



CRISIS MANAGEMENT PREPAREDNESS ASSESSMENT

What Your Financial Organization Needs to Go
From Just a Plan, to an Actionable Program

INTRODUCTION

We live in uncertain times. Organizations face an unprecedented range of threats arising from a confluence of social, cultural, economic and political factors and an ever continuing dependence on technology.

The risks range from long standing scenarios such as extreme weather, major accidents and corporate malfeasance, product malfunctions, to more recent issues such as a social media embarrassment, violent civil disturbances, the increasing number of active shooter incidents and the upswing in cyber-attacks.

The global pandemic, which from March 2020 impacted every facet of daily life, highlighted how even the best organized company can be surprised and unprepared for a massive new issue predicted by few.

Just 62 percent of organizations have a crisis management plan, according to a survey conducted in 2020 by PR News and business continuity consultancy [CS&A](#). Another 13 percent of respondents said they believed a plan existed but they had never seen it.

Of those that said they had a plan, less than half said that it was up-to-date.

At the time of the survey, CS&A senior partner Dirk

Lenaerts observed: “It is striking to see how many companies believe they are prepared to handle a crisis because they have a plan in place, which may or may not be up to date.”

How would your organization fare if it was struck tomorrow by a data hack, an active shooter event, a social media debacle, or any of the many other potential threats? How up-to-date is your crisis management plan and the supporting resources? Is it fully actionable for the right stakeholders connected to your organization?

In the first critical moments of a crisis, an up-to-date, fully actionable program improves your speed of response with the most accurate data to minimize financial impact, maintain business continuity, protect your company's reputation, and in some cases, save lives.

An outdated, ineffective, inaccessible plan leads to confusion, a slow response and endangers your employees, properties, reputation and even the future of the business.

The time to analyze your issues and crisis preparedness is now, *before* the next crisis hits.

By completing an assessment of your response protocols, vulnerabilities, resources, technology and training, you will be equipped to respond quickly and effectively to a fast-moving, modern crisis.

This Guide takes you through a best-practice assessment of your plan, as well as helping measure your updated plan's performance and determine how to best move forward with a full crisis program, to prepare your organization for when the worst happens.



DOES YOUR CURRENT PLAN REQUIRE AN ASSESSMENT?

You may wonder if your plan needs an assessment at this point in time. To find out, think about how your current plan stacks up against best practices for your particular industry. How do corporations similar to your own handle crises? What seems to be working that you have yet to incorporate into your own plan?

RockDove Solutions created a simple 2-minute drill with a series of easy to answer questions to help you assess whether it is time to upgrade your issues and crisis preparedness.

Yes	No	Do you have a crisis plan?
Yes	No	Was the plan updated in the past year?
Yes	No	Could you access the plan from anywhere?
Yes	No	Do you have a team in place to manage a crisis?
Yes	No	Are the contact details for team members up to date?
Yes	No	Has the plan and the team been exercised with a drill in the past year with plausible yet severe scenarios?
Yes	No	Can you quickly activate the team any time of night or day?
Yes	No	Have you identified key risks for your organization?
Yes	No	Do you have a risk intelligence program?
Yes	No	Are the appropriate stakeholders educated and aware?

0~3 IF YOU ANSWERED YES TO THREE OR LESS:

Hope is not a strategy for crisis response! You need to assess your planning immediately or you could suffer a big loss if a crisis hits your organization.

4~6 IF YOU ANSWERED YES TO BETWEEN FOUR AND SIX QUESTIONS:

While you have some protection - you are depending on a big slice of luck as well. Assess your plan and strengthen where necessary.

7~9 IF YOU ANSWERED YES TO BETWEEN SEVEN AND NINE QUESTIONS:


You are likely to be a winner in a crisis - an assessment will identify areas of planning where you still need to tie up loose ends.

10 IF YOU ANSWERED YES TO ALL TEN QUESTIONS:

Congratulations - your plan and preparedness are complete.

HOW TO CONDUCT THE CRISIS PLAN AUDIT

To assess your plan, you will assess its performance in four key areas:

- 
- 🔑 Risk Scenarios
 - 🔑 Technology
 - 🔑 Communication
 - 🔑 Training

1. RISK SCENARIOS

A Risk Assessment helps determine current and potential areas of threat to your organization's business and reputation. Risks evolve over time and new ones appear - such as the pandemic in 2020. Even if you have conducted a Risk Assessment in the past, it may be time to refresh and update it.

