

REMEDY

WHITE PAPER

Crisis Response System

*An Innovative Solution for Protecting Your People
and Critical Infrastructure*

Table of Contents

Executive Summary 1

The Importance and Complexity of Effective Crisis Management 2

Automation Strengthens Crisis Management Efforts 3

Selecting the Right Crisis Management System. 4

Support for all Four Phases of Crisis Management 4

Immediate Emergency Notification 4

Immediate Information Dissemination 4

Workflow Automation. 5

Integration with Emergency Information Centers 5

On-the-Fly Process Modification 5

Integration with Internal Business and Process Systems 5

An Underlying Architecture that Supports Scalability and Performance 6

Remedy Crisis Response System 6

Solution Overview 6

Command and Control Console 6

Issue Tracking 7

Communication and Coordination. 7

Readiness Support. 7

Integration with Internal and External Systems 7

Conclusion 8

Executive Summary

In recent years, events ranging from natural disasters and industrial accidents to the Oklahoma City bombing and the attacks on the Pentagon and World Trade Center have taken a significant toll on organizations of all types and sizes. These include businesses, community organizations, educational institutions, and government agencies. Hurricane Andrew, for example, resulted in approximately \$18 billion in losses in 1992 and the Northridge Earthquake in 1994 resulted in approximately \$15 billion in losses.

Catastrophes and terrorist attacks highlight the need for businesses, community organizations, and federal, state, and local governments to be able to respond quickly and effectively to unexpected events and situations. Each organization must maintain an appropriate level of security, protection, and safety for its people, as well as for corporate and public infrastructure, such as buildings, information technology (IT) resources, information and knowledge in databases, telephones, and transportation assets. Moreover, organizations in both the public and private sectors need to integrate their approaches so they can coordinate their efforts, collaborating seamlessly across organizational boundaries.

Events of the past few years have brought about a heightened awareness of the need for clearly defined, effective crisis management procedures. As a result, crisis management is becoming a top priority across organizations of all types—public and private, large and small. Crisis management encompasses the activities that enable a business or government agency to plan for, respond to, and recover from an event. A comprehensive crisis management strategy prepares an organization for all types of crises, including natural disasters, hazardous materials incidents, terrorism, security breaches, cyberterrorism, civil disturbances, and human error.

Organizations that do not have a well-defined crisis management strategy need to develop such a strategy to ensure appropriate levels of security, protection, and safety. At the same time, organizations that already have a strategy in place need to evaluate its effectiveness in light of recent experiences. These experiences have taught us that even the best laid plans are not sufficient to respond to unforeseen or unprecedented events.

Technology offers organizations new opportunities to enhance their crisis management capabilities. Crisis response resources can greatly improve the ability to plan for, respond to, and recover from a variety of emergencies. As a result, organizations can minimize injuries and loss of life, mitigate damage, and ensure a speedy return to business as usual.

This paper begins by defining crisis management and examining the advantages of an effective crisis management strategy. It then describes the role that technology can play in enhancing crisis management capabilities and identifies requirements for an effective crisis management system. Finally, it introduces the Remedy Crisis Response System, which gives organizations the ability to manage a crisis from initial discovery through closure with all the alerts, notifications, and actions required to deploy and manage the required resources.

The Importance and Complexity of Effective Crisis Management

The Federal Emergency Management Agency (FEMA) defines an emergency (or crisis) as “any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility’s financial standing or public image.”

Organizations can limit injuries and damages and return to normal operations more quickly by implementing a well-thought-out crisis management strategy. Crisis management involves four major phases: readiness, recognition, response, and recovery (see figure 1).

- The readiness phase involves assessing risks, identifying vulnerabilities, mitigating vulnerabilities and risks, developing contingency plans, documenting procedures for the most likely emergency situations, establishing interactions that need to take place among organizations and agencies, training, testing preparedness, and continuously refining policies and procedures. Readiness also includes positioning critical resources for the time of need.

