

Maintaining Business Continuity After a Natural Disaster

Learn from a compliance officer's real-life perspective

By Jeff Pigott

Business continuity audits should evaluate how organizations care for people—not just how they preserve operations. Living through Hurricane Ian showed me that regulatory compliance, ethical leadership, and workforce resilience are inseparable during a crisis.

Business continuity often involves policies, risk assessments, and emergency preparedness plans. When disaster strikes, teams test those documents in real time—under pressure, uncertainty, and loss. Hurricane Ian reminded me that compliance obligations do not pause during crises; they intensify.

This article reflects on maintaining business continuity during Hurricane Ian from the perspective of a healthcare compliance officer. It highlights regulatory responsibilities, operational constraints, and audit lessons that continuity leaders can apply in healthcare and other regulated industries.

Regulatory expectations do not stop for disasters

Healthcare organizations that participate in Medicare and Medicaid must maintain comprehensive emergency preparedness programs. Federal regulations under [42 CFR Part 482](#) require all-hazards risk assessments, emergency plans, communication protocols, and training and testing programs. These requirements apply not only to hospitals but also to rural health clinics (RHCs) and federally qualified health centers (FQHCs), which also comply with applicable federal, state, and local emergency preparedness rules.

Could it happen to you?

Rebuild by Design's [Atlas of Accountability](#) shows that 95.5% of U.S. residents live in counties with recent disaster declarations. Page one of their Atlas of Accountability Fact Sheet, presented at Appendix B, details disaster declarations across county and congressional districts from 2011 to 2024.

From an audit perspective, emergency preparedness is not a paper exercise. Regulators expect plans to be executable, scalable, and responsive to real world conditions—conditions that rarely follow forecasts or assumptions.

Organizational context: Scale matters in crisis

At the time of Hurricane Ian, I served as Vice President of Compliance and Internal Audit at Lee Health in Fort Myers, Florida. The system included multiple acute care hospitals, specialty hospitals, a children's hospital, a rehabilitation hospital, and more than 100 outpatient sites. Approximately 14,000 employees and more than 900 physicians supported those operations.

This scale magnified every operational decision during the storm. Auditors evaluating business continuity should consider organizational size, geographic dispersion, and dependency on workforce availability as core risk factors.

Preparation: What plans often miss

Lee Health established core preparedness capabilities before Ian, including an incident command structure, staff training, evacuation planning, communication protocols, resource management, and continuity plans for critical services. Technology supported many of these controls, but the storm quickly proved that teams also needed durable manual alternatives.

Hurricane Ian revealed that even well designed plans may not fully address:

- Rapidly shifting forecasts
- Geographic isolation
- Staffing constraints
- Communication failures
- Financial strain during extended outages



Teams make hundreds of time-sensitive decisions during an event.

For auditors, this underscores the importance of stress testing emergency plans against worst case scenarios rather than likely ones.

To prepare for that kind of disruption, leaders must define and document a decision tree before a crisis. Teams make hundreds of time-sensitive decisions during an event: they shut down services, alter workflows, redirect patients, adjust staffing, and approve emergency purchases. When leaders pre-authorize thresholds and delegations, they reduce delays and keep decisions consistent across sites.

Auditors can test this readiness by reviewing training records, drill outcomes, downtime job aids, and incident command logs from prior events. They can also observe functional exercises that force teams to operate without normal tools—no shared drives, limited email, and degraded electrical and/or phone service. When staff cannot demonstrate a manual workflow for registration, medication administration, or documentation, auditors should flag the gap as an operating risk, not just a training preference.

Compliance teams should also plan for privacy and security during downtime. Staff may rely on paper notes, ad hoc phone calls, and improvised workspaces during an evacuation or unit consolidation. Leaders should provide clear guidance on minimum necessary disclosures, secure storage for paper records, and controlled access to patient information when normal badge systems and cameras fail.

Forecasting: Risk versus reality

In the days leading up to landfall, official forecasts focused attention on Tampa Bay, with Fort Myers largely absent from early National Hurricane Center statements. Less than 24 hours before full impact, Ian's path shifted south and compressed the organization's decision timeline.

Auditors should recognize that reliance on forecasts alone can create a false sense of security, and organizations should avoid designing continuity around forecast precision.

