2

DOMAIN

TOPIC TWO

Incident Response, Continuity and Disaster Recovery

10% of the exam

The availability leg of the triad, applied to systems and to people

AT A GLANCE

A small domain worth full marks

10%

of the exam — roughly ten questions

6

lessons in this topic

~75

minutes

Why not to overinvest

- The smallest of the five domains by weight
- If you fall behind on the schedule, this is the domain to cover thinly
- Domains 1, 3 and 4 are roughly 72% of the exam between them

Why not to skip it either

- The content is definitional and the term list is short
- Full marks here are realistic in a way they are not in Domain 4
- One distinction — IR versus BC versus DR — carries most of it

THE CORE OF THIS DOMAIN

Three plans, one sequence

Three distinct plans in a sequence — not three names for the same thing.

This one distinction carries most of the marks

- The dominant question hands you a scenario and asks which of the three applies — position in time is the discriminator

THE SEQUENCE

Read this until the ordering is automatic

IR responds so the business keeps operating.
BC keeps it operating throughout.
DR returns it to normal.

- INCIDENT RESPONSE — first, as the event unfolds
- BUSINESS CONTINUITY — alongside and after IR, for as long as the crisis lasts
- DISASTER RECOVERY — last, activated when IR and BC have not been enough
- They are three distinct plans, not three names for the same thing

ONE EVENT, THREE PLANS

A hurricane floods the primary office

The same event triggers all three plans, in sequence and partly in parallel.

- IR — accounting for staff, safe shutdown, assessing damage in the first hours
- BC — next week: staff relocated or working remotely, a reduced but functioning service
- DR — rebuilding the flooded office and its systems, then moving back
- Realistic incidents run all three at once. Questions isolate one on purpose

BEYOND THE TECHNICAL

This domain is partly about people

What continuity planning actually covers

- Where staff go if the building is unusable
- How people are contacted and how they report status
- Communications with families in a serious event
- Evacuation, safety officers, and physical danger
- Premises, suppliers and customers — not only systems

The examinable principle

- The health and safety of staff, customers and the public ranks above continuity of service
- Where a question offers "protect people" against "maintain operations", people win
- If a scenario mentions fire, flood or structural danger, safety is the answer

LESSON MAP

The six lessons

1	**Incident terminology**	Event, alert, incident, breach, intrusion, exploit, zero-day
2	**Incident response**	Goal, priority order, four phases, plan, team, escalation limits
3	**Business continuity**	Goal, importance, scope beyond IT, degraded service
4	**Components of a BC plan**	BIA, MTD, RTO, RPO, call trees, activation, testing
5	**Disaster recovery**	Goal, plan components, backups, site types, testing ladder
6	**Telling the three apart**	The sort that carries the domain, plus consolidation

Lesson 2.6 is where most of the marks are. Everything before it exists to make that sort reliable.

2.1

LESSON

Incident Terminology

OBJECTIVE

Use the incident vocabulary precisely, and place each term correctly relative to the others.

- Event, alert, incident, breach — each narrower than the last
- Intrusion, exploit and vulnerability
- Zero-day, and why it changes the response
- The distinctions the exam builds distractors from

LESSON 2.1

These terms are not interchangeable

They look like synonyms in casual use.
The exam treats them as a strict hierarchy.

- EVENTS are everything — millions a day
- ALERTS are the subset that monitoring flagged
- INCIDENTS are the subset that genuinely threaten security
- BREACHES are the subset of incidents where information was lost or disclosed
- Each is narrower than the last. Getting the ordering right answers a surprising number of questions

LESSON 2.1 — THE CORE FOUR

Each term, precisely

Event	Any observable occurrence in a system or network. Completely neutral. A user logging in is an event; a file being saved is an event.
Alert	A notification that an event or pattern of events may warrant attention. Generated by tooling. Not proof of anything.
Incident	An event that actually or potentially jeopardises the confidentiality, integrity or availability of information or a system, or violates policy.
Breach	Loss of control, compromise, unauthorised disclosure or unauthorised acquisition of information. A specific kind of incident.

The threshold that matters: an incident is an event with adverse security consequence.

