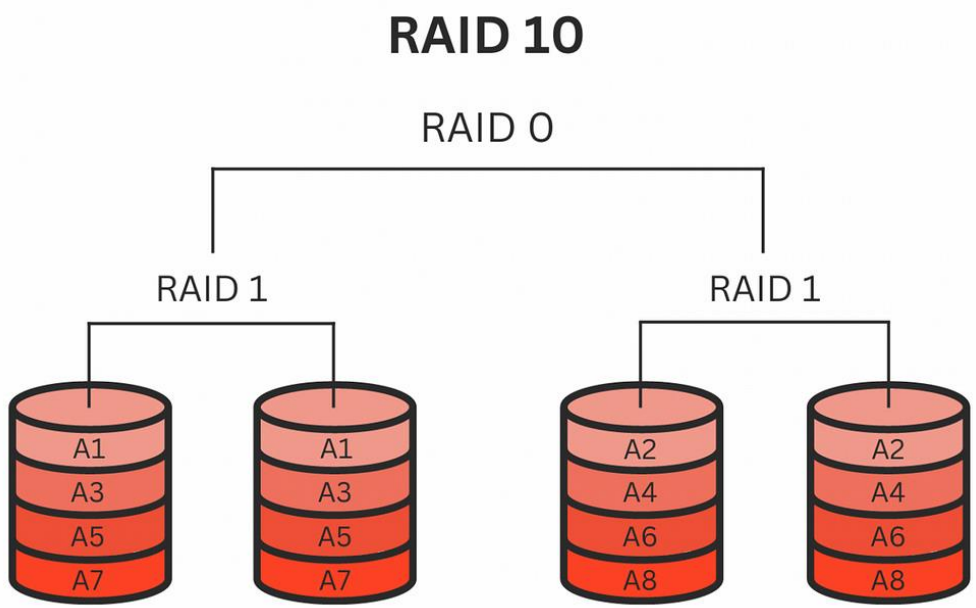
Understand System Resilience, High Availability, and Fault Tolerance

Protecting Hard Drives

RAID-10 combines mirroring (RAID-1) and striping (RAID-0): it mirrors data for redundancy and stripes it for performance. It's the best of both worlds, if you've got the hardware.

Key Points:

- High performance (like RAID-0).
- High fault tolerance (like RAID-1)—can survive one disk failure per mirrored pair.
- Requires at least four disks.
- Great for high-availability, high-speed environments like databases.



CISSP Relevance: RAID-10 is ideal for systems needing speed and resilience, but it's more expensive in terms of storage efficiency (50% usable space).

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Protecting Hard Drives

RAID Level	Min Disks	Redundancy	Performance	Fault Tolerance	Storage Efficiency	Use Case
RAID-0	2	None	High	None	100%	Speed-focused, non-critical systems
RAID-1	2	Yes	(-)Write / (+)Read	1 disk	50%	Critical data, high availability
RAID-5	3	Yes (single parity)	(+)Read / (-)Write	1 disk	~67–94%	Balanced performance & protection
RAID-6	4	Yes (dual parity)	(+)Read / (-)(-)Write	2 disks	~50–88%	Large arrays, higher fault tolerance
RAID-10	4	Yes (mirror + stripe)	(+)(+)High	Multiple (1 per mirror pair)	50%	High-speed, high-availability apps

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Protecting Servers

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Protecting Servers

Think of failover like a relay race baton handoff—if one runner falls, the next is already sprinting.

Failover is the automatic switching to a backup system or component when the primary one fails.

It's all about **keeping services running** without user disruption.

Key Points:

- Can apply to servers, networks, databases, etc.
- Typically involves redundant systems standing by or running in parallel.
- Should be automated and tested regularly.

CISSP Relevance: Failover supports high availability and system resilience—both essential to the Availability piece of the CIA triad.

CHAPTER 18

Understand System Resilience, High Availability, and Fault

Think of failover like a relay race baton handoff—if one runner falls, the next is already sprinting.

