CONTINUITY HUB • POST-CRISIS REVIEW PRINT PACK

Section 1: 24-Hour Hot Wash Capture Sheet & Rapid Operational Debrief

Current version — Oct 31, 2026. Update history: https://continuityhub.org/post-crisis-review-after-action-reports-lessons-learned/
Grounding: ContinuityHub Post 23 • Hot Wash Operational Debrief Protocol

Standard Operating Mandate: Conduct within **24 hours** of crisis stabilization. Gather core responders while events, timeline details, and emotional impressions are fresh. Purpose: Capture immediate observations, flag unresolved safety/continuity hazards, and outline investigation questions for the 2–4 week formal After-Action Review.

Incident & Hot Wash Session Metadata

ADMINISTRATIVE REGISTER

Incident Identifier / Name: _____
Incident Date & Duration: _____
Stabilization Timestamp: _____
Hot Wash Session Time: _____
Hot Wash Facilitator (Neutral): _____
Incident Commander: _____
Responders Present: _____

1. What Went Well During Response? (Successful Tools, Procedures & Actions)

STRENGTHS

Identify response activities that met objectives, rapid decisions, resilient workarounds, and reliable systems:

[Positive Finding 1]: _____
[Positive Finding 2]: _____
[Positive Finding 3]: _____

2. What Could Be Improved? (Process Delays, Bottlenecks & Tool Failures)

FRICTION POINTS

Document where execution diverged from plans, communications lagged, resources fell short, or roles conflicted:

[Friction Point 1]: _____
[Friction Point 2]: _____
[Friction Point 3]: _____

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

IMMEDIATE TRIAGE

Flag unresolved safety hazards, system vulnerabilities, customer notifications, or legal/regulatory exposures:

[Immediate Hazard 1]: _____ • Owner: _____ • Due: ___h
[Immediate Hazard 2]: _____ • Owner: _____ • Due: ___h

4. What Questions Need Further Investigation? (Roadmap for Formal AAR)

FORENSIC ROADMAP

Identify timeline discrepancies, missing telemetry logs, technical root cause questions, or vendor disputes for the 2–4 week review:

[Forensic Question 1]: _____
[Forensic Question 2]: _____

CONTINUITY HUB • POST-CRISIS REVIEW PRINT PACK

Section 2: Formal After-Action Review (AAR) — Questions 1 & 2 Worksheet

Current version — Oct 31, 2026. Update history: https://continuityhub.org/post-crisis-review-after-action-reports-lessons-learned/
Grounding: ContinuityHub Post 23 • Four-Question AAR Framework (Planning vs Reality)

The Four-Question Core Protocol: Evaluates performance against intended objectives without personal blame. Conducted **2–4 weeks** post-crisis to allow complete recovery while operational memory remains intact.

QUESTION 1: WHAT WAS SUPPOSED TO HAPPEN? (PLANNING & EXPECTATIONS)

BASELINE OBJECTIVES

Examine pre-existing Business Continuity Plans (BCP), Disaster Recovery Plans (DRP), emergency SOPs, and expected response milestones:

Planning Dimension	Documented Standard / Expected Procedure	Key Assumptions Made During Planning
Detection & Escalation Monitoring, threshold triggers, initial alerts	_____	_____
Team Activation & Command Call trees, command center, succession	_____	_____
Containment & Mitigation System failovers, physical isolation, safety	_____	_____
Stakeholder Communication Staff, customers, media, regulators	_____	_____
Recovery & Restoration RTO/RPO targets, service resumption	_____	_____

QUESTION 2: WHAT ACTUALLY HAPPENED? (FACTUAL TIMELINE & DIVERGENCE)

REALITY RECONSTRUCTION

Reconstruct actual decisions and milestones from incident logs, dispatch records, and participant accounts. Isolate points of divergence:

Timestamp	Actual Event / Action Taken	Divergence From Plan / Expected Standard	Verified Source
T + 00:00	_____	_____	[ ] Log [ ] Alert
T + _____	_____	_____	[ ] Decision Log
T + _____	_____	_____	[ ] Comms Record
T + _____	_____	_____	[ ] Telemetry
T + _____	_____	_____	[ ] Responders
T + _____	_____	_____	[ ] Vendor Log

QUESTION 3: WHY DID IT HAPPEN THAT WAY? (CAUSAL ANALYSIS & SYSTEMIC GAPS)

CAUSAL ANALYSIS

Analyze root causes of divergence between plan and execution. Avoid individual blame; dissect procedural, training, and capability factors:

