The State of Situational Risk Intelligence

The Importance of Digital Risk Tools in the Modern Risk Management Era

Executive Summary

Integrated Risk Management (IRM) defines the tools and processes that organizations leverage to obtain a holistic view of their risk exposure. It plays a critical role in helping achieve operational resilience.

The risk practices of yesterday are inadequate for the businesses of today. As operations become increasingly global and the pressures of proactive risk management are mounting from both a formal regulatory as well as an informal reputation standpoint manual efforts or a robust insurance policy are insufficient. Comprehensive workflows and policies supported by Digital technology must be put in place so risk professionals can make the right decisions at the right times.

External operational risks, such as natural and man made hazards are not only some of the most devastating risks but also some of the most difficult to manage. The two industry leading solutions that address these risks are DisasterAware Enterprise (DAE) and Everbridge's Virtual Command Center