# RESILIENCE

# OPERATIONS MANUAL

## FIRST EDITION

### VERSION 1.4

**Outcome First.**
**Operational Truth Always.**
**Technology that Empowers Human Judgment.**

**Published by Mavensoft Technologies, LLC**
Fully Integrated Operational Alignment - August 20, 2026

## Document Control

| | |
|---|---|
| **Document** | Resilience Operations Manual |
| **Version** | 1.4 |
| **Status** | CURRENT - FIRST EDITION - VERSION 1.4 |
| **Owner** | Mavensoft Technologies |
| **Publication date** | August 2026 \| Fully integrated operational alignment August 20, 2026 |
| **Review cycle** | After each deployment, exercise, major incident, or material process change |

Copyright © 2026 Mavensoft Technologies. All Rights Reserved.

# Copyright, Confidentiality, and Use

Copyright © 2026 Mavensoft Technologies. All Rights Reserved. This manual contains confidential and proprietary operational methods, workflows, terminology, and service standards. It may be used only by Mavensoft personnel, authorized contractors, clients, and advisors under applicable agreements. No portion may be reproduced, distributed, adapted, or incorporated into another work without prior written authorization, except as permitted by law or agreement.

This manual establishes an operational baseline. Client command authority, statutory responsibilities, approved emergency plans, applicable professional standards, and mandatory public-sector requirements remain controlling.

## Revision History

| Version | Date | Status | Summary |
|---|---|---|---|
| 1.4 | August 20, 2026 | CURRENT | Fully integrated Gatekeeper information/access doctrine; shared and restricted handling; AI/human review; High Alert posture; Dynamic Incident Access; connector/source mapping; cybersecurity; Phase 0 readiness; reporting and lifecycle alignment. |
| 1.3 | August 15, 2026 | Superseded by 1.4 | Data-source and change-awareness refinement: source/timestamp/freshness/health awareness, material-change handling, OTHER capture path, and action/ownership/verification linkage. |
| 1.2 | August 13, 2026 | Superseded | Utility communications/restoration alignment; degraded-visibility context preservation and reconciliation; client-state mapping; strengthened communications value and existing-system boundaries. |

# Using This Manual

This manual is designed to be read in sequence during implementation and then used as a practical field reference. Readers may use the Table of Contents, glossary, acronyms, representative examples, checklists, and index to locate guidance relevant to their responsibilities.

- Foundations explains the purpose, operating doctrine, and three foundation resources.
- Chapters 1-14 establish the operating baseline, roles, workflows, communications, evidence, handoffs, deliverables, equipment, and failure response.
- Chapters 15-24 carry the operational record from First Awareness through All Clear, The Morning After, and Full Closure, with examples and visual references.
- Chapter 25 explains how the practice is sustained.
- Chapter 26 contains the current operational alignment for Gatekeeper, operating postures, access, connectors, AI-assisted processing, security, and 24/7 support.
- The back matter provides definitions, acronyms, references, revision control, and an index.

# Foundations

## The Purpose of Resilience

Resilience helps first responders and operational teams preserve Operational Truth - the most accurate and current operational understanding available - so they can maintain clarity, make timely and informed decisions under pressure, and navigate with confidence from First Awareness through Full Closure.

## Operational Truth

Operational Truth is the most accurate, current, verified, and responsibly maintained operational understanding available at a given moment. It distinguishes what is known, what is unknown, what has changed, what evidence supports the record, and what remains to be verified. Operational Truth evolves as the operational understanding is refined through additional verified information while preserving the integrity of the operational record.

## The Three Foundation Documents of Resilience

Together, the Landing Pages, Operations Manual, and Terms and Conditions explain why Resilience exists, how it operates, and the framework under which it is implemented and used.

- Resilience Landing Pages - purpose, capabilities, implementation approach, and practical value.
- Resilience Operations Manual - preparation, practice, implementation, activation, use, continuity, recovery, and closure.
- Resilience Terms and Conditions - responsibilities, services, commitments, implementation, electronic acceptance, security/data, and commercial terms.

## Core Principles

**Outcome First.** Every capability and action should improve the operational outcome.

**Operational Truth Always.** Maintain the most accurate, current, verified, and responsibly maintained operational understanding available.

**Technology that Empowers Human Judgment.** Technology organizes, preserves, connects, and assists. Authorized people decide.

## Operational Lifecycle

First Awareness → Preparation and Readiness → Watch → High Alert → Red Alert → lower posture as conditions stabilize → All Clear → Recovery Mode → The Morning After → Full Closure

# Table of Contents

Foundations

1. Purpose and Scope

2. Operational Doctrine

3. Service Model and Boundaries

4. Operating Postures

5. Roles and Responsibilities

6. Liaison Qualifications

7. Mission Control Workflow

8. Required Questions

9. Communications and Connectivity

10. Information Verification and Evidence

11. Shift Handoff

12. Deliverables

13. Equipment and Technology Requirements

14. Escalation and Failure Modes

15. Operational Information Now

16. The Morning After

17. First Awareness through Full Closure

18. Quality Standards and Performance Measures

19. Training, Readiness, and Operational Exercises

20. Operational Communications and Information Exchange

21. Operational Equipment and Field Technology

22. Operational Energy, Continuity, and Redundancy

23. Operational Roles and Responsibilities

24. Operational Templates, Examples, and Visual Reference Guide

25. Putting Resilience into Practice

26. Current Operational Alignment

Appendix A - Glossary

Appendix B - Acronyms

Appendix C - Operational References

Revision History

Index

# 1. Purpose and Scope

The Resilience Operations Manual defines what Mavensoft personnel, Client liaisons, authorized support staff, and authorized incident participants are expected to do during normal operations, Watch, High Alert, Red Alert, Recovery Mode, and related readiness or post-operational work. It establishes a consistent way to preserve Operational Truth while supporting - but never replacing - authorized human judgment and Client command authority.

## 1.1 Purpose

- Create a dependable operating standard for Mavensoft Resilience services.
- Define expectations, qualifications, deliverables, communications practices, access controls, information handling, and equipment.
- Ensure that important information does not disappear between people, systems, departments, organizations, or shifts.
- Support faster coordination without creating a competing chain of command.
- Provide a foundation for training, pressure testing, quality assurance, and future certification.

## 1.2 Scope

This manual applies to Resilience Mission Control activities, remote or onsite liaison support, operational logging, communications coordination, information verification, Gatekeeper access and handling rules, shift handoff, executive reporting, Watch, High Alert, Red Alert, Recovery Mode, Dynamic Incident Access, connector/source mapping, and after-action support.

## 1.3 Out of Scope

- Mavensoft personnel do not assume Incident Commander authority unless separately contracted, qualified, and formally designated by the Client.
- Mavensoft does not replace 911, emergency dispatch, utility control rooms, WebEOC, SCADA, CAD, radio systems, or other systems of record.
- Mavensoft does not independently authorize tactical field action, evacuation, re-energization, medical care, public messaging, or regulatory closure.
- Mavensoft does not label public information "Trusted & Verified"; public release authority remains with the Client.

## Operating Intent

Resilience is the continuity layer around existing people and systems. It maintains an accurate operational picture, connects the right authorized parties, records what changed, protects restricted information appropriately, and keeps unresolved work visible.

# 2. Operational Doctrine

Outcome First.

Every action should support the operational outcome, not merely complete a task or populate a field.

Operational Truth Always.

The working picture must distinguish what is known, unknown, assumed, disputed, outdated, or awaiting verification.

Technology that Empowers Human Judgment.

Technology accelerates observation, connection, and recordkeeping. Authorized people remain responsible for decisions.

Drift Happens. Observe. Verify. Reset.

Operational awareness can deteriorate during quiet periods, staging, shift changes, and apparent resolution - not only during peak crisis.

Conditional Green Requires Presence.

When operations proceed under conditions, monitoring increases. Named safeguards, owners, evidence checks, and escalation triggers remain active until ordinary Green is justified.

## 2.1 Operational Truth Categories

- Known / Confirmed - supported by an authorized source or reliable evidence.
- Unknown / Needs Assessment - material information that has not yet been established.
- Watch Point - a signal, condition, dependency, or risk that requires active observation.
- Conflicting - credible sources do not agree.
- Outdated - previously accurate information that may no longer represent current reality.
- Claimed Complete - completion has been reported but not yet verified.

# 3. Service Model and Boundaries

Mavensoft Resilience operates as a Mission Control and continuity support function. It gathers, organizes, verifies where possible, connects, records, escalates, and hands off operational information. It is not a sensor manufacturer, dispatch agency, incident command replacement, or substitute for client expertise.

