



TECHNICAL LEARNING AND ASSESSMENT DOSSIER

ISO/IEC 27035 – Incident Management & Recovery

Course + certificate

800,00 €

VAT excluded

Course code

ISO27035-IMR

Minimum duration

480 min

Final pass score

70%

Dossier issue

13/10/2026

1. Course identity, purpose and scope

Advanced bilingual pathway on information security incident management: preparation, detection, triage, analysis, containment, eradication, recovery, coordination and lessons learned according to the ISO/IEC 27035 family.

This extended technical dossier describes the pathway as published in CIWZ Academy on the issue date. It consolidates purpose, references, learning architecture, module contents, assessment system, passing criteria and certificate conditions. It does not replace the official texts of the standards, laws, guidelines or schemes referenced.

2. Normative, regulatory and technical references

ISO/IEC 27035-1:2023; ISO/IEC 27035-2:2023; ISO/IEC 27035-3:2020; ISO/IEC 27035-4:2024; integration references ISO/IEC 27001:2022 + Amd 1:2024 and ISO/IEC 27002:2022

References are used as the learning and assessment framework within the limits of published content and available sources. For professional application, the official and current versions of the referenced documents always prevail.

3. Learning architecture and assessment system

- 10 structured learning modules
- minimum tracked time: 480 min
- intermediate-check bank: 240 questions
- active final-exam bank: 180 questions
- final exam: 30 questions selected from the bank
- passing threshold: 70%
- Access to the pathway through the personal Academy profile or a corporate assignment.
- Sequential study of the modules, with server-side recording of progress and required minimum time.

- Intermediate checks linked to modules to verify understanding, application capability and quality of reasoning.
- Final exam unlock only after the pathway requirements have been completed.
- Protected final exam assembled by the platform through selection from the active course question bank.
- Recording of the result and, where applicable, the option to request the final certificate.

4. Official catalogue technical information

Course technical sheet

Specialist bilingual ISO/IEC 27035 pathway with 10 slide-based chapters, 480 server-tracked minimum minutes, 24 intermediate questions per chapter, 180 no-repeat final questions, and scenarios covering triage, investigation, containment, eradication, recovery, coordination and lessons learned.

5. Detailed course syllabus

The following syllabus is derived from the active modules published on the platform. Each module shows its minimum study time and the size of its available intermediate-check bank.

01 Foundations, principles and the incident-management lifecycle

Minimum time: 45 min | Intermediate questions: 24

02 Governance, preparation and response capability

Minimum time: 50 min | Intermediate questions: 24

03 Detection, reporting and quality of initial information

Minimum time: 45 min | Intermediate questions: 24

04 Triage, classification, severity and decision

Minimum time: 50 min | Intermediate questions: 24

05 Technical analysis, investigation and evidence

Minimum time: 55 min | Intermediate questions: 24

06 Response: containment, eradication and risk control

Minimum time: 55 min | Intermediate questions: 24

07 Recovery, controlled restoration and return to normal operations

Minimum time: 55 min | Intermediate questions: 24

08 Communication, obligations and cross-organization coordination

Minimum time: 45 min | Intermediate questions: 24

09 Lessons learned, metrics, exercises and improvement

Minimum time: 40 min | Intermediate questions: 24

10 Major-incident simulation, recovery readiness and auditability

Minimum time: 40 min | Intermediate questions: 24

6. Developed module-by-module contents

The following pages analytically describe the content actually associated with each platform module. The structure is designed so that learners, companies, HR, Quality, HSE or CISO functions can understand precisely what is studied and assessed.

MODULE 01**Foundations, principles and the incident-management lifecycle**

- Minimum required time: 45 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

The pathway distinguishes event, security event, incident and operational crisis, clarifying the purpose, boundaries and interactions of incident management. Incident management is a governed lifecycle: prepare, detect and report, assess and decide, respond, and learn.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Foundations, principles and the incident-management lifecycle” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Define taxonomy, activation criteria, accountability, authority and interfaces with the ISMS, risk management, business continuity, service management and crisis management.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept

residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Policy, process model, role matrix, classification criteria, escalation workflow, event register and links to risk and continuity.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

An anomaly is closed as a technical fault, but privileged credentials and sensitive data are involved. The critical point is recognizing when an event becomes an incident and activating the appropriate process.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can

increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Foundations, principles and the incident-management lifecycle” to new scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 02**Governance, preparation and response capability**

