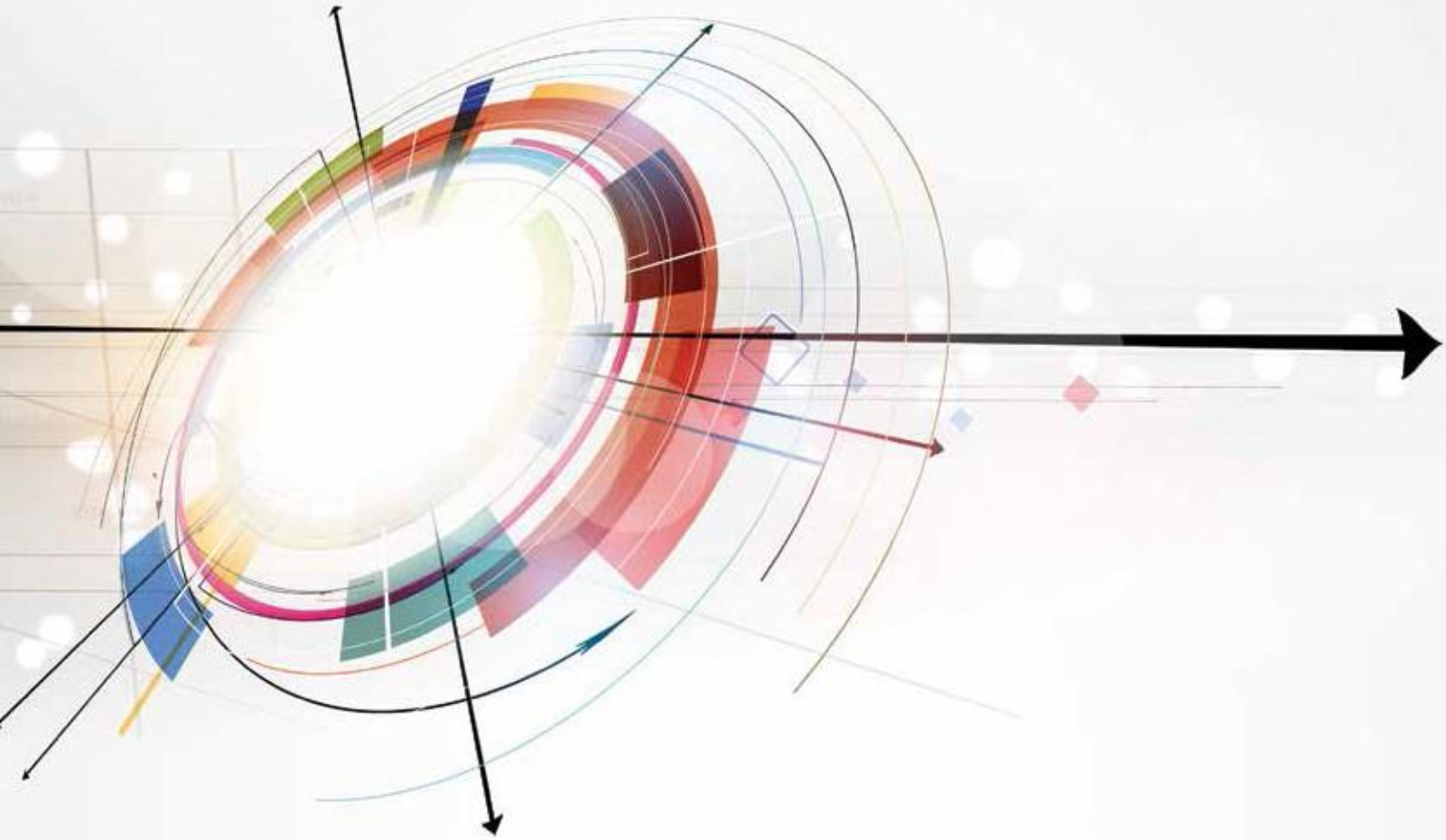


Issue 7

GLOBAL PERSPECTIVES AND INSIGHTS:

Crisis Resilience

The Institute of Internal Auditors | Global

Contributors

Melissa Agnes
Co-founder, Agnes + Day – *Canada*

James Lukaszewski
President, The Lukaszewski Group Division, Risdall – *United States*

Héctor Ricardo Parra, CIA, CRMA, CISA, CFE
Manager, CYA Consulting and Auditing – *Colombia*

John Rapa
President and CEO, Tellefsen and Company, LLC – *United States*

Advisory Council

Previous Issues

To access previous issues of Global Perspectives and Insights, visit www.theiia.org/gpi.