LESSON 2.1 — THE REST

The supporting terms

Intrusion	A security event, or set of events, constituting a deliberate incident in which an intruder gains or attempts unauthorised access.
Exploit	A particular attack, or the code or method used to take advantage of a vulnerability. The TECHNIQUE.
Vulnerability	The weakness the exploit uses. Carried over unchanged from Domain 1.
Threat	A potential cause of an unwanted incident. Also carried over from Domain 1.

Exploit is the technique; vulnerability is the hole it goes through. Do not swap them.

Zero-day

A vulnerability unknown to those who would need to fix it, for which no patch yet exists.

- The name refers to the defender having had zero days' warning
- It matters to the exam because the usual response — patch it — is unavailable
- Response is compensating controls: segmentation, monitoring, disabling the affected feature
- Note that the vulnerability is not itself an incident. Nothing has happened yet

LESSON 2.1 — WORKED EXAMPLES

Name the term

A monitoring system flags 400 failed logins from one address in a minute.

An alert, generated from events. Whether it becomes an incident depends on analysis — it might be a misconfigured application retrying.

Analysis confirms an attacker succeeded and read customer records.

An incident, a breach, and an intrusion — all three fit. A question asking for the most specific applicable term wants breach.

A researcher discovers a flaw in widely used software and no patch exists.

A zero-day vulnerability. Not an incident — nothing has happened yet.

A firewall logs and blocks a connection attempt.

An event, and arguably an alert. Not an incident — the control worked and nothing was jeopardised.

LESSON 2.1 — QUICK CHECK

Answer before advancing

1. An attacker encrypts a company's files with ransomware but takes no copies. Is this a breach?

2. Why is a zero-day especially difficult to respond to?

3. Which is the broadest category: event, alert, incident, or breach?

LESSON 2.1 — ANSWERS

Check your reasoning

1. No

It is an incident, and a severe one, but no information was disclosed or acquired — so it is not a breach. Availability was attacked, not confidentiality. This distinction has real legal weight, which is why the exam bothers with it.

2. Because no patch exists

The defender cannot remediate the underlying weakness and must rely on compensating controls — segmentation, monitoring, disabling the affected feature — until a fix is released.

3. Event

Events are everything observable. Alerts are the flagged subset, incidents the security-relevant subset, breaches the disclosure subset. Each is narrower than the one before.

2.2

LESSON

Incident Response

OBJECTIVE

State the goal of incident response, list the phases and plan components, describe the team, and explain the limits of a responder's authority.

- The goal — and what it is not
- The priority order in any scenario
- Four phases, with containment before eradication
- The cross-functional team, and decisions that must escalate

LESSON 2.2 — THE GOAL

What incident response is for

The goal

- Limit the damage and restore normal operations as quickly as possible
- NOT to catch the attacker
- NOT to assign blame
- Evidence gathering may happen alongside — it is not the objective

The priority order

- 1. Protect life and safety — always first
- 2. Contain the damage
- 3. Preserve evidence, where it does not conflict with the above
- 4. Restore operations

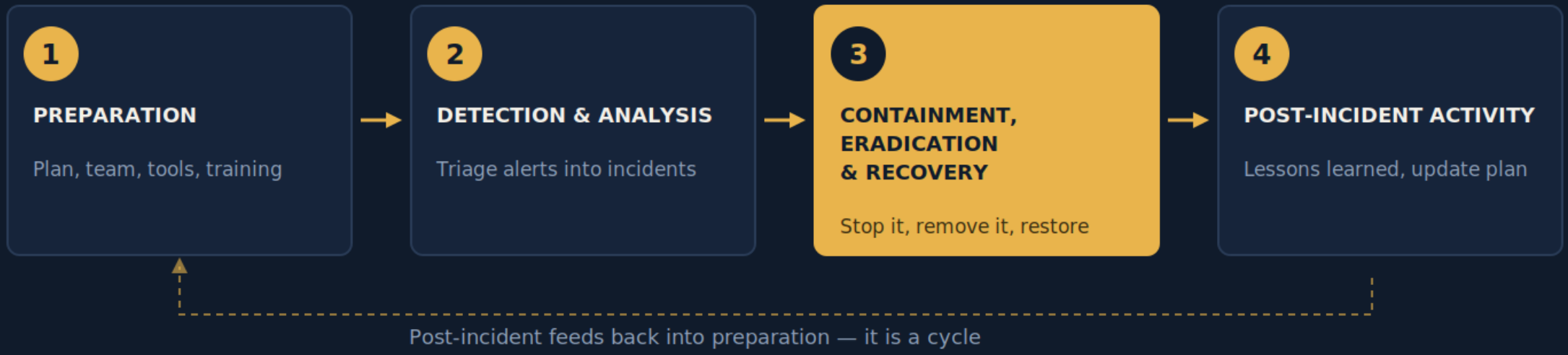
The item candidates skip

- If an incident involves fire, flood or structural danger, people leave before anyone touches a server. A scenario describing staff gracefully shutting down systems during a flood has the priority wrong

