SOC investigation and handover workbook

Operational workbook | English · Template to adapt | v3.0 · 2026-10-16

Template version: 3.0. Designed for a smaller organization that may outsource IT and monitoring, this workbook assumes neither an internal forensic team nor continuous availability. An internal coordinator owns the case and business decisions. Providers execute and document assigned tasks within their actual access and contractual authority.

How to use this workbook. Sections 1–6 provide the operational sequence. Apply the responsibilities, provenance checks and forms in sections 7–9 before collection and maintain them during investigation. Section 10 is the worked example; section 11 supports handover acceptance. Detailed references apply at the relevant action: their later position does not mean preparation happens after closure.

Type: operational workbook to complete. Copy this document for each incident. It organizes evidence, hypotheses and decisions without replacing your response policy or specialist forensic acquisition. Adapt the bracketed fields before use.

Approval and scope

Field	Value to complete
Organization and template reference	[TO COMPLETE: organization, reference]
Version, owner, approver	[TO COMPLETE: version, SOC lead, approver]
Approval and next review	[TO COMPLETE: dates]
Incident reference and classification	[TO COMPLETE: identifier, confidentiality]
Incident lead and deputy	[TO COMPLETE: names, trusted contacts]
Authorized systems and period	[TO COMPLETE: scope, time boundaries]

The incident lead sets priorities. The analyst records observations and limitations. The evidence custodian controls storage and access. Technical owners authorize actions on their systems. The legal or data protection contact determines applicable collection, retention and notification requirements. These responsibilities are proposed assignments: reconcile them with existing delegations and supplier contracts before adoption.

1. Open the case

☐ Record the initial report, its author and receipt time with time zone.

☐ Describe observed impact separately from potential impact.

☐ State the investigation question: account, endpoint, connection or operation to explain.

☐ Identify affected services and their owners.

☐ Record collection authority and known restrictions.

☐ Schedule the next situation update: [TO COMPLETE: time, participants].

Initial summary: “We observe [TO COMPLETE: verifiable fact] within [TO COMPLETE: scope]. We are trying to establish [TO COMPLETE: question]. At this stage, [TO COMPLETE: main uncertainty] remains unknown.” Avoid attributing an action or intention to a person using an IP address alone. Keep a distinction between the affected system, the account used and the person believed to be involved.

2. Maintain the evidence register

Assign a stable identifier to each item. Preserve the original in controlled storage and work on a copy where possible. A file digest helps check that data has not changed; it does not independently establish the truth of the contents or the author's identity. Record the integrity check actually performed, rather than assuming that the collection tool preserved everything.

Item	Source, collection and operator	Storage and integrity	Limitations
E-001	[TO COMPLETE: system, method, filter, time, person]	[TO COMPLETE: repository, digest, check]	[TO COMPLETE: coverage, losses, clock]

For every transfer, add sender, recipient, time, purpose and integrity check. Do not put secrets into the workbook: reference their authorized storage instead. Set retention and deletion according to [TO COMPLETE: internal rules, preservation constraints]. Check permissions on shared folders and external responders' access. A reference that the receiving analyst cannot open is a handover problem to resolve, not a completed transfer.

3. Build the timeline

Keep event time, ingestion time and observation time separate. Record the original time zone before normalization. Make every clock correction explicit. A missing log can result from unavailable collection, expiration or a failure. Record which sources were searched and the periods they cover, so another analyst can understand what the search establishes and what it cannot establish.

Original / normalized time	Observed event	Item	Interpretation and confidence
Fictional example: 10:05 UTC / 10:05 UTC	A forwarding rule appears on test account A	E-001, fictional example	Creation confirmed; human actor not attributed
[TO COMPLETE: time, precision]	[TO COMPLETE: operation, result, target]	[TO COMPLETE: item]	[TO COMPLETE: interpretation]

4. Test hypotheses

Hypothesis	Supporting evidence	Contradictory evidence	Next check and owner
[TO COMPLETE: testable explanation]	[TO COMPLETE: items]	[TO COMPLETE: items or unknown]	[TO COMPLETE: action, owner, due point]

Look for an authorized explanation and an independent observation. Distinguish “not found in the sources searched” from “did not happen.” Revise a conclusion when new evidence contradicts it; preserve the previous conclusion and the reason for the change. Timing correlation alone does not establish causation or attribution. Explain a confidence assessment with evidence and limitations rather than an unexplained numerical score.

5. Record decisions and their effects

Decision	Rationale and evidence	Authorization	Execution and verification
[TO COMPLETE: action, target]	[TO COMPLETE: benefit, risk, alternatives]	[TO COMPLETE: decision maker, time]	[TO COMPLETE: operator, result, check, rollback]

If urgency requires containment before collection, record what evidence becomes unavailable. For a deferred measure, state the accepted risk, accountable owner and reassessment point. A completed command does not by itself show that the intended effect occurred. Keep the result check linked to the original decision, including an unexpected result or an unsuccessful rollback.