- The recognition phase allows you to identify when your organization is threatened and is accomplished by regularly monitoring events. Threats can exist both within your organization and external to your organization. External threats can come from multiple sources (e.g. suppliers, partners, customers, outside agencies) and often require joint collaboration in order to effectively assess the impact to your organization.
- The response phase involves deploying the crisis response team, establishing a command and control structure, providing team members information and guidance on what critical tasks need to be accomplished, maintaining information flow between team members and managing the crisis through resolution. The goal of this phase is to establish continuity of operations (COOP) or business continuity.
- The recovery phase includes necessary activities required to restore capabilities to normal operations. Organizations today are driven to implement a crisis management strategy for a variety of reasons. Not only is it the right thing to do, it is also the smart thing to do from a business perspective. An effective crisis management strategy limits personal injuries and saves lives, minimizes property damage and financial loss, significantly reduces liability, and allows faster return to normal business operations.

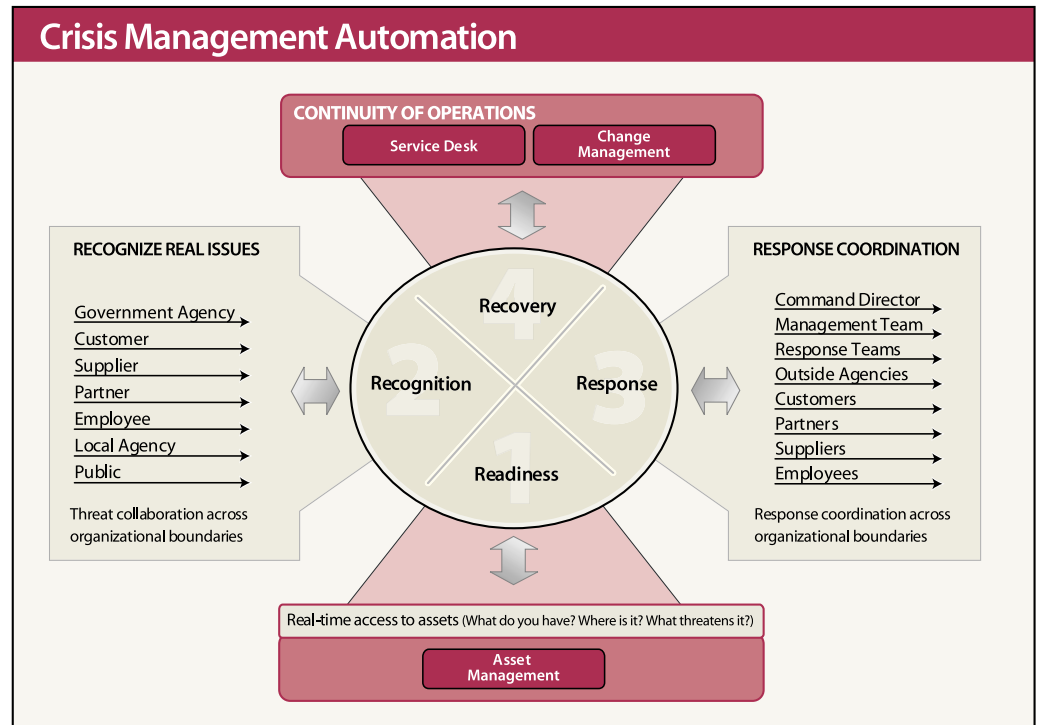


Figure 1.

Automation Strengthens Crisis Management Efforts

Because of the complexity of crisis management and the uncertainty that accompanies unplanned events, developing a strategy for effective crisis management is a challenge. Organizations are made up of complex infrastructures and multifaceted interrelationships among people, places, and things. In the event of a crisis, the organization must coordinate activities not only internally, but also with multiple external organizations—customers, government agencies, suppliers and business partners, media, and other public notification organizations, emergency organizations, and police and fire departments.

