CONTINUITY HUB • POST-CRISIS REVIEW

24-Hour Hot Wash Quick Card: The First Debrief on One Card

Current version — Oct 31, 2026. Update history: https://continuityhub.org/post-crisis-review-after-action-reports-lessons-learned/
Grounding: ContinuityHub Post 23 • Review Types & Timing Field Standard

THE 24-HOUR HOT WASH WINDOW & GOVERNING STANDARD

Timing & Operational Mindset: Conducted within **24 hours** of crisis stabilization while operational details, friction points, and communication lags are fresh and personnel remain in the crisis response mindset.
Core Purpose: Capture immediate observations and ensure critical safety or continuity issues are resolved before personnel disperse. Precedes the formal After-Action Review (2–4 weeks) and Executive Review (4–8 weeks).

1. Post-Crisis Review Lifecycle: Three Tiers & Timing Architecture

TIMING STANDARDS

Review Type	Target Timing	Participants	Purpose & Deliverables
Hot Wash (Debrief)	< 24 HOURS	Core crisis team & active responders	Immediate observation capture, critical safety/continuity triage, and investigation questions for formal review. Output: Brief operational debrief notes.
Formal After-Action Review (AAR)	2–4 WEEKS	Full crisis team, affected departments, partners, SMEs	Comprehensive lifecycle analysis (detection to recovery), 4-question AAR framework, root cause analysis, prioritized recommendations with owners & timelines. Output: Formal AAR report.
Executive Review	4–8 WEEKS	Senior leadership & executive sponsors	Strategic review of organizational resilience, financial implications, resource allocations, policy updates, and executive oversight. Output: Strategic directive & capital budget approvals.

Hot Wash Ground Rules (Learning vs Blame)

FACILITATION

- **Strict Blame-Free Environment:** Establish at the outset that the objective is organizational learning, systemic improvement, and gap identification—not personal culpability.
- **Neutral Facilitation:** Run by a lead without contested decisions; maintain psychological safety across all hierarchy tiers.
- **Time-Boxed Focus:** Keep to 30–60 minutes; capture facts, observations, and immediate risks without prematurely writing policy.

Incident Stabilization Handover Header

LOG HEADER

Incident Name: _____ **Date/Time:** _____
Incident Commander: _____ **Hot Wash Lead:** _____
Core Responders Present: _____

PROMPT 1 What Went Well During Response? (Positive Capabilities & Rapid Execution)

Identify procedures, tools, communication channels, individual actions, or automated alerts that functioned effectively:

1. [Capability / Tool / Team]: _____
2. [Specific Success / Timely Handoff]: _____
3. [Resilient Workaround / Effective Action]: _____

PROMPT 2 What Could Be Improved? (Friction Points, Gaps & Lags)

Document where expectations diverged from reality, communication slowed, procedures were missing, or resources fell short:

1. [Process Delay / Information Gap]: _____
2. [Tool Failure / Access Bottleneck]: _____
3. [Role Confusion / Procedural Ambiguity]: _____

CONTINUITY HUB • POST-CRISIS REVIEW

24-Hour Hot Wash Quick Card: Immediate Triage & Evidence Lock

Current version — Oct 31, 2026. Update history: https://continuityhub.org/post-crisis-review-after-action-reports-lessons-learned/
Grounding: ContinuityHub Post 23 • Critical Issues & Investigation Protocol

PROMPT 3 **What Critical Issues Need Immediate Attention? (< 24–48h Operational Triage)**

Isolate residual hazards, exposed systems, customer notification obligations, vendor escalations, or regulatory deadlines:

1. [Safety / Regulatory / Customer Risk]: _____
2. [Operational Vulnerability / Active Threat]: _____
3. [Immediate Remediation Required Today]: _____

PROMPT 4 **What Questions Need Further Investigation? (Formal AAR Roadmap)**

Questions requiring forensic data, timeline reconciliation, vendor logs, or interview follow-ups for the 2–4 week AAR:

1. [Timeline Discrepancy / Detection Lag]: _____
2. [Technical Root Cause / Failure Mode]: _____
3. [Contractual / SLA / Financial Question]: _____

2. Critical Evidence Preservation Checklist (Lock Down Within 24 Hours)

AUDIT TRAIL DEFENSE

Before responders resume normal duties, preserve all primary documentation required for the formal After-Action Report:

Status	Documentation Source	Specific Records to Secure & Preserve	Custodian / Location
[ ]	**Incident Logs & Timestamps**	Dispatch logs, ticketing system time entries, system monitoring alert timestamps.	Incident Log Keeper / SIEM
[ ]	**Decision Logs & Rationale**	Command team decision logs, situational briefing notes, emergency escalation sign-offs.	Incident Commander / Scribe
[ ]	**Communication Records**	Emergency broadcast logs, automated call tree delivery receipts, customer email blasts, Slack/Teams transcripts.	Communications Lead
[ ]	**Financial & Procurement Records**	Emergency purchase authorizations, contractor callout invoices, overtime logs, vendor receipts.	Finance / Procurement Lead
[ ]	**Technical Telemetry & Backups**	Forensic memory dumps, firewall/network packet logs, server access logs, immutable backup snapshots.	Infrastructure / Security Lead

3. Immediate Action Items (< 48-Hour Resolution Sign-Off)

ACTION PROTOCOL

Critical Issue Identified	Mandatory Immediate Action	Owner	Deadline	Sign-Off
_____	_____	_____	___ hrs	[ ] Done
_____	_____	_____	___ hrs	[ ] Done
_____	_____	_____	___ hrs	[ ] Done
_____	_____	_____	___ hrs	[ ] Done

Hot Wash Facilitator Sign-Off: _____ **Date & Time Completed:** _____