6. Prepare handover and closure

☐ Summarize established facts, open hypotheses, impact and uncovered scope.

☐ Transfer accessible evidence references and restrictions.

☐ List pending actions, owners, due points and escalation criteria.

☐ Confirm the coordination channel and next handover.

☐ Ask the incoming analyst to restate priorities; record acceptance.

☐ At closure, assign residual monitoring, corrections and follow-up ownership.

☐ Check retention, restrictions and authorized deletion of temporary copies.

Limitations: this workbook does not guarantee that evidence will be legally admissible. Investigations involving people, sensitive information or critical systems require appropriate authority. Notification deadlines depend on applicable obligations; have competent advisers determine them. Do not insert a deadline copied from a different jurisdiction without checking that it applies.

Put the workbook into service

Before first use, the template owner checks that responders can access evidence storage, find a source event and use the handover channel. A completed field without a verifiable reference does not turn a hypothesis into a fact. If a source is missing, record who can supply it, what period remains recoverable and which decision is blocked. Set follow-up objectives locally according to urgency and available resources.

Proposed quality check	Result to retain
A colleague locates evidence using the workbook	[TO COMPLETE: item, reviewer, result]
A decision links to authorization and a verified effect	[TO COMPLETE: decision, check, gap]
The incoming team knows uncertainties and priorities	[TO COMPLETE: acceptance, owner, next step]

Before distribution, the incident lead checks that each important conclusion links to evidence or is explicitly a hypothesis. Prepare a restricted summary when recipients do not need personal or technical details. Corrections retain the previous version reference, author and reason. Handover acceptance transfers responsibility for agreed actions; it does not remove documented uncertainty.

7. Make the case usable in an outsourced environment

For an organization of approximately 80 staff, appoint an internal person who can reach business owners, authorize agreed expenditure and obtain interruption decisions. IT may collect records while an MSSP analyzes its alerts. Neither provider should be assumed to control every SaaS record. Establish who can export data and confirm an action for each service.

Proposed function	Decision responsibility	Execution and backup
Internal coordinator	Priorities, recipients, follow-up and escalation	[TO COMPLETE: person, deputy, independent channel]
Business owner	Impact, sensitive information access, recovery acceptance	[TO COMPLETE: management or service owner]
IT or SaaS provider	Technical decisions within delegation	[TO COMPLETE: provider, backup contact, actual rights]
Internal analyst or MSSP	Technical conclusions and limitations	[TO COMPLETE: analyst, reviewer, out-of-hours route]

Before collection, record assets, identities, SaaS services, remote work, supplier access, investigation period and exclusions. Include data location, export capabilities, contractual restrictions and the owner authorizing access. Personal equipment and industrial systems require specific decisions; this workbook grants no authority to intervene in them. Mark an unavailable capability explicitly rather than allocating it to an uncontacted provider.

If a contact is unavailable, use the backup and contractual escalation route. Record attempts, time, impact and the next decision point. A request sent to a provider remains requested, not completed. Meanwhile, an internal decision maker may restrict activity through available authorized means or explicitly accept a documented temporary risk. They must not assume administrative access that nobody has verified.

8. Control provenance, quality and clocks

For each export, record the interface or query, time parameters, selected time zone, filtering and pagination. Check that the exported period matches the request. Record license restrictions, sampling or truncation. If a provider supplies only a screenshot, state what it establishes and request source events where the reasoning needs them. Preserve the provider's explanation of any unavailable fields.

Distinguish native records, documented exports, indirect observations and reported information. This is a proposed working classification, not a universal legal evidence scale. A useful statement can guide a search without proving a sign-in. A detection tool may normalize a value; preserve its source link before interpreting that field. Explain the transformations used, including changes introduced during subsequent analysis.

Quality check	Question	Consequence to record
Coverage	Was the category enabled during the events?	[TO COMPLETE: covered or unknown period]
Time	Are source time, zone and offset known?	[TO COMPLETE: conversion, margin, uncertain order]
Completeness	Was the export complete, paginated or limited?	[TO COMPLETE: exclusions, further collection]
Transformation	Original field or enrichment?	[TO COMPLETE: mapping, version, limitation]

Do not force precise ordering when clock accuracy or offset prevents it. Describe a time window and preserve both possibilities. NIST SP 800-86 discusses system clock and time-zone differences; justify any working margin through local observations rather than a universal numerical tolerance. The timeline must allow a later reviewer to distinguish a measured offset from an analyst's assumption.