Leaders need clear triggers—such as expected wind fields, storm surge probabilities, or utility pre-shutoff notices—that prompt early actions even when the exact track remains uncertain. Early action buys time for staffing, supply staging, clinical service adjustments, and patient movement.

Auditors can evaluate this capability by reviewing how leaders set triggers, who approves escalation steps, and how quickly teams execute them. A strong program documents time-stamped decisions, shows consistent criteria across facilities, and demonstrates that leaders can reverse or scale decisions safely as conditions change. A weak program depends on informal judgment that varies by leader and site.

The event: Making compliance decisions under extreme conditions

On September 28, 2022, Hurricane Ian made landfall near Fort Myers as a Category 4 storm and caused catastrophic damage. Nearly all of Lee County lost power. Water systems suffered damage and contamination risks. Communications infrastructure failed across large areas, which reduced situational awareness, slowed coordination, and forced leaders to run hospitals like field operations. Teams managed sanitation workarounds, secured potable water, and controlled access to clinical spaces when building conditions degraded. Leaders also balanced immediate clinical needs against longer-term safety concerns, such as infection control, waste disposal, and environmental hazards.

Technology risk intensified during the response. Power instability and limited connectivity can interrupt electronic health records, telemetry, and identity systems. When teams switch to manual workarounds, they often create new privacy and security exposure through paper records, unsecured devices, and improvised communications. Compliance and IT leaders should plan for this shift and provide clear guardrails that keep care moving while limiting avoidable exposure.

As another audit example, test whether emergency purchasing controls work under crisis speed. Select a sample of storm-related purchases (for example, fuel deliveries, water, temporary services, and critical supplies) and trace each item from request to approval to receipt. Confirm that leaders used documented emergency authorities, captured vendor terms, and reconciled invoices after operations stabilized. When teams bypass normal procurement systems, auditors should verify that leaders still prevented duplicate ordering, controlled price spikes, and documented why they chose each vendor under constrained conditions.

Supply chain constraints also reshaped control expectations. Leaders needed fuel, water, food, linens, pharmaceuticals, and contracted services at the same time vendors faced road closures and their own outages. A mature continuity program pre-identifies emergency suppliers, establishes receiving locations, and sets purchasing controls that remain workable during a crisis. Auditors should confirm that emergency purchasing still requires accountability, documentation, and post-event reconciliation.

As the hurricane advanced, [Lee Health experienced](#) loss of water pressure and sanitation systems, contaminated community water supply, sporadic cellular communication, and storm surge that impacted hospital facilities.

Compliance leaders supported real-time decisions about patient acuity, evacuation feasibility, resource allocation, and regulatory obligations while leaders protected patient safety and workforce well-being. We focused on two disciplines: We helped teams act decisively, and we helped them document decisions clearly enough to withstand post-event scrutiny.

Evacuation: Continuity of care when moving patients

In the immediate aftermath, Lee Health coordinated with local, regional, and national partners to evacuate patients to hospitals across Florida and neighboring states. We evacuated Golisano Children's Hospital first, including 67 NICU infants transferred within 24 hours without an adverse event. We then evacuated two additional hospitals and moved more than 400 patients over several days.

A weak business continuity program depends on informal judgment that varies by leader and site.

Evacuation requires more than transportation. Teams must maintain patient identification, medication continuity, clinical handoffs, and accurate documentation while conditions change minute by minute. Leaders also need current transfer agreements and clear criteria that define when they shelter in place versus evacuate, especially for high-acuity units such as NICUs, ICUs, and behavioral health.

Auditors can test evacuation readiness by requesting transfer logs, bed-tracking records, receiving facility confirmations, and time-stamped decisions from incident command. They should also test how the organization protects patient information during transfers and how it reconciles paper documentation back into systems after normal operations resume. Those artifacts demonstrate whether the organization can execute continuity of care, not just describe it in policies.

From an audit perspective, evacuation performance depends on controls that remain functional during crisis conditions:

- Coordinate with external partners and activate mutual-aid and transfer agreements quickly
- Maintain decision logs and patient movement documentation that leaders can review and defend later
- Sustain minimum clinical, privacy, and safety controls while teams operate on manual processes

When auditors scope continuity, they should include evacuation as a cross-functional process that touches clinical operations, IT, privacy, facilities, transportation, and external communications. Teams can only execute safely when staff responsible for each function understand their role and share the same operational picture.