LESSON 2.2 — THE PHASES

Four phases, in this order

Containment comes before eradication. Stop the bleeding, then remove the cause.



Most value is created in phase 1

- Plan, team, training and tools all exist before anything happens

Frequently tested ordering

- Containment before eradication — never the other way round

LESSON 2.2 — PHASE DETAIL

What happens in each phase

1. Preparation	Everything done BEFORE an incident: writing the plan, forming and training the team, acquiring tools, exercises, establishing communications channels.
2. Detection & analysis	Recognising something is happening, and determining what it is, how far it has spread and how serious. Where alerts get triaged into incidents.
3. Containment, eradication & recovery	Contain — stop the spread. Eradicate — remove the cause. Recover — restore service and confirm systems are clean. In that order.
4. Post-incident activity	The lessons-learned review. What happened, what worked, what changes. Feeds back into preparation, making the process a cycle.

What the written plan contains

Structured around the phases

- Preparation — the policy, team roster, tools, training schedule
- Detection and analysis procedures — what to monitor, thresholds, severity classification
- Containment, eradication and recovery procedures — the actual steps
- Post-incident activity — how the review runs and who owns the actions

Plus the practical apparatus

- A clear definition of what counts as an incident
- An escalation path, agreed in advance
- Contact details for the team and for external parties
- Communications templates, so nobody drafts a customer notice under pressure

LESSON 2.2 — THE TEAM

Cross-functional by design

Leading and technical

- Team leader / incident manager — coordinates, makes calls, owns the timeline
- Information security — analysis and technical response
- IT, systems and network staff — hands on the affected systems

Business and legal

- Management — authority to make business decisions
- Legal counsel — regulatory obligations, notification duties, liability
- Human resources — wherever an employee is involved

Comms and physical

- Communications / PR — statements to customers, press and staff
- Physical security, and in some organisations a safety officer
- Two structures: a dedicated permanent team, or a virtual team called together when needed

Legal and HR are the two functions candidates forget. Incidents are not purely technical problems.

LESSON 2.2 — AUTHORITY

Decisions the responder cannot make

1	**Take a system offline**	A technically obvious containment step can cost more than the incident. That is a business decision for management.
2	**Notify customers**	Notification of customers, regulators or law enforcement carries legal and reputational consequence. Legal and senior management decide.
3	**Pay a ransom**	Never a technical decision. Legal, financial and reputational dimensions, decided at senior level.
4	**Accept residual risk**	From Domain 1: only senior management or the named risk owner may accept a risk. Recovery does not change that.
5	**Speak to the press**	Communications and PR own external statements. An improvised comment can create liability.

The responder's job is to give management accurate information fast — and to have the escalation path agreed before the incident.

LESSON 2.2 — WORKED EXAMPLES

What is right or wrong here?

Malware spreads laterally. The responder isolates the affected subnet, then removes the malware.

Correct order — containment, then eradication.

During a flood in the server room, staff begin shutting systems down gracefully.

Wrong priority. Life and safety first — evacuate, then worry about systems.

A responder discovers a customer data breach and emails affected customers directly.

Wrong. Notification is a legal and management decision, not the responder's call.

After resolution, the team documents what happened and updates the plan.

Post-incident activity, feeding back into preparation. Exactly right.

LESSON 2.2 — QUICK CHECK

Answer before advancing

1. Put these in order: eradication, detection and analysis, post-incident activity, containment, preparation.

2. A responder wants to disconnect the main e-commerce server to contain an attack. Who decides?

3. Why are legal counsel and HR on an incident response team?

LESSON 2.2 — ANSWERS

Check your reasoning

1. Preparation → detection and analysis → containment → eradication → post-incident activity

Containment, eradication and recovery are usually grouped as one phase, but their internal order still runs containment first.

