EMERGENCY MANAGEMENT INSIGHTS – AN INTERNAL AUDIT PERSPECTIVE ON PREPARATION THROUGH RECOVERY

Radgia Cook, Global Healthcare Quality & Safety Compliance Leader
Lauren DeBree, Associate Director

March 2021

Table of Contents

Abstract

With the rapid progress of the COVID-19 pandemic throughout the country, healthcare organizations (HCOs) would be well-advised to include internal audit in their continued emergency preparedness and recovery activities, utilizing an all-hazards approach. An all-hazards approach is defined by the Centers for Medicare and Medicaid Services (CMS) as "…an integrated approach to emergency preparedness planning that focuses on capacities and capabilities that are critical to preparedness for a full spectrum of emergencies or disasters, including internal emergencies and a man-made emergency, or natural disaster (or both)." Organizations that are not prepared for simultaneous events or pandemic resurgence have little time to bring their hospitals and systems up to compliance with new regulatory standards considering ever-increasing regulatory scrutiny. Not only will lives depend on it, but the future of the organization as a key contributor to the healthcare infrastructure of your community is also at stake. To prepare for events and regulatory compliance in the current environment, it is incumbent upon healthcare facilities to perform a thorough audit of all Emergency Management (EM) activities. Standardization through automation can assist in all phases of the Emergency Management continuum.

In this white paper, we will address key areas, including an all-hazards approach to your hazards vulnerability analysis (HVA) and its integration into your emergency operations plan; demobilization and supply chain resiliency plans and their impact on recovery efforts; incorporation of after-action reporting and lessons learned into your business impact analysis (BIA); and business continuity planning (BCP) for an expedited, effectual recovery.

The Emergency Management Challenge

Major disruptions and the realization of catastrophic risks, often unforeseen, are leaving hospitals vulnerable and poorly prepared to respond, as we are currently experiencing in the COVID-19 environment. Emergency incidents often occur without notice or warning, forcing hospitals to quickly adjust from normal operations to implementing the relevant emergency response plan to accommodate an emergency scenario, such as a sudden influx of patients or a severe weather event. It is vital for hospitals to ensure their staff and equipment are in a constant state of preparedness. Ensuring hospital personnel and resources are fully prepared for an incident can be logistically challenging. Patient care must remain the priority, while also protecting and maintaining the safety of all patients and professionals.

A key organizational step in disaster preparedness is understanding which potential emergency events are likely to occur in and around your organization. This can be straightforward in some instances – for example, hurricanes are more likely to occur in certain areas during specific seasons. Regions with historical earthquake activity already have specialized requirements that account for the hazard, such as building codes. Facilities must also be ready, however, for an unusual or unexpected disaster or for concurrent disasters to occur. For example, a simultaneous event of a hurricane during COVID-19 would create additional organizational risk that a hospital may not be prepared to address. Internal audit departments can play a role in facilitating hospital preparedness for both likely and unexpected disasters through a review of the organization's emergency preparedness program, including appropriate documentation and training to ensure the hospital is prepared to respond to whatever emergency scenario they may face. Internal audit can also participate in tabletop exercises and drills to assist the organization in the incident response from a risk management perspective. Once an emergency occurs and the incident command center (ICC) has been activated, Internal audit can be involved in an advisory function by participating in command center activities. During the recovery phase, Internal audit can also help ensure that key lessons learned are reviewed and documentation and training occurs as

needed. The internal audit department possesses valuable skills that can assist the organization in all phases of Emergency Management, from preparation to recovery.

Regulatory Oversight

In addition to the practical benefits of a strong EM program, EM activities are also regulated by both CMS and accrediting agencies such as The Joint Commission (TJC). Reviewing their requirements on a regular basis and staying abreast of changes that occur is important to ensure your hospital's EM program remains compliant. Internal audit can assist with this endeavor by determining whether the current EM program meets all standards. In addition to normal accreditation surveys, recent guidance indicates TJC is currently requesting policies for proof of compliance, including the emergency operations plan (EOP) and event-specific plans related to the top five to ten incidents for the facilities based on their HVA. TJC is requesting this documentation electronically and is expected to review these plans as part of upcoming surveys for comprehensiveness, facility specificity, ease of understanding, and training. See the below excepts from a TJC memo issued on July 1, 2020 for details around these survey procedures. The memo indicates why it is even more vital for each hospital to ensure documentation exists to detail the processes in place during the COVID-19 pandemic.