Workforce resilience: Learn from history

Leaders carried a critical lesson from Hurricane Irma in 2017. During the aftermath of that storm, some leaders terminated employees who could not report to work quickly, which triggered reputational damage and rehiring issues. During Ian, leadership committed to more flexibility and communicated that commitment clearly.

The organization's relief efforts restored operational capacity. When employees lose housing, transportation, childcare, or basic supplies, attendance policies alone cannot restore

Communications infrastructure failed across large areas, which reduced situational awareness, slowed coordination, and forced leaders to run hospitals like field operations.

staffing. Leaders must address practical barriers so staff can return safely and sustainably.

Workforce continuity also requires structured controls: leaders must track who is available, redeploy staff across sites, confirm credentials and competencies, and manage fatigue during extended response periods. Auditors can test these controls by reviewing staffing rosters, redeployment records, just-in-time training materials, and evidence that leaders monitored rest cycles and safety incidents.

Things that were done differently after Hurricane Ian that provided audit opportunities:

- Paid all employees for three weeks regardless of work status
- Reimbursed insurance deductibles for damaged vehicles
- Provided transportation assistance
- Offered legal and FEMA claim support
- Supplied basic necessities such as scrubs, food, and transportation support

Auditors should treat workforce resilience as a core continuity objective. If the organization cannot locate staff, communicate expectations, provide basic support, and redeploy qualified personnel, every other continuity control degrades quickly. Effective programs plan for workforce disruption with the same rigor they apply to power, water, and IT.

Community impact: External dependencies extend organizational risk

Hurricane Ian disabled television and radio stations and disrupted a meaningful portion of regional wireless infrastructure, which complicated efforts to locate and support employees and to coordinate logistics across the community.

Leaders often underestimate how quickly external dependencies fail. Roads close, fuel becomes scarce, and vendor delivery routes collapse. Even when a facility remains structurally sound, it can lose practical access to supplies, staff, and information. Continuity planning must

therefore include the community environment, not just the enterprise footprint.

Auditors can add value by mapping the organization's external dependencies—power, water, fuel, roads, telecom, and public messaging—and by verifying practical workarounds for the first 72 hours. Teams should maintain alternate communications methods (i.e., text messages have a better chance of reaching recipients than a phone call when cellular networks may be compromised), offline contact directories, and predefined rally points. They should also document which leaders coordinate with emergency management and how they share updates internally.

Auditors should incorporate community infrastructure and utility dependencies into continuity risk assessments.

Be better prepared: Lessons for auditors and compliance leaders

Auditors add the most value when they translate a disaster story into testable criteria. After Ian, I returned to the same question: Would our controls still work if we lost power, clean water, and reliable communications for days? Most organizations answer that question with policies. Strong organizations answer it with practiced behaviors, delegated authority, and evidence that leaders can make ethical decisions under pressure.

- Audit the first 72 hours: Test how teams operate before outside support restores utilities, logistics, and staffing.
- Control emergency purchasing: Enable rapid procurement while preserving documentation, approvals, and post-event reconciliation.
- Map community dependencies: Validate workarounds for fuel, water, roads, and telecom so continuity does not collapse when the community fails.
- Close the loop: Run an after-action review with owners, deadlines, and retesting so the organization confirms improvement before the next event.

These lessons apply beyond hurricanes and beyond healthcare. Floods, wildfires, cyber incidents, and prolonged utility failures create the same continuity challenge: Leaders must protect people and information while they sustain critical services with fewer resources and less certainty.

Conclusion

Hurricane Ian reinforced the role compliance officers and auditors play during crises. We do not enforce rigid rules in a vacuum; we help leaders make ethical, defensible decisions while operations degrade. We also help teams preserve evidence and tell an accurate story later, when regulators, boards, insurers, and communities ask what happened and why.