Crises can involve unexpected and unprecedented events, such as the September 11, 2001 terrorist attacks and ensuing anthrax attacks. Fortunately, organizations can dramatically improve their ability to respond to crises, even unexpected ones, through the use of technology. There are various software tools available that can significantly enhance crisis management processes:

- Communication and collaboration tools allow widely dispersed teams to communicate and collaborate in developing, documenting, testing, and executing response and recovery procedures for various types of crises. These tools can also allow processes to interact with each other, triggering events automatically without the need for human intervention.
- Information management tools make a variety of up-to-the-minute information immediately available to crisis management teams at any time from anywhere. As a result, response and recovery personnel have access to infrastructure information, organizational information, knowledge bases, possible crisis scenarios, and response and recovery procedures and checklists.
- Automatic notification tools immediately alert the right people at the right time through a variety of means, including telephone, pager, and e-mail.
- Activity management tools such as workflow automation and monitoring, status checking, and escalations enable management as well as response and recovery personnel to keep tabs on the situation for more effective control.

These tools can help throughout all four phases of crisis management. In the readiness and recognition phases, information management tools can help organizations assess the impact of possible crises. The crisis management staff can determine what assets the organization owns, along with the associated replacement costs. Management can examine the role of the individual assets in the company's business and make determinations of impact and priority. The tools also help the crisis management staff in conducting drills to identify vulnerabilities and test readiness.

In the crisis response phase, notification tools speed deployment of response teams and permit immediate, simultaneous notification of team members, management, and other affected individuals using multiple communications media. Information management tools facilitate crisis assessment as well, providing information such as the location of critical assets. These tools make essential information instantly available to everyone involved. Response teams can access procedures and checklists to speed execution of response tasks. Information can be accessed from anywhere at any time through the Web—from both wired and wireless devices. Activity management tools allow response teams, management, and even appropriate external organizations to monitor activities and ensure that escalations occur if procedures are not being followed in a timely, coordinated way. These tools also help crisis management personnel identify when COOP is achieved.

In the recovery phase, automatic notifications can alert management and others when it is time to commence recovery—triggering the deployment of recovery teams. Information management tools help recovery personnel determine what assets must be replaced to return to normal operations. Communication and collaboration tools enhance coordination and communication among team members and enable rapid development of an appropriate recovery plan. Activity management tools provide monitoring and status reporting capabilities to keep the recovery team, management, and other stakeholders up-to-date on recovery progress. They also help with assessing response and recovery processes and with calculating costs associated with the response.

Selecting the Right Crisis Management System

To be effective, a crisis management system should offer a variety of features and rich functionality. The following characteristics can serve as criteria for comparing competing offerings, enabling organizations to identify the solution that will deliver the most value:

- Support for all four phases of crisis management
- Immediate emergency notification
- Immediate information dissemination
- Workflow automation
- Integration with emergency information centers—both inside and outside the organization
- On-the-fly process modification
- Integration with internal business and process systems
- An underlying architecture that supports scalability and performance

Support for all Four Phases of Crisis Management

Developing and maintaining a crisis management strategy is an ongoing and iterative process that spans all four phases of crisis management. Information collected during the recovery and response phases feeds back into readiness activities to enable continuous improvement of the organization's capabilities.

Because of this tight relationship across phases, it is essential that the software support all aspects of crisis management, including:

- Assessing risk, creating policies and procedures, and testing the strategy.
- Entering and classifying possible crises.
- Establishing a command and control structure.
- Sending alerts and notifications.
- Tracking crisis response activities.
- Identifying when COOP or business continuity is in place.
- Initiating recovery procedures.
- Tracking recovery through to completion.
- Auditing and reporting on the effectiveness of response and recovery procedures for continuous improvement.

Immediate Emergency Notification

Every second counts in those critical first few minutes of a crisis. Slow response can result in an out-of-control situation that increases injuries, loss of life, and monetary losses. Many notifications must be sent out to a wide variety of recipients. Normal communications devices, such as telephones and cellular phones may not be available, so multiple, alternative communications methods must be accessible. Manual notification processes—such as placing phone calls, paging, and other traditional means of contacting response team members, management, and other impacted parties—are slow. Moreover, they're error prone, so important recipients could easily be missed.