Resilience is designed to operate across and around existing operational systems rather than duplicate them. Depending on the Client environment, those systems may include SCADA, ADMS/DMS/OMS, AMI, grid-edge sensors, historians, digital twins, enterprise messaging, radio, dispatch, and other systems of record. Resilience preserves the human operational context around those sources: what changed, what is confirmed, what remains uncertain, what decision was made and why, who owns the next action, what must be watched, and what must carry forward.

## 3.1 Core Service Promise

### Core Promise

Maintain operational truth closer to real time, keep it accessible to authorized parties, preserve backup access, and prevent critical actions or unknowns from disappearing across shifts and systems.

## 3.2 Expected Client Experience

- A named Mavensoft liaison or support team.
- A clearly defined intake and escalation path.
- A current operational picture that shows what changed, what remains open, and who owns next action.
- Reliable communications bridging and backup methods.
- Consistent reports and handoffs.
- Visible distinctions between facts, assumptions, unknowns, and pending verification.

# 4. Operating Postures

**Normal**
Purpose: Preparedness and ordinary continuity
Typical cadence: Client-defined
Activation: Routine operations
Exit condition: No elevated condition

**Watch**
Purpose: Heightened observation and coordination
Typical cadence: Approximately every 8 hours / 3 times daily unless adjusted
Activation: Emerging risk, uncertainty, or increased attention
Exit condition: Risk stabilizes, escalates, or posture changes

**High Alert**
Purpose: Enhanced or continuous continuity oversight before or during materially elevated conditions
Typical cadence: Accelerated, condition-driven update cycles
Activation: Materially increased uncertainty, operational dependency, or need for sustained Mission Control coordination
Exit condition: Conditions stabilize, escalate to Red Alert, or authorized leadership changes posture

**Red Alert**
Purpose: Active elevated incident support
Typical cadence: Ordinarily 2-4 hour operational refresh cycle, with 24x7 Mission Control where specifically authorized and resourced
Activation: Material incident or Client activation
Exit condition: Immediate threat contained; urgent actions assigned; unknowns and residual risks documented; authorized approval to lower posture or declare All Clear

**Recovery Mode**
Purpose: Recovery, carryover, follow-up, and verification
Typical cadence: Risk-based review cadence
Activation: All Clear / containment with unresolved recovery work
Exit condition: All closure conditions satisfied and authorized Full Closure

## 4.1 Posture Reduction Rule

A higher posture does not become Normal merely because the visible event has ended. Reduction requires appropriate containment or stabilization, assignment of urgent actions, visibility of unknowns and residual risks, named owners, next actions, handoff readiness, and authorized human approval. The operation may move through a lower posture before All Clear when conditions warrant.

# 5. Roles and Responsibilities

Client Incident Commander / Authorized Lead

Primary responsibility: Owns command decisions and incident objectives

Authority: Directs client operations

Must not do: Must not delegate statutory or command authority implicitly

Client Administrative Contact

Primary responsibility: Contract, access, invoicing, approvals, and executive coordination

Authority: Approves administrative actions within authority

Must not do: Must not be assumed to hold operational command unless designated

Client Operational Liaison

Primary responsibility: Primary bridge between client operations and Mavensoft

Authority: Provides authorized updates and validates access

Must not do: Must not filter out material unknowns or disagreements

Mavensoft Resilience Liaison

Primary responsibility: Maintains operational picture, coordinates communications, logs changes, supports handoffs

Authority: May request clarification, connect parties, and escalate per protocol

Must not do: Does not make tactical decisions or overstate verification

Mavensoft Mission Control Lead

Primary responsibility: Supervises quality, staffing, posture, and escalation

Authority: Assigns Mavensoft resources and quality controls

Must not do: Does not override client command

Subject-Matter Expert

Primary responsibility: Provides specialized analysis when requested

Authority: Advises within expertise

Must not do: Does not assume command unless separately designated

## 5.1 Liaison Duty Standard

The liaison must remain calm, neutral, precise, reachable, and disciplined. The liaison protects the integrity of the operational record and connects authorized parties without becoming the source of unapproved tactical direction.

# 6. Liaison Qualifications

## 6.1 Minimum Qualifications

- Clear spoken and written communication.
- Ability to listen, summarize, and confirm without distortion.
- Calm performance under pressure and competing demands.
- Experience with emergency operations, public safety, utilities, healthcare, infrastructure, military, dispatch, call-center escalation, or comparable operational environments.
- Ability to use conference calling, video platforms, shared dashboards, secure messaging, and incident logs.
- Professional judgment about when to ask, when to connect, and when to escalate.
- Willingness to state "unknown" rather than guess.
- Confidentiality, neutrality, and respect for chain of command.

## 6.2 Preferred Backgrounds

- Retired or part-time firefighters, emergency managers, dispatchers, utility operators, public works supervisors, military operations personnel, healthcare incident coordinators, or experienced service-desk escalation personnel.
- Incident Command System familiarity.
- Experience with shift handoff, situation reporting, field verification, or regulated documentation.

## 6.3 Disqualifying Behaviors

- Inventing answers, minimizing unknowns, or treating a green dashboard as proof that reality is green.
- Bypassing client command structure.
- Creating alarm without evidence or proportionality.
- Failing to document material communications or ownership.
- Using recordings or sensitive information outside authorized policy.

# 7. Mission Control Workflow

*Operational note: The workflow below is executed and recorded in the Resilience system and continuous operational record. This Manual is instructional; the white space is not intended as a paper incident workbook.*

**1. Receive the signal, request, report, alert, or activation.**

**2. Identify source, time, location, affected operation, and urgency.**

**3. Classify information as confirmed, unknown, watch point, conflicting, outdated, or claimed complete.**

**4. Confirm the authorized client lead and communication pathway.**

**5. Connect required parties by telephone, conference bridge, video, radio interface, or secure messaging as available.**

**6. Record what changed, the current reality, open items, ownership, next action, and review time.**

**7. Escalate when defined triggers are met or acknowledgement is absent.**

**8. Maintain the operational picture through the active cycle.**

**9. Prepare handoff and recovery carryover.**

**10. Preserve the record for after-action review and authorized reporting.**

## 7.1 First Alert Intake

- Who is reporting?
- What happened?
- Where?
- When?
- What is the immediate consequence?
- What is confirmed?
- What is still unknown?
- Who has authority?
- Who must be connected now?
- What is the next review time?

## 7.2 Mission Control Display - Minimum Fields

- Incident or operational issue name and ID.
- Posture and activation time.
- Current reality statement.
- What changed since last cycle.
- Known / Confirmed.
- Unknown / Needs Assessment.
- Watch Points.
- Open items and owners.
- Next actions and due times.
- Escalations.
- Communication status.

- Handoff readiness.
- Recovery or closure state.

# 8. Required Questions

## 8.1 Questions the Liaison Should Be Able to Answer

- What is happening now?
- What changed?
- What has been confirmed and by whom?
- What remains unknown?
- What is the operational impact?
- Who owns each open item?
- What happens next?
- By when?
- Who needs to know?
- Who has acknowledged?
- What could cause escalation?
- What is the backup communication method?
- What must carry to the next shift?
- What evidence supports recovery or closure?

## 8.2 Questions the Liaison Must Not Answer Without Authority

- Whether the public is safe.
- Whether evacuation is required.
- Whether equipment may be energized or returned to service.
- Whether a site is legally or technically closed.
- Whether an incident is over.
- Whether public information may be released.
- Whether a regulatory requirement has been satisfied.

# 9. Communications and Connectivity

The communications function should operate like a disciplined modern switchboard: receive, identify, connect, conference, record metadata, confirm acknowledgement, and preserve backup pathways. The liaison is not a 911 dispatcher unless separately qualified and authorized, but should adopt the same seriousness about accuracy, connection, and logging.

Resilience does not replace the Client's existing radios, telephones, email, messaging systems, conference platforms, dispatch systems, incident-management systems, operational data feeds, or utility control systems. Its value is the continuity layer across those methods: material information should reach the right authorized people, remain connected to the Current Reality, ownership, next action, acknowledgement, and escalation path, and survive changes in personnel, shifts, systems, and connectivity.

A successful operational communication is not merely sent. Where the information is material, Resilience should help make it received, understood, acknowledged, connected to action, and preserved in the continuous operational record.

## 9.1 Required Capabilities

- Incoming and outgoing voice calls.
- Three-way calling and multi-party conference bridging.
- Video conferencing and screen sharing.
- SMS or secure messaging.
- Email distribution and acknowledgement tracking.
- Call and event metadata logging.
- Primary, secondary, tertiary, and last-resort contact methods.
- Ability to reconnect dropped participants and create a backup bridge.
- Authorized recording when lawful, disclosed, and approved.

## 9.2 Communications Hierarchy

- Primary - client-designated operational channel.
- Secondary - alternate enterprise voice/data channel.
- Tertiary - backup cellular, satellite, radio, or alternate bridge.
- Last resort - preplanned contact tree, runner, mutual-aid path, or other approved method.