Organizations measure preparedness by how they perform under worst-case conditions, not by how polished their binders look during calm weather. Leaders should build programs that work when utilities fail, communications fragment, and staff face personal loss. Auditors can reinforce this mindset by testing operating effectiveness, not just policy completeness. The checklist at Appendix A reflects lessons informed by Hurricane Ian.

To strengthen continuity now, start with three actions:

- 1) validate decision triggers and delegated authorities,
- 2) run a functional downtime exercise that forces manual operations, and
- 3) confirm that evacuation, communications, and workforce support plans produce usable documentation. These steps build readiness and give leadership credible assurance before the next event tests the organization.



Jeff Pigott is Compliance Director and Privacy Officer at Summit Medical Group in Knoxville, Tennessee. He has 40 years of experience, including 30 in healthcare. You can contact him at pigottjeffrey@gmail.com or on [LinkedIn](#).

Evacuation performance depends on controls that remain functional during crisis conditions.

Appendix A

Auditor Checklist: Business Continuity and Emergency Preparedness

This checklist is designed to help auditors evaluate whether an organization's emergency preparedness and business continuity program is operationally effective—not merely compliant on paper.

1. Regulatory compliance and governance

- ☐ Does the organization maintain a documented emergency preparedness program that meets Medicare and Medicaid Conditions of Participation, including all-hazards risk assessments, emergency plans, communication plans, and training/testing programs?
- ☐ Are emergency preparedness requirements clearly extended to all applicable entity types (e.g., hospitals, RHCs, FQHCs), with evidence of compliance across the enterprise?
- ☐ Is executive leadership formally involved in emergency preparedness governance and activation decisions?

2. Risk assessment and planning assumptions

- ☐ Does the organization's risk assessment account for forecast uncertainty, including rapidly shifting disaster paths and incomplete early warnings?

- ☐ Are plans stress-tested against worst-case scenarios rather than most likely events (e.g., loss of utilities, water contamination, infrastructure failure)?
- ☐ Does the plan address risks related to geographic isolation, staffing shortages, and communication failures?

3. Command center and incident management

- ☐ Is there a documented command center structure with clear activation criteria and escalation protocols?
- ☐ Is there evidence that the command center can be partially or fully activated in advance of an event based on emerging risk signals?
- ☐ Are roles and responsibilities clearly defined for compliance, legal, operations, and clinical leadership during emergencies?

4. Communication resilience

- ☐ Does the organization maintain redundant communication methods to operate during widespread cellular, broadcast, and internet outages?
- ☐ Is there a documented process for locating and accounting for employee safety when traditional communication channels fail?
- ☐ Are communication protocols tested under conditions that simulate infrastructure failure?

5. Patient care continuity and evacuation

- ☐ Are patient evacuation plans documented, scalable, and coordinated with external agencies and receiving facilities?
- ☐ Is there evidence of decision-making criteria for assessing patient acuity and prioritizing evacuations during emergencies?
- ☐ Are evacuation outcomes tracked, including adverse events, to support post-incident review and regulatory scrutiny?

6. Workforce resilience and ethical considerations

- ☐ Does the emergency plan explicitly address workforce impact, including transportation, housing loss, and personal hardship?
- ☐ Are policies in place to prevent punitive employment actions that could create legal, ethical, or reputational risk following disasters?
- ☐ Are financial assistance programs (e.g., payroll continuation, deductible reimbursement, transportation support) governed by documented internal controls?

7. Infrastructure and utility dependencies

- ☐ Does the organization assess dependency on community utilities such as water, power, sewage, and communications infrastructure?
- ☐ Are contingency plans documented for operating with limited or contaminated water supply and reduced fire suppression capability?
- ☐ Is generator capacity, duration, and maintenance validated against extended outage scenarios?