2. Management

Taking revenue-generating production systems offline is a business decision whose cost may exceed the incident's. The responder recommends; management authorises.

3. Because incidents are not purely technical

Legal handles regulatory notification duties, evidence handling and liability exposure. HR is needed whenever an employee is implicated — as an insider threat, a victim, or a witness — because employment consequences follow their own process.

2.3

LESSON

Business Continuity

OBJECTIVE

State what business continuity is for, distinguish it from the other two plans, and justify the investment.

- The different question BC asks
- What continuity looks like in practice
- Five reasons organisations fund it
- Why continuity is not an IT project

LESSON 2.3 — THE GOAL

Operating despite the crisis

The question BC asks

- Not "how do we stop this?"
- But "how do we keep serving customers while this is going on?"
- Continuity accepts that the disruption is happening
- It plans around the disruption rather than against it

What that looks like in practice

- A manual paper process when the system is down
- A second site, or staff working from home
- A backup supplier when the primary one fails
- Phone orders when the website is offline

One thing to be clear about

- Continuity usually means degraded but adequate service — the critical functions only, not business as usual at full capacity

LESSON 2.3 — WHY IT MATTERS

Justifying an invisible investment

1. **Survival** — A significant share of organisations suffering an extended outage without a plan do not recover. Extended downtime kills companies.
2. **Revenue** — Every hour of downtime has a cost, and it is usually calculable — which makes the plan fundable.
3. **Obligation** — Many contracts and regulators require a tested plan. Not having one can itself be a violation.
4. **Reputation** — Customers forgive an incident handled well and remember one handled badly.
5. **People** — Staff need to know what to do, where to go, and that someone has thought about their safety.

Continuity planning is expensive and produces nothing visible until the day it is needed — which is why the exam expects you to defend it.

LESSON 2.3 — SCOPE

Continuity is not an IT project

It covers premises, staff, suppliers and communications — systems are only one part.

- Where people go if the building is unusable
- How people are contacted, and how they report their status
- Which functions are critical and which can pause
- Who has the authority to declare the plan active
- How customers, suppliers and regulators are told what is happening

LESSON 2.3 — QUICK CHECK

Answer before advancing

1. A retailer's payment system fails. Staff record sales on paper and process them later. IR, BC, or DR?

2. Why can business continuity be a contractual requirement rather than just good practice?

3. Does business continuity mean maintaining full normal capacity?

LESSON 2.3 — ANSWERS

Check your reasoning

1. Business continuity

An alternate process keeps the business trading while the system is down. Fixing the payment system would be DR; diagnosing the failure would be IR. One event, three plans.

2. Because a customer's own continuity depends on its suppliers

Organisations routinely require suppliers to hold tested plans, and regulators require them in sectors where outages harm the public — finance, healthcare, utilities. Absence of a plan can be a compliance finding in itself.

3. No

Continuity normally means degraded but adequate service, covering the critical functions identified by the business impact analysis. Non-critical functions are expected to pause.

2.4

LESSON

Components of a Business Continuity Plan

OBJECTIVE

Describe what a BC plan contains, and define the timing metrics that drive it.

- The business impact analysis, and why everything flows from it
- MTD, RTO, RPO and MTTR
- The plan's components
- Availability of the plan, and testing

Everything flows from the BIA

The business impact analysis works out which functions matter most,
what they depend on, and what it costs when they stop.

- It produces the PRIORITY ORDER — what gets restored first and what can wait
- You cannot protect everything equally, so something has to decide
- A BUSINESS exercise, not an IT one — IT supplies dependency information
- Every later step in continuity and recovery planning inherits its output