Collaborate with colleagues in all parts of the organization, as this will give you a fuller context of the risks. Ask colleagues to identify the threats they worry about most for the entire organization and for their own area of responsibility, whether it be a function or geographic region.

Consider every aspect of the organization to understand what risks are posed by factors such as:

- Potential for natural disasters and extreme weather
- Facilities and locations
- IT network and other technologies and the potential of ransomware and malware
- Stakeholders and their relationship with the organization
- Regulators and policy makers
- Customer loyalty and trust
- Regional politics and culture in areas where there are company locations
- People and workplace culture

Next, review all documents and resources that pertain to crisis preparedness, communication, and response, looking for potential vulnerabilities. Be sure to consider new threats that may have emerged since the documents were written. Examine the content to ensure that it is still relevant based on changes within and outside your organization that might have an impact, such as new leadership, upgraded IT systems, company expansion including acquisitions, environmental conditions and new competitors.

In addition, consider whether your plans addresses, and are consistent with, local or federal codes or regulations that apply to your industry, especially when there have been new laws passed since the plan was last revised.

Also examine what has happened to competitors. What issues and crises have they faced? How successfully did they navigate the threat? What can we learn from their example? What are the issues and threats to our industry as a whole?

2. TECHNOLOGY ASSESSMENT

Next, determine if the appropriate platform and tools are in place to collaborate and respond to an emerging risk or crisis event.

These may include mass notification and risk intelligence systems, messaging apps, social media platforms, email, mobile phones, website file-sharing tools such as Google Drive, and an issue and crisis platform.

Ask yourself the following questions:

- How are crisis plans and/or playbooks stored?
- How are the plans distributed and shared as the event is emerging?
- When the plans are updated, how is the updated content shared with members of the crisis team?
- Is there an emergency mass alert notification system in place?
- Do we have the right level of resources to manage and monitor company and third-party platforms?
- What tools exist to make the crisis plan more dynamic and collaborative, and more of a full-scale crisis program?
- How do we enable effective collaboration among team members?
- How do we keep a record of decisions and actions during the event?
- Are there after action reports that ensure future learning?

If the answers to these questions reveal shortcomings in your crisis response tools and systems, it is time to undertake research on new technologies available for streamlining crisis response, management and preparedness.





3. COMMUNICATION ASSESSMENT

Effective communication can be the difference between quickly resolving a crisis and experiencing a business-changing catastrophe.

A successful crisis communication plan should include the following:

- A simple straightforward response framework
- Clear activation and escalation criteria
- Clearly defined crisis team members and alternates, with full contact details
- Identities and contact details for key stakeholders of the organization
- Well defined and tested communication channels
- Pre-approved and tested crisis communication policies and protocols
- Legally pre-approved templates and messaging

Crisis team members: There should be a process of validating the team members and their contact details on a regular basis, at least quarterly. Inevitably people leave the organization or change roles on a regular basis, so updates are required more frequently than other content in the crisis plan. It is easier and more effective if members of the team are all connected via a mobile crisis app, as then updates are automatically uploaded from a central administrator.

Ability to contact key stakeholders. Take a look at your current plan's stakeholders, and ask yourself whether it reflects your organization as it exists today. Consider all the people you might need to contact during a crisis to lessen its impact and emerge on the other side unscathed. Think beyond your employees and customers to include stakeholders such as the media, investors, government entities, regulators, vendors, sales channel partners, local authorities where you have a company location and anyone else who might be impacted by a particular threat.

Your plan should also define stakeholder "owners": key contacts within your organization who are responsible for providing updates to the tiered stakeholder list and help

manage communications during a crisis response.

Well defined communication channels. Are you leveraging the best methods for communicating within the crisis team, plus internal and external stakeholders during a crisis? Many crisis plans still rely upon emails, manual call trees, and crisis telephone lines for distributing important information during an emergency. These are unreliable, especially outside normal business hours or on public holidays, where key team members may not be carrying or monitoring their business devices. There are some threats, such as an active shooter, which require immediate and effective mass communication to all employees or members of an institution (such as students). How well would your organization be able to deliver such an alert?