Protec

Failov

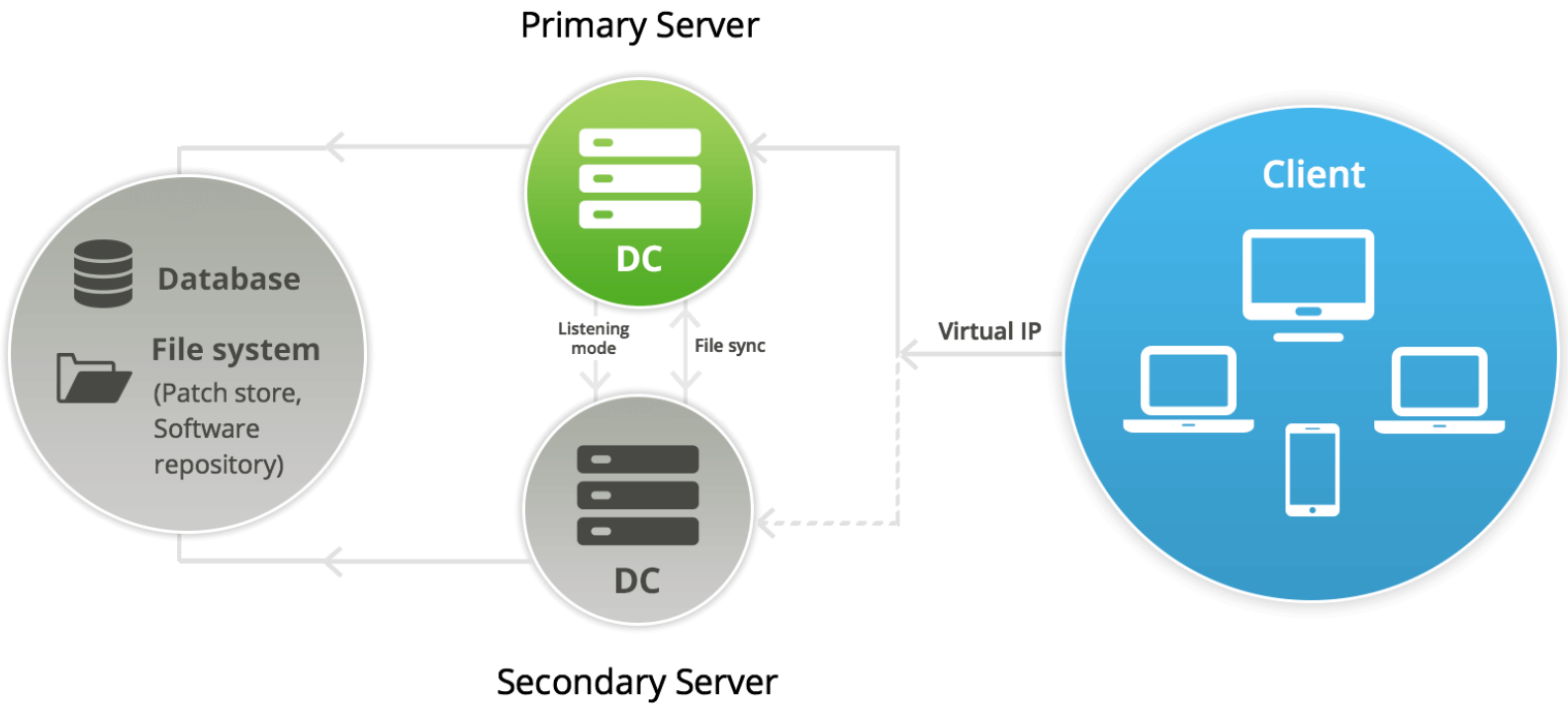
primary

n the

It's all a

Key P

- Car
- Typ
  by
- Sho



orts high availability and system resilience—both essential to the Availability piece of the CIA triad.

CHAPTER 18

Think of it like multiple checkout lanes—no one line gets too long.

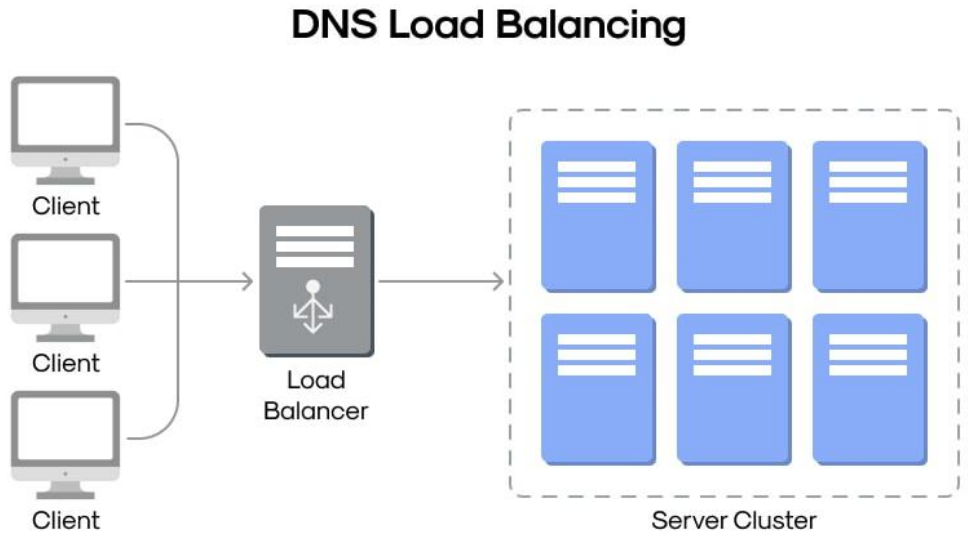
Understand System Resilience, High Availability, and Fault Tolerance

Protecting Servers

Load balancing distributes incoming traffic or processing load across multiple systems or resources to **optimize performance** and prevent overload.

Key Points:

- Common in web servers, app servers, databases.
- Can be hardware or software-based.
- Enhances availability, scalability, and fault tolerance.



CHAPTER 18

Think of it like life support for your data center—if the juice cuts out, you need backup lungs now, not later.

Understand System Resilience, High Availability, and Fault Tolerance

Protecting Power Sources

Protecting power sources means ensuring that systems have a reliable and uninterrupted flow of electricity, even during outages or fluctuations, to maintain uptime and prevent data loss or hardware damage.

Key Components:

- **Uninterruptible Power Supply (UPS)**: Provides immediate, short-term power during outages—gives time to shut down or switch to generators.
- **Backup Generators**: Long-term power solution for extended outages.
- **Power Conditioning**: Regulates voltage and filters surges/spikes.
- **Redundant Power Feeds**: Multiple circuits to prevent single points of failure.
- **Battery Monitoring & Maintenance**: Ensures backup power actually works when needed.

CISSP Context: Protecting power supports availability, part of the CIA triad, and is a must-have in disaster recovery and business continuity planning.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Trusted Recovery

CHAPTER 18

Think of it like waking up from surgery: you don't just want to survive—you want all your organs accounted for and no one messing with your wallet while you're under.

Understand System Resilience, High Availability, and Fault Tolerance

Trusted Recovery

Ensures that a system can return to a **secure state after a failure or crash**, without compromising security controls or exposing sensitive data.

Key Points:

- Preserves security policies and integrity during and after recovery.
- Prevents unauthorized access, data corruption, or bypassing of controls.
- Can include automated or manual recovery processes, system logs, and integrity checks.

CISSP Angle: Trusted recovery is a key part of system resilience and supports both integrity and availability within the CIA triad.

CHAPTER 18

Think of it like waking up from surgery: you don't just want to survive—you want all your organs accounted for and no one messing with your wallet while you're under.

Understand System Resilience, High Availability, and Fault Tolerance

Trusted Recovery

Ensures that a system can return to a **secure state after a failure or crash**, without compromising security controls or exposing sensitive data.

Manual Recovery

- Human intervention required to restore the system.
- Often used for sensitive or complex systems where automated recovery could introduce risk.
- Ensures that security controls are checked before reactivation.

Example: Admin must verify file integrity before restarting a crashed secure server.

CHAPTER 18

Think of it like waking up from surgery: you don't just want to survive—you want all your organs accounted for and no one messing with your wallet while you're under.

Understand System Resilience, High Availability, and Fault Tolerance

Trusted Recovery

Ensures that a system can return to a **secure state after a failure or crash**, without compromising security controls or exposing sensitive data.