Rapid response, on the other hand, can bring a crisis under control and minimize disruption to the business. Crisis response software that automates the alert and notification process through a variety of methods dramatically accelerates response time. This simultaneous notification ensures that response teams are deployed in a timely manner and that all the right people arrive on the scene promptly. Evacuations can be carried out more quickly and employees can be notified to stay away from dangerous areas. This can translate into saving lives and reducing potential damage.

The software should also track responses to notifications to ensure the response team is assembled and that backups are contacted for any response team members who are unavailable. Escalation rules must be in effect and managed automatically in case key individuals are not available.

Immediate Information Dissemination

The software must provide tools that permit easy dissemination of accurate and complete information about how to handle the emergency, including:

- Evacuation plans.
- Fire protection plans.
- Security procedures.
- Plant closing policies.
- Hazardous material planning.

This ensures that all affected personnel have the information they need to maintain their safety. It also ensures that corporate communications and legal personnel have the information they need to brief all stakeholders and to keep employees, next of kin, partners, suppliers, customers, community organizations, government agencies, and the media informed throughout crisis response and recovery. Ideally, the software should enforce different levels of access privileges so that each person receives information appropriate to their role. This capability also ensures that information can be distributed to external organizations, such as the media, in a controlled manner.

A system that provides these capabilities eases employee fears and eliminates confusion. It helps employees determine what they should and should not do and informs them when it is safe to return to work. It also ensures that top management has the information required to make critical decisions related to resource allocation and problem resolution, saving even more lives.

Workflow Automation

When emergencies are reported, the person reporting the problem may be under duress. Information supplied may be vague, incomplete, or inaccurate. It is imperative that processes be initiated quickly and monitored to ensure successful completion, despite the lack of full details about the emergency. Software that offers proactive workflow is highly effective at extracting relevant information—often more so than human beings. Workflow automation capabilities can take over, assigning the proper priority and initiating the appropriate emergency response. This ensures that nothing “falls through the cracks.” Workflow automation supports the dissemination of emergency information, requests, workflows, and accelerations throughout the organization. It allows for escalating the level of a crisis as new information is gathered, enhancing the ability of the response team to bring about a successful end to the crisis.

Integration with Emergency Information Centers

Depending on the crisis, external agencies may provide the most up-to-date information about the event and may be the source of the original emergency notification. To leverage these external resources, the software

should support real time links to groups such as local emergency planning committees, fire and police, National Weather Service, FEMA, the American Red Cross, civil defense agencies, and other entities. This type of integration is vital to obtaining reliable, timely information.

Ideally, the level of integration should enable multiple businesses, government agencies, and other organizations to work through a single command, control, and communications center. This center should consolidate all the tools that the crisis management and crisis response personnel need to identify what is happening and to assimilate confusing and hastily acquired information. Integration should be tailored based on relationships and roles in the organization, from executive decision making to support personnel and the general workforce.

On-the-Fly Process Modification

During a crisis, many events are unexpected and cannot be planned for. To handle the dynamic nature of a crisis, crisis response teams need to be able to perform rapid, on-the-fly emergency process modification. This capability is vital to saving lives and restoring services, as well as getting the organization back to work. As a result, the software should be highly adaptable, enabling all authorized users—not just technical personnel—to modify procedures and apply them in real time. For example, if an unplanned event occurs and no response procedure has been defined, it should be easy to start with a procedure for an event that closely matches the current one, and then quickly adapt that procedure to accommodate the specifics of the new situation.

Integration with Internal Business and Process Systems

Accurate and timely information is essential to bringing crises under control. As a result, crisis response software must integrate with a variety of internal systems. An organization’s fire response or burglar alarm system may generate events on its own. Integration between the crisis response software and these systems enables the events to be passed directly to a crisis management operator who can then evaluate and classify the events. Integration with asset management systems helps the recovery team determine what assets are affected and the cost of replacing those assets.