Reader Feedback

Send questions or comments to **globalperspectives@theiia.org.**

Contents

Internal Audit and Crisis Resilience

The possibility of a crisis severely disrupting an organization's ability to operate looms today like never before, given the pace with which global threats evolve. Incidents of sophisticated cyber sabotage, volatile weather patterns, terrorism attacks, and labor disruptions are escalating, and can strike, obviously, without warning. With these crisis events and the inability to continue operations and meet objectives comes damage to an organization's reputation and its ability to meet stakeholder expectations.

Yet a recent study reveals a broad gap between board members' awareness of potential crises and their organizations' actual crisis readiness. Being able to recognize potential crises, effectively handle such interruptions, and return to normal operations is extremely difficult. Gaining the capacity to do this quickly and efficiently with the minimum amount of impact — to be crisis resilient — is that much harder, and the ultimate goal.

Crisis experts agree the key to being crisis resilient is preparation and that internal audit is positioned to play a key role in the process. Auditors' breadth of skills, position in the organization, and deep knowledge of operations can help their businesses prepare for the inevitable crisis and move the organization from crisis aware to crisis resilient — ready to resist, react to, and recover from major disruptive events.

Crisis experts agree the key to being crisis resilient is preparation and that internal audit is positioned to play a key role in the process.

A Crisis of Confidence Revealed

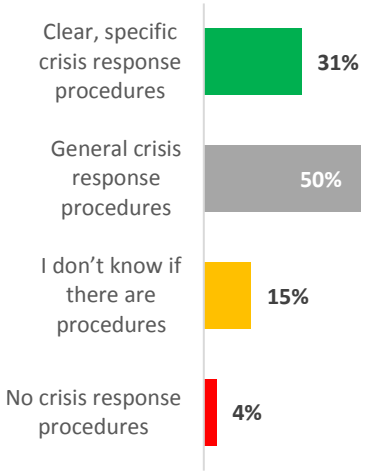
Through a 2016 joint study by Deloitte Touche Tohmatsu Limited and Forbes Insights of more than 300 board members from across the globe, Deloitte gained key insight into the confidence boards have in their organizations' awareness of crisis-level threats and ability to deal with them.

More than three quarters of surveyed board members (76 percent) believe that their organizations would respond effectively to a crisis tomorrow, according to the survey report. Yet less than half said their companies monitor for troubles ahead or have "playbooks" for likely crisis scenarios (49 percent each). One-third don't even know if they have a playbook.

Only half of the respondents said they have had specific discussions with management about crisis prevention, or have engaged with management to understand what has been done to support crisis preparedness. When it comes to specific crises, the survey uncovered steep gaps between recognition and readiness. For example, the crisis area that makes board members feel the most vulnerable is corporate reputation (73 percent), yet only 39 percent said they had a plan to address it. Of those who had endured a crisis, less than one-third (30 percent) felt they recovered their reputation in less than a year — 16 percent said it took four years or more.

This lack of crisis readiness was confirmed in a recent IIA poll. Among nearly 1,500 internal audit professionals participating in a crisis risk webinar, less

Exhibit 1: Crisis Response Procedures



Source: Polling question from February 2017 IIA North America webinar titled Crisis-Proofing Your Organization. Question: How would you describe your organization's crisis response procedures? Internal auditor respondents only. *n* = 1,467.

than a third (31 percent) said their organization has "clear, specific crisis response procedures." Four percent had no crisis response procedures, half had general crisis response procedures, and a worrisome 15 percent did not know if procedures exist (Exhibit 1).

These studies point to the fact that there is plenty of room for improvement when it comes to handling crises. "Organizations can make very tangible, measurable investments in the planning and exercises that turn crisis awareness into crisis resilience," Deloitte said in its report. "And they can also make investments that help them anticipate adverse events before they blossom into full-blown crises."

John Rapa, president and CEO of Tellefsen and Company LLC, sees internal audit as a key stakeholder in crisis planning — a valuable "voice of reason" for the plan's strategy, tactics, scope, assumptions, and constraints.

