CERTLABZ CERTIFICATION BOARD

Certified Incident Response Professional (CIRP)

Ten Sample Questions

These ten questions are written at the difficulty of the live exam. Six carry a figure, a data table, a configuration or a code listing; four are plain scenario questions, as on the live paper. Every one is a scenario a working incident responder would meet, and none of them appears in the live question bank.

The live exam is multistage adaptive: how you score on one stage selects the difficulty of the next, so no two candidates sit the same paper. It is a performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions, which means you build, sequence or complete something rather than only choosing from a list. Answers and full explanations follow each question here; the live exam does not disclose item-level answers.

Question 1 — Domain 3: Analysis and Investigation — TIMELINE

Emma Wilson reconstructs an intrusion from central logs. The key events, in days before detection, are below.

Figure 1.1 Reconstructed events, in days from initial access to detection.

What does this timeline tell the responder about scoping and log retention?

A. The incident began about 27 days before detection, so scoping needs logs older than the dwell time or the entry point is lost.

B. The incident began at detection on day 27, so only the last day of logs is relevant to fully scope the intrusion.

C. The phishing email is irrelevant once the EDR alert has fired, so the investigation can safely start from day 27.

D. The lateral movement on day 9 is the true start, so logs before day 9 add nothing useful to the investigation.

Correct answer: A
Dwell time here is about 27 days: initial access on day 2 (of the 30-day window), detection on day 27. If log retention is shorter than the dwell time, the phishing entry and early lateral movement are already gone, and scoping cannot reach the real start. Retention must exceed typical dwell time for exactly this reason.

Question 2

Domain 5: Specific Incident Types

DATA

James Carter investigates a cloud mailbox after a user reports missing invoices. The audit log shows the sequence below.

Time	Event	Detail
08:40	Sign-in success	From a hosting-provider IP, unknown device
08:41	New inbox rule	Move messages containing "invoice" to Archive, mark read
08:42	New forwarding	Forward all mail to an external address
08:45	OAuth consent	Third-party app granted Mail.Read

Table 2.1 Mailbox audit events for the affected account.

Beyond resetting the password, what must the response remove to evict the adversary?

A. The inbox rule, the forwarding, the OAuth consent and any live sessions or tokens, since each survives a password reset alone.

B. Only the inbox rule that hides invoices, because that is the mechanism the user actually noticed as missing mail.

C. Only the external forwarding address, because that is the sole route by which data is leaving the mailbox now.

D. Nothing further, because resetting the account password immediately invalidates every rule, consent and session.

Correct answer: A
BEC persistence lives in mailbox rules, forwarding, granted OAuth apps and live tokens, all of which survive a password change. Removing only one mechanism, or assuming the reset clears everything, leaves the adversary a way back. Evicting means revoking sessions and tokens and removing every rule and consent.

Question 3

Domain 3: Analysis and Investigation

DATA

Olivia Davis must collect evidence from a live, compromised host without losing what matters most.

Evidence	Where it lives	Lost when
Running processes, network connections	Volatile memory	The host is powered off
Injected code and decryption keys	RAM	The host is powered off
Malware binary and timestamps	Disk	The disk is wiped or overwritten
Historical logons	Central log store	Retention expires

Table 3.1 Evidence sources for the host.

In what order should the evidence be collected?

A. Memory and live state first, then the disk image, then rely on the central logs, following the order of volatility.

B. The disk image first because it is the largest and most complete single source of forensic evidence available.

C. The central logs first because they are already collected and therefore the quickest evidence to secure.

D. Whichever source is easiest to reach first, since collection order does not affect the evidence that survives.

Correct answer: A
The order of volatility (RFC 3227) says capture what disappears first: memory and live network state before power-off, then the disk, then archival logs. Fileless malware and keys exist only in RAM, so taking the disk first, or treating order as unimportant, loses the most fragile and often the most valuable evidence.

Question 4

Domain 4: Containment, Eradication and Recovery

DATA

Liam Anderson leads the response to an intrusion using stolen domain credentials across many hosts. A colleague proposes the plan below.

```
Step 1: reset each abused account as it is noticed
Step 2: isolate the first infected host, monitor the rest
Step 3: clean malware on that host
Step 4: wait for the full investigation before touching other systems
```

Listing 4.1 The proposed response plan.

Why is this plan unsound, and what is the correct approach?

A. Piecemeal resets and single-host isolation tip off the adversary; scope fully, then contain and reset all access at once.

B. The plan is sound as written, because handling one account and one host at a time keeps the response controlled.

C. The only fault is Step 3, which should clean the malware before the host is isolated from the rest of the network.

D. The only fault is Step 4, which should wait even longer so that the investigation is completely finished first.

Correct answer: A
A credential-based intrusion has many footholds. Resetting accounts one at a time and isolating one host warns the adversary, who adapts or destroys evidence while retaining access elsewhere. The sound approach is to scope the full footprint, then contain hosts and reset all compromised credentials and tokens in a coordinated action.

Question 5

Domain 4: Containment, Eradication and Recovery

DATA

After a ransomware incident, Ava Thompson evaluates four recovery candidates. The objective is RTO 4 hours, RPO 1 hour.

Backup	Age	Status	Restore test
A. Nightly to same domain share	6 h	Encrypted by the ransomware	n/a
B. Hourly to immutable cloud store	45 min	Intact, offline copy	Restores in 3 h
C. Weekly to tape	5 days	Intact	Restores in 10 h
D. Snapshot on the same host	30 min	Deleted by the adversary	n/a

Table 5.1 Recovery candidates.