"The Joint Commission will assess how an organization adapted their infection control and Emergency Management processes in response to the pandemic and will focus its review on current practices to ensure the organization continues to provide safe care and work in a safe environment…"

Auditor's Tip: Ensure all CMS and other regulatory requirements are satisfied by your entity's EM program.

Staff Training and Preparedness

Conducting tabletop and community exercises and training staff on emergency preparedness plans are critical elements. Staff must be trained to fully understand the correct processes to follow in an emergency. They must be provided with opportunities to practice their emergency response roles and responsibilities to facilitate response for emergency preparedness, utilizing an all-hazards approach.

What is involved?

Audit should confirm that the following processes are occurring to ensure adequate emergency preparation:

- All tabletop and community exercises should include documentation detailing the scenario, process, approach description, staff engagement, communication protocols, and after-action reporting.

What Is a Hazard Vulnerability Analysis (HVA)?

HVA is the process for identifying the hospital's highest vulnerabilities in four main categories of emergency events: natural, human, technological and hazardous materials. The HVA takes into consideration the direct and indirect impact these hazards may have on the hospital and its surrounding community epidemiology. An HVA provides the hospital with a basis for determining the most likely events and potential demands on emergency services and other resources that could occur during a crisis so that effective preventive measures can be taken, and a coordinated disaster response plan can be developed.

A well-executed HVA provides a systematic approach to identifying the hazards or risks that are most likely to have an impact on a healthcare facility and its community-based activities. A multidisciplinary team should be formed to perform the HVA. Conducting a risk assessment/HVA is also a regulatory requirement. The most effective HVAs utilize a model that ranks each hazard by evaluating probability, severity, and impact. This will provide perspective into the top ten risks in your organization and allow for further analysis of the facility's internal and external preparedness. The HVA should occur on at least an annual basis, or whenever significant changes to the organization's environment occur. For example, with the COVID-19 pandemic being an active emergency, HVAs should be reconfigured and reperformed to reprioritize the top organizational risks, while considering simultaneous events. An additional area of consideration due to events in 2020 is an emphasis on preparedness for both domestic and external terrorist acts.

For example, in October 2020, Hurricane Delta caused structural damage and flooding at several hospitals, requiring generator power and alternate water sources for several weeks while simultaneously treating COVID-19 patients and addressing COVID-19 concerns such as sanitation, isolation, and social distancing. This resulted in an all-hazards approach during the current pandemic for subsequent emergency plan activation. Preparation, training, and communication were vital to ongoing operations and recovery efforts.

Updating the Emergency Operations Plan (EOP) and Ancillary Plans

Hospitals should validate all existing EM plans have been updated to include the highest risk events from their HVA and to include infection control criteria, based on the current COVID-19 pandemic. These plans should be updated annually or as changes occur. Examples of plans that should be updated include the infection control plan, evacuation plan, surge plan, and continuity of operations plan.

Command Center and Roles and Responsibilities

It is essential to have a predefined, structured command center with matrixed roles and responsibilities established and activated when an emergency occurs. Examples of commonly used command center structures are available through the Hospital Incident Command System (HICS) and the National Incident Management System (NIMS). A definition of the Incident Command System (ICS) follows (as defined by Federal Emergency Management Agency [FEMA]):

*The **Incident Command System (ICS)** is a standardized hierarchical structure that allows for a cooperative response from the organization and that takes into account the local community as well as multiple state and governmental agencies, to organize and coordinate response activities without compromising the decision-making authority of local command. ICS ensures that the most pressing needs are met, and that precious resources are used without duplication or waste.*

The primary role of ICS is to establish planning and management functions for respondents to work in a coordinated and systematic approach. These functions can include but are not limited to:

- *Emergency planning*
- *Using common terminology*
- *Creating a unified command structure*
- *Coordinating resource management and allocation*
- *Integrating communication media response and updates*

The five most important considerations internal audit should validate when reviewing the ICS are the following:

- A **Command Section** responsible for developing, directing, and maintaining communication and collaboration with the multiple agencies on-site and working with the local officials, the public, and the media to provide up-to-date information regarding the disaster.

- The **Operations Section** to address tactical operations, coordinate the command objectives, and organize and direct all resources to the disaster site.

- The **Planning Section** to provide the necessary information to the Command Center to develop the action plan that will accomplish the objectives and collect and evaluate information as it is made available.

- The **Logistics Section** provides personnel, equipment, and support for the Command Center. It handles the coordination of all services involved in the response, from locating rescue equipment to coordinating the response for volunteer organizations.

- The **Finance Section** accounts for funds used during the response and recovery aspect of the disaster. It monitors costs related to the incident and provides accounting analyses.