"Internal audit should be a sounding board to those responsible for plan development, implementation, and maintenance," Rapa said. "Auditors should have a consultative role and provide assurance oversight in plan preparation, to add value and improve the effectiveness of risk management oversight."

Why Resilience?

Internal auditors are aware of the many different concepts and documents within an organization that address unexpected interruptions, such as crisis management, business continuity management, incident response, disaster recovery, and IT service continuity management. Internal audit often participates in the development of these plans. But many of these documents are specific to a segment of the business: business continuity management is based more on maintaining the value of the business. A component of that is crisis management, a process for restoring operations.

However, a crisis can involve much more than getting the business going again, when lives are lost, a product is contaminated, customers' personal data is stolen, or a CEO is humiliated.

Internal auditors are positioned to expand their roles related to crises, to step back and consider the big picture — the broad organizational objectives and risks to them. They can help prepare their boards, executives, and employees for a crisis, provide assurance over readiness, and help instill a crisis-resilient culture.

Multiple concepts and definitions for crisis situations and the confusion that unclear terminology can cause in an incident response was recognized as a problem by thought leader DRI International. Its solution was the creation of *The International Glossary for Resilience*. DRI first compiled the terms used in crises relating to business continuity, disaster recovery, or risk management. After sorting 2,189 unique terms to the most applicable, then vetting the list

through a selection committee, it published in one document the more than 250 best definitions from 26 industry sources.

Resilience is defined in the Glossary as "the adaptive capacity of an organization in a complex and changing environment," credited to ASIS International, a global community of security practitioners. The main definition is followed by a.) the organization's ability "to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event" and b.) the "capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must."

The poetic vision of degrading gracefully during a crisis is the driving force behind the work of crisis experts such as Melissa Agnes and James Lukaszewski. Both think thorough preparation and the role-playing of scenarios are the best ways to ease through a crisis.

"Crises are show-stopping, people-stopping, product-stopping, reputation-redefining events that create victims and/or explosive visibility," said Lukaszewski, an author, speaker, and crisis management consultant. The key to survival, he said, is to work with leadership to develop plans that manage the first minutes and hours of a crisis, that reflect fundamentally sound thinking, and understand the power of victims.

Agnes, an international crisis management strategist and speaker, recommends her clients practice crisis scenarios to assure they have the "right internal escalation processes, the right people in the room to make decisions, and the readiness to communicate."

Resist

A crisis can be defined simply as when risk becomes reality, according to Colombia-based consultant Hector Parra. "Since every corporation exists to satisfy the stakeholders' needs, it seeks to accomplish objectives related to strategy, operations, information, and compliance. As the objectives are all in the future, there is uncertainty, and accomplishing the objectives could be affected by risks," Parra said. "So we can say that a crisis is a strong risk materialization."

The first step in trying to prevent risks from materializing into a crisis is identifying what those risks are.

Strategist Agnes counsels her clients about how to see crisis coming. "One approach is to ask management the concerns that are most worrisome. The top five or 10 high-risk scenarios is a good place to start because it gives you direction," she said. "Once you've identified the risks, you can do a deep dive. Talk to all members of management to understand their perspective. Going through the motions of your top high-risk scenarios is really best practice for preparedness."

Prepare Organization for Different Crisis Scenarios

Melissa Agnes advises clients to think through crisis scenarios for the organization's highest risks and capture the nuances from one crisis to another. Steps to take include:

- Determine the governance structure for crisis management in each scenario.
- Identify the crisis management team for each.
- Assign roles and responsibilities for each department and specific individuals.
- Prepare an internal escalation process.
- Decide who your constituents and key stakeholders are and what their expectations will be.
- Prioritize action items or considerations requiring attention in the first 24 to 48 hours.
- Think through questions you will receive at the onset and the answers you can give.

Lukaszewski, who uses the name "America's Crisis Guru®," agrees. "Successful readiness is always scenario-based," he said. "Failure to practice means responses will also fail."

The resulting plans, which guide both resisting and reacting, can greatly benefit from internal audit's keen eye over the development and execution processes. The experts recommend prioritizing the plan by likelihood of a crisis happening, level of impact, and collateral damage potential.

"Crisis planning should be designed considering the worst scenario, according to the risk ranking and using a top-down approach, from the extreme risks to the low ones," advised Parra. "Each form of crisis planning should have a particular approach, depending on the case, especially depending on who is affected: employees, communities, customers, shareholders."