Automated Recovery

- System recovers automatically after a failure.
- Quick but must maintain security configurations and controls during recovery.
- Typically used for less critical or time-sensitive systems.

Example: A server auto-reboots after a crash and resumes normal operations while preserving audit logs.

CHAPTER 18

Think of it like waking up from surgery: you don't just want to survive—you want all your organs accounted for and no one messing with your wallet while you're under.

Understand System Resilience, High Availability, and Fault Tolerance

Trusted Recovery

Ensures that a system can return to a **secure state after a failure or crash**, without compromising security controls or exposing sensitive data.

Automated Recovery Without Undue Loss

- Automated recovery that ensures no loss of data or security—everything resumes exactly where it left off.
- Focuses on data consistency and control integrity.
- More complex, but vital for transactional or high-security systems.

Example: A financial system restores to the last known good state without losing in-flight transactions.

CHAPTER 18

Think of it like waking up from surgery: you don't just want to survive—you want all your organs accounted for and no one messing with your wallet while you're under.

Understand System Resilience, High Availability, and Fault Tolerance

Trusted Recovery

Ensures that a system can return to a **secure state after a failure or crash**, without compromising security controls or exposing sensitive data.

Function Recovery

- Ensures that only the authorized system functions resume after recovery.
- Prevents unauthorized processes or bypassing of controls.
- Critical for multi-function systems or those with varied access levels.

Example: Only approved services restart after recovery—not admin tools or debug modes.

These recovery types ensure that systems don't just reboot—they reboot right, without handing attackers an open door or losing critical data.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Quality of Service (QoS)

CHAPTER 18

Think of QoS like the VIP lane on a highway—important traffic always gets through first.

Understand System Resilience, High Availability, and Fault Tolerance

Quality of Service (QoS)

Refers to the ability to manage network traffic to ensure the performance of critical applications and services—especially when bandwidth is limited or networks are congested.

Key Features

- **Traffic prioritization**: High-priority data (like VoIP or video conferencing) gets precedence over less critical traffic.
- **Bandwidth allocation**: Guarantees minimum throughput for key services.
- **Latency/jitter control**: Reduces delays and variability in data delivery.

CISSP Context: QoS supports **availability and performance**, particularly in environments where service degradation = business disruption. It's vital in BCP/DR, network security, and SLA compliance.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Understand System Resilience, High Availability, and Fault Tolerance

Think of QoS like the VIP lane on a highway—important traffic always gets through first.

Quality of Service (QoS)

Bandwidth
- The maximum amount of data that can be transmitted over a network in a given time.
- Measured in Mbps, Gbps, etc.
- Think of it as highway width—the more lanes, the more traffic it can carry.

Latency
- The time it takes for data to travel from source to destination.
- Measured in milliseconds (ms).
- Low latency = faster responsiveness.
- Like the travel time on that highway.

Jitter
- The variation in latency between data packets.
- Causes choppy audio/video and poor real-time communication.
- Like traffic randomly speeding up and slowing down on the road.

Packet Loss
- When data packets fail to reach their destination.
- Results in incomplete or corrupted data (e.g., dropped calls, buffering).
- Can be caused by congestion, hardware faults, or interference.

Interference
- Any external signal disruption that degrades data transmission.
- Common in wireless networks (e.g., microwaves, walls, overlapping Wi-Fi).
- Think static on a radio—it messes with the signal clarity.

CHAPTER 18

Recovery Strategy

Think of it as the playbook for getting back in the game after taking a major hit.

A predefined plan for restoring critical business functions and IT systems after a disruption or disaster.

Key Elements:

- Aligned with **Business Impact Analysis (BIA)** findings.
- Includes plans for data recovery, system restoration, alternate sites, manual workarounds, and communications.
- Focused on meeting **Recovery Time Objectives (RTO)** and **Recovery Point Objectives (RPO).**

CISSP Relevance: A solid recovery strategy ensures availability and continuity, reducing downtime and limiting loss after a disaster. It's a key component of Disaster Recovery Planning (DRP) and Business Continuity Planning (BCP).

CHAPTER 18

Recovery Strategy

Business Unit and Functional Priorities

Think of it like triage in an ER—you fix what's bleeding out first, not what's got a sprained ankle.

Within a Recovery Strategy, identifying Business Unit and Functional Priorities means ranking which parts of the business must be restored first to minimize impact and resume operations effectively.

Why it matters:

- Some functions (e.g., finance, customer service, order processing) may be mission-critical, while others (e.g., marketing, R&D) can tolerate more downtime.
- Prioritization is driven by the Business Impact Analysis (BIA).
- Helps allocate resources, recovery timeframes (RTOs), and determine failover sequencing.

CISSP Angle: This process ensures recovery efforts align with the organization's survival and strategic goals, not just technical dependencies.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Crisis Management

Think of it as the quarterback calling plays mid-crisis—tech fixes nothing if people are panicked and the brand's on fire.

The part of the recovery strategy that focuses on coordinating response efforts, communication, and leadership during a disaster or major disruption.

Key Components:

- Command structure for decision-making during chaos.
- Clear communication plans (internal and external).
- Public relations and media handling.
- Emotional support, legal considerations, and regulatory reporting.

CISSP Relevance: Crisis management ensures the human and organizational side of recovery is handled with clarity and control—reducing confusion, maintaining trust, and enabling faster technical recovery.

CHAPTER 18

Recovery Strategy

Workgroup Recovery

Think of it like a backup office-in-a-box, ready to spin up when HQ goes dark.

Workgroup Recovery refers to the restoration of essential teams or departments, typically by relocating them to pre-arranged alternate workspaces with the equipment and tools needed to resume operations.

Key Features:

- Supports critical personnel (e.g., finance, customer service, IT ops).
- Often uses dedicated recovery centers or hot/warm sites.
- Includes desks, phones, systems, connectivity, and sometimes even housing/logistics.

CISSP Context: Workgroup recovery ensures people—not just systems—can get back to work, which is vital for business continuity and meeting recovery time objectives (RTOs).

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of hot, warm, and cold sites like coffee: hot is ready to sip, warm needs a microwave, cold is just beans and water.