An Underlying Architecture that Supports Scalability and Performance

A software solution capable of standing up to the demands of a crisis must have several additional characteristics. It must be robust both in terms of scalability in handling the volume of interaction generated by a crisis and in terms of availability during a crisis. Built-in redundancy is essential to ensuring access and continuity even if there is an impact to the system. It must be both light and reactive during a crisis. Additionally, it should not require the entry of large volumes of data to identify the crisis or to indicate that an activity has been completed.

During a crisis, the volume of information is likely to be high and a number of interactions must occur in a very compressed timeframe. As a result, the system must be capable of handling many interactions across many different environments quickly and efficiently. For example, it must be able to deliver a high volume of messages swiftly and accurately using a variety of mechanisms. This ensures that appropriate actions can be taken in a timely manner. A bottleneck within the tracking or communication of issues would seriously hinder crisis resolution.

Remedy Crisis Response System

Remedy is adapting its platform technologies and software solutions to help public and private sector organizations prepare for, respond to, and recover from unexpected events ranging from acts of terrorism to natural disasters. With its breadth and depth of technology platforms and software solutions, Remedy has gained considerable expertise in developing software with advanced tracking, notification, escalation, approval, impact analysis, and other functions that are directly applicable to the needs of crisis management and response.

Remedy's Crisis Response System provides government agencies and businesses with a solution designed to bolster preparedness and improve the ability to protect people and critical assets during a crisis. The Crisis Response System provides an environment and infrastructure to allow for crisis planning and preparation within an organization. Furthermore, it gives organizations the ability to manage a crisis from initial discovery through closure, with all the alerts, notifications, and actions required to harness the necessary resources. It offers real-time views of information, details of the current status of activities, and the ability to trigger actions that need to be performed. The Crisis Response System connects to disparate data-

bases and applications within agencies and companies, and among agencies and companies, providing a unified view of data and status, coupled with coordinated and consolidated action.

The Crisis Response System offers numerous benefits:

- Faster response to a crisis
- Effective communication between response teams and impacted groups
- Effective coordination of response teams
- Faster recovery time
- Reduced liability exposure due to negligence
- Better use of all assets, including people, equipment, and property

Solution Overview

The Crisis Response System is built on the Action Request System® (AR System®). This Web-optimized development environment delivers superior workflow capabilities, giving organizations the ultimate flexibility in building and running powerful, easy-to-use, global applications. Remedy has built complete business solutions on the AR System, including help desk, IT system management, and customer support solutions. In addition, Remedy customers have implemented a wide variety of specialized enterprise applications that leverage the advanced workflow capabilities of the AR System.

The Crisis Response System components include a command and control console, issue tracking, communication and coordination, planning and preparedness support, and integration with internal and external systems.

Command and Control Console

The command and control console provides a single point of contact and control for the Crisis Response System users. It encompasses a system of prioritization, standard response strategies for classes of crises, and robust methods for mapping a nonstandard crisis into existing procedures. Crisis management personnel use the console to gain visibility and insight into the status of activities required to respond to the crisis and reach COOP. Key metrics are presented graphically, dynamically, and in real time through easy-to-read color-coded graphs, charts, and meters. An organization can set thresholds that trigger warnings and notifications when procedures are not being followed properly and in a timely manner.

The console is accessible through a Windows client or Web browser, enabling people to monitor important processes and identify issues at a glance, at any time and from any location. Response team members and management use the console to navigate effectively through to a successful conclusion to the crisis.

Issue Tracking

The system provides a means for entering the initial crisis report and classifying the crisis. Information can be entered and updated through the Web using traditional desktop and laptop computers as well as wireless devices such as Wireless Access Protocol (WAP)-enabled phones and personal digital assistants (PDAs) running Palm and Windows CE operating systems.

Reporting and classification trigger a chain of automatic processes based on the procedures identified for that classification. Alerts are routed to the appropriate people by e-mail, pager, phone, and other means defined in the procedure. Internally, this includes response team members, management, and legal and public relations departments. Externally, notifications go to such entities as the police, fire department, Center for Disease Control, and the American Red Cross, as appropriate. If team members do not respond within specified time frames, backup personnel are notified. For example, an explosion in a manufacturing plant would trigger notifications to the response team, plant manager, fire and police, and the appropriate local disaster assistance agency. Depending on the rules defined by the crisis management staff, the Crisis Response System might also trigger notifications to corporate legal and public relations departments as well as to a sister plant that needs to cover the loss of production capacity in the affected plant.