## 9.3 Multi-Party Connection Procedure

1. **Confirm the purpose and authorized participants.**
2. **Establish the primary bridge.**
3. **State who is present and who is missing.**
4. **Confirm the decision owner.**
5. **Summarize the issue and current known facts.**
6. **Record decisions, actions, owners, and times.**
7. **Repeat back material decisions for confirmation.**
8. **Provide the next check-in time and backup bridge information.**
9. **Document disconnections, failed contacts, and unanswered acknowledgements.**

## 9.4 Degraded Communications and Reconciliation

Loss or degradation of a communications path is first a loss of visibility; it does not necessarily mean local operations or field devices have stopped. During the gap, Resilience preserves the operational context available to authorized people, including what was known, what remained unknown, local observations and actions, decisions, ownership, safeguards, and items requiring later reconciliation.

When connectivity returns, the restored technical record and the human operational record should be reconciled. Material differences, delayed telemetry, locally retained information, actions taken during the gap, unanswered acknowledgements, and remaining limitations should be reviewed before the restored path is treated as a complete operational picture.

## Recording Rule

Recordings must never be assumed. Use only where lawful, contractually authorized, disclosed to participants, securely stored, access-controlled, and subject to retention policy. When recording is unavailable or inappropriate, maintain a timestamped operational log.

# 10. Information Verification and Evidence

## 10.1 Verification Standard

The liaison should identify the source and confidence of material information. Verification may come from an authorized human, system evidence, photo/video, instrument reading, field inspection, independent confirmation, or documented supervisory approval. The liaison records verification; the liaison does not manufacture it.

## 10.2 Sensor or Automated Alert Intake

- Alert source and timestamp.
- Asset or location.
- Signal type and confidence.
- Suspected hazard or condition.
- Human reviewer.
- Dispatch or inspection decision.
- Drone or remote inspection authorization, if applicable.
- Evidence obtained.
- Residual risk.
- Clear-to-Leave or recovery authorization, if applicable.

## 10.3 Evidence Labels

- Observed.
- Reported.
- System-generated.
- Photographic/video.
- Instrument or telemetry.
- Supervisor-confirmed.
- Independent verification.
- Pending evidence.
- Conflicting evidence.

# 11. Shift Handoff

Every handoff must preserve continuity, not merely transfer a list. The outgoing liaison remains responsible until the incoming liaison acknowledges readiness or a supervisor accepts the handoff exception.

## 11.1 Eight-Part Shift Packet

### 1. What Changed.

### 2. Current Reality.

### 3. Open Items.

### 4. Next Actions.

### 5. Drift / Risk.

### 6. Escalations.

### 7. Handoff Ready.

### 8. Close / Carry.

## 11.2 Handoff Quality Test

- Can the incoming liaison explain the current reality without relying on the outgoing liaison?
- Are owners and due times visible?
- Are unknowns and watch points explicit?
- Are communication failures and backup paths documented?
- Are decisions separated from assumptions?
- Is the next review time clear?

# 12. Deliverables

Mission Control Operational Picture

Purpose: Shared current reality

Minimum content: Posture, changes, knowns, unknowns, owners, next actions

Typical timing: Continuous / each operational cycle

Situation Report

Purpose: Structured incident summary

Minimum content: Impact, actions, risks, decisions, needs

Typical timing: Client-defined cadence

Executive Brief

Purpose: Decision-oriented summary

Minimum content: What matters, what changed, decisions needed, exposure

Typical timing: As agreed / major change

Shift Packet

Purpose: Continuity across personnel changes

Minimum content: Eight-part packet

Typical timing: Every handoff

Decision Log

Purpose: Preserve accountability and rationale

Minimum content: Decision, owner, time, basis, follow-up

Typical timing: Continuous

Communication Log

Purpose: Record connection and acknowledgement

Minimum content: Call/bridge/message metadata and outcome

Typical timing: Continuous

Recovery Carryover

Purpose: Prevent premature closure

Minimum content: Residual risks, pending evidence, owners, reviews

Typical timing: At entry to Recovery Watch

After-Action Package

Purpose: Learning and improvement

Minimum content: Timeline, findings, lessons, actions

Typical timing: Post-incident

# 13. Equipment and Technology Requirements

## 13.1 Minimum Liaison Workstation

- Reliable computer with current security updates and encrypted storage.
- Two displays preferred; one display minimum with tested window-management procedure.
- Business-grade headset with noise control and backup headset.
- Primary telephone and backup telephone or softphone path.
- Reliable broadband connection and independent backup connectivity where feasible.
- UPS battery backup for workstation, network equipment, and primary communications.
- Approved video-conferencing and conference-bridge capability.
- Secure access to Resilience, client systems, contact lists, and document repository.
- Clock synchronized to an authoritative time source.
- Privacy-appropriate workspace.

## 13.2 Mission Control Equipment - Enhanced

- Multi-line or cloud communications console.
- Conference bridge with host controls.
- Call queue and transfer capability.
- Large operational display or shared virtual display.
- Redundant internet providers or cellular failover.
- Portable power and extended-runtime UPS.
- Secure recording and retention system when authorized.
- Printer/scanner only where operationally necessary.
- Satellite, radio gateway, or client-provided interoperability tools when required.

## 13.3 Equipment Readiness Categories

- Necessary - required to activate safely and reliably.
- Recommended - materially improves performance or redundancy.
- Wish List - beneficial but not required for initial operation.

# 14. Escalation and Failure Modes

Status: Approved Working Baseline - July 28, 2026

## 14.1 Purpose

This chapter defines how Mavensoft recognizes, stabilizes, documents, and corrects failures within the Resilience continuity-support function. The objective is to preserve an accurate operational picture, maintain ownership and handoff continuity, and support informed client judgment when communications, information, people, processes, or technology do not perform as expected.

Client operational authority remains unchanged. Mavensoft supports the client through established pathways and does not independently activate Watch, activate Red Alert, declare All Clear, or otherwise change the client's operational posture.

## 14.2 Governing Principles

- Outcome First.
- Operational Truth Always.
- Technology that Empowers Human Judgment.
- Preserve the distinction between observed fact, reported information, inference, and verified attribution.
- Make uncertainty visible rather than smoothing it over.
- Act decisively within the assigned continuity-support role and follow the client's established authority and escalation path.
- Match verification effort to the potential operational consequence of being wrong.

## 14.3 Common Continuity-Support Failure Modes

- Primary, secondary, or tertiary communications fail or are not acknowledged.
- Information becomes stale, conflicting, incomplete, or trapped with one person or system.
- An action has no confirmed owner, deadline, or acknowledgement.
- A shift handoff occurs without acceptance or without a usable current-reality summary.
- Reported completion is treated as verified closure without the required evidence or confirmation.
- A quiet period is mistaken for stability while unresolved work or residual risk remains.
- Technology displays a favorable status that does not agree with human observation or evidence.
- Documentation, timestamping, recording, synchronization, staffing, or liaison availability fails.
- An unresolved item disappears from the active operational picture.
- A statement, confession, or claim of responsibility is accepted as verified attribution without corroboration.

## 14.4 Detection and Initial Assessment

A possible failure is treated first as a condition to be assessed, not as a conclusion. The liaison or support team shall identify what changed, when it changed, who observed or reported it, which operations may be affected, and what remains unknown.

1. Record the source and timestamp.
2. Classify the information as Confirmed, Reported, Inferred, Conflicting, Unknown, or Outdated, as applicable.
3. Identify the immediate operational consequence if the information is wrong or delayed.

4. Determine whether a temporary safeguard, alternate channel, or increased review cadence is needed.
5. Notify the appropriate client contact through the established pathway when the condition may affect client action or awareness.

## 14.5 Proportionate Verification and Attribution

A claim of responsibility, completion, causation, or status is evidence, but it is not automatically proof. Verification shall test the claim against available independent facts and the consequence of error.

Verification may include timestamps, physical location, travel feasibility, access records, sensor or system records, photographs, video, communications, witness accounts, physical evidence, and collaboration among people holding different parts of the operational picture.

The depth and urgency of verification shall be proportionate to the seriousness, reversibility, and potential consequence of the decision. Trivial uncertainty should not consume resources needed for consequential work. High-consequence uncertainty requires disciplined preservation of evidence, corroboration, expert involvement when appropriate, and a clear record of what is known and unknown.

Operational standard: Do not assume. Verify. Do not over-investigate trivial uncertainty. Match the depth of verification to the potential consequence of being wrong.

## 14.6 Immediate Stabilization

6. State the current known facts and material unknowns.
7. Prevent unverified information from being presented as confirmed.
8. Restore or establish a usable communication path.
9. Keep unresolved items visible.
10. Confirm the authorized client lead, decision owner, action owner, next action, and review time.
11. Apply a temporary safeguard or manual continuity method when appropriate.
12. Record all material changes made during stabilization.