Which backup should be used, and why?

A. Backup B, because it is intact and offline, meets the one-hour RPO, and its three-hour restore is within the four-hour RTO.

B. Backup A, because a six-hour nightly copy on the domain share is the most recent complete backup that is available.

C. Backup C, because tape stored for five days is the most trustworthy medium even though its restore takes ten hours.

D. Backup D, because a 30-minute snapshot on the host gives the smallest possible data loss of all four candidates.

Correct answer: A
Ransomware targets reachable backups: A is encrypted and D is deleted, so both are useless. C is intact but its 10-hour restore breaks the 4-hour RTO and its 5-day age breaks the 1-hour RPO. Only B is intact, offline, recent enough for the RPO and fast enough for the RTO. Immutable, offline copies are what survive.

Question 6

Domain 6: Post-Incident, Communication and Legal

DATA

A confirmed breach exposes personal data of EU residents and the company is publicly traded in the US. The team lists possible obligations.

Obligation	Trigger
Notify the supervisory authority without undue delay, target 72 hours	Breach of EU residents' personal data
Notify affected individuals	The breach is likely to be a high risk to them
Public disclosure on a short timeline	The incident is material to investors
Maintain chain of custody	Evidence may be used in legal action

Table 6.1 Candidate obligations and their triggers.

What does this table imply for how the incident is run?

A. Several duties on different timelines can fire from one incident, so legal is engaged early and materiality is assessed promptly.

B. Only the 72-hour GDPR notification matters, so the other three obligations can be handled after the incident closes.

C. Public disclosure can always wait until the annual report, so the securities obligation does not affect the response timeline.

D. Chain of custody is a purely technical concern and does not need to involve legal counsel at any point in the response.

Correct answer: A
A single incident can create privacy, securities and evidentiary duties at once, each on its own clock. That is exactly why legal counsel is engaged at the start and materiality is assessed early: the response has to run the notification and disclosure timelines in parallel with the technical work, not after it.

Question 7 Domain 1: Incident Response Foundations and Governance

During a major incident, the technical lead wants to take a revenue-generating system offline to contain the threat, and a business executive objects. How should this be resolved?

A. The incident commander decides within the authority the plan granted, escalating high-impact trade-offs to a named business owner.

B. The most senior person present by job title makes the call on the spot, regardless of what the response plan says.

C. The technical lead always overrides the business, because containing the security threat must take priority every time.

D. The decision is deferred until after the incident is over, so that it can be made calmly with complete information.

Correct answer: A
Decision rights and escalation thresholds for business-impacting actions belong in the plan, agreed before the incident. The incident commander acts within that authority and escalates the biggest trade-offs to the accountable business owner. Seniority-by-title, a technical veto, and deferring the decision all fail under real time pressure.

Question 8

Domain 4: Containment, Eradication and Recovery

A server was deeply compromised with an unknown persistence mechanism. The team debates whether to clean it in place or rebuild it from a known-good image. Which course is sound, and why?

A. Rebuild from a known-good image, because a deep compromise can hide persistence that in-place cleaning may miss entirely.

B. Clean it in place, because rebuilding is always slower and the malware that was found has already been removed safely.

C. Clean it in place and monitor, because a rebuild would destroy the forensic evidence still needed for the investigation.

D. Leave the server running as is, because taking it offline would breach the recovery time objective the business set.

Correct answer: A

For a deep or uncertain compromise, rebuild-from-known-good is the only reliable way to be sure no backdoor remains; cleaning in place risks leaving hidden persistence. Evidence is preserved by imaging before the rebuild, not by leaving a compromised host in production, and running it as is simply keeps the adversary's access alive.

Question 9

Domain 5: Specific Incident Types

A ransomware group has encrypted systems and also claims to have stolen and will publish sensitive data unless paid. The company has clean, tested backups. How does the data-theft claim change the response?

A. Even a clean restore does not resolve the exposure, so scope what was taken and engage legal and communications for the breach.

B. The clean backups fully resolve the incident, so the restore can proceed and the data-theft claim can be disregarded.

C. Data-theft claims from ransomware groups are always bluffs, so no breach handling or notification work is required at all.

D. The incident becomes purely a recovery task once backups exist, and paying the ransom is the only way to stop publication.

Correct answer: A

Double extortion adds a data-breach event on top of the encryption. Restoring systems from backup recovers availability but does nothing about the stolen data or the disclosure threat, which carry their own notification and legal duties. The claim must be scoped, not assumed a bluff, and payment neither guarantees silence nor removes the obligations.

Question 10

Domain 6: Post-Incident, Communication and Legal

An organisation closes out a serious incident and wants the review to be worth the time. What most determines whether the lessons-learned review actually reduces future risk?

A. It produces tracked actions with named owners and dates that change detections, controls and the plan, then verifies them.

B. It documents in detail exactly which individual made the mistake that allowed the incident to happen in the first place.

C. It is held a year later at the annual audit, when there is time to reflect on the incident with full hindsight.

D. It records that the incident was contained and closes the ticket, since the technical work has already been completed.

Correct answer: A

A review adds value only when it becomes owned, dated actions that actually change detection coverage, controls and the response plan, and someone verifies they were done. Blame hunting discourages honesty, holding it a year later loses the detail, and simply closing the ticket wastes the most useful data the organisation has.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Companion to objectives document CIRP-001. https://certlabz.com/certifications/certified-incident-response-professional.html