LESSON 2.4 — THE METRICS

Four metrics, defined precisely

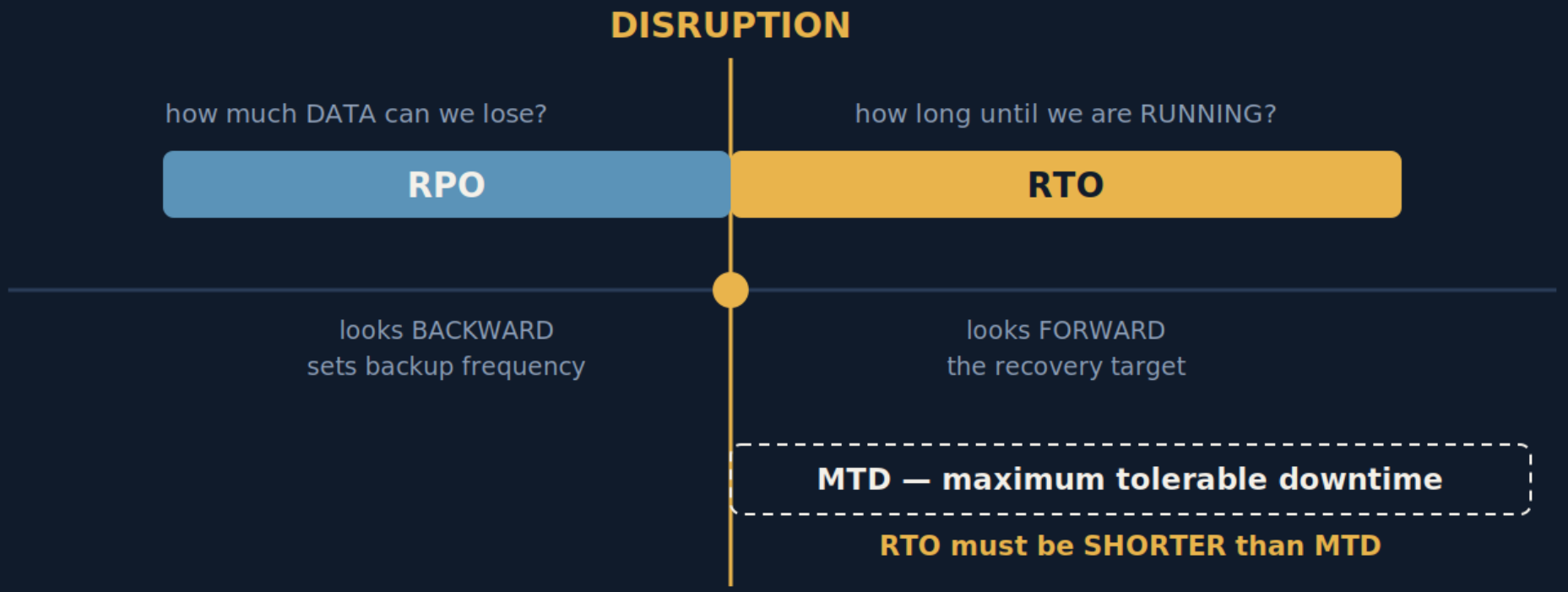
MTD	Maximum Tolerable Downtime. The longest a function can be unavailable before the damage becomes unacceptable or unrecoverable. Set by the business.
RTO	Recovery Time Objective. The target time to restore a function after a disruption. Must be SHORTER than MTD.
RPO	Recovery Point Objective. The maximum acceptable DATA LOSS, expressed as time. An RPO of four hours means backing up at least every four hours.
MTTR	Mean Time to Repair. The average time to fix a failed component. A measure of maintainability, not a planning target.

If your recovery target exceeds the maximum downtime you can tolerate, the plan has already failed on paper.

LESSON 2.4 — THE TIMELINE

Put the disruption in the middle

Put the disruption in the middle. RPO sits behind it, RTO in front of it.



MTTR — mean time to repair — measures maintainability. It is not a planning target.

LESSON 2.4 — COMPONENTS

What the plan contains

People and contacts

- The BC team, with contact details and named alternates
- Notification systems and call trees
- Contact numbers for critical services and third parties — utilities, landlord, insurer, key suppliers, emergency services

Decisions and procedures

- Activation criteria — what triggers the plan, and who declares it
- Immediate response procedures and checklists, usable under stress
- Critical business functions in priority order, from the BIA
- Alternate operating procedures and locations
- Communications plans for staff, customers, regulators and press

The two the exam likes

The plan must be available when systems are not

- A plan stored only on the file server that just went down is useless
- Printed copies, offsite copies, and copies held by team members at home are all standard
- This is the single most quotable point in the lesson

The plan must be tested

- An untested plan is an assumption
- Testing surfaces the wrong phone numbers
- The departed staff member still listed as the lead
- The alternate site with no network connectivity
- Plans decay — the environment changes and the document does not

LESSON 2.4 — QUICK CHECK

Answer before advancing

1. An organisation backs up hourly. What does that tell you about its RPO?

2. Which comes first: the BIA, or the priority order for restoring systems?

3. A company determines its order system must be back within 4 hours, and beyond 12 hours the business would not recover. Name both metrics.