Supply Chain Resiliency Plan

The healthcare supply chain involves the flow of numerous product types from manufacturer to patient and requires the participation of various stakeholders who work in concert to achieve the goal of meeting patient care needs. Supply chain implications for public health events differ from those of a natural hazard in that public sector partners – via public health officials (state, local, and federal, including the Strategic National Stockpile [SNS]) – can play a significant role in supply chain operations through activation of programs, determination of the language to be included in emergency declarations and public messaging, and more. Vendors for commonly needed products during these events, including vaccines and personal protective equipment (PPE), are often limited. Depending on the nature of the event, demand for these products can far exceed production capacity.

Internal audit should verify that a supply chain resiliency plan is in place to focus on considerations for providers and patients and includes a risk management perspective of the role that manufacturers and distributors play in the supply chain process. The plan should address manufacturer and distributor roles and key vulnerabilities and provide for pre-event, response, and recovery considerations for the necessary components of the healthcare supply chain.

Manufacturers	
Role in Healthcare Supply Chain	**Key Vulnerabilities**
o Create and manufacture medical products such as PPE, gloves, and gowns o Produce disposable and durable products and medications o Monitor and respond to shortages o Maintain quality standards for all manufactured products	o Raw materials/product disruption o Spike in demand outpaces production o Limited number of vendors for needed products o Damage to factory/utilities o Overseas production vulnerability o The lack of a risk mitigation plan

Distributors	
Role in Healthcare Supply Chain	**Key Vulnerabilities**
o Responsible for delivering medicines and supplies from manufacturers to providers and healthcare facilities such as vaccines and PPE o 92% of prescription drug sales are handled by distributors o Maintain quality standards for all products distributed	o Spikes in customer orders due to pandemic surges o Road damage/infrastructure damage o Product shortages o Impacts to labor force

Supply chain resiliency plans should include the following sections:

- **Pre-event** - Identify hazards, vulnerabilities, and threats – Focus on events that could significantly disrupt supply delivery or compromise current supplies and those that are most

likely in specific regions.

- **Response -** Forecasting needs – Ability to provide care hinges on having needed supplies on-site and a plan for replenishment. Anticipating supply needs, and capacity for receiving and storing them, are key activities for responses.
- **Recovery -** Resume normal operations and communicate the resumption of normal allocation/delivery/activities with distributors and organization partners.

Auditor's Tip: Supply chain resiliency plans need to address event-specific criteria. For example, COVID-19 supply chain requirements are different than those for a natural event such as a hurricane or earthquake.

Demobilization Planning

When an emergency of global proportions occurs, organizations mobilize through their command center to provide a strategic unified response. As the emergency moves toward a return to normal, an effective demobilization plan (DP) is an important component of a hospital's recovery plan to restore operations efficiently and effectively. Demobilization is the orderly, safe, and efficient return of all aspects of an incident response to its original state. An organization's DP should adopt a phased approach to ensure resurgence possibilities are addressed. Internal auditors should validate that a DP provides a standard framework that can be modified for Command Center personnel and leadership to achieve a comprehensive and effective recovery. Demobilization will look different for every hospital. Each organization is unique in how it has deployed and dealt with emergency preparedness, such as the COVID-19 response.

Internal audit should determine whether the demobilization plan:
- Identifies gaps in processes,
- Provides considerations and recommendations,
- Provides external and internal communication processes, and
- Includes potential timelines regarding a phased approach for a timely and efficient return to the "new normal."

The demobilization processes validated by internal audit should:

- Utilize a cross-functional teaming approach with representation from all aspects of an organization's emergency response.
- Ensure that resources utilized during the response have been returned to their pre-incident status. Resources are defined as, but not limited to, temporary locations and utilization of designated spaces, equipment and supplies, and emergency engagement personnel such as volunteers, clinicians, and community resources.
- Consider the possibility for reoccurrence at any time during or after the emergency incident.
- Include key milestones that result in an emergency response decline.

The DP should be included as a component within the overall emergency preparedness plan. A demobilization unit should be established and can be utilized, engaged, or deployed at any point in an emergency incident life cycle. Demobilization planning should begin as soon as possible to facilitate resource availability.