Alternate processing sites are pre-arranged backup locations where an organization can resume IT operations if the primary site becomes unavailable due to disaster or disruption.

Types of Sites:

- **Hot Site**: Fully equipped, real-time data replication—ready instantly.
- **Warm Site**: Partially equipped—some setup required before use.
- **Cold Site**: Basic space with power and HVAC—bring your own gear.

CISSP Relevance: These sites are essential for meeting Recovery Time Objectives (RTOs) and maintaining availability, a core pillar of the CIA triad.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like an empty apartment—you've got the keys, but it's BYO-everything.

A **Cold Site** is a bare-bones backup location with basic infrastructure only—power, HVAC, and space—but no hardware, data, or staff pre-installed.

Key Points:

- Lowest cost, but slowest to activate.
- Requires manual setup of equipment, systems, and data restoration.
- Suitable for non-time-sensitive operations or as part of a layered recovery strategy.

CISSP Angle: Cold sites are budget-friendly but not ideal for low RTOs. Still valuable as a fallback option in multi-tiered recovery planning.

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like a stocked Airbnb—you've got furniture and Wi-Fi, but you still need to unpack your gear.

A **Warm Site** is a partially equipped alternate location with some hardware, software, and connectivity pre-installed, but not fully operational until systems and data are restored.

Key Points:

- Mid-range cost and recovery time.
- Typically requires data synchronization and some manual setup.
- A balance between the low cost of cold sites and the fast activation of hot sites.

CISSP Context: Warm sites are ideal for businesses that need moderate recovery speed and functionality without the high expense of hot sites.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like a backup office that's already up and running—you just walk in and pick up where you left off.

A **Hot Site** is a fully operational, fully equipped backup location that mirrors the primary site in real-time or near real-time. It's ready to take over almost instantly if disaster strikes.

Key Points:

- Includes hardware, software, network connectivity, and data replication.
- Highest cost, but lowest recovery time (RTO).
- Often used by mission-critical operations (e.g., financial institutions, healthcare).

CISSP Context: Hot sites are vital for organizations with low tolerance for downtime—they support high availability and business continuity with minimal disruption.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like a backup office that's already up and running—you just walk in and pick up where you left off.

Site Type	Setup Time	Cost	Equipment/Readiness	Data Availability	Best Use Case
Cold Site	Long (days to weeks)	Low	Basic infrastructure only	None—manual restore needed	Cost-conscious, non-critical ops
Warm Site	Moderate (hours to days)	Medium	Partial systems installed	May need data sync	Balanced need for recovery speed/cost
Hot Site	Immediate (minutes)	High	Fully equipped & operational	Real-time or near real-time	Mission-critical, low-downtime tolerance

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like a data center on wheels—ready to roll when your main site's a crater.

A **Mobile Site** is a transportable, self-contained recovery facility, typically housed in a truck or trailer, that can be deployed to a specific location when needed.

Key Points:

- Equipped with IT hardware, power, communications, and workspace.
- Can be delivered quickly to any site with physical access.
- Used when fixed recovery sites aren't available or practical.

CISSP Context: Mobile sites offer flexibility and portability, especially for remote locations, disaster zones, or organizations with limited physical recovery options.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Think of it like a data center on wheels—ready to roll when your main site's a crater.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like having a backup office that materializes out of thin air—if the security gods allow it.

Cloud computing offers a virtual alternate processing environment by hosting infrastructure, platforms, and services offsite, typically through a third-party provider.

Key Benefits for Recovery:

- Acts as a scalable, on-demand hot site—no need for physical setup.
- Supports rapid recovery and failover through Infrastructure as a Service (IaaS) or Disaster Recovery as a Service (DRaaS).
- Reduces cost and complexity of maintaining dedicated alternate sites.

CISSP Angle: Cloud enhances availability and resilience while simplifying recovery strategy implementation, but it requires strong controls for data security, access, and compliance.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Alternate Processing Sites

Think of it like a cyber buddy system—*"If your office floods, come use mine… as long as mine's still dry."*

A **Mutual Assistance Agreement (MAA)** is a pre-arranged pact between two organizations to support each other during a disaster, typically by sharing resources, personnel, or facilities.

Key Features:

- Can include workspaces, IT systems, equipment, or staff.
- Cost-effective, but may be risky if both parties are affected by the same event.
- Must be formalized, tested, and periodically reviewed.

CISSP Context: MAAs are a low-cost alternative to commercial recovery sites, but their success depends on clear terms, compatibility, and trust between partners.

Think of it like a cyber buddy system—*"If your office floods, come use mine… as long as mine's still dry."*

Cautions with MAAs

1. **Shared Risk Exposure** - If both organizations are in the same region or supply chain, a single disaster could impact both, making the agreement useless.
2. **Resource Contention** - During a real crisis, the "helping" organization may prioritize its own recovery, leaving little capacity to support others.
3. **Compatibility Issues** - Hardware, software, or processes may not be compatible—different platforms, network setups, or security controls can hinder recovery.
4. **Lack of Testing or Maintenance** - Many MAAs are signed and forgotten. If not regularly reviewed and tested, they may be worthless when needed.
5. **Legal & Compliance Challenges** - Data handling, privacy laws, and regulatory requirements (e.g., HIPAA, GDPR) can be violated if sensitive systems or data are shared improperly.
6. **Undefined Terms or Vague SLAs** - Ambiguities in the agreement can lead to confusion, delays, or legal disputes during a crisis.
7. **Personnel Availability** - Key staff from the assisting organization may not be available, especially during a widespread emergency.

terms, compatibility, and trust between partners.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Database Recovery

CHAPTER 18

Recovery Strategy

Database Recovery

Think of it like the heart of your business—if it doesn't restart properly, the rest is just limbs twitching.

Database recovery is crucial because databases often store the most critical and sensitive business data—customer records, transactions, financials, operational data, and more. Without it, the business can't function.

Why It Matters:

- **Data Loss = Business Loss**: Downtime or corruption can lead to lost revenue, compliance violations, and reputational damage.
- **Supports Recovery Point Objectives (RPOs)**: Ensures data is restored to the correct point in time.
- **Tied to Recovery Time Objectives (RTOs)**: Determines how fast essential data-driven operations can resume.
- Involves backup strategies, replication, and integrity checks to ensure data accuracy and completeness post-disaster.