"Crisis planning should be designed considering the worst scenario, according to the risk ranking and using a top-down approach, from the extreme risks to the low ones."

— Hector Parra

The action plan should include as many details as you can sort out, such as steps for the first 24 hours, the first 48 hours, proactive statements, reactive responses, roles in pre-identified areas, types of communication, and legal requirements, to name a few. If the plan addresses the worst-case scenarios, it should be adaptable to lesser disasters. The plan should include activation protocols, and provide a reporting method for employees, often best positioned to see the early indicators of a crisis situation.

Testing and Training

Lukaszewski recommends testing the plan so when something actually happens, the organization can more easily shift into response mode. In addition to drills, use coaching and training, right way/wrong way problems, simulation, and tabletop exercises that allow everyone to walk through their roles. After every training, update the plan. "Ask yourself and each participant in the exercise, what do we now know we need to know more about? What else is going to happen because this just happened?" Lukaszewski said.

Training is crucial. For example, when it comes to preventing a cyber crisis, internal audit can reach out to employees and put in a personal light the role they can play, help organize awareness events, and educate staff on best practices regarding changing passwords, using multifactor authentication, and opening unfamiliar emails. Some organizations routinely test employees by sending suspicious emails that if opened result in an instant date for a training session. Trained auditors can better understand about system patches, emphasize how important it is to test IT controls regularly, and learn from available frameworks.

Preparation can be individualized for each scenario, but basic concerns should carry through. "Different crises have different impacts," Agnes said. "What doesn't change is stakeholder expectations and concerns. Make sure you go through an initial list of considerations for what to pay attention to, then work out your responses including any actions that might be different depending on the situation."

Lukaszewski has developed a "readiness equation," and said that three-quarters of "readiness" is having accurate contact information to quickly find "people who can say yes."

"Getting decisions made is one of the biggest barriers to crisis response," he said. The right contact list will take you 75 percent of the way toward removing those barriers. The remaining ingredients, Lukaszewski said, include 15 percent pre-authorization — decisions that can be made in advance, such as securing the purchase order you will need to get cars to move people if the need arises. Eight percent is extensive scenario preparation and testing, and 2 percent is surprise. It's surprise that makes the situation a crisis.

Agnes agrees, and said the plan should provide for having the right people in the room as a way of assuring the right escalation process. "The right internal escalation protocols that get the right people in the room at the right time will allow you to do one of two things: either escalate very quickly when faced with full-fledged crisis, or avoid unnecessary escalation if the situation doesn't require it," she said. The "right people" means having a representative of each business unit, sector, and stakeholder group to allow the situation to be viewed broadly, not just from the perspective of legal, compliance, the CEO, or HR, she said.

> "Getting decisions made is one of the biggest barriers to crisis response."
>
> — James Lukaszewski

Rapa calls this group an Incident Management Team or Crisis Management Team, and also recommends it be cross-functional and cross-domain, including, for example, executive management, operations, technology, legal, media relations, and client relations.

During planning, prepare for situations where the organization itself is not in a crisis but is part of an industry or territory where a crisis is occurring, advised *Internal Auditor* magazine in its April 2017 issue. For example, Ford quickly separated itself from the Volkswagen crisis with a statement about not using defeat devices, wrote J. Michael Jacka. The article, "Resilience Through Crisis," also warns that designated spokespeople must have the right combination of media skills and executive authority, and the plan should include detailed information for contacting the media.

Fully working through a scenario can take months — to build your escalation process, find the gaps, and prepare a full organizationwide reaction. Lukaszewski recommends only planning one or two scenarios a year.

And while a thorough plan will make a big difference, the experts agree there is no one-size-fits-all.

"Attempting to create a crisis or incident management plan that is all encompassing for every perceived or foreseen type of threat is challenging, if not impossible," said Rapa.

Once a preparedness program is created, the next step is to foster a crisis-ready culture that will allow the organization to embrace resilience.

React

By being proactive and understanding the process, internal audit can help the organization develop a level of comfort when crisis occurs that people will understand instead of being worried and defensive.

Internal audit can assure an up-to-date crisis management plan fully addresses the incident and the aftermath, and verify the ability to activate an incident response team. As the crisis unfolds, audit can assess, for example, the scope of the event, the need for third parties, the reputational risk, and the security of an off-site data storage site. Internal audit can work with in-house counsel to verify the legal ramifications, and work with HR to help investigate an employee situation, or determine if qualified personnel will be available to staff an incident. Auditors can help the organization communicate openly and regularly with the public, staff, business partners, and stakeholders.