- Minimum required time: 50 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Preparation enables a consistent response under pressure. It includes commitment, policy, plans, playbooks, teams, competence, contacts, tools, communications and periodic exercises. Capability must be designed before the incident, not during it.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Governance, preparation and response capability” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Build the Incident Management Team and Incident Response Team, define availability, authority levels, playbooks, secure channels, suppliers, authority contacts and mobilization criteria.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept

residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Current roster, RACI matrix, call tree, runbook, tool inventory, third-party agreements, exercises and training records with effectiveness checks.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

Ransomware strikes during the weekend and nobody knows who can authorize a production-system shutdown. The gap is not technical: it is a preparedness and authority defect.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can

increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Governance, preparation and response capability” to new scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 03**Detection, reporting and quality of initial information**

- Minimum required time: 45 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Well-managed incidents begin with signals that are collected, correlated and reported promptly. Different sources — people, logs, EDR, SIEM, network, cloud, suppliers, customers — may reveal different parts of the same phenomenon.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Detection, reporting and quality of initial information” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Define reporting channels, minimum information, initial priority, time synchronization, log preservation and criteria for distinguishing noise, false positive, event and incident.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Tickets, reliable timestamps, original logs, correlated alerts, source, affected assets, accounts, technical indicators, initial impact and escalation chain.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

The SIEM generates many abnormal-authentication alerts and one is ignored because it resembles earlier ones. Soon after, access to a critical repository emerges: correlation and quality of initial assessment are required.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse "service restored" with "incident resolved".
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Detection, reporting and quality of initial information” to new

scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 04**Triage, classification, severity and decision**

- Minimum required time: 50 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Triage turns a report into an operational decision. Severity and priority do not automatically coincide: impact, urgency, assets, data, spread, persistence, attacker capability, legal requirements and dependencies must be considered.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Triage, classification, severity and decision” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Apply repeatable criteria, determine the response level, establish escalation and immediate objectives, while retaining the ability to reclassify as new evidence emerges.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Severity matrix, business-impact criteria, data classification, dependencies, decision log, priority rationale and reclassification timestamps.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

A single compromised account appears “low impact”, but it belongs to a cloud administrator. Priority changes because of privileges, potential blast radius and persistence capability.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Triage, classification, severity and decision” to new scenarios.

Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 05**Technical analysis, investigation and evidence**

- Minimum required time: 55 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Analysis should build a reliable timeline and distinguish facts, hypotheses and conclusions. The operational objective is to understand what happened, what remains active, which systems are involved and which actions are safe without destroying useful evidence.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

"Technical analysis, investigation and evidence" should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Preserve evidence, document acquisitions, validate sources, correlate indicators, reconstruct timelines, identify the root entry point and distinguish cause, vector, impact and persistence.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept

residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Hashes, forensic images or exports where relevant, raw logs, timeline, IOCs, queries, analyst notes, chain of custody and evidence collection/retention decisions.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

A host is immediately reimaged to restore service. The service returns, but the ability to understand persistence and attack scope is lost: recovery and investigation must be coordinated.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can

increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Technical analysis, investigation and evidence” to new scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 06**Response: containment, eradication and risk control**

- Minimum required time: 55 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Response should reduce harm without creating greater risks. Containment limits propagation; eradication removes known causes and persistence; both require decisions, success criteria and control of side effects.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Response: containment, eradication and risk control” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Choose among isolation, blocking, revocation, segmentation, suspension, workaround and permanent remediation, considering operational impact, residual risk, evidence and dependencies.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Action log, approvals, isolated hosts/accounts, blocked IOCs, changed configurations, remediated vulnerabilities, persistence indicators and post-eradication checks.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

Blocking an entire segment stops the attacker but interrupts an essential service. The team must choose proportionate containment and document risk and rationale.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse "service restored" with "incident resolved".
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Response: containment, eradication and risk control” to new scenarios.

Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 07**Recovery, controlled restoration and return to normal operations**

- Minimum required time: 55 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Recovery is not simply “turning systems back on”. The organization should show that causes were treated, systems are trustworthy, data are intact and restoration does not reintroduce the incident. The interface with business continuity and disaster recovery is essential.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Recovery, controlled restoration and return to normal operations” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Define go/no-go criteria, restoration priorities, clean restore, validation, heightened monitoring, rollback, service ownership and an observation period before closure.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept

residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Validated backups, restore tests, known-good baselines, vulnerability closure, credential reset, heightened monitoring, business acceptance, applicable RTO/RPO and return-to-service decision.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

A database is restored from a technically valid backup that predates the latest synchronization. Recovery must balance integrity, data loss, dependencies and business priorities.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can

increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Recovery, controlled restoration and return to normal operations” to new scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 08**Communication, obligations and cross-organization coordination**