Failure / Divergence	Information Available to Responders	Underlying Systemic / Environmental Causes	Primary Root Cause Classification
Notification & Assembly Lag	_____	_____	[ ] Process Gap [ ] Training Need [ ] Capability / Tool Deficit
Situational Awareness Blindspot	_____	_____	[ ] Process Gap [ ] Training Need [ ] Capability / Tool Deficit
Delayed Crisis Communication	_____	_____	[ ] Process Gap [ ] Training Need [ ] Capability / Tool Deficit
Authority / Succession Confusion	_____	_____	[ ] Process Gap [ ] Training Need [ ] Capability / Tool Deficit

QUESTION 4: WHAT SHOULD WE DO DIFFERENTLY NEXT TIME? (CORRECTIVE ACTIONS)

IMPROVEMENT STRATEGY

Formulate specific, actionable improvements directly addressing the root causes identified above. Prioritize by operational impact and feasibility:

Specific & Actionable Improvement Commitment	Target Dimension	Priority Level	Owner / Department	Target Completion
_____	Procedure Update	HIGH IMPACT	_____	___ Weeks
_____	Plan Revision	MEDIUM IMPACT	_____	___ Weeks
_____	Capability Building	HIGH IMPACT	_____	___ Months
_____	Personnel Training	QUICK WIN	_____	___ Weeks
_____	Tooling / Automation	STRATEGIC	_____	___ Months

Implementation Standard: Prioritize "Quick Wins" (implementable within 2–4 weeks) to establish momentum before embarking on complex multi-month capability procurements.

1. TIMELINE ANALYSIS & BOTTLENECK DIAGNOSTIC

TIMELINE VELOCITY

Audit the progression velocity through each response phase. Were decision-making intervals realistic? Did information flow rapidly?

Response Phase	Target Duration	Actual Duration	Variance (+/-)	Observed Bottleneck or Acceleration Driver
Detection to Alert	≤ ____ min	____ min	____ min	_____
Alert to Activation	≤ ____ min	____ min	____ min	_____
Assessment to Decision	≤ ____ min	____ min	____ min	_____
Decision to Action	≤ ____ min	____ min	____ min	_____
Containment to Recovery	≤ ____ hrs	____ hrs	____ hrs	_____
Recovery to Normal	≤ ____ hrs	____ hrs	____ hrs	_____

2. RESOURCE UTILIZATION & BUDGET IMPACT AUDIT

RESOURCE EFFICIENCY

Assess deployment efficiency. Were resources deployed effectively? Were critical activities under-resourced or over-allocated?

Resource Category	Deployment Effectiveness & Availability	Shortage / Surplus / Bottleneck	Optimization Prompt for Next Time
Personnel & Staffing Crisis team, technical SME responders	_____	_____	Could fewer personnel have resolved this with better tooling?
Facilities & Infrastructure EOC, backup workspaces, DR sites	_____	_____	Did physical/virtual workspace facilitate cross-team coordination?
Technology & Tooling Dashboards, alert systems, satellite links	_____	_____	Were critical tools accessible under degraded conditions?
External Partners & Vendors Contractors, forensic teams, legal counsel	_____	_____	Did vendor SLAs meet actual response requirements?

Financial & Budget Prompt Audit:

Pre-Approved Crisis Budget: $_____ **Actual Emergency Spend:** $_____ **Budget Variance:** $_____ ([ ] Under [ ] Over)

Primary Cost Drivers: [ ] Overtime Labor [ ] Emergency Contractor Callouts [ ] Hardware Expedited Freight [ ] Regulatory/Legal Fees

CONTINUITY HUB • POST-CRISIS REVIEW PRINT PACK

Section 4: AAR Planning Checklist & Structured 4–8 Hour Agenda Guide

Current version — Oct 31, 2026. Update history: https://continuityhub.org/post-crisis-review-after-action-reports-lessons-learned/
Grounding: ContinuityHub Post 23 • AAR Planning, Neutral Leadership & Session Management

1. AAR PLANNING & PREPARATION CHECKLIST

OPERATIONAL READINESS

Verify all governance, personnel, and documentation requirements prior to convening the formal AAR session:

Status	Planning Requirement	Mandatory Implementation Criteria	Verification / Lead
[ ]	**Neutral Review Leader**	Designate an AAR leader without direct operational responsibility for contested crisis decisions, enabling completely objective analysis.	Lead: _____
[ ]	**Participant Diversity**	Assemble full crisis team, department heads whose operations were disrupted, key field responders, external partners, and technical SMEs.	Register Confirmed: [ ]
[ ]	**Pre-Session Document Pack**	Gather incident logs, decision records, communications, financial receipts, and action plans in advance to prevent time-wasting searches.	Dossier Distributed: [ ]
[ ]	**Dedicated Time Allocation**	Schedule 4–8 hours for major incidents in an uninterrupted setting to enable deep root-cause exploration rather than superficial review.	Calendar Locked: [ ]
[ ]	**Psychological Safety Rules**	Establish ground rules prioritizing organizational learning over punishment, maintaining strict confidentiality of sensitive internal debriefs.	Rules Read at Opening: [ ]