"What you want is to make risk management, crisis prevention, and crisis response an integral part of the organization through every layer."

— Melissa Agnes

"A successful response team will be deeply engrained in an organization and will help the company identify and understand the risk and enable executive management to make the best decisions to mitigate risk to the company," Rapa said. "Internal audit should have an oversight role in the deployment of a plan that has been vetted by key stakeholders."

When a disaster occurs, the first action is to activate the emergency response, to save lives, and to protect assets, according to Parra. A reaction should be measured in minutes or hours. An important initial step is internal and external communication about what happened and what are the immediate next steps, Parra said. For example, when a bank in Colombia had a system failure affecting online transactions, immediate communication to the customers and authorities, informing about the problem and the remedial actions, avoided a panic, he said.

He advises internal audit to help evaluate the seriousness of a crisis by looking at the impacts to accomplishing objectives, people, reputation, assets including data and information, and to environmental regulations.

Judging the seriousness of the crisis goes back to thought beforehand, Agnes said. By smoothly implementing a well-thought through plan, the organization will help create a crisis-ready culture.

"That means you can't just create a plan and leave it on a shelf. Even if you review it once a month, it's still not enough, because there are constant factors changing in the world that impact us in crisis," she said. "What you want is to make risk management, crisis prevention, and then crisis response an integral part of the organization through every layer. Your team members need to know the plan so well that it becomes instinctive. You want them to know exactly what they are expected to do and what the best course of action is — building muscle memory."

One of the most important aspects of reaction is communication. "Staying

silent is your downfall," Agnes said. "It used to work, but not anymore."

Lukaszewski calls silence the "most corrosive, toxic strategy you can choose." He recommends organizations communicate intentionally, with "candor, openness, and truthfulness." Representatives should be "accessible, responsive, transparent, engaged, and ready to clarify, comment, and correct as needed."

Social media is a great benefit today as crisis teams can send out quick, short messages that show they're actively addressing the problem, Lukaszewski said. He recommends establishing a SMART group: Social, Media, Action/Attack, Response, Team.

"Your goal is to act quickly and effectively. There will be mistakes because it is a crisis. Every day, you'll spend 50 percent of your energy and 25 percent of your resources fixing yesterday's mistakes," Lukaszewski said. "Remember, your response can be technically perfect, but if you bungle the victims and the communications, this is how your response will be remembered. Think quickly, incrementally, and take action. The longer it takes to respond, the more your reputation is being damaged."

He also recommends building a webpage for each scenario that stays dark on the site until it is needed. When activated, it can provide facts and data, Q&As, issues at stake, and interactive features.

"How your company follows the plan will have a direct impact on how management is perceived — both internally by staff and externally by customers, business partners, the media, regulators, etc.," Rapa said. Common sense reactions he recommends include:

- Remain calm.
- Communicate broadly and frequently with all constituents depending on the nature and scope of the incident.
- Follow the plan, but make adjustments as events unfold.
- Follow up. Follow up. Follow up.

Lukaszewski always reminds clients to manage the victim dimension. "Victims need visibility, need to talk," he said. "Smart companies facilitate these conversations. What victims want most is someone to say 'sorry'. Management must set a positive tone."

Recover

Internal audit can help the organization recover from a crisis by evaluating and reporting on the effectiveness of the organization's efforts, assessing such things as the long-term effect on reputation, the process for recovering data, the controls on any third parties used, and the adequacy of resources assigned to response and training.

The Perfect Apology

America's Crisis Guru offers his "Ingredients of a Perfect Apology":

- Verbal or written admission of responsibility for causing pain and suffering.
- Specific recognition and description of damage caused.
- Lessons learned and changes to be made to prevent the situation from happening again.
- Ask for forgiveness.
- Offer of restitution.

Skip even one of these ingredients and your apology will have little credibility.