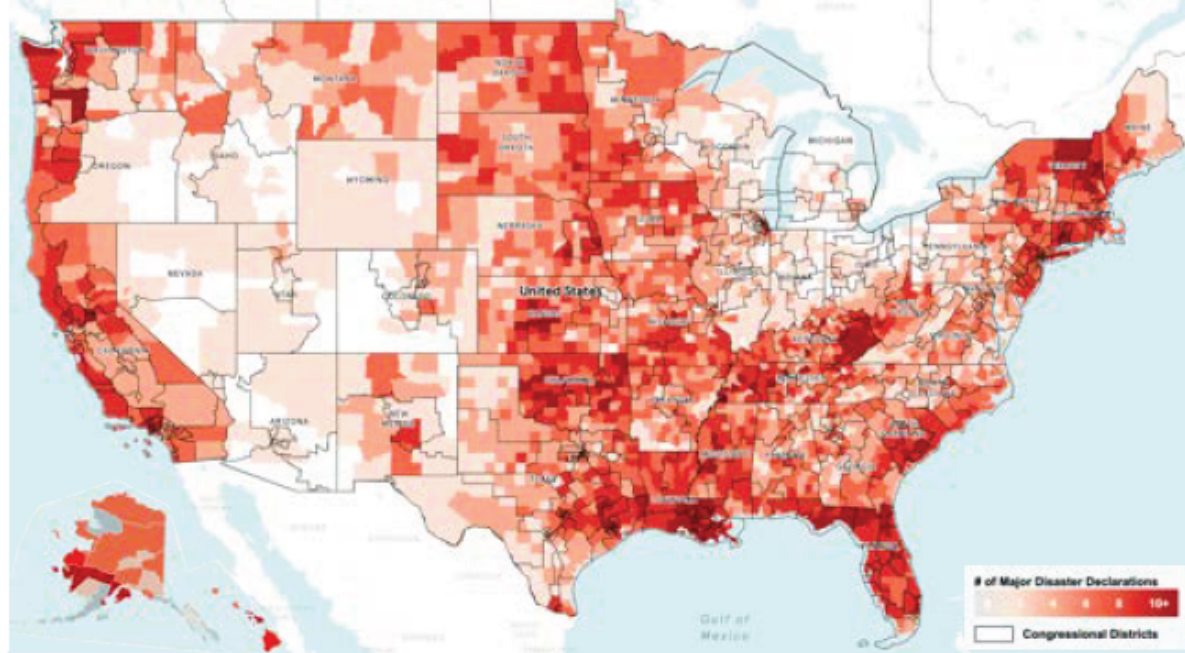
8. Post-event review and continuous improvement

- ☐ Is there a formal post-incident review process to identify gaps, document lessons learned, and update emergency plans?
 - ☐ Are emergency preparedness lessons shared across the organization and incorporated into training and drills?
 - ☐ Does leadership acknowledge that emergency preparedness requires flexibility and judgment beyond written plans?
-

Appendix B

ATLAS OF ACCOUNTABILITY

COUNTY-LEVEL DISASTER DECLARATIONS AND CONGRESSIONAL DISTRICTS (2011-2024)



As extreme weather continues to impact the U.S., Rebuild by Design launches the Atlas of Accountability, a mapping tool designed to help communities and policymakers understand their localized, climate-fueled exposure to extreme weather disasters. The tool builds on Rebuild by Design's 2022 report, "Atlas of Disaster," which analyzes county-level extreme weather disaster declarations and post-disaster federal assistance. The analysis highlights the urgency of bipartisan cooperation and the need to unite across the urban-rural divide.

99.5% OF CONGRESSIONAL DISTRICTS include a county that received a major disaster declaration for extreme weather between 2011 and 2024, amounting to **\$117.9 BILLION** in federal post-disaster assistance from FEMA and HUD CDBG-DR.

FINDINGS

80% OF STATES	EXPERIENCED 10 OR MORE MAJOR DISASTER DECLARATIONS
28 STATES	HAD EVERY COUNTY IMPACTED BY A MAJOR DISASTER DECLARATION
39 DISASTERS	CALIFORNIA HAD THE HIGHEST COUNT IN THE U.S., SOME OF WHICH INCLUDED DECLARATIONS FOR TRIBAL GOVERNMENTS
22 DISASTERS	WASHINGTON COUNTY IN VERMONT, RECORDED THE HIGHEST NUMBER OF MAJOR DISASTER DECLARATIONS
HIGHEST PER CAPITA	STATES WITH THE HIGHEST PER CAPITA POST-DISASTER ASSISTANCE SPAN ACROSS BOTH POLITICAL AFFILIATIONS: LOUISIANA, HAWAII, NEW YORK, VERMONT AND NEW JERSEY.