A digest calculated after receipt checks stability of the received copy; it does not establish that the provider exported the complete source. Ask how collection was performed and preserve the answer. Any useful conversion produces an identifiable working copy; do not silently replace the original. Retain superseded files with the reason for correction and the link to their replacement.

9. Additional forms to copy

Transfer record	Value to complete
Item, version and purpose	[TO COMPLETE: identifiers, authorized use]
Sender and recipient	[TO COMPLETE: identity, role, authority]

Transfer record	Value to complete
Departure, receipt and channel	[TO COMPLETE: zoned times, secure means]
Receipt check	[TO COMPLETE: digest or appropriate check, result, reservation]

Uncertainty record	Value to complete
Unresolved question	[TO COMPLETE: attribution, period or operation]
Consulted and missing data	[TO COMPLETE: items, coverage, reason]
Decision still possible	[TO COMPLETE: proportionate protection, limitations]
Next check	[TO COMPLETE: owner, expected source, decision point]

An exception records the unmet requirement, reason, risk and compensating controls actually available. The business owner or designated authority accepts or rejects it; an analyst must not turn missing proof into approval. After adoption, this model requires expiry and an early reassessment trigger, using a locally chosen period. Expiry requires another decision rather than silent renewal.

Exception record	Decision to complete
Gap and scope	[TO COMPLETE: missing control, systems, period]
Protection and limitations	[TO COMPLETE: measure, evidence, residual risk]
Authority and rationale	[TO COMPLETE: decision maker, reason, date]
End and reassessment	[TO COMPLETE: expiry, trigger, remediation owner]

10. Complete worked example — entirely fictional

Fictional company Workshop-80 has 80 staff and provider-administered SaaS email. At 08:20 UTC, finance reports an unrecognized forwarding rule. The internal coordinator opens INC-EX-01. IT collects records because the MSSP can access alerts only. Every person, account and action in this example is fictional; none describes an actual customer or incident.

Fictional item	Provenance and collection	Storage and check	Limitation
EX-E1	SaaS audit export, account A filter, 08:35 UTC, provider operator	Restricted EX repository, received copy and digest recorded in fictional log	Export covers 07:00–08:35 UTC only
EX-E2	Rule screenshot, 08:39 UTC, email owner	Same repository, original/copy distinguished	Does not independently identify the human actor
EX-E3	Business-owner account, 08:45 UTC	Dated note with identified author	Authorized purpose not found; statement needs corroboration
EX-E4	Separate provider confirmation and check, 09:05 UTC	New dated note with identified operator and service	Rule check only; sessions still unverified

Fictional time	Fact and item	Hypothesis or limitation	Next action
08:12 UTC	Rule created on account A, EX-E1	Operation confirmed; session link unknown	Request available sign-in records
08:20 UTC	Finance report, EX-E3	Does not establish exfiltration	Identify affected messages and period
08:50 UTC	Rule removal requested	Not yet executed	Obtain provider state check
09:05 UTC	Provider confirms removal and check, EX-E4	Application sessions remain unchecked	Continue identity/application containment

Fictional management accepts temporary account restriction despite delayed order processing. Decision EX-D1 identifies the delegated coordinator, provider execution, verified rule removal and open session check. An authorized business change remains possible until approval history is checked. The interim conclusion is a disputed operation, not an identified human perpetrator. The case records the operational impact alongside the protection decision.

At the fictional 09:30 UTC handover, the incoming analyst locates EX-E1, restates both unknowns and accepts three tasks: check sessions, establish affected messages and seek business authorization. The coordinator retains decision ownership. The case cannot close merely because the rule disappeared; residual actions need owners and the conclusion must stay within the evidence actually available.

11. Check completeness and accept handover

☐ An internal owner and deputy are reachable independently of the suspect account.

☐ Every major conclusion has evidence, a limitation or explicit hypothesis status.

☐ Authorized responders can reproduce queries and periods searched.

☐ Transfers and corrections preserve provenance and versions.

☐ Requested, executed and verified actions are distinct.

☐ Decisions under uncertainty identify authority, risk, compensation and reassessment.

☐ The incoming responder confirms evidence access, priorities, contacts and next decisions.

☐ Temporary copies and provider access have removal conditions.

Closure is separate from handover. It states covered scope, facts, accepted unknowns, business consequences and actions tracked elsewhere. The owner approves distribution and storage; competent functions determine applicable retention and obligations. A later review should be able to understand why a decision was reasonable using information available at that time, without treating an interim judgement as final certainty.

Working references

NIST SP 800-61 revision 3 places incident response within risk management. NIST SP 800-86, published in 2006, provides a forensic collection and analysis framework; its technical examples need current review. These tables and procedures are editorial proposals to adapt, without certification or compliance guarantees.