



Focus on: Making crisis simulations matter Deloitte's Crisis Management Solutions

Private and confidential
2021



A plan is only a plan until you put it to the test.

You know it's coming. But not when, where, or how big. You'll sleep a lot better if you're confident that your crisis management plan works. And the only way to earn that confidence is with a program of effective, multidimensional simulations that test your entire team and the organisation that stands behind it. Do you feel this is 'for real' while it's happening? That's one test of effectiveness. Do you feel you really learned something afterward? That's an even bigger one.

There is more than one way to approach a simulation. The ones that create lasting value go far beyond the theatrics of a simple 'fire drill' that focuses only on a short-term crisis. An effective crisis simulation puts the organisation to a stringent test, whether or not the scenario represents the worst case. It demands the right questions and the right responses.

It cascades realistically from one decision point to another. It plays through both your external and internal worlds. And it leaves participants feeling they've truly learned something by testing their responsibilities under trying circumstances that subject them to uncertainty, ambiguity, and conflicting and incomplete information—where there is often less known than unknown—so the crisis modus operandi permeates all levels of the organisation.

The foundation of this approach is preparation. The objective might be an orderly exploration of strategic market risk, a dramatic moment-to-moment sequence of scenarios and responses, or something in between. The trigger might involve technical failure, market disruption, natural events, or deliberate malfeasance. In each case, the effort an organisation puts into planning and customising its crisis simulation approach can pay off many times over when a real crisis strikes—in personal preparedness, process improvement, team coherence, and raw confidence. The result is a team that is more confidently equipped to handle crisis, faster in reacting to it, and ready to scale up the necessary resources for response and recovery.

Begin with a scenario? That's your first mistake.

Instead, begin with a purpose. What is your organisation trying to prepare for? When crisis happens, how do you want to look coming out the other side?

Only with a clear objective can you construct a scenario that will advance it. And while the situation may be fictional, the stakes are real. The effectiveness of a crisis response can make or break an organisation's reputation—and reputation can count for as much as one-quarter of an organisation's market value.¹ The average organisation can expect a value-destroying event at least once every five years.² Crisis simulation is not a place for shortcuts. Incredibly, there are still some organisations that don't use simulations at all—but more and more are realising the benefits and putting their plans into practice for preparation that really counts.

Designing across all dimensions

To protect organisational value, a crisis simulation should be as multidimensional as the real world in which a real crisis might play out. Whether real or imagined, it should include externalities, including realistic injections of 'news' and stakeholders with agendas different from your own.

People should interact as they would in real life. They should consider and challenge the impact each decision will have on finance, customers, strategy, and operations—and those decisions should have palpable consequences. If participants run up against the limits of the simulation, the simulation hasn't been designed broadly enough.

A maturity-based approach

Depending upon the purpose of the simulation, the scenario design, and the resources available, simulation approaches will vary. At one end of the scale, a simulation can be as simple as a discussion of likely scenarios.

A world of crisis triggers

Crises can be malicious, accidental or completely random. Most organisations are susceptible to threats from more than one of these potential triggers

Malevolence & cyber	Misdeeds and financial crime	Financial disruption	Technological and industrial	Confrontations	Other catastrophes
Deliberate acts such as cyber attacks or product tampering	The ever-present risk of fraud or other criminal activity	Unforeseen failures that threaten a company's very existence	Complex systems fail, either through accident, mismanagement, or sabotage	Legal, commercial, geopolitical, military conflicts	Natural or man-made destructive events that disrupt almost everything

The next level is a formal rehearsal of roles that tests strategies, information flows, and communications in a highly realistic, scripted environment. The most intense simulations can rival military 'war games' in their dynamic use of worst-case scenarios and immersive, even stressful environments. When participants make decisions, they must consider the consequences those decisions will have days, weeks, and even months down the line. Just as important, decisions need to be made at the right levels. Executives need to be confident others will handle the tactics while they focus on the outcomes, key stakeholders, and future consequences. Getting ahead of the game is critical for them.

An organisation could choose a specific place along this spectrum to stage a needed simulation, or it might stage a progressive program that builds through simulations of increasing challenges following its organisational maturity.

No matter what type of simulation your organisation chooses to conduct, realism is invaluable. The simulation should mirror your internal world as well as your external environment, including customers, regulators, competitors, suppliers, and governments, whenever appropriate and possible. It should help participants reach sound decisions while information assails them from many directions. The more realistic the experience, the more confidence it will build in you and your teams. It's also vital to include the entire organisation, from the board and leadership to the front lines. This is the only way to test decision-making authority and escalation paths.