CISSP Angle: Database recovery supports integrity and availability in the CIA triad and is a pillar of business continuity and resilience.

CHAPTER 18

Recovery Strategy

Database Recovery

Think of it like sending a secure care package of your data to a bunker every night—slow, but safe.

Electronic Vaulting is the process of transmitting backup data electronically—usually in batches—from the primary site to a secure offsite location.

Key Points:

- Often used for database backups or other critical data.
- Data is typically sent on a schedule, not in real-time.
- Helps ensure offsite redundancy in case of physical disasters.

CISSP Relevance: Electronic vaulting supports disaster recovery and data integrity by keeping copies offsite—away from whatever might take down the main facility.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Strategy

Database Recovery

Think of it like a digital black box recorder for your database—tracking every move in case you need to replay the whole thing.

Remote Journaling is the near real-time transmission of transaction logs or journal entries from the primary system to a remote location, allowing for rapid database recovery.

Key Points:

- Captures system or database activity (not full data sets).
- Enables faster recovery by applying logs to a previous backup.
- Useful for minimizing data loss (lower RPO) in high-change environments.

CISSP Relevance: Remote journaling helps maintain data integrity and continuity, especially in systems where every transaction matters (e.g., banking, logistics).

CHAPTER 18

Recovery Strategy

Database Recovery

Think of it like a digital twin living in another city—whatever happens here, it's instantly reflected there.

Remote Mirroring is the process of replicating data in real-time from a primary system to a remote backup system, creating an exact, continuously updated copy.

Key Points:

- Provides instant failover capability with minimal or no data loss.
- Supports very low RPOs and RTOs.
- Requires high-bandwidth, secure connections and robust infrastructure.

CISSP Relevance: Remote mirroring is ideal for mission-critical systems where downtime or data loss is unacceptable—maximizing availability and integrity.

CHAPTER 18

Recovery Strategy

Database Recovery

Think of it like a digital twin living in another city—whatever happens here, it's instantly reflected there.

Method	Data Sync Timing	What's Transmitted	Recovery Speed	Data Loss (RPO)	Cost - Complexity	Best Use Case
Electronic Vaulting	Scheduled (batch-based)	Full data backups	Slow (hours to days)	High (since last backup)	Low	Basic offsite backups for non-critical data
Remote Journaling	Near real-time	Transaction logs / journals	Moderate (faster than vaulting)	Medium (few minutes)	Medium	Systems needing fast recovery without full mirroring
Remote Mirroring	Real-time	Full live data replication	Fast (near-instant failover)	Very low (seconds or none)	High	Mission-critical systems with no downtime tolerance

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Plan Development

Think of recovery plan development as the ultimate “fire drill” blueprint—useless if it’s missing, but life-saving if it’s well-built and practiced.

CHAPTER 18

Think of recovery plan development as the ultimate “fire drill” blueprint—useless if it’s missing, but life-saving if it’s well-built and practiced.

Recovery Plan Development

Importance of Recovery Plan Development

Recovery plan development is the process of creating detailed, actionable strategies and procedures to restore IT systems, data, and business operations after a disruption. It’s where all the BIA, risk assessments, and policy planning turn into real-world action.

Why It’s Critical:

- Minimizes downtime and financial loss during a crisis.
- Ensures personnel know exactly what to do—reduces panic and guesswork.
- Supports legal, regulatory, and compliance requirements.
- Builds organizational resilience and stakeholder trust.
- Enables effective testing and training, closing the gap between theory and execution.

CHAPTER 18

Recovery Plan Development

Think of recovery plan development as the ultimate “fire drill” blueprint—useless if it’s missing, but life-saving if it’s well-built and practiced.

Recommended Resources:

NIST Special Publications

- NIST SP 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- Gold-standard framework for federal and commercial use.
- https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

ISO/IEC Standards

- ISO/IEC 27031 – Guidelines for ICT readiness for business continuity
- Offers international best practices for ICT-focused recovery planning.

FIEC IT Examination Handbook

- Particularly the Business Continuity Planning Booklet
- Used by financial institutions—rich with practical guidance.
- FFIEC BCP Handbook - https://ithandbook.ffiec.gov/

Disaster Recovery Institute (DRI) & Business Continuity Institute (BCI)

Offer certifications, toolkits, and frameworks for recovery and continuity planning.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Plan Development

Emergency Response

CHAPTER 18

Recovery Plan Development

Emergency Response

Think of it as the “triage team” in a crisis—it doesn’t fix everything, but it keeps things from getting worse fast.

Emergency Response refers to the immediate actions taken to protect life, limit damage, and stabilize the situation when a disaster or major incident first occurs.

Key Components:

- Evacuation procedures, first aid, fire suppression.
- Notification and alerting protocols (staff, authorities, stakeholders).
- Initial incident containment (e.g., shutting off systems or power).

CISSP Context: Emergency response is the first phase of an effective recovery plan—it kicks off the transition from chaos to controlled recovery. It protects both people and critical assets, setting the stage for continuity and restoration.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Plan Development

Personnel and Communications

CHAPTER 18

Recovery Plan Development

Personnel and Communications

Think of it like a tactical ops team—everyone knows their job, who to report to, and how to signal when things go sideways.

In recovery planning, Personnel and Communications refer to defining roles, responsibilities, and communication protocols to ensure a coordinated and effective response during and after a disaster.

Key Elements:

- **Assign roles**: Recovery team leads, liaisons, technical staff, communications officers.
- **Contact lists**: Up-to-date info for staff, vendors, emergency services.
- **Communication plans**: Internal (employees) and external (media, stakeholders) messaging.
- **Redundant channels**: Email, phone trees, SMS alerts, radios—in case primary systems fail.

CISSP Relevance: Effective personnel management and clear communication prevent confusion, accelerate recovery, and maintain trust and compliance throughout the incident lifecycle.

CHAPTER 18

Recovery Plan Development

Assessment

Think of it as the triage phase in a disaster response—figuring out what's broken, what's still functional, and what to fix first.