Communication policies & protocols: The crisis plan should also address clearly how and when communications should take place. This means that the difference between an issue and a crisis should be defined and the appropriate response protocols agreed beforehand. Clearly, it would be inappropriate to deploy the full crisis team and resources for an event that is a small, manageable threat. Therefore the plan should lay out what constitutes a crisis, how the communications should escalate for more serious threats and who is added to the response team as the crisis gains in seriousness.

Also, determine whether physical systems— including phone lines, websites, and email servers—could handle an uptick in traffic during a crisis. If you use a "ghost" website to serve as a central information clearinghouse for stakeholders to visit during an emergency, be sure it loads quickly and reliably.

Pre-approved templates and messaging: For those early frantic hours of an emerging crisis, it is helpful to create templates and messaging for the highest risk scenarios that you identified during your Risk Assessment. Examples include content for employee announcements, social media notifications and press statements. Templates would cover the basic details of what occurred, how the organization has responded and what steps will be taken in the coming hours. Any of this kind of content in the plan must be pre-approved by Legal, as this will save valuable time and enable a faster, more organized communications response.

4. EDUCATION AND AWARENESS ASSESSMENT

Assess how well your organization is coaching and preparing the crisis team members to fulfil their individual duties to effectively and quickly deploy the crisis program and the supporting technology when the worst happens.

- Are people aware of their responsibilities?
- Do they understand the supporting technology?

Leading practices suggest running a training drill at least annually in which a plausible and severe threat scenario is presented to the team and they are asked to respond and make decisions as they would in a real situation.

As well as giving the team an opportunity to learn the ropes in a safe environment, feedback from observers to the exercise and the team members themselves will help identify and address weaknesses in the steps and protocols laid out in the program.

Team members, and senior executives, who would be expected to handle the media, particularly the broadcast media, during a crisis should undergo additional spokesperson training in how to navigate and effectively deliver a message when the interviewer is adopting an adversarial approach.



UPDATING THE PLAN AND STRENGTHENING THE CRISIS PROGRAM

Once you have completed the assessment of your plan, consider any gaps or limitations that you discovered, and then add updates and changes that will optimize your crisis response. Gaining the input for the draft plan from members of the crisis team, their perspective will help ensure you have addressed all the issues and that each section is clear and actionable in the moment of crisis.

Through revising your plan, leveraging technology, collaborating with and educating your team and conducting exercises, you take your organization from having a crisis plan, to having a crisis management program.



MEASURE PERFORMANCE OF THE IMPROVED PROGRAM

Once the new program is deployed, set aside time to run through the updated documents and protocols to measure their performance. Management Consultants Deloitte developed a complete [crisis management framework](#), specifically for COVID issues that also has a wider application. The framework includes this simple checklist to assess the performance of your new crisis program:

1. Establishes clear ownership and roles, so no key activities are overlooked
2. Ensures all key functions are accounted for in the crisis management response
3. Creates protocols and templates, allowing smoother communication among crisis team members
4. Provides overview of resources and tools needed by the team
5. Identifies others important in the process (i.e. the link between the CMP, the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP))
6. A crisis management battle box provides a central repository for all key documents, tools templates, procedures etc.
7. The entire CMT are able to access the CMP at short notice (Ideally it should be part of the battle box)