After-Action Reporting

After-action reporting (AAR) is defined as a retrospective analysis on an exercise, drill or event based on a sequence of goal-oriented actions undertaken, generally by the user. An AAR is an important tool used to provide feedback after a training or actual event. It summarizes what occurred during the event, analyzes actions taken, and identifies areas needing improvement. An after-action report also enables organizational compliance tracking and, most importantly, allows an organization to update both their emergency operations plan and their business continuity plan. Auditors should validate that there is a central repository for the after-action reports, business continuity plans, and emergency operations plans and ensure that the latest versions are accessible to all staff. In addition, memorandums of understanding with community partners should be updated as needed based on the AAR findings. Internal auditors should validate the following:

- AARs are based on actual or potential events.
- AARs capture what happened, how the organization responded, and an analysis of the response.
- Documentation of specific actions to ensure proper procedures are understood and followed.
- AARs should identify organizational strengths.
- AARs should identify weaknesses and how they can be corrected.

Auditor's Tip: Emergency situations provide organizations opportunities to learn from the past and prepare for the future through after-action reporting.

Internal Audit's Role in Emergency Preparedness

Assess & Anticipate – HVA	Plan – Emergency Preparedness & Operations Plans	Crisis Preparedness & Management – Event Plans & Training	Recovery Activities
• Confirm annual committee HVA review • Assess all HVA categories for accuracy • Ensure risk calculations are reasonable	• Confirm EOP plan contains required sections, including ICC roles and responsibilities and communication protocols	• Validate top 5 to 10 events have facility specific plan • Confirm training has occurred • Validate processes for plan initiation	• Confirm AAR lessons learned are integrated in EOP • Audit the BIAs • Confirm testing has occurred on BIAs • Validate BCPs

Disaster Recovery Processes

A Disaster recovery plan is developed based on the performance of multiple processes, including the following:

- AARs
- Risk assessments
- Risk analyses
- Business impact assessments
- Business continuity plans
- Disaster recovery plans

Understanding the difference between a risk assessment and a business impact analysis is important. Facilities should conduct both risk assessments and business impact analyses.

What is the difference between a business risk assessment and a business impact analysis?

A business impact analysis:

- Identifies business impact when processes are not functional or available
- Is based on an inability to perform a process
- Is used to identify how quickly the process must be available
- Is not concerned with why a process is unavailable, only when it needs to be available
- Helps determine what technology or planning is needed for functional recovery

An EM risk assessment:

- Identifies situations where business processes are impacted such as elective procedures being stopped
- Determines the probability of the risk occurring.
- Pinpoints threats and hazards across all areas – human, natural, technology and chemical/biological
- Assists in determining how to prevent impact/outages
- Can be referred to as a threat and risk assessment (TRA)

It is not possible to have a complete business continuity strategy without conducting both a BIA and business risk assessment. When only a BIA is performed, the recovery focus is typically on IT. Risk assessments provide an overall view of risks to the organization. When only a risk assessment is performed, the financial and nonfinancial business impacts are not considered. BIAs and Risk assessments should be performed and updated on a regular basis and one cannot replace the other. Best practices include integrating the two, sharing information whenever possible, and presenting management with a single view that enables them to make more informed business decisions.

BIAs and TRAs are two long-standing components of any business continuity (BC) methodology. They remain two of the most critical components of any BC program, as major strategy and funding decisions will be made based on their results and how critical the department functions are to the enterprise.

We believe the two need to be integrated, as the combined studies provide a comprehensive view of both business process criticality and risk. The BIA and TRA summary for a site should include the following:

- List of the most critical business units and processes at the site
- List of the top ten threats (e.g., hurricane, severe weather, hazmat, etc.) from your HVA, making sure active shooter and infectious disease/pandemic are included
- Status of the mitigating controls (e.g., backup power, network redundancy, physical security) at the site
- Site risk rating which is dependent on critical business units, threats, and state of the mitigating controls

Business continuity plans focus primarily on operations and disaster recovery plans largely focus on IT to support operations. Auditors should confirm that leadership is involved so various departments can better understand processes that should continue uninterrupted in addition to the supporting applications.

Plans should be comprehensive and be in-line with the following best practices:

- Plans should be updated and strengthened based on the results of the tabletop or full-scale drills.
- BCP plans should be tested prior to finalization.
- Disaster recovery plans should be tested prior to acceptance.
- Tests should occur at least annually, utilizing either a tabletop simulation or a full-scale emergency drill.

Internal audit should validate that every facility has a comprehensive list of processes and procedures by department and identifies applications and systems needed to continue operations with a prioritization plan to ensure a quick recovery to normal operations.

Business Continuity Plan/Recovery Planning

Business continuity plans are the lifeline for keeping HCOs viable and operational to provide care for the community during and after an emergency. During an event such as the COVID-19 pandemic, HCOs must activate both their required emergency preparedness plans and their business continuity plans. An emergency preparedness plan is intended to prepare for and address an ongoing emergency, whereas the business continuity plan reduces economic impact to the organization during an event, allowing it to maintain critical business and logistical functions. Further, business continuity plans help HCOs recover and get back to business as usual more quickly and effectively.