In the context of recovery execution, Assessment is the phase where the organization evaluates the scope and impact of the disaster to determine what systems, data, and operations have been affected, and what recovery actions are needed.

Key Activities:

- Identify the nature and extent of the damage or disruption.
- Assess affected systems, facilities, personnel, and data integrity.
- Determine what can be salvaged and what must be restored or rebuilt.
- Guides the decision on which recovery strategies to activate (e.g., failover, site relocation, data restoration).

CISSP Relevance: Assessment is essential for informed decision-making during a crisis. It ensures the recovery effort is accurate, prioritized, and resource-efficient, preventing wasted time or missteps.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it as your “save game” system for the enterprise—without it, when you crash, you start from zero.

Backups and storage strategies are the core of data recovery planning, ensuring that critical information can be restored after a disaster or system failure.

Key Components:

- **Backup types**: Full, incremental, differential, and image-based.
- **Storage locations**: Onsite, offsite, cloud, and hybrid.
- **Retention policies**: Define how long backups are kept and rotated.
- **Encryption & access controls**: Protect backup data from unauthorized access or tampering.

CISSP Context: Proper backup and storage strategies ensure data integrity, availability, and support recovery objectives like RPO (how much data you can afford to lose) and RTO (how fast you need it back).

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it as your “save game” system for the enterprise—without it, when you crash, you start from zero.

Full Backup

A Full Backup is a backup method that copies all selected data—every file, every time—regardless of when it was last changed.

The archive bit on every file is reset, turned off, or set to 0.

Key Points:

- Easiest to restore from (single backup set).
- Takes the longest time to perform and requires more storage.
- Typically done periodically, with incremental or differential backups in between.

CISSP Relevance: Full backups are the foundation of most recovery strategies—they provide a complete data snapshot, essential for comprehensive restores.

and RTO (how fast you need it back).

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it as your “save game” system for the enterprise—without it, when you crash, you start from zero.

Incremental Backup

An Incremental Backup only copies data that has changed since the last backup—whether it was a full or another incremental.

Only files that have the archive bit turned on, enabled, or set to 1 are duplicated.

The archive bit on all duplicated files is reset, turned off, or set to 0.

Key Points:

- Much faster and smaller than full backups.
- Requires less storage space.
- Restore process is slower—you need the last full backup plus all subsequent incrementals.

CISSP Relevance: Incremental backups are efficient for daily or frequent backups, balancing resource use with recovery needs—but they require careful management to ensure restore integrity.

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it as your “save game” system for the enterprise—without it, when you crash, you start from zero.

Differential Backup

A Differential Backup copies all data that has changed since the last full backup—regardless of any previous differential backups.

Only files that have the archive bit turned on, enabled, or set to 1 are duplicated.

The archive bit is left unchanged.

Key Points:

- Larger than incremental over time, but faster to restore.
- Only need the last full backup and the most recent differential.
- Grows in size each day until the next full backup.

CISSP Relevance: Differential backups strike a balance between **restore speed and backup size**—ideal when you want **simpler recovery** without daily full backups.

and RTO (how fast you need it back).

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it as your “save game” system for the enterprise—without it, when you crash, you start from zero.

Differential Backup

A Differential Backup copies all data that has changed since the last full backup—regardless

Backup Type	What It Backs Up	Backup Speed	Restore Speed	Storage Use	Restore Requires
Full	All selected data	Slow	Fast	High	Only the latest full backup
Incremental	Changes since last **any** backup	Fast	Slow	Low	Last full + **all** incrementals since
Differential	Changes since last **full** backup	Moderate	Moderate	Medium	Last full + latest differential

or

ged.

CISSP Relevance: Differential backups strike a balance between **restore speed and backup size**—ideal when you want **simpler recovery** without daily full backups.

and RTO (how fast you need it back).

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it like copying your files to an external SSD instead of a dusty old tape—quicker, cleaner, and more modern.

Disk-to-Disk (D2D) Backup involves copying data directly from a primary storage system to a secondary disk-based storage system, instead of using tapes or other slower media.

A **Virtual Tape Library (VTL)** is a disk-based storage system that emulates traditional tape drives and libraries, allowing backup software to write to disks as if they were tapes.

Key Points:

- **Faster backup and recovery** compared to tape.
- Supports **automation, deduplication**, and **quick restores**.
- Can be used as a step before long-term **disk-to-tape** or **cloud archiving**.

CISSP Relevance: D2D enhances **availability and recovery speed**, making it ideal for systems that need **rapid RTOs** and frequent backup cycles.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Plan Development

Backups and Storage Strategies

Think of it as your data's insurance policy—useless if you don't pay the premiums, update the policy, or check the paperwork.

Backup best practices are the strategies and controls that ensure your backup processes are reliable, secure, and effective when recovery is needed.

1. Follow the 3-2-1 Rule:

- Keep **3** copies of data
- On **2** different media types
- With **1** copy offsite

2. Test Your Backups

Regularly verify restores to ensure backup integrity and effectiveness.

3. Automate Where Possible

Use scheduled, automated backups to reduce human error.

4. Encrypt Backup Data

Protect backups both in transit and at rest to preserve confidentiality.

5. Monitor and Log Backups

Track success/failure, and alert on issues.

6. Use Tiered Storage

Match data value to appropriate storage (e.g., hot, warm, cold).

7. Secure Physical Media

Prevent theft, loss, or damage of tapes/disks.

8. Align with RTO/RPO Goals

Choose backup frequency and type based on business impact.

CHAPTER 18

Recovery Plan Development

Software Escrow Arrangements

Think of it like a data prenup—you don't want to need it, but if things go south, it's there to save your ass.

A **Software Escrow Arrangement** is a legal agreement where the source code and other critical components of proprietary software are held by a trusted third party (escrow agent), to be released to the licensee under specific conditions.

Key Triggers for Release:

- Vendor goes out of business
- Vendor fails to maintain or support the software
- Breach of contract

CISSP Relevance: Escrow protects availability and continuity of business-critical software, especially when it's custom or vendor-dependent—reducing the risk of being locked out if the vendor vanishes.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Recovery Plan Development

Recovery vs. Restoration

CHAPTER 18

Recovery Plan Development

Recovery vs. Restoration

Though often used interchangeably, in recovery planning they have distinct meanings.