- Minimum required time: 45 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Incidents often cross organizational boundaries. Communication should be authorized, accurate, timely and consistent. ISO/IEC 27035-4 adds the perspective of coordination among multiple organizations and its effects on internal processes.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

"Communication, obligations and cross-organization coordination" should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Map internal and external parties, notification criteria, channels, shareable detail levels, coordination responsibility, dependency management and message alignment.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept

residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Communication matrix, authority/CSIRT/supplier contacts, decision log, notifications, approved messages, information-sharing agreements and coordination records.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

A cloud provider sees malicious activity before the customer, while a partner hesitates to share IOCs for contractual reasons. Coordination should be prepared and governed before the crisis.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can

increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Communication, obligations and cross-organization coordination” to new scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 09**Lessons learned, metrics, exercises and improvement**

- Minimum required time: 40 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

Administrative closure is not the same as risk closure. Lessons learned turn the incident into improvement: causes, controls, process, roles, tools, communications and training should be reviewed with evidence.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Lessons learned, metrics, exercises and improvement” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Conduct post-incident reviews, separate blame from accountability, update risk assessment, SoA, playbooks and training, and define actions with owners, deadlines and later effectiveness review.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

PIR report, cause analysis, action tracker, risk/control updates, MTTD/MTTA/MTTR metrics interpreted with care, exercise results and action-effectiveness checks.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

Mean response time improves, but reopened incidents increase. The positive metric does not by itself prove effectiveness: solution quality and recurrence must also be read.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse "service restored" with "incident resolved".
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Lessons learned, metrics, exercises and improvement” to new

scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

MODULE 10**Major-incident simulation, recovery readiness and auditability**

- Minimum required time: 40 min
- Available intermediate-check bank: 24 questions

1. Operational objective of this chapter

The final module integrates the entire lifecycle into a decision simulation: detection, triage, analysis, containment, eradication, recovery, communication, coordination and improvement. The objective is to demonstrate repeatable capability, not a theoretical sequence.

The objective is to make decisions under pressure while preserving traceability, proportionality and continuity between the security process, business needs and available evidence.

- Connect the topic to the correct incident-management phase.
- Separate facts, hypotheses, decisions and outcomes.
- Identify the information required before action.

2. Position within the ISO/IEC 27035 family

“Major-incident simulation, recovery readiness and auditability” should be read within the ISO/IEC 27035 family: Part 1 for principles and process, Part 2 for preparation and lessons learned, Part 3 for ICT response operations and Part 4 for cross-organization coordination.

The course uses these references as an operational architecture integrated with the information security management system.

- Do not treat response as an isolated SOC activity.
- Keep handovers clear among governance, technical teams, business and external parties.
- Review the process when risks, technology or dependencies change.

3. Operational process and decision criteria

Run tabletop and technical exercises, define injects, success criteria, observers, decision logs, recovery checkpoints, escalation and post-exercise action plans.

A sound process defines triggers, minimum inputs, authority levels, escalation criteria and exit conditions. During critical moments decisions should be fast but reconstructable.

- Define who decides and on what basis.
- Set what must be recorded before and after action.
- Provide controlled exceptions for high-urgency scenarios.
- Associate every action with verifiable success criteria.

4. People, roles and handovers

The IMT, IRT, SOC, IT operations, privacy, legal, communications, business continuity and business owners may have different responsibilities. Handover quality is often the real weakness.

Clarity does not mean bureaucracy: it means knowing who may isolate, notify, restore, communicate and accept

residual risk.

- RACI or equivalent matrix.
- Availability and deputies.
- Alternative secure channels.
- Technical and management escalation.
- Authority for recovery decisions.

5. Evidence and timeline

Scenario, timeline, decisions, technical logs, timings, handovers, escalation, recovery evidence, communications, debrief, gap register and follow-up through effective closure.

The timeline should show what was known at each point and why a decision was made. Avoid retrospective reconstruction that mixes information known at the time with facts discovered later.

- Synchronized timestamps.
- Source and reliability of data.
- Decision, owner and rationale.
- Effects of the action.
- Evidence preserved before changing systems where relevant.

6. Applied scenario

During an exercise the team correctly contains malware but does not involve the business owner before restoration. The gap shows that maturity also depends on interfaces, not only technical skill.

First separate facts from assumptions. Then identify the immediate objective, the risk to limit, the proportionate action and the evidence that will determine whether to continue, change strategy or roll back.