Effective business continuity plans start with leadership buy-in and with a business continuity team that can tackle the plan development.

- **Category 1:** Processes that, if not continually performed, pose an immediate threat to employee or patient safety and/or pose an immediate negative financial impact. These processes must remain uninterrupted or be performed frequently to prevent an immediate negative impact.
- **Category 2:** Processes that, if delayed or stopped, can cause a large negative impact to the HCO and stakeholders. This includes internal and external contractually required obligations with vendors, employees, or patients. The function can be disrupted temporarily but must be reestablished within 24 to 48 hours.
- **Category 3:** Contractually required processes with vendors, employees, or patients, both external and internal, that could cause a minor negative impact if suspended or delayed. These processes may be disrupted temporarily or suspended during an emergency and resumed as soon as possible.

Once the identification and categorization of processes occurs, the next step is determining the necessary resources to carry out each process. This would include memorandums of understanding with all partners, third parties and suppliers, which should include any special skills required to perform functions and associated dependencies. Determination of the number of personnel trained and qualified in each service will help to reallocate resources more easily. An organizational matrix that details the skill sets required for all essential roles will ensure that they remain filled. Maintaining an updated record of employee-related information such as licenses and certifications and completed training will allow facilities to fill essential roles and facilitate demobilization of workers within the organization as needs arise.

Auditors should validate the following:

- Regular, transparent communications occur that reassure employees and align with current communication protocols.
- Monitoring of state and federal initiatives of support occurs, such as 1135 waivers and the Coronavirus Aid, Relief, and Economic Security (CARES) Act, including completion of all documentation requirements.
- Determinations of how the event affects budgets and business plans to assess financial and operational risks, including the evaluation of short-term liquidity (e.g., terms and conditions on loans and contracts with creditors and investors).
- Legal teams have been consulted for advice on potential liabilities and risk mitigation.
- Business continuity plans are reviewed and updated by department or service.
- Memorandums of understanding are utilized with community, state, and local authorities and vendors.
- Contact continues with suppliers regarding ability to accommodate supply chain needs, the reset of business assumptions and updates to memorandums of understanding, as necessary.
- The organization is keeping recovery in mind as decision-making and actions are taking place during the crisis.

- Continuous monitoring and subsequent execution of strategy revisions are occurring during the emergency.

Conclusion

One of the biggest lessons learned from the current COVID-19 pandemic has been the importance of an all-hazards approach to Emergency Management. This begins with accurately assessing risks through the annual HVA assessment (to identify the top five to 10 hazards); updating the EOP and ancillary plans to address the top hazards and to include simultaneous events; creating, reviewing, and updating the supply chain and demobilization plans; and implementing a comprehensive strategy for recovery to include BIAs and BCPs. Organizations today have realized the importance of being continually prepared for any potential emergency scenario.

About the Authors

Radgia Cook is Protiviti's Global Quality and Safety Leader, with over 18 years of experience spanning both information technology and healthcare as an operations management leader and adviser. Ms. Cook excels at identifying and analyzing current industry trends and leading excellence and process engineering initiatives, instilling operational and organizational excellence, and directing regulatory compliance and advisory engagements across the healthcare landscape. She has developed compliance software applications, implemented IT strategies, and built cross-functional teams. Her areas of expertise include program and operations management, advisory and strategic services for TJC regulatory accreditation, integrations and implementations, and medical device. Ms. Cook is an accreditation and regulatory compliance expert.

Lauren DeBree is an Associate Director in Protiviti's Dallas office and has more than 15 years of consulting, compliance, internal audit, and operations experience. Ms. DeBree works with numerous healthcare providers to assess and improve processes to achieve desired outcomes. In addition to her internal audit and consulting experience, Ms. DeBree worked as a Revenue Cycle Manager for a multi-hospital healthcare system, advancing processes and achieving success in key revenue cycle areas.

protiviti®

About AHIA

Assoc. of Healthcare Internal Auditors

About AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services.

Interested? Contact a member of the AHIA White Paper Subcommittee.

Subcommittee

Alan Henton, White Paper Chair
alan.p.henton@vumc.org

Linda Greer
lamizgre512@gmail.com

Debi Weatherford
debi.weatherford@piedmont.org

Laura L. Sak-Castellano
Laura.Sak-Castellano@aah.org

Deborah Pazourek, AHIA Board Liaison
Deborah.L.Pazourek@medstar.net