Recovery:

- Focuses on resuming critical business and IT operations after a disruption.
- Often involves alternate sites, failovers, or backup systems.
- Goal: Get things running ASAP, even if it's not perfect or permanent.

Restoration:

- Involves fully returning systems, data, and infrastructure to their original state before the disaster.
- Can include rebuilding, reinstalling, reconfiguring, or replacing damaged components.
- Goal: Complete return to normalcy—the long-term fix

CHAPTER 18

Recovery Plan Development

Recovery vs. Restoration

Think of recovery as throwing on a spare tire—restoration is getting the full tire replaced and rebalanced.

Though often used interchangeably, in recovery planning they have distinct meanings.

Recovery:

- Focuses on resuming critical business and IT operations after a disruption.
- Often involves alternate sites, f
- Goal: Get things running ASAP,

Restoration:

- Involves fully returning systems, data, and infrastructure to their original state before the disaster.
- Can include rebuilding, reinstalling, reconfiguring, or replacing damaged components.
- Goal: Complete return to normalcy—the long-term fix

CISSP Relevance: Recovery is short-term continuity; restoration is long-term rebuilding. Both are critical but serve different phases of the disaster response lifecycle.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Training, Awareness, and Documentation

CHAPTER 18

Training, Awareness, and Documentation

Think of it like a fire drill with a manual—you train, you remember, and you have a guide when the smoke hits.

Training, Awareness, and Documentation ensure that everyone knows their role, responsibilities, and procedures during a disaster—and can act effectively under pressure.

Key Components:

- **Training**: Hands-on instruction for staff on executing the DR plan (e.g., failover procedures, manual workarounds).
- **Awareness**: Organization-wide understanding of what to do, who to contact, and how to respond.
- **Documentation**: Clearly written, up-to-date plans, runbooks, contact lists, and diagrams—stored securely and accessibly.

CISSP Relevance: Even the best DR plan is worthless if people don't know it exists or how to use it. This component supports preparedness, compliance, and effective response.

2025 CISSP MENTOR PROGRAM

CHAPTER 18

Testing and Maintenance

Think of it like checking your fire extinguisher—you don't want to learn it's empty when the flames are already there.

Testing and Maintenance are critical activities that ensure a disaster recovery plan remains effective, up-to-date, and executable when a real incident occurs.

Key Components:

- **Testing:**
  - Validates the workability of the DR plan.
  - Types include walkthroughs, simulations, parallel testing, and full interruption testing.
  - Reveals gaps, errors, or unrealistic assumptions.
- **Maintenance:**
  - Keeps the plan current with system, personnel, and business changes.
  - Triggered by system upgrades, staff turnover, policy changes, or lessons learned.

CISSP Relevance: A DR plan is a living document. Without regular testing and maintenance, it risks being outdated, ineffective, or dangerously misleading during a real crisis.

CHAPTER 18

Testing and Maintenance

Read-Through Testing

Think of it like proofreading your emergency manual—low impact, but vital for catching paper-based "gotchas."

Read-Through Testing (also called a Checklist Review) is the most basic form of disaster recovery testing, where key personnel review the DR plan line by line to verify accuracy and completeness.

Key Features:

- No system disruption—purely document-based.
- Participants check for outdated contacts, incorrect procedures, or missing steps.
- Often used as a preliminary test before deeper exercises.

CISSP Relevance: Read-throughs help ensure the plan remains logically sound and aligned with current operations, forming the foundation for more advanced testing.

Think of it like a war game on paper—talk it out before you have to live it out.

CHAPTER 18

Testing and Maintenance

Tabletop Testing

Tabletop Testing is a discussion-based disaster recovery exercise where team members gather to talk through their roles, decisions, and actions in response to a simulated disaster scenario.

Key Features:

- No technical systems involved—purely scenario-based.
- Focuses on coordination, communication, and decision-making.
- Helps identify gaps in the plan, role confusion, or procedural weaknesses.

CISSP Relevance: Tabletops test the human element of disaster recovery—ensuring the team can think clearly, communicate effectively, and follow the plan under pressure.

CHAPTER 18

Testing and Maintenance

Walk-Through Testing

Think of it like a rehearsal—you're walking the stage, hitting your marks, and making sure nothing falls apart before showtime.

Walk-Through Testing (or Structured Walkthrough) is a step-by-step review of the disaster recovery plan, where participants go through their specific responsibilities and procedures in detail.

Key Features:

- More detailed than a tabletop—participants may reference systems or tools, but no live systems are impacted.
- Validates procedures, interdependencies, and communication flows.
- Often used to train staff and refine procedural accuracy.

CISSP Relevance: Walk-throughs help validate the logic and flow of the DR plan, ensuring that roles, sequences, and documentation are accurate and actionable.

CHAPTER 18

Testing and Maintenance

Simulation Testing

Think of it like a fire drill with smoke machines—close to real, but safe enough to learn from.

Simulation Testing is a hands-on, scenario-driven exercise where teams respond to a mock disaster using actual tools, communications, and procedures—but without disrupting real systems.

Key Features:

- Involves realistic conditions and live coordination, but no system failover or downtime.
- Tests response times, team coordination, and decision-making under pressure.
- Often used to evaluate the effectiveness of both the plan and the team.

CISSP Relevance: Simulation testing helps identify operational gaps and team weaknesses that don't show up in tabletop or walk-through tests—making it critical for maturing the DR strategy.

CHAPTER 18

Testing and Maintenance

Parallel Testing

Think of it like a dress rehearsal with full lighting and sound—everything's real, but the audience is still watching the main show.

Parallel Testing involves activating backup systems and processing data simultaneously with the primary systems—without disrupting normal operations.

Key Features:

- Validates that recovery systems can perform critical operations under real workloads.
- Production systems stay live, while backups run in the background.
- Helps test data synchronization, system integrity, and failover readiness.

CISSP Relevance: Parallel testing bridges the gap between non-intrusive tests and full operational confidence, making it a vital step before attempting full-interruption testing.

CHAPTER 18

Testing and Maintenance

Full-Interruption Testing

Think of it like a controlled crash test—you're slamming the brakes for real to see if the airbag deploys. High risk, high reward.