How to start

First, decide on the objectives. Then think like a movie producer. Carrying out a crisis simulation isn't unlike producing a movie. What's the storyline? The scenario? How do I turn it into a script that determines who will say what to whom and when? This script is known as a Master Events List, or MEL. But a MEL must be more than just a script—because a script follows a prescribed narrative line. A MEL

enhances realism by anticipating and accounting for all the decision points in the simulation, so cause and effect remains realistic from beginning to end. When participants interact with a MEL using real data in a real physical setting, the lessons are real as well.

Next, find the limit. A simulation that doesn't challenge people won't teach them anything. But a simulation that carries them past the breaking point will teach only humiliation and poor morale. Designing scenarios that deliver the most useful stress without going over the line is part science, part art form.

And that's the easy part. The weeks that lead up to a simulation take rigorous planning. The hours that pass during a simulation are engaging, emotional, even entertaining. When the simulation ends, the real work resumes—because collecting the lessons and applying them to create a stronger crisis management plan is where the real value lies.

Simulations in action

Banking on peace of mind

A major global universal bank wanted to identify areas of potential weakness within its critical infrastructures. Through a two-day, bank-wide exercise that used a purpose-built web content management site, they worked through a simulation that included media injects, as well as a live professional journalist and media team. The results included improved coordination of work-streams, validation of the bank's information and process flows, and a set of new contingency/workaround options that weren't in place before.

Gold-medal confidence

The London Organizing Committee of the 2012 Olympic and Paralympic Games conducted more than 200 simulations to prepare for the event. In an environment of rapid growth and dependence on a large number of public and private delivery partners, these simulations helped the organizers define 'ready' and build a robust, risk-based approach to being ready for everything from day one. It was a philosophy and mindset, put into action through simulations and wargames, that were at the very heart of the success of the Games.

Crisis Simulations Maturity Model

Increasing Aware Rehearsed Maturity (IM)	Aware	Rehearsed	Prepared
Definition	<ul style="list-style-type: none"> Individuals and teams are aware of IM roles and responsibilities Basic understanding of how to use processes and tools defined in IM policy standard and supporting documents 	<ul style="list-style-type: none"> Individuals and teams are practiced in applying IM processes and tools, including application of experiential judgment Supporting plans/procedures validated 	<ul style="list-style-type: none"> Individuals and teams are trained, motivated, and engaged — a culture of preparedness Senior executives and stakeholders are confident that incidents of any nature can be managed in a controlled way
Training (examples)	<p>Initial training to:</p> <ul style="list-style-type: none"> Raise awareness and build a consistent understanding of IM policy and supporting documents across key individuals and teams Familiarise key staff with individual roles and responsibilities 	<p>Enhanced training to:</p> <ul style="list-style-type: none"> Develop understanding of how to use key IM documentation (e.g., decision models) and apply experiential judgment Enable staff to further understand their individual roles within key tasks 	<p>Advanced training to:</p> <ul style="list-style-type: none"> Develop understanding of how to use key IM documentation (e.g., decision models) and apply experiential judgment Enable staff to further understand their individual roles within key tasks
Simulation (examples)	<p>Desktop</p> <ul style="list-style-type: none"> Training based Informative Consensus building Walkthrough scenarios, passive environment 	<p>Simulation</p> <ul style="list-style-type: none"> Practice IM roles and processes Examine assumptions Increased pressure and focus on timely decision-making Scripted, active environment 	<p>War games</p> <ul style="list-style-type: none"> Stress test assumptions Worst-case scenarios Cross group involvement Free play, interactive resistant environment

Powerful preparedness

A major US energy provider wanted to evaluate the current standards, practices and capabilities, and corporate and network preparedness to mitigate large-scale power failures in the light of rising cyber and physical attacks on power stations. The wargaming session provided conditions and frames necessary to examine and validate large-scale incident response procedures, including stress testing the interoperability and ability to respond to and replace transformers. The exercise provided comprehensive and actionable insights to enhance stakeholder interoperability and cross communication—for planning, implementing, and defeating security attacks on networks.

Crisis Management Solutions

No one knows when a turn of events will demand the best your organisation can deliver. No matter what form it takes—whether it's front-page news or a quiet struggle only you know about—crisis is a moment of truth that tests your readiness, resilience, and character.

Deloitte's Crisis Management Solutions team is here to help organisations prepare for, respond to, and emerge stronger from major crisis events. In addition to its access to a global team of experienced crisis management specialists, Deloitte has resources in every industry and discipline who can help bring experience and realism to crisis planning.

Disruptive events bring not only danger, but also opportunity—the “unforeseen advantage” you can seize if you're prepared.

This paper is part of our commitment to provide insights that help board members and senior executives navigate the crisis management lifecycle, including readiness, response, and recovery.

Contacts

ROHIT MAHAJAN

President – Risk Advisory
Deloitte India

✉ rmahajan@deloitte.com

VISHAL JAIN

Partner, Risk Advisory

✉ jainvishal@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms. This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTI LLP).

This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTL LLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed

on information sourced from such sources. None of DTTL, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.