2. STANDARD 4–8 HOUR AAR FACILITATION AGENDA TEMPLATE

SESSION ARCHITECTURE

Time / Block	Agenda Module	Facilitation Objective & Discussion Deliverables	Session Lead
Module 1 (0:00 – 0:30)	**Opening & Ground Rules**	State purpose (learning, not blame), establish confidentiality, confirm agenda, review incident scope and objective benchmarks.	AAR Leader
Module 2 (0:30 – 1:30)	**Q1: What Was Supposed to Happen?**	Examine pre-crisis plans, expected timelines, procedures, and assumptions. Establish consensus on what the organization intended to do.	Planning Lead / BCM
Module 3 (1:30 – 3:00)	**Q2: What Actually Happened?**	Reconstruct timeline chronologically using records and participant testimony. Identify specific divergence points between plan and reality.	Operations Lead / Responders
Break (3:00 – 3:30)	**Executive Recess**	Informal team break; session scribe compiles initial divergence list and maps timeline clusters on board.	All
Module 4 (3:30 – 5:00)	**Q3: Why Did It Happen That Way?**	Execute 5-Whys root cause discovery on major failures. Distinguish process gaps, training needs, and capability shortfalls.	AAR Leader / SMEs
Module 5 (5:00 – 6:30)	**Q4: What Should We Do Differently?**	Formulate specific, measurable countermeasures. Link every action to an identified root cause; prioritize by impact/feasibility.	Department Heads
Module 6 (6:30 – 7:30)	**Action Commitments & Ownership**	Assign named owners, required resources, and realistic completion deadlines for all quick wins and strategic initiatives.	AAR Leader / Sponsors

CONTINUITY HUB • POST-CRISIS REVIEW PRINT PACK

Section 5: Formal AAR Report Structure & Lessons Learned Extractor

Current version — Oct 31, 2026. Update history: https://continuityhub.org/post-crisis-review-after-action-reports-lessons-learned/
Grounding: ContinuityHub Post 23 • Observation > Lesson Learned > Application Methodology

1. FORMAL AFTER-ACTION REPORT (AAR) STANDARD OUTLINE

DELIVERABLE STANDARD

• **1. Executive Summary:** High-level incident summary, core successes, primary systemic gaps, top 5 prioritized improvement actions.
• **2. Incident Overview:** Chronology, severity classification, affected business units, geographic scope, operational/financial impact.
• **3. Response Effectiveness:** Evaluation against planned RTOs/RPOs, BCP compliance, crisis management team performance.
• **4. Root Cause Analysis:** Detailed findings across process gaps, personnel training needs, and technical capability shortfalls.
• **5. Prioritized Recommendations:** Actionable countermeasures with assigned department owners, required budget, and target dates.
• **6. Validated Lessons Learned:** Enduring principles generalizable to future crises.

2. LESSONS LEARNED EXTRACTOR WORKSHEET (ARTICLE REFERENCE MODELS + BLANK ROWS)

ORGANIZATIONAL MEMORY

Convert factual observations into enduring organizational principles using the **Observation → Lesson Learned → Application** method:

Specific Incident Observation	Generalizable Lesson Learned	Actionable Organizational Application
Manual call tree reached only 60% of team members within required timeframe	**Automated notification systems are essential for crisis team activation**	Implement automated notification system reaching all team members within 10 minutes
Lack of real-time visibility into incident status slowed decision-making	**Situation awareness dashboards improve crisis decision-making speed**	Develop real-time dashboard displaying key incident metrics and response status
Customer communication delay created stakeholder confusion	**Pre-established communication templates enable rapid crisis communication**	Develop communication templates and message frameworks for common crisis scenarios
Incident command succession unclear after primary IC became unavailable	**Pre-established succession planning ensures continuity of decision authority**	Document incident commander succession and validate alternates understand authority
[Incident Observation 1]: _____	[Generalizable Principle]: _____	[Specific Application]: _____
[Incident Observation 2]: _____	[Generalizable Principle]: _____	[Specific Application]: _____

AAR Documentation Sign-Off: _____ **Executive Review Presentation Date:** _____