STAY VIGILANT

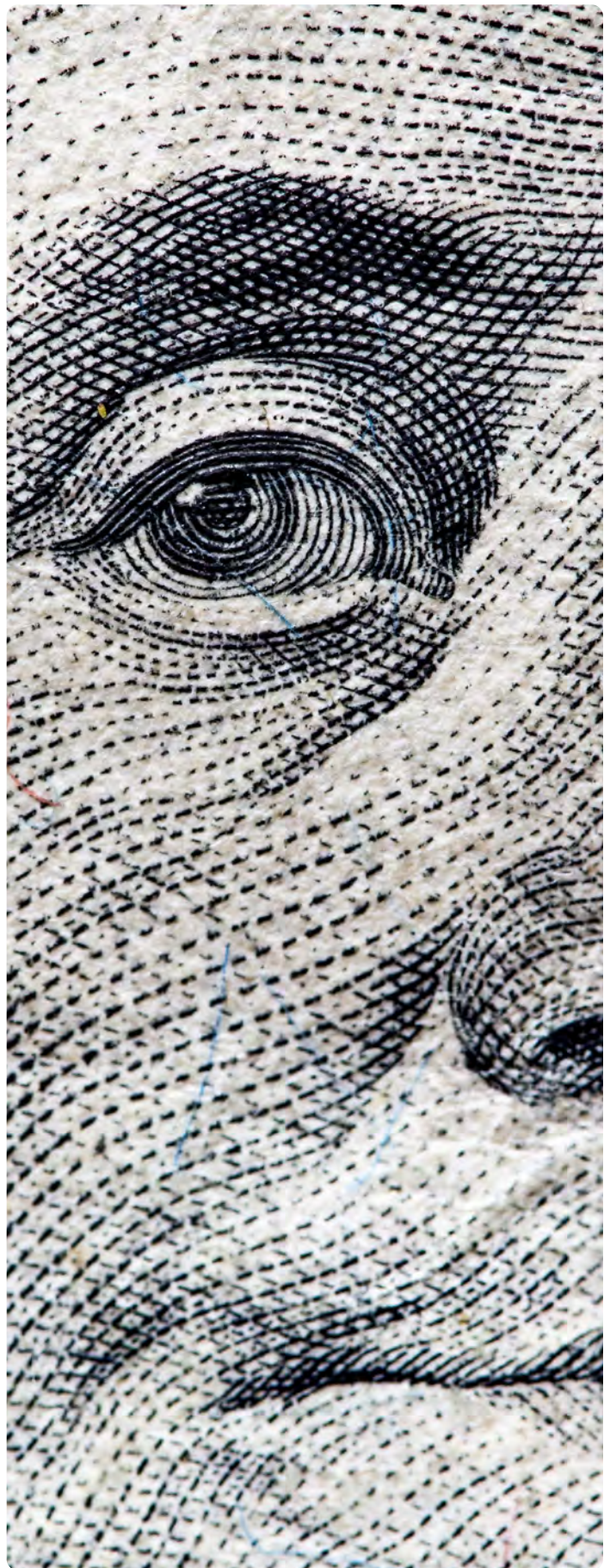
Following the assessment of your plan, and development of your program, it is important to stay vigilant so that your organization is always prepared for a crisis. There are two relatively simple ways to do so - research continually and regroup often.

Research should become a natural part of your daily responsibilities. Monitor social media and collect data continually so that you are always aware of potential threats to your organization.

You also need to be aware of how your organization is being portrayed on social media, the traditional media, websites and emerging platforms where your organization may become a topic of conversation. Even without costly monitoring services, you can set Google alerts for your company's name as well as relevant hashtags, industry keywords and competitors. Ensure that you, or someone within your department, continually checks these resources and flags things such as negative articles, threatening comments or news of an emerging event relevant to your business.

Finally, regroup often. Get the crisis team together quarterly to talk about the program, emerging issues or swap news about best practices in crisis management. Partner with HR to host regular refresher training sessions to ensure that employees know how to react in a crisis.

Continually analyze and test the program, adapting it to new circumstances. It is surprisingly easy to outgrow a crisis program, so regularly assess it for vulnerabilities and gaps as your organization grows and changes.



CONCLUSION

A crisis management program should be a living process updated throughout the year to ensure that your organization is prepared for crises that could strike at any moment.

It should be highly actionable and accessible, allowing every crisis team member to gain quick and easy access to vital crisis information at any time and from any location.

Mobile technology and specialist platforms allow organizations to create crisis management programs that are always up-to-date and actionable, putting information into the hands of the people who need it at precisely the moment of crisis.

Crisis preparedness is a challenging, time consuming task. However, when armed with an effective program and the right technology, you are prepared for anything that might come your way and have the ability to turn a potentially devastating event into a positive effect on your organization's reputation.



About



RockDove Solutions

RockDove Solutions is based outside of Washington, DC and the developer of **In Case of Crisis 365**, an award-winning, issue and crisis management platform. We support some of the most recognized brands, including hundreds of organizations public and private, large and small.

Our mission is simple:

We help organizations move from static plans and generic company tools, to a purpose-built issue and crisis management platform.

If you'd like to learn more about **RockDove Solutions**, or our platform **In Case of Crisis 365**, [please reach out to us](#), or [request a demo today](#).