LESSON 2.4 — ANSWERS

Check your reasoning

1. Its RPO is no shorter than one hour

Hourly backups mean up to an hour of data could be lost. If the stated RPO were 15 minutes, the backup schedule would not support it — a common real-world gap between policy and practice.

2. The BIA comes first

The priority order is one of its outputs. You cannot rank functions before analysing their impact and dependencies.

3. RTO is 4 hours; MTD is 12 hours

RTO sits inside MTD, which is correct. An RTO longer than the MTD would be logically impossible as a plan.

2.5

LESSON

Disaster Recovery

OBJECTIVE

State the goal and trigger of disaster recovery, list the plan's components, and choose backup and site strategies against a requirement.

- The goal, and the asymmetry with continuity
- Components of a DR plan
- Full, incremental and differential backups
- Hot, warm and cold sites, and the testing ladder

LESSON 2.5 — THE GOAL

Ending the degraded state

The goal and the trigger

- Return the organisation to normal operations
- Restore the systems, data, facilities and services that continuity was standing in for
- Activated when IR and BC have NOT been sufficient
- The last of the three plans

The asymmetry worth noticing

- BC accepts a degraded state and works within it
- DR is the effort to END the degraded state
- If a scenario is still in crisis, it is BC — not DR
- If the crisis has passed and rebuilding is happening, it is DR

LESSON 2.5 — COMPONENTS

What a DR plan contains

For different audiences

- An executive summary — high-level overview for senior management
- Department-specific plans — recovery is not uniform across a business
- Technical appendices — system inventories, configurations, dependencies, vendor contacts, network diagrams

Decisions and process

- Recovery priorities, inherited from the BIA
- Roles and responsibilities, including who declares the disaster over
- Testing and evaluation procedures, with a schedule
- Backup and restoration procedures

Same two rules as the BC plan

- Copies must be accessible when systems are not, and the plan must be maintained as the environment changes

Three backup strategies

Incremental optimises backup speed. Differential optimises restore speed.

FULL

Everything, every time

Slowest to back up
Simplest to restore

INCREMENTAL

Changed since the LAST backup of any kind

Fastest to back up
Restore needs full + ALL since

DIFFERENTIAL

Changed since the last FULL backup

Restore needs full + ONE differential

Store backups offsite, and test the restores — an untested backup is a hypothesis.

The trade-off is the point

- Incremental optimises backup speed · differential optimises restore speed · full optimises simplicity

LESSON 2.5 — RESTORE CHAINS

Which sets do you need?

Full backup Sunday, incrementals Monday to Thursday. Failure occurs Friday.

Sunday's full plus all four incrementals — five sets. Any one of them failing breaks the chain.

Full backup Sunday, differentials Monday to Thursday. Failure occurs Friday.

Sunday's full plus Thursday's differential only — two sets. Faster and far less fragile.