The Crisis Response System provides an easy means for response team members to log completed activities, enabling everyone involved to understand:

- What is currently being done.
- What has been completed.
- What still needs to be done and in what order.

The system provides full audit trails of all activities that take place during the response to a crisis. As a result, the organization has a log of the actions taken and a timeline for those actions. These logs provide a record

of what happened, who responded, and when. Crisis management personnel can use the logs to review and improve procedures for the future.

Communication and Coordination

The Crisis Response System facilitates communication and coordination among all parties involved. People have immediate access to appropriate procedures, the location of critical resources, up-to-the-minute information on current status of the response, detailed information on external conditions, who is available, where they are, what they can do, and the best means of contacting them. The system provides message sharing, bi-directional channels, and flexibility for reactive and proactive notices. As a result, all involved parties can maintain close communication and coordinate their efforts for maximum efficiency.

Readiness Support

The Crisis Response System enhances the readiness phases by providing tools for documenting policies and procedures. It also ensures the rapid retrieval of information regarding preparations and the past/present use of supplies and resources. Furthermore, it supports drills to test readiness and assess the effectiveness of procedures.

Integration with Internal and External Systems

The system integrates with internal and external systems to enhance readiness, recognition, response, and recovery efforts. For example, the Crisis Response System integrates with any applicable internal service desk. It allows items that are reported but do not meet the criteria to be classified as a crisis to be sent to other systems for normal processing.

During the recovery phase, the Crisis Response System can hook into these internal and external systems to initiate activity using normal business processes. The Crisis Response System also connects to asset management systems for the discovery and status of many categories of assets. As a result, organizations can automatically determine what assets will be required to return to normal operations. Finally, integration with outside organizations and government agencies enables the organization to obtain accurate, up-to-date information through Crisis Response System to enhance the ability to respond to and recover from the event.

Conclusion

The need for a comprehensive crisis management system is rapidly becoming a top priority across government agencies and businesses. The good news is that technology offers organizations fresh opportunities to develop or strengthen their crisis management capabilities. Crisis response software can greatly enhance the ability to plan for, respond to, and recover from a variety of emergencies. Consequently, organizations can minimize injuries and loss of life, mitigate damage, and ensure a speedy return to business as usual.

The Crisis Response System, built on the AR System development platform, provides the underlying technology for a command and control system to help ensure immediate response to crisis situations. The Crisis Response System product components also include issue tracking, communication and coordination, readiness support, and integration with internal and external systems.

The Crisis Response System product will allow an organization to manage an event from initial discovery through closure, with all the alerts, notifications, and actions required to harness the necessary resources. In addition, it will offer real-time views of information, details of the current status of activity, and the ability to trigger actions.

Finally, the Crisis Response System connects to disparate databases and applications within agencies and companies, and among agencies and companies, providing a unified view of data and status coupled with coordinated and consolidated action. With the Crisis Response System, Remedy continues its long tradition of helping government agencies and businesses manage and protect their people and critical assets.

About Remedy, a BMC Software company

Remedy delivers Service Management software solutions that enable organizations to automate and manage internal and external service and support processes. With more than 7,000 customers worldwide and over 10 years of product development and investment, Remedy, a BMC Software company, delivers out-of-the-box, best-practice applications that help our customers align service and support with business objectives, improve service levels, manage assets, and lower costs. All Remedy applications, including Help Desk, Asset Management, Change Management, Service Level Agreements, and Customer Support, are built on the highly flexible Action Request System, empowering customers to easily adapt their Service Management solution to unique and changing requirements. Remedy. Your Business, Your Way.™

Remedy Headquarters
1030 West Maude Avenue
Sunnyvale, CA 94085 USA

Tel: 408.571.7000
Fax: 408.571.7001
www.remedy.com