## 14.7 Response to Communications or Technology Failure

Treat degraded communications as a change in visibility and confidence, not automatically as a change in the underlying field condition. Preserve the best available operational context while alternate paths, local/manual methods, and source systems continue according to Client procedures.

13. Declare and timestamp the failed or degraded channel or service.
14. Move to the preplanned secondary, tertiary, or last-resort method as necessary.
15. Notify affected participants through an independent path when available.
16. Re-establish the bridge and verify critical participants.
17. Restate the current operational picture before resuming normal discussion.
18. Reconcile decisions, instructions, acknowledgements, and updates made during the gap.
19. Record duration, impact, workaround, restoration, and any remaining limitation.
20. Test the restored capability before treating it as reliable.

## 14.8 Response to Information Conflict

21. Preserve each material version with its source and timestamp.
22. Classify the issue as Conflicting rather than selecting the most convenient account.
23. Identify the operational consequence of the disagreement.

24. Seek the most authoritative available source or corroborating evidence.
25. Notify the authorized client contact when the conflict could affect action or posture.
26. Record interim safeguards and decisions.
27. Update the current operational picture when the conflict is resolved while preserving the historical record.

## 14.9 Response to Ownership, Acknowledgement, or Handoff Failure

28. Mark the item as Unassigned, Ownership Unconfirmed, Acknowledgement Missing, or Handoff Not Accepted, as applicable.
29. State the required action, deadline, and operational consequence.
30. Request explicit assignment, acknowledgement, or acceptance through the established pathway.
31. Keep the item active and visible until responsibility is confirmed or the client directs otherwise.
32. Confirm transfer whenever ownership changes.
33. Conduct a corrected handoff when the original handoff was incomplete or not accepted.

## 14.10 Response to Evidence or Closure Conflict

Reported Complete is a claim of completion, not final closure. When evidence, inspection, observation, approval, dependency, or residual risk conflicts with a reported status, the discrepancy shall remain visible.

34. Record the claimed status and the conflicting evidence or missing requirement.
35. Identify what remains, why it remains, the owner, due date, required evidence, dependency, escalation trigger, and next review date.
36. Use Partial Closure - Pending when the primary work may be complete but one or more closure conditions remain.
37. Reopen an item when new evidence or changed conditions invalidate the prior closure basis.
38. Do not represent Full Closure until the required verification and authorization are complete.

## 14.11 Internal Mavensoft Escalation and Corrective Action

When the failure originates within the Mavensoft support function, the Operational Liaison shall escalate internally according to impact and urgency. Internal escalation may include the Program Manager, technical support, staffing leadership, security or compliance resources, and the Mavensoft executive sponsor.

Internal escalation does not replace client notification or client authority. Corrective action shall identify the failure, containment, owner, expected restoration time, client impact, workaround, verification method, and follow-up review.

## 14.12 Documentation, Review, and Faithfulness to Operational Truth

Every material continuity-support failure shall record what happened, when it happened, how it was detected, the operational impact, what was known and unknown, actions taken, owners, acknowledgements, restoration or closure basis, and lessons requiring follow-up.

Resilience personnel shall remain faithful to operational truth as it is currently known. They shall distinguish confirmed facts from reports, assumptions, interpretations, and unresolved uncertainty. When information conflicts or remains incomplete, the discrepancy shall be made visible rather than smoothed over. Errors shall be corrected promptly, and changes in understanding shall be documented

clearly. The purpose is not to create the appearance of certainty, but to preserve an accurate and usable operational picture for human judgment.

Chapter close: Not perfectly, but faithfully. Operational Truth Always.

# Chapter 15

## Operational Information Now

### 15.1 Purpose

Operational Information Now collects, verifies, organizes, preserves, and distributes need-to-know operational information that supports authorized field and executive decision-makers while an event is actively unfolding. Chapter 15 continues until All Clear.

### 15.2 Current Operational Picture

- What happened and what changed.
- What is happening now.
- What is confirmed, reported, conflicting, or unknown.
- Current posture and activation time.
- Open items, owners, acknowledgements, next actions, and review times.
- Watch Points, residual risk, dependencies, and pending decisions.
- Communication, equipment, and system-health status.

A change in information may require a change in action. When a material source update changes the operational picture, Resilience should preserve what changed, the source and timestamp, who needs to know, whether ownership changed, what action is now required, acknowledgement where applicable, and the resulting verified condition.

### 15.3 Information Sources

Authorized sources may include people, field observations, weather and lightning services, GIS, SCADA, sensors, cameras, drones, radio, dispatch, email, secure messaging, voice, maps, documents, photographs, video, and approved external feeds.

Source configuration should also provide an OTHER pathway for a material condition, source, dependency, action, or consequence that was not anticipated during setup. An important operational fact should not be lost merely because it does not fit a predefined category.

### 15.4 Verification States

| State | Meaning |
|---|---|
| Confirmed | Supported by an authorized source or reliable evidence. |
| Reported | Attributed information not yet independently confirmed. |
| Unknown | Material information that has not been established. |
| Needs Verification | Information requiring additional source or evidence review. |
| Conflicting | Credible sources disagree or available evidence is inconsistent. |
| Updated | Later verified information refines the current operational understanding. |

## 15.5 Quick Access

Operational Information Now should be accessible through Mission Control, desktop, laptop, tablet, mobile, and approved alternate-access methods. Primary access, backup access, and backup-to-the-backup should be identified where practical.

## 15.6 Reporting

- Situation Reports
- Executive Briefs
- Eight-Part Shift Packets
- Decision Logs
- Communication Logs
- Timeline views
- Maps and evidence packages

## 15.7 End State

*Chapter 15 reaches its operational end state when authorized Client personnel declare All Clear and Mavensoft records the transition. The operational record continues into Recovery Mode and The Morning After.*

# Chapter 16

## The Morning After

### 16.1 Purpose

The Morning After transforms the running operational record into a complete and enduring record that supports wind-down, recovery, accountability, organizational learning, and Full Closure.

### 16.2 Beginning the Morning After

The Morning After begins after All Clear. Operational tempo may slow, but discipline does not. All unresolved work, residual risk, pending evidence, notifications, repairs, inspections, testing, and accepted continuing responsibilities remain visible.

### 16.3 Required Review

- Incident recap and executive summary.
- Verified timeline and posture changes.
- Decision and communications review.
- What worked, what drifted, missed signals, and unresolved questions.
- Recovery work, owners, evidence, dependencies, and next review times.
- Offline record reconciliation and correction history.
- Lessons learned and improvement actions.
- Readiness implications for the next event.

### 16.4 Comprehensive Final Report

- Executive Incident Summary
- Comprehensive Operational Report
- Verified timeline
- Decision and communications history
- Recovery and remaining-work reconciliation
- Evidence package
- Lessons Learned and Improvement Recommendations
- Final Operational Record and Archive Package

### 16.5 End State

*Chapter 16 ends at Full Closure - Full Stop. All known operational responsibilities have been completed or formally transferred, required evidence has been verified, records have been completed and preserved, and authorized Client leadership has approved closure.*

# 17. First Awareness through Full Closure

## 17.1 Official Lifecycle Checklist

| Stage | Completion test |
|---|---|
| First Awareness | Something has changed or may require attention. Record source, time, location, significance, and initial unknowns. |
| Initial Assessment | Confirm Current Reality, decision authority, affected operations, communication paths, and next review. |
| Preparation and Readiness | Establish liaisons, access, equipment, communication alternatives, ownership, Gatekeeper handling, and evidence requirements. |
| Watch | Increase monitoring, structured updates, ownership verification, and escalation awareness when authorized by the Client. |
| High Alert | Increase continuity oversight, accelerate update cycles, coordinate Mission Control and designated support resources when authorized. |
| Red Alert | Provide coordinated incident support, frequent refresh cycles, shift continuity, decision continuity, and Mission Control support when authorized. |
| Lower Posture | Reduce operational tempo while maintaining controls appropriate to remaining risk when conditions stabilize but All Clear is not yet appropriate. |
| All Clear | Authorized Client personnel conclude active elevated-posture services; Mavensoft records the transition. |
| Recovery Mode | Carry unresolved work, residual risk, verification, repair, inspection, and follow-up forward. |
| The Morning After | Review the complete operational record, reconcile changes, and prepare the comprehensive report. |
| Full Closure | Complete or formally transfer all responsibilities, verify evidence, preserve the record, and obtain authorized closure approval. |

## 17.2 Closure Principle

Resilience treats closure as a verified state transition, not a single generic label. Client terminology may differ by industry and jurisdiction and should be mapped during implementation rather than replaced.