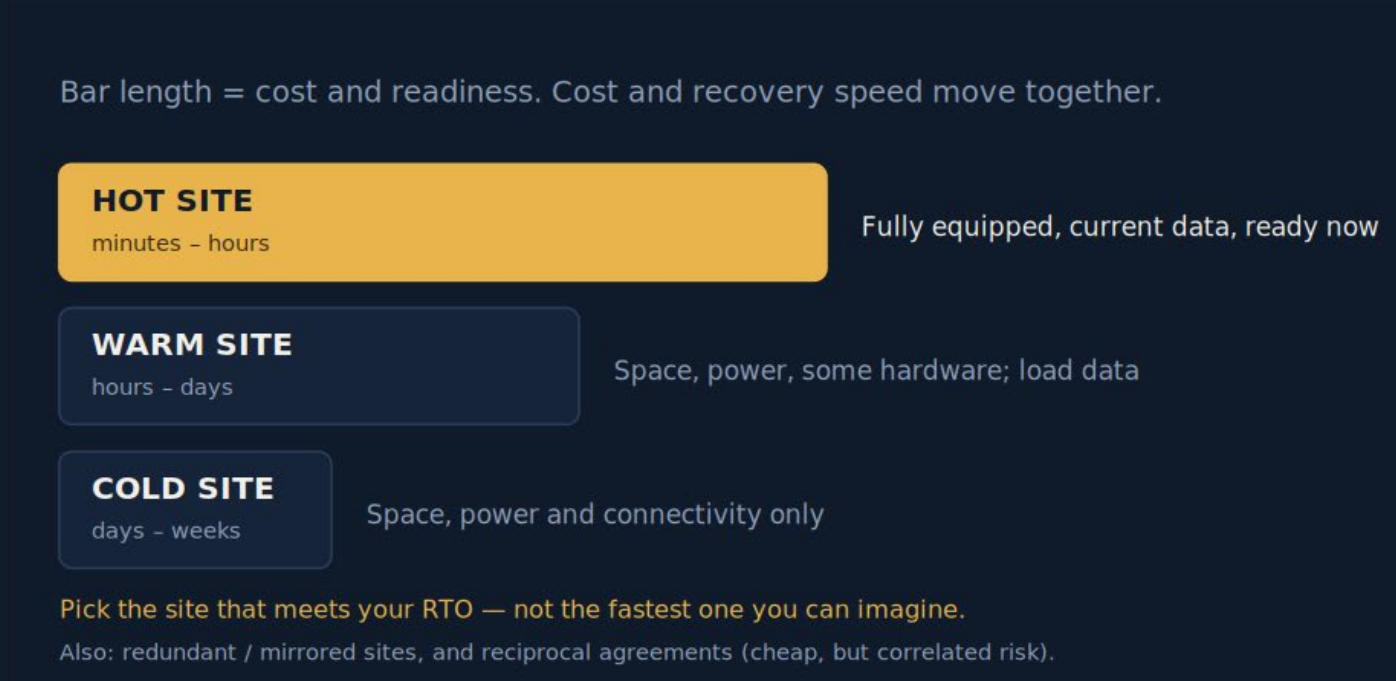
Backups stored in the same building as the systems they protect.

A single fire or flood destroys both. Offsite storage is not optional.

Backups that have run successfully for two years and never been restored.

A hypothesis, not a backup. Silent backup failure is common — test the restores.

Recovery site types



Match the site to the RTO

- A four-hour RTO rules out a cold site. A three-week RTO cannot justify a hot one

Two more options to know

- Redundant / mirrored sites, and reciprocal agreements — cheap, but correlated risk

LESSON 2.5 — SITE DETAIL

The three site types

Hot site	Fully equipped, fully operational duplicate with current data. Ready in minutes to hours. Most expensive by far, shortest recovery time.
Warm site	Space, power, connectivity and some hardware installed, but data must be loaded and configuration finished. Hours to days.
Cold site	Space, power and connectivity only. Everything else must be brought in and built. Days to weeks. Cheapest to maintain.
Reciprocal	Two organisations agree to host each other. Cheap and unreliable — the partner's capacity and willingness during a real disaster are uncertain.

Cost and recovery speed move together. A regional flood hitting both parties to a reciprocal agreement is the standard cautionary example.

Increasing realism, increasing disruption

1	**Read-through / checklist**	Team members review their own copies. Cheapest, catches obvious gaps and out-of-date details.
2	**Tabletop / walkthrough**	The team talks through a scenario together. Surfaces disagreements about who does what.
3	**Simulation**	A scenario is role-played with some real actions taken. More realistic, still low risk.
4	**Parallel test**	Recovery systems are brought up while production keeps running. Realistic without endangering service.
5	**Full interruption**	Production is actually stopped and recovery systems take over. Most realistic, most dangerous — rarely done.

Most organisations stop at parallel testing. A full interruption test that fails means you caused your own outage.

LESSON 2.5 — QUICK CHECK

Answer before advancing

1. Which backup type needs the fewest sets to restore, after a full backup?

2. An organisation's RTO is three weeks and budget is minimal. Which site type?

3. Why is a full interruption test rarely performed?

LESSON 2.5 — ANSWERS

Check your reasoning

1. Differential

The last full backup plus a single differential — two sets. Incremental needs the full backup plus every incremental taken since, so the chain is longer and more fragile.