Full-Interruption Testing is the most aggressive and realistic form of disaster recovery testing, where primary systems are intentionally shut down and operations are fully shifted to recovery systems.

Key Features:

- Simulates a real disaster by cutting over to alternate sites or systems.
- Validates the entire recovery process—from detection to restoration.
- Carries significant risk of disruption if not planned and controlled carefully.

CISSP Relevance: This test proves whether the DR plan actually works in the real world—but should only be done if the organization is confident and prepared for potential fallout.

Think of it like a controlled crash test—you're slamming the

Test Type	Description	Systems Affected	Risk Level	Primary Purpose
Read-Through	Team reviews the plan for accuracy and completeness	None	Low	Validate documentation
Tabletop	Discussion-based scenario walk-through	None	Low	Test coordination and decision-making
Walk-Through	Step-by-step review of responsibilities and procedures	None (may reference tools)	Low	Verify procedural clarity
Simulation	Hands-on mock scenario using actual tools/procedures	No production impact	Medium	Test real-time response and communication
Parallel	Run backup systems in sync with live systems (no switch-over)	Backup systems only	Medium	Validate recovery system functionality
Full-Interruption	Shut down production and shift to recovery systems entirely	All systems affected	High	Validate full end-to-end recovery

CHAPTER 18

Testing and Maintenance

Lessons Learned

Think of it as your post-game film review—you might've survived the hit, but now it's time to train smarter for the next one.

Lessons Learned is the post-recovery (and/or post-testing) analysis phase where the organization reviews what worked, what failed, and how to improve the disaster recovery process for future incidents.

Key Activities:

- Analyze the effectiveness of the DR plan and team response.
- Identify gaps, delays, miscommunications, or unexpected issues.
- Update documentation, procedures, and training based on findings.
- Often captured in an After Action Report (AAR).

CISSP Relevance: This phase is critical for continuous improvement, ensuring the recovery strategy evolves with new threats, business changes, and real-world insights.

CHAPTER 18

Testing and Maintenance

Test Communications

Think of it like testing the fire alarm—you need to know it's loud, clear, and gets everyone moving when it counts.

Test Communications refers to the regular validation of emergency communication channels and procedures to ensure that people can be reached and information can flow effectively during a disaster.

Key Activities:

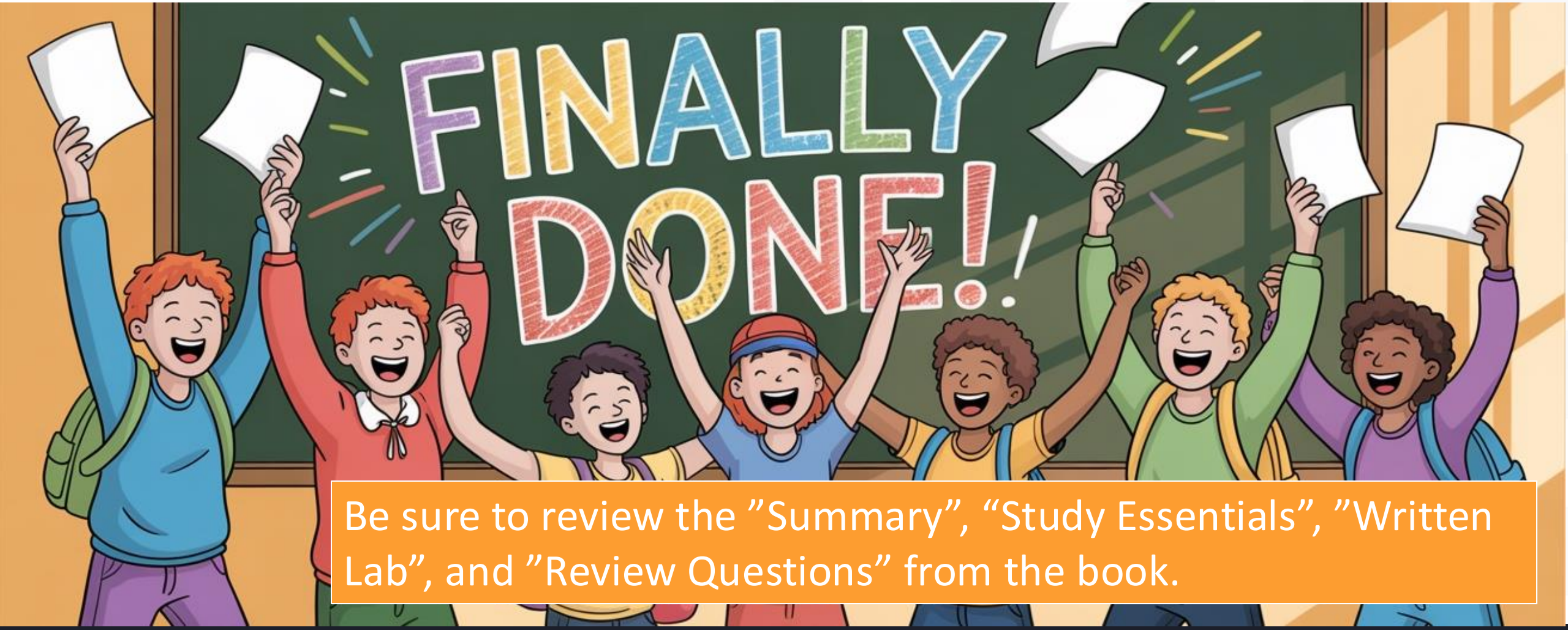
- Verify contact info for staff, vendors, and emergency responders.
- Test email alerts, phone trees, SMS systems, and backup channels.
- Confirm roles and responsibilities for who communicates what, when, and to whom.
- Include in DR tests and drills to assess response time and clarity.

CISSP Relevance: Effective communication is essential for coordinated response, reduced downtime, and ensuring safety—especially under stress or chaos.

2025 CISSP MENTOR PROGRAM

CHAPTER 18
Disaster Recovery Planning

CONGRATULATIONS!
You stuck it out. (only 110 slides later)



Be sure to review the ”Summary”, “Study Essentials”, ”Written Lab”, and ”Review Questions” from the book.