Source: *Lukaszewski on Crisis Communication: What Your CEO Needs to Know About Reputation Risk and Crisis Management*, Rothstein Associates Inc. Brookfield, CT, © 2013, James E. Lukaszewski

Improve Resilience Plan with a Post-crisis Review

Lessons learned following a crisis can be invaluable to the internal audit function. By incorporating these experiences into the plan, the organization can move even closer to being crisis resilient. Questions John Rapa often asks when things quiet down include:

- How was the incident uncovered?
- Who knew about it first?
- Who were the "first responders" that identified the effect of the disruption?
- How was the response to the incident handled by management? By staff?
- How well and how often did the company communicate with staff, clients, key business constituents, key service providers, regulators, the media?
- Was a post-mortem review conducted as to the root cause, effects, and impacts to the business, as well as lessons learned?
- Was an action plan implemented to address any deficiencies, risks, or additional threats?

Post-crisis actions help the organization in the future improve the crisis resilience plan and should include documentation and application of lessons learned, Parra said. Even incidents that turn out to be insignificant should be written up and the recap stored for future reference.

The recap should include the cause, effect, response, elapsed time to full restoration of services, action items, lessons learned, and more, Rapa said.

"The post-incident review is a place where internal audit should play a major role," Agnes said. "Internal auditors need to assess, review, and improve. Again, sit down with the right people in the room, take a look at the incident and ask, for example, what could we have been done differently, how do we make sure this incident doesn't happen again, were the action plans and communications useful?" she said. "After the group answers the questions, discuss, evaluate, and then improve. Strengthen the plans and test them again with a simulation."

When internal audit plays an influential role in implementing lessons learned — both within the organization and in the audit plan — it provides an opportunity to move from a supportive to a front-seat role in the organization.

"For auditors who don't feel they have enough of a role, find ways to demonstrate your value and get a seat at that table," Agnes advised. "What committees meet on a regular basis where these kinds of things are reviewed? What committees already exist where members are talking about some form of crisis, prevention management, and preparedness? If you have a seat, then audit will have a say and input on the day-to-day programs that go on."

Closing Thoughts

"Your response will be criticized by people who weren't there, quoting people who weren't there either," Lukaszewski said. "Stay focused on resolving the most important issues."

He advises his clients to continuously evaluate vulnerabilities, manage exposure, and routinely brief management and the board on threats.

A simple terminology change can make the process easier. "The word *crisis* irritates leadership, because few, if any, leaders believe that a crisis will ever happen to them," Lukaszewski said. "*Readiness* helps them better understand what they need to do."

Agnes says it sounds cliché, but the best form of crisis management is crisis prevention. "Identify top risks and put in place measures to prevent the preventable, clearly," Agnes said, "but then assure measures for effective management of the unpreventable."

Even given the complex and changing environment that is a crisis, an organization can be adaptive, resist being affected, return to normal quickly,

maintain its functions and structures, and degrade gracefully. With key issues identified; scenarios actualized; website pages developed; messages structured and sequenced; and a plan installed, tested, and updated regularly, internal audit can help leadership to not only be ready for a crisis, but the whole organization to become crisis resilient.

Characteristics of a Crisis Resilient Organization

- A senior person is responsible for crisis resiliency.
    - There is a designated chain of authority for decision-making in the event of a crisis.
    - There is an up-to-date communication and response tree to manage any crisis.
- A crisis resilience plan is in place which:
    - Includes all key business functions.
    - Identifies all key stakeholders (internal and external) and methods for communicating status as the crisis is managed.
    - Identifies key risk scenarios and specific response procedures.
    - Includes a disaster recovery component related to IT operations.
    - Is communicated and understood throughout the organization.
    - Is tested on a regular basis.
        - Following periodic testing, results are shared and corrective action steps are developed.
    - Provides procedures for post-crisis review and implementation of lessons learned.
- Periodic risk assessments are conducted; the crisis plan is revised based on a changing risk environment.
- A designated backup facility is ready and available in the event of loss of physical location or the capacity to store data securely.
- Internal audit has a seat at the table in providing input, assessing risk, and periodically testing the crisis resilience plan.

For More Information

Internal Auditor magazine, "Resilience Through Crisis," J. Michael Jacka, April 2017 (*www.theiia.org*)

Deloitte, "A Crisis of Confidence," 2016 (*www.deloitte.com*)

DRI International, *International Glossary for Resilience* (*www.drii.org*)

The IIA Practice Guide: Business Continuity Management (*www.theiia.org*)

"The Security Intelligence Center – Next Steps: Beyond Response to Anticipation," Internal Audit Foundation and Crowe Horwath (*www.theiia.org*)

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The opinions expressed in Global Perspectives and Insights are not necessarily those of the individual contributors or of the contributors' employers.

Copyright