2. A cold site

With a three-week recovery target there is no justification for warm or hot facility costs. Matching the site to the RTO, rather than reaching for the fastest option, is the tested skill.

3. Because it deliberately halts production

If recovery fails, the organisation has caused its own outage. It is the most realistic test and the most dangerous, so it is reserved for mature programmes with heavy preparation.

2.6

LESSON

Telling the Three Apart

OBJECTIVE

Classify any scenario as incident response, business continuity or disaster recovery — reliably and quickly.

- The time-position test
- Cue words for each plan
- A practice set, including deliberate boundary cases
- The consolidation set to produce from memory

LESSON 2.6 — THE TEST

One question does the sorting

Where in time does this sit?

- Something is happening right now and someone is reacting to it → INCIDENT RESPONSE
- The disruption is ongoing and work is continuing by other means → BUSINESS CONTINUITY
- The crisis has passed and normal service is being rebuilt → DISASTER RECOVERY
- Apply it before reading the answer options

LESSON 2.6 — CUE WORDS

The vocabulary each plan uses

INCIDENT RESPONSE

- detect · contain · isolate
- eradicate · triage · analyse
- alert · first response · escalate

- Language of reacting to something live

BUSINESS CONTINUITY

- alternate site · workaround
- manual process · call tree
- remain operational · critical functions
- degraded service · relocate staff

- Language of carrying on regardless

DISASTER RECOVERY

- restore · rebuild · recover data
- return to normal · backups
- failback · reconstitute · RTO met

- Language of putting things back

LESSON 2.6 — PRACTICE

Sort these before you look

Isolating an infected laptop from the network

IR — containment

Staff working from home for three weeks after a fire

BC — operating through

Routing calls to a third-party centre while phones are down

BC — alternate delivery

Rebuilding the server room and migrating services back

DR — return to normal

Restoring a database from Tuesday's backup

DR — restoration

Paper charts while the records system is down

BC — manual workaround

Analysing logs to determine how an attacker got in

IR — detection and analysis

Declaring an emergency and activating the call tree

IR shading into BC — the handover

The last item is deliberately on the boundary. Declaration is immediate response; the call tree is a BC component.

LESSON 2.6 — BOUNDARIES

When a scenario genuinely straddles two plans

The overlap is real

- A hot site can be the DR mechanism, or the way the business stays operational during a crisis
- Activating a call tree is both an immediate response and a continuity component
- Real incidents run all three plans at once

How to decide

- Choose on the STATED PURPOSE of the action, not the mechanism used
- Standing in during the crisis → BC
- Restoring after it → DR
- A well-written question will not put you on a boundary — if it feels genuinely ambiguous, re-read for the purpose

CONSOLIDATION

Produce these, don't just recognise them

Sequences

- The three plans, in order:
- IR → BC → DR

- The four IR phases:
- prepare · detect & analyse ·
- contain, eradicate & recover ·
- post-incident

- Containment before eradication

Hierarchies and metrics

- Event · alert · incident · breach
- Each narrower than the last

- RPO · RTO · MTD · MTTR
- RTO must be shorter than MTD
- RPO sets backup frequency

- Everything flows from the BIA

Choices and rules

- Full · incremental · differential
- Incremental = since any
- Differential = since full

- Hot · warm · cold
- Cost and speed move together

- Life and safety outranks everything
- Legal and HR sit on the IR team

Ten percent of the exam and a short list. This is the domain where full marks are realistic.

EXAM TECHNIQUE

How this domain is tested

1	**Scenario → plan**	The dominant form. Given an activity, is it IR, BC or DR? Apply the time-position test.
2	**Definition match**	Event, alert, incident, breach — or RPO versus RTO. Straight recall.
3	**Ordering**	Phase order, or the testing ladder. Containment before eradication; read-through before full interruption.
4	**Fit to constraint**	Site type given an RTO or budget; backup type given a restore-time requirement.
5	**Who decides**	Notification, shutdown, ransom, risk acceptance — all escalate to management or legal.
6	**Restore chain**	Given a backup schedule and a failure date, which sets are needed?

Six patterns, and the first one carries the most marks by a wide margin.

Next: Domain 3

Access Controls

22% of the exam. Physical and logical controls, and naming the access control model from a description.

Before you move on: can you state the purpose of IR, BC and DR in one sentence each, and say which one a paper-based workaround belongs to?