- What is the first verifiable fact?
- Which decision cannot be delayed?
- Which evidence could be lost by acting too soon?
- Which function must be involved before the next step?

7. Recurring failure modes

Incidents are often mishandled not because tools are missing but because decisions are uncoordinated: severity fixed too early, containment without impact assessment, restoration before eradication, inconsistent communications or closure without effectiveness review.

A mature process makes these failure modes visible and turns them into preventive criteria.

- Do not confuse “service restored” with “incident resolved”.
- Do not rely on a single source to confirm scope.
- Do not destroy evidence during remediation without a conscious decision.
- Do not close without follow-up actions and owners.

8. Recovery and resilience

Whatever the chapter topic, recovery should be considered from the beginning. Containment and analysis decisions can

increase or reduce restoration time, while overly rapid recovery can reintroduce compromise or data loss.

Recovery readiness means go/no-go criteria, trusted baselines, tested backups, known dependencies and heightened monitoring after return to service.

- Verify restore prerequisites.
- Confirm configuration, credential and data integrity.
- Define an observation period.
- Maintain a rollback plan.

9. Useful metrics and indicators

Metrics should support decisions, not reward speed at the expense of quality. MTTD, MTTA and MTTR are useful only when read with severity, recurrence, reopened incidents, detection coverage and recovery quality.

A seemingly positive metric may hide under-reporting or premature closure.

- Detection time segmented by severity.
- Containment time and restoration time separately.
- Reopened or recurring incidents.
- Overdue post-incident actions.
- Exercise outcomes and recurring gaps.

10. Audit and capability review

An effective audit follows an incident or exercise from first evidence to closure: trigger, classification, decisions, actions, recovery and lessons learned. The objective is not to confirm that a plan exists but that capability works under realistic conditions.

Sample different cases by severity, technology, site and third-party involvement.

- Compare playbooks with actual behaviour.
- Verify handover time and quality.
- Look for evidence of corrective-action effectiveness.
- Assess whether criteria were applied consistently.

11. Decision lab

Imagine new information changes the initial assessment: a privileged account, a second tenant, a suspicious backup or an external notification. Decide what must be reclassified and which action becomes the priority.

Maturity is visible in the ability to change a decision without losing control and traceability.

- New fact.
- Impact on severity.
- Revised decision.
- Required authorization.
- Evidence to collect.
- Expected effect and verification.

12. Summary and preparation for the check

To pass the check you should be able to apply “Major-incident simulation, recovery readiness and auditability” to new scenarios. Questions do not reward rote memorization; they require the most defensible action based on criteria, evidence and risk.

Before the test, explain how the topic affects detection, decision, response, recovery and improvement.

- Identify the criterion before the action.
- Separate remediation, recovery and closure.
- Seek at least two independent sources for material decisions.
- Always verify effectiveness after action.

7. Assessment system, final exam and passing criteria

- Intermediate checks are linked to individual modules and provide progressive learning control before access to the final assessment.
- The final assessment consists of 30 questions selected from the active course bank. The platform applies an anti-repetition logic for new attempts when the bank size allows it.
- Final question-bank size detected at generation time: 180 active questions.
- Published passing threshold for the course: 70%.
- Questions are intended to assess not only recall but also interpretation, application, evidence selection, scenario assessment and quality of decision-making, depending on the subject matter.

8. Tracking, learning continuity and session integrity

- Path status, completed modules and recorded time are managed server-side when the course uses the Academy learning mode.
- The platform allows the pathway to resume from the recorded point and retains the results of required checks.
- Assessment sessions may be subject to the integrity and proctoring controls enabled by the platform and described in the applicable usage rules.
- Technical and integrity events support assessment and do not replace professional judgement where human review is required.

9. Certificate, use and limitations

The CIWZ certificate, where provided by the pathway and requested after passing, records the result achieved in the stated CIWZ pathway or assessment. It does not automatically replace personnel certification, professional registration, statutory licence, legal qualification or credentials issued by third-party bodies where such requirements are imposed by the applicable scheme.

10. Commercial and tax conditions

- Course + certificate: 800,00 € VAT excluded.
- UAE VAT is applied to UAE customers according to billing data and the applicable tax rules.
- Any specific commercial terms, agreements or corporate orders override the public price only when formally accepted by Certificato IWZ FZCO.

11. Dossier document control

- Document automatically generated by CIWZ Academy from the course data published at the time of the request.

- Course code: ISO27035-IMR
- Document language: EN
- Generation date: 13/10/2026
- For normative and professional application, the current official sources and any applicable procedures/schemes prevail.