# Chapter 18

## Quality Standards and Performance Measures

### 18.1 Purpose

Quality is measured by whether authorized users can understand current reality, ownership, risk, next action, and the integrity of the record.

### 18.2 Quality Standards

- Accuracy - information is attributed, classified, and updated as understanding is refined.
- Timeliness - significant changes reach the appropriate people while they can still affect decisions.
- Completeness - open work, ownership, evidence, unknowns, and review times remain visible.
- Continuity - shift changes, communications failures, and equipment changes do not break the operational thread.
- Traceability - material entries retain source, timestamp, status, and change history.
- Clarity - reports separate current reality from background detail and unresolved questions.
- Accountability - every material action has an owner, acknowledgement, next action, and review point.
- Closure quality - completed work is verified, transferred, or formally dispositioned.

### 18.3 Representative Shift Packet Standard

The outgoing Mavensoft Operational Liaison prepares the Shift Packet with the Client Local Operational Liaison and sends it to the incoming Client and Mavensoft liaisons. The handoff is effective when the incoming team acknowledges the packet and can explain current reality, open work, owners, Watch Points, and next actions.

### 18.4 Record Integrity and Changes

Nothing favorable or unfavorable is silently removed. Records may be corrected, updated, restricted, or supplemented while preserving the original entry and the reason for the change.

| Change reason | Use |
|---|---|
| Updated | Later verified information refines the record. |
| Recording error | The original entry did not accurately reflect what was received or intended. |
| Misinformation | Information was later shown to be materially false or unreliable. |
| Other | A documented reason approved under the applicable record procedure. |

Restricted handling may apply to classified information, information under investigation, privileged material, and records available only through authorized legal channels.

## 18.5 Invoice Record Support

Operational service records should preserve authorization, posture, activation time, transition time, applicable minimum service periods, and supporting entries needed for accurate accounting and review.

# Chapter 19

## Training, Readiness, and Operational Exercises

### 19.1 Purpose

Mavensoft provides training on the use of Resilience as an essential deliverable of the engagement.

### 19.2 Phase 0 Readiness

Phase 0 provides rigorous onboarding, configuration preparation, orientation, training, scenario walkthroughs, and pressure testing to prepare the Client for Phase 1.

### 19.3 Exercise Cadence

- Short operational exercises may be conducted for approximately one hour within the normal work cadence.
- Compressed exercises may simulate eight to twelve hours of activity during approximately two to four hours of training.
- Extended pressure tests should be reviewed and conducted as needed. The current recommended guideline is approximately every six months.

### 19.4 Participation

The assigned Mavensoft Operational Liaison should generally participate when practical. Continued participation strengthens familiarity, shared terminology, communications, handoff discipline, and effective use of Resilience over time.

### 19.5 Cooperating Organizations

Mavensoft encourages Clients to invite neighboring agencies, mutual-aid partners, and other organizations with whom they expect to operate during significant incidents when joint participation supports readiness.

### 19.6 Readiness Principle

*Operational readiness is strengthened through periodic practice. Resilience should become familiar before it is needed under pressure.*

# Chapter 20

# Operational Communications and Information Exchange

## 20.1 Purpose

Mavensoft provides Operational Communications and Information Exchange to help authorized personnel collect, verify, organize, preserve, and distribute need-to-know information throughout the operational lifecycle.

## 20.2 What It Is

Operational Communications and Information Exchange is the disciplined movement of operational information between authorized people, systems, and organizations. It transforms many individual observations into one shared operational understanding.

## 20.3 Information Types

- Text and secure messaging
- Voice recordings and radio summaries
- Photographs and multiple-image sequences
- Video and live feeds
- Maps, GIS layers, GPS, and 3D imagery
- Weather, lightning, flood gauges, utility and sensor readings
- Documents, checklists, and evidence
- AI-assisted summaries, comparisons, translation, and draft reports

## 20.4 AI-Assisted Processing

Approved AI tools may organize information, compare photographs over time, identify possible changes, summarize voice or video, translate language, and prepare draft reports. Outputs requiring operational use are reviewed by authorized people.

## 20.5 Communications Paths

Use Client-approved primary, secondary, tertiary, and last-resort paths appropriate to the operating environment. Resilience does not claim ownership of the underlying network or replace existing communications redundancy. It records which path is active, whether the path is degraded, who has acknowledged critical information, and what alternate method is available if the preferred path fails.

| Capability | Primary | Secondary | Tertiary |
|---|---|---|---|
| Internet | Enterprise connection | Cellular hotspot | Satellite or approved mesh |
| Voice | Primary telephone or radio | Alternate carrier or talkgroup | Satellite or field relay |
| Operational record | Resilience | Local synchronized copy | Approved offline continuity form |

## 20.6 Offline Operations

Where supported, authorized users may continue capturing text, photographs, video, voice, timestamps, GPS, assignments, checklists, decisions, local observations, and ownership while connectivity is unavailable. Source systems or field devices may also retain technical information locally according to their own design. Resilience should preserve synchronization status and failed transfers and identify material items that require reconciliation when communications return.

## 20.7 Closing Principle

Systems may preserve technical data during communications loss. Resilience preserves operational context during communications loss. When connectivity returns, both records should be reconciled so that delayed data, human actions, changed assumptions, and unresolved work are brought back into one current operational understanding.

*Operational Information Now is not about collecting the most information. It is about delivering the most useful verified information to the people who need it while it can still influence decisions.*

# Chapter 21

# Operational Equipment and Field Technology

## 21.1 Purpose

Operational equipment and field technology support access, collection, preservation, and communication of Operational Information Now wherever responsibilities take authorized personnel.

## 21.2 Equipment Categories

### Computing

- Desktop workstations
- Laptops and rugged laptops
- Tablets and iPads
- Mobile phones

### Communications

- Radios
- Satellite terminals
- Mobile hotspots
- Secure messaging devices
- Portable mesh equipment

### Information Collection

- Cameras
- Helmet and body cameras
- Drones
- Thermal cameras
- Portable scanners
- 3D imaging tools

### Position and Rescue

- GPS and GIS-enabled devices
- Personal locator beacons
- Avalanche transceivers
- Marine emergency beacons
- Emergency roadside call boxes

### Environmental Monitoring

- Weather stations
- Lightning detection
- Flood and water-level sensors
- Air-quality sensors
- Utility and infrastructure sensors

### Field Support

- Portable printers
- Chargers and spare batteries
- Rugged cases
- Headsets
- Portable lighting
- Protective storage

## 21.3 Equipment Familiarization

Mavensoft provides familiarization with agreed Resilience equipment and workflows included within implementation. Personnel gain confidence through regular use, inspection, charging, access verification, and practice with alternate methods.

## 21.4 Equipment Readiness Checklist

- ☐ Available and operational
- ☐ Charged or fueled
- ☐ Communications verified
- ☐ Credentials and permissions verified
- ☐ Accessories and protective cases available
- ☐ Spare batteries and chargers available
- ☐ Backup and tertiary equipment identified
- ☐ Maintenance and replacement needs recorded

## 21.5 Closing Principle

*Operational equipment extends human capability. Its greatest value is realized when it is reliable, familiar, available, and ready before it is needed.*

# Chapter 22

# Operational Energy, Continuity, and Redundancy

## 22.1 Purpose

This chapter supports continued access to Resilience during routine operations, degraded conditions, and disruptions by making energy, communications, equipment health, and practical alternatives visible.

## 22.2 Primary, Secondary, and Tertiary Capability

Primary is the normal preferred method. Secondary is the alternate used when the primary method is degraded or unavailable. Tertiary is the additional contingency when both primary and secondary methods are unavailable or insufficient.

*One method supports operation. Two methods improve continuity. Three methods provide greater resilience.*

## 22.3 Uninterruptible Power Supplies

A UPS provides immediate temporary power for selected workstations, networking, communications, dispatch consoles, servers, security systems, control-system workstations, and charging stations. Planning should consider load, runtime, battery condition, recharge time, status visibility, maintenance, and transfer to longer-duration power.

## 22.4 Generator Capability

| Type by output | Representative use |
|---|---|
| Small portable output | Lighting, radios, charging, limited field computing, small pumps within rated capacity. |
| Medium portable or mobile output | Incident command posts, communications trailers, temporary facilities, selected pumps, limited building circuits. |
| Large mobile output | Emergency operations centers, public facilities, water or wastewater infrastructure, communications sites, larger pumps. |
| Permanently installed generation | Hospitals, public-safety facilities, treatment plants, pump stations, dispatch centers, critical infrastructure. |

## 22.5 Battery Systems

- Handheld rechargeable batteries
- Phone, tablet, laptop, camera, and drone batteries
- Portable power stations
- UPS battery banks
- Vehicle and auxiliary batteries
- Facility and emergency-lighting battery systems
- Large stationary storage systems where applicable

## 22.6 Operational Health and Feedback

- Connected / Disconnected
- Weak Signal / Signal Lost
- Last Successful Communication
- Battery Percentage and Estimated Runtime
- Fuel Level and Estimated Range
- Generator Load and Runtime
- UPS Status
- Feed and Sensor Health
- Synchronization and Offline Status
- AI Processing Status
- Storage Remaining
- Maintenance Required

### 22.6.1 Data Source and Change Awareness

Connected information sources should identify source, timestamp, freshness, communication or synchronization status, and material changes when technically available. Predefined classifications should include an OTHER pathway so an important condition is not lost simply because it was not anticipated during configuration.

A material change should remain visible until its operational consequence, ownership, required action, acknowledgement where applicable, and required verification are understood. Resilience does not replace the source system; it preserves the operational meaning and continuity created by the change.

*Users should not have to guess whether an important operational capability is functioning.*

## 22.7 Operational Story - The Pump Station

At 6:42 PM, heavy rainfall raises the wet-well level at a municipal pump station. Commercial power fails. The UPS preserves controls, alarms, telemetry, and communications while the standby generator starts.

| Time | Operational status |
|---|---|
| 6:42 PM | Commercial power lost; Pump Station 3 UPS active at 91%; estimated UPS runtime 46 minutes; generator starting; wet-well level rising. |
| 6:44 PM | Generator running at 64% load; fuel 58%; estimated runtime 13 hours; Pump 1 operating; Pump 2 available; water level stabilizing. |
| 7:18 PM | Primary cellular path intermittent; secondary carrier active; tertiary satellite path available. |
| 8:05 PM | Fuel forecast may not cover expected restoration window; Utilities Operations Supervisor owns fuel delivery; flooded road is a Watch Point. |

Continuity succeeds because the current power source, remaining capacity, communication path, ownership, next action, and changing conditions remain visible.

## 22.8 Closing Principle

*Operational continuity is strengthened when energy, communications, equipment, and system health remain visible, familiar, and supported by practical alternatives.*

# Chapter 23

## Operational Roles and Responsibilities

### 23.1 Purpose

Clear responsibilities help information move efficiently, preserve continuity, maintain ownership, and support informed human judgment.

| Role | Primary contribution |
|---|---|
| Client Executive Sponsor | Supports organizational adoption, resources, alignment, and significant executive decisions. |
| Incident Commander or Authorized Operational Lead | Directs incident objectives, priorities, resources, and Client operational decisions. |
| Client Local Operational Liaison | Provides local operational knowledge, geography, terminology, relationships, source access, ownership confirmation, and onsite continuity. |
| Mavensoft Operational Liaison | Maintains Operational Information Now, organizes and attributes information, supports verification, prepares reports and handoffs, and preserves continuity through Full Closure. |
| Mission Control Lead | Coordinates Mavensoft support, staffing, quality review, continuity, escalation support, and additional resources. |
| Technical Support | Supports access, permissions, connectivity, synchronization, software availability, and restoration. |
| Finance and Accounting | Generates and reviews accurate invoices and required accounting records from the authorized operational service record. |
| Domain Specialist | Provides specialized knowledge relevant to emergency management, fire service, utilities, infrastructure, healthcare, communications, engineering, or other agreed domains. |

### 23.2 Operational Story - The Bridge

8:12 AM - A Public Works field supervisor reports earthquake damage to a bridge with photographs, location, time, traffic impact, and initial observations.

The Client Local Operational Liaison recognizes the bridge, local geography, alternate routes, departments, and immediate ownership requirements.

The Mavensoft Operational Liaison records source, timestamp, verification status, open questions, owner, next action, and next review time in Operational Information Now.

Utilities report a gas line beneath the bridge. Police establish traffic control. Emergency Management requests an impact assessment. A structural engineer is assigned.

Mission Control preserves the combined operational picture. Authorized Client decision-makers see current status, unknown structural condition, gas-line concern, traffic impact, owners, and next decision time.

## 23.3 Visual Workflow

Field Supervisor → Client Local Operational Liaison ↔ Mavensoft Operational Liaison → Operational Information Now → Mission Control → Authorized Decision-Makers

## 23.4 Handoff

At shift change, outgoing Client and Mavensoft liaisons brief incoming counterparts. The Eight-Part Shift Packet identifies current reality, changes, open items, owners, unknowns, Watch Points, next actions, and next review. The handoff is complete when the incoming team can explain the operational picture and accepts responsibility.

## 23.5 Closing Principle

*Operational Truth is preserved through clearly understood responsibilities, trusted working relationships, and disciplined handoffs.*

# Chapter 24

## Operational Templates, Examples, and Visual Reference Guide

### 24.1 Purpose

This chapter provides representative templates, completed examples, visual workflows, and quick-reference materials illustrating how Resilience is used from First Awareness through Full Closure.

### 24.2 Representative Scenario - Flood Escalation

| Time | Operational event |
|---|---|
| 6:15 AM | The National Weather Service issues a Flood Watch. Current Client posture remains Normal while local conditions, gauges, soil saturation, pump status, and staffing are reviewed. |
| 7:10 AM | River levels rise and Public Works reports standing water. Authorized Client personnel activate Watch. Client and Mavensoft liaisons are assigned. |
| 9:35 AM | The National Weather Service issues a Flood Warning. A field supervisor submits timestamped photographs, GPS, video, and voice description showing water crossing Mill Road. |
| 9:47 AM | Local flooding expands and Pump Station 3 load rises. Authorized Client personnel activate Red Alert. |
| 10:18 AM | Pump Station 3 primary cellular path becomes intermittent. Secondary communications activate. Pump Station 3 communications UPS battery is 84%, with estimated runtime of 7 hours 40 minutes. |
| 1:45 PM | Outgoing liaisons prepare and acknowledge the Eight-Part Shift Packet. Handoff becomes effective at 2:00 PM. |
| 5:20 PM | Rainfall decreases and water levels stabilize. Authorized Client personnel return the operation from Red Alert to Watch. |
| 8:10 PM | Authorized Client personnel declare All Clear. Watch and Red Alert services conclude. Recovery Mode, The Morning After, and Full Closure continue as part of the engagement. |
| Next morning | The Morning After review reconciles the timeline, open work, ownership, residual risk, equipment and communications issues, and required evidence. |
| Four days later | Roadways reopen, pump performance is verified, records are reconciled, the final report is completed, and authorized Client leadership approves Full Closure. |

### 24.3 Operational Information Now - Representative Layout

#### Current Posture

- Red Alert; activated 9:47 AM; next review 2:30 PM.

#### Current Reality

- NWS Flood Warning active.

- Three roads affected.
- Pump Station 3 operating under elevated load.
- Primary cellular path degraded; secondary path active.
- No evacuation order active.

### Known and Confirmed

- Flood Warning issued.
- Water crossed Mill Road.
- Barricades installed.
- Pump Station 3 operating.

### Unknown or Needs Assessment

- Utility restoration duration.
- Mill Road roadbed condition.
- Western neighborhood access status.

### Watch Points

- Pump load
- River gauge trend
- Additional rainfall
- Fuel and battery runtime
- Roadbed deterioration

## 24.4 Eight-Part Shift Packet - Completed Example

| Packet element | Completed example |
|---|---|
| 1. What Changed | Flood Watch advanced to Flood Warning; Client activated Watch and Red Alert; Mill Road closed; primary pump-station communications degraded; secondary path active. |
| 2. Current Reality | Flooding remains localized; river levels stabilizing; three roads closed; no evacuation active. |
| 3. Open Items | Roadbed inspection; western access verification; generator fuel delivery; public-information update. |
| 4. Next Actions | Confirm inspection results; review river gauge; verify fuel delivery; prepare executive update. |
| 5. Drift / Risk | Early road-closure report preceded barricade verification; pump demand may reduce runtime; public reports may outpace confirmed information. |
| 6. Escalations | Notify leadership if river levels rise; escalate if generator runtime falls below six hours without confirmed fuel. |
| 7. Handoff Ready | Access, communications, ownership, and incoming understanding confirmed. |
| 8. Close / Carry | Carry all four open items. |

## 24.5 Situation Report - Representative Example

Flooding remains active but localized. River levels have stabilized during the latest review period. Three road closures remain in effect. Pump Station 3 continues operating through backup communications. No evacuation order is active.

- What changed: barricades verified; western access limited to emergency vehicles; fuel delivery confirmed; rainfall forecast reduced.
- Priorities: maintain pump operations; inspect Mill Road; preserve emergency access; maintain public-information consistency.
- Decision point: reassessment at 4:30 PM.

## 24.6 Executive Brief

| Field | Representative content |
|---|---|
| Current posture | Red Alert |
| Trend | Stabilizing |
| Leadership needs to know | Three roadways affected; no evacuation; pump operational; secondary communications functioning; fuel delivery confirmed. |
| Decision required | None immediately. |
| Next decision point | 4:30 PM operational review. |
| Primary risk | Additional rainfall or pump interruption could reverse the stabilizing trend. |

## 24.7 Decision and Communication Logs

| Time | Decision | Authorized by | Basis |
|---|---|---|---|
| 7:10 AM | Activate Watch | Client Authorized Representative | Flood Watch, rising gauges, local reports |
| 9:47 AM | Activate Red Alert | Client Authorized Representative | Flood Warning, road flooding, pump concern |
| 5:20 PM | Return to Watch | Client Authorized Representative | Stabilizing conditions |
| 8:10 PM | Declare All Clear | Client Authorized Representative | Immediate threat contained |

## 24.8 Operational Health Reference

| Category | Representative states |
|---|---|
| Connection | Connected; Weak Signal; Intermittent; Signal Lost; Secondary Path Active; Offline Capture Active |
| Power and runtime | Commercial Power Available; UPS Active; Generator Running; Battery Percentage; Fuel Percentage; Estimated Runtime |
| Information processing | Uploading; Received; Verification Pending; AI Draft Prepared; Human Review Required; Delivered; Delivery Failed |
| Forms and submissions | Draft Saved; Required Information Missing; Submission in Progress; Submission Received; Confirmation Sent; Retry Required |

*Users should not have to guess whether an important capability or submission is functioning.*

## 24.9 All Clear Transition Checklist

- ☐ Authorized Client personnel declared All Clear
- ☐ Date and time recorded

- ☐ Mavensoft recorded the transition
- ☐ Immediate threat contained or stabilized
- ☐ Urgent work completed or assigned
- ☐ Open items have acknowledged owners
- ☐ Residual risks and unknowns remain visible
- ☐ Required recipients informed
- ☐ Recovery responsibilities transferred
- ☐ Operational records preserved

## 24.10 Comprehensive Final Report

39. Incident identification and executive summary
40. First Awareness and complete posture timeline
41. Current Reality by significant phase
42. Major decisions and authorizations
43. Communications and system-health timeline
44. Ownership and handoffs
45. Evidence and verification
46. Corrections and updated information
47. All Clear
48. The Morning After
49. Recovery work
50. Full Closure verification
51. Remaining transferred obligations
52. Authorized approval
53. Record-preservation status

## 24.11 Full Closure Checklist

- ☐ All known work completed or formally transferred
- ☐ Accepting owners recorded
- ☐ Required evidence attached
- ☐ Required approvals recorded
- ☐ Communications and offline records reconciled
- ☐ Corrections linked to original entries
- ☐ Restricted records preserved under appropriate controls
- ☐ Recovery actions completed
- ☐ Comprehensive Final Report completed
- ☐ Authorized Client leadership approved Full Closure

## 24.12 Visual Production Note

Final published displays may use current Resilience screens, focused refinements, or clearly labeled representative placeholders. Final fields, integrations, and presentation may vary by Client configuration and operating environment.

# Chapter 25

## Putting Resilience into Practice

### 25.1 Purpose

Resilience is an operational practice that helps organizations preserve Operational Truth, maintain continuity, and support informed human judgment while conditions continue to change.

### 25.2 Operational Readiness

- Maintain current information.
- Practice communications and alternate paths.
- Review responsibilities and access.
- Validate equipment and system health.
- Exercise workflows and handoffs.
- Refine procedures through experience.

### 25.3 Continuous Improvement

Every incident, exercise, and review provides an opportunity to ask what was understood well, where drift began, what restored clarity, and what should be improved before the next event.

### 25.4 Working Together

Fire, law enforcement, emergency management, public works, utilities, healthcare, transportation, executive leadership, and cooperating organizations contribute different responsibilities. Resilience helps preserve shared operational understanding across those boundaries.

### 25.5 The Three Foundation Documents

The Landing Pages introduce. The Operations Manual explains and demonstrates. The Terms and Conditions establish the engagement, responsibilities, services, commitments, and commercial framework.

### 25.6 Mavensoft Commitment

Mavensoft supports Clients through thoughtful implementation, practical training, familiar operational relationships, ongoing support, and continuous refinement of the platform and methods.

### 25.7 Closing Principles

**Outcome First.**

**Operational Truth Always.**

**Technology that Empowers Human Judgment.**

### 25.8 Final Statement

*Resilience helps first responders and operational teams preserve Operational Truth—the most accurate and current operational understanding available—so they can maintain clarity, make timely and*

*informed decisions under pressure, and navigate with confidence from First Awareness through Full Closure.*

***Not perfectly, but faithfully.***

# 26. Current Operational Alignment

This chapter states the current integrated operating direction for Version 1.4. It aligns Gatekeeper, operating postures, Dynamic Incident Access, connectors and information sources, AI-assisted processing, cybersecurity, 24/7 Operational Support, and Phase 0 readiness with the rest of this manual.

Implementation should map each authorized information source to what is received, expected update cadence, source and timestamp, freshness and health indicators, material-change triggers, ownership, required action, evidence and verification expectations, exception handling, and the authorized people or roles who may receive the information. Configuration should include an OTHER path for unforeseen but material information.

## 26.1 Gatekeeper - Controlled Access for Authorized Participants

Gatekeeper protects Operational Truth before information drives action. It governs who may see information, what may enter the shared operational picture, what requires additional verification or qualified-human review, what AI may touch or summarize, and what may cross operational boundaries.

Resilience may use a shared operational lane for information appropriate to the authorized operating team and a restricted professional or sensitive lane for information requiring narrower access. Restricted information does not automatically cross into the shared operational picture. Any permitted transfer should preserve source, qualification, authorization, and the reason the information is operationally relevant.

Gatekeeper does not replace incident command, professional judgment, legal authority, or Client decision responsibility. Authorized people decide.

## 26.2 AI-Assisted Processing and Trust

Approved AI tools may organize information, compare photographs over time, identify possible changes, summarize voice or video, translate language, and prepare draft reports. Trust is not blind. AI output may be incomplete, wrong, manipulated, or inappropriate for operational use. Material output should remain attributable and qualified and should receive authorized human review where the consequence warrants it.

Access controls also govern what AI may touch, analyze, summarize, or expose. Sensitive or professionally restricted information should not be made available to an AI process merely because it exists within the broader engagement.

## 26.3 Watch Support

Watch is the elevated-awareness posture used when conditions require closer observation while operations continue. Watch Support increases monitoring, verification, liaison coordination, ownership confirmation, Current Reality review, escalation awareness, communication-path checks, safeguards, and readiness support. Unless otherwise agreed, the ordinary Watch cadence is approximately three structured updates per 24-hour period.

## 26.4 High Alert Support

High Alert is used when operational risk, uncertainty, dependency, or tempo requires enhanced or continuous monitoring beyond ordinary Watch. High Alert may include accelerated update cycles, active continuity oversight, Mission Control coordination, and designated support resources when authorized.

## 26.5 Red Alert Support

Red Alert is used for active or imminent disruption requiring coordinated incident support. Red Alert Support includes accelerated reporting, verified updates, clear handoffs, named decision authority, escalation visibility, communications continuity, decision continuity, shift-to-shift continuity, and sustained operational awareness. Ordinarily, operational refresh cycles occur every 2-4 hours. 24x7 Mission Control applies where specifically authorized and resourced.

## 26.6 Liaison Support

Resilience Support Liaisons work with designated Client Operational Liaisons to preserve communication flow, ownership, handoffs, verification, escalation awareness, and continuity. Liaison support does not replace Client incident command, operational control, or decision responsibility.

## 26.7 Dynamic Incident Access

During Watch, High Alert, or Red Alert operations, authorized responders may be added as operational needs change through verified invitation, individual credentials, role-based permissions, time-limited access where appropriate, and View Only access where appropriate. Access may be reviewed, changed, or revoked as conditions and responsibilities change.

Identity verification, invitation history, role assignment, activity logging, and immediate revocation controls should be preserved so rapid collaboration does not compromise security, accountability, or Operational Truth.

## 26.8 Connection, Connector, and Access Deliverables

Phase 0 and implementation must establish primary, backup, tertiary, and last-resort communication and access paths appropriate to the Client environment. Approved methods may include secure portal or workspace access, multifactor authentication where required, cellular connectivity, satellite or Starlink connectivity where available, offline tools, battery backup, and other approved alternate methods. An untested backup pathway should not be described as reliable.

Connection and connector deliverables should identify Client and Resilience liaisons, activation and escalation contacts, role and permission mapping, approved source systems, information received, expected cadence, source/timestamp/freshness/health, material-change triggers, primary and alternate paths, verification rules, Dynamic Incident Access procedures, access logging, revocation procedures, exception handling, and an OTHER path.

## 26.9 Degraded Connectivity and Reconciliation

Where degraded-connectivity operations are part of the engagement, implementation should define how locally captured operational context, delayed system information, manual actions, and restored data will be reconciled after connectivity returns, including responsibility for resolving discrepancies and updating Current Reality.

## 26.10 Cybersecurity and Security

Cybersecurity is an ongoing concern and continuous focus rather than a separate product lane. Appropriate safeguards may include access controls, permissions, authentication, encryption, monitoring, logging, backups, and other controls appropriate to the Client environment and accepted scope. Security controls should protect information without obscuring authority, change history, unresolved work, or required action.

## 26.11 Observe While You Act

Training should develop the ability to act effectively while simultaneously observing the changing operational picture: what is happening, what changed, what is verified, what remains uncertain, who owns the next action, and whether current assumptions still match reality.

## 26.12 Post-Operational Review

After exercises, significant elevated-posture periods, and major operational transitions, teams should conduct a structured Post-Operational Review to identify what worked, what changed, where information drifted, what was missed, what decisions mattered, what handoffs succeeded or failed, what remained unresolved, and what should be changed in training, procedures, systems, or readiness preparation.

## 26.13 Operational Deliverables

The continuous operational record supports the Mission Control Operational Picture, Situation Reports, Executive Briefs, Eight-Part Shift Packets, Decision Logs, Communication Logs, Recovery Carryover, timeline views, verification records, communications-gap and reconciliation records, After-Action material, and the Final Operational Record. Material records should preserve source, timestamp, verification status, significance, ownership, next action, acknowledgement, and next review time where applicable.

## 26.14 Posture Authority and Commercial Alignment

Only authorized Client personnel may activate Watch, High Alert, or Red Alert, change posture, declare All Clear, or authorize Full Closure. A single incident may move Normal Operations → Watch → High Alert → Red Alert → lower posture as conditions stabilize → All Clear → Recovery Mode → The Morning After → Full Closure while preserving one continuous operational record.

Commercial treatment, minimum periods, and any special staffing requirements follow the applicable accepted Terms and Order. Billing follows authorized operational posture and must never determine or prolong an operational posture.

# Appendix A - Glossary

**All Clear:** The declaration by authorized Client personnel that active elevated-posture services conclude and the operation transitions into Recovery Mode.

**Client Local Operational Liaison:** The Client-designated person who provides local operational knowledge, coordination, source access, ownership support, and continuity.

**Conflicting Information:** Information from credible sources that disagrees or cannot yet be reconciled.

**Current Reality:** The most accurate known operational status at a given time based on available facts, evidence, ownership, verification, and documented updates.

**Degraded Visibility:** A condition in which communications, telemetry, system access, or other information pathways are incomplete, delayed, contradictory, or unavailable, reducing confidence in the current operational picture without necessarily indicating that local operations have stopped.

**First Awareness:** The first reliable indication that something has changed or may require operational attention.

**Full Closure:** The authorized end state after all known responsibilities are completed, transferred, or dispositioned; required evidence and records are complete; and closure is approved.

**Gatekeeper:** Mavensoft Resilience's controlled-access and information-governance function for protecting Operational Truth. It governs authorized participation, information visibility, verification, restricted handling, AI access, qualified-human review, and controlled movement of information into the shared operational picture.

**High Alert:** A Client-authorized posture requiring enhanced or continuous monitoring, accelerated update cycles, active continuity oversight, Mission Control coordination, and designated support resources as agreed.

**Mission Control:** The coordinated support function used to maintain Current Reality, ownership, handoffs, escalation awareness, structured updates, and continuity.

**Operational Information Now:** The current, need-to-know operational picture available to authorized users while conditions are changing.

**Operational Truth:** The most accurate, current, verified, and responsibly maintained operational understanding available at a given moment.

**Recovery Mode:** The period after All Clear in which carryover, verification, residual-risk review, follow-up, reporting, and closure continue.

**Red Alert:** A Client-authorized posture requiring coordinated incident support, frequent refresh cycles, shift continuity, active support, and Mission Control coverage as agreed.

**Watch:** A Client-authorized elevated-readiness posture requiring increased monitoring, structured updates, ownership verification, and early escalation awareness.

**Mavensoft Operational Liaison:** The Mavensoft-provided person who maintains Operational Information Now, organizes and attributes information, supports verification, prepares reports and handoffs, and preserves continuity.

**Mission Control:** The coordinated support function used to maintain Current Reality, ownership, handoffs, escalation awareness, structured updates, and continuity.

**Operational Information Now:** The current, need-to-know operational picture available to authorized users while conditions are changing.

**Operational Truth:** Operational Truth is the most accurate, current, verified, and responsibly maintained operational understanding available at a given moment. It distinguishes what is known, what is unknown, what has changed, what evidence supports the record, and what remains to be verified. Operational Truth evolves as the operational understanding is refined through additional verified information while preserving the integrity of the operational record.

**Primary / Secondary / Tertiary:** The preferred method, alternate method, and additional contingency identified for a critical capability.

**Recovery Mode:** The period after All Clear in which carryover, verification, residual-risk review, follow-up, reporting, and closure continue.

**Red Alert:** A Client-authorized posture requiring intensive continuity coordination, frequent refresh cycles, shift continuity, active support, and Mission Control coverage as agreed.

**Shift Packet:** The eight-part handoff package: What Changed; Current Reality; Open Items; Next Actions; Drift/Risk; Escalations; Handoff Ready; Close/Carry.

**The Morning After:** The disciplined review and reconciliation period following All Clear that carries the operational record toward Full Closure.

**Watch:** A Client-authorized elevated-readiness posture requiring increased monitoring, structured updates, ownership verification, and early escalation awareness.

**Watch Point:** A condition, signal, dependency, or uncertainty that requires continued observation or a defined review point.

# Appendix B - Acronyms

| Acronym | Meaning |
|---|---|
| AI | Artificial Intelligence |
| CAD | Computer-Aided Dispatch |
| EOC | Emergency Operations Center |
| GIS | Geographic Information System |
| GPS | Global Positioning System |
| ICS | Incident Command System |
| IT | Information Technology |
| NWS | National Weather Service |
| OT | Operational Technology |
| SCADA | Supervisory Control and Data Acquisition |
| SMS | Short Message Service |
| UPS | Uninterruptible Power Supply |

# Appendix C - Operational References

Operational references should be confirmed and updated during implementation according to the Client's jurisdiction, responsibilities, systems, and approved plans.

- National Weather Service watch, warning, and emergency terminology.
- Client emergency operations plans, continuity plans, mutual-aid agreements, and escalation procedures.
- Incident Command System and Emergency Operations Center procedures used by the Client.
- Applicable public safety, utility, healthcare, transportation, infrastructure, and regulatory procedures.
- Client-specific communications plans, radio plans, GIS, CAD, SCADA, and system-of-record guidance.
- Resilience Terms and Conditions and accepted Order.
- Resilience Landing Pages and implementation materials.

# Index

Acknowledgement - Chapters 7, 11, 18, 23, 24

AI-assisted processing - Chapters 20, 22, 24, 26

All Clear - Foundations; Chapters 4, 15-17, 22, 24, 26

Client Local Operational Liaison - Chapters 5, 19, 23, 24, 26

Communications failure - Chapters 9, 14, 20, 22, 26

Connector / information-source mapping - Chapters 20, 26

Decision Log - Chapters 12, 15, 18, 24, 26

Dynamic Incident Access - Chapter 26

Evidence - Chapters 10, 14-18, 24, 26

First Awareness - Foundations; Chapters 17, 24, 25

Full Closure - Foundations; Chapters 16-18, 23-26

Gatekeeper - Chapters 1, 26; Glossary

High Alert - Foundations; Chapters 1, 4, 17, 26; Glossary

Mission Control - Chapters 7, 9, 15, 20, 22-24, 26

Operational Information Now - Foundations; Chapters 15, 20, 22-24

Operational Truth - Foundations; Chapters 1, 2, 10, 14-18, 20, 23-26

Primary / Secondary / Tertiary - Chapters 20-22, 24, 26

Recovery Mode - Foundations; Chapters 4, 16, 17, 22, 24, 26

Red Alert - Foundations; Chapters 1, 4, 14-17, 22, 24, 26

Restricted information handling - Chapter 26; Glossary

Shift Packet - Chapters 11, 15, 18, 23, 24, 26

Situation Report - Chapters 12, 15, 18, 24, 26

The Morning After - Foundations; Chapters 16, 17, 24, 26

Watch - Foundations; Chapters 1, 4, 14, 15, 17, 22, 24, 26

Watch Point - Chapters 2, 7, 15, 17, 22-24

# RESILIENCE

**Outcome First.**
**Operational Truth Always.**
**Technology that Empowers Human Judgment.**

***Not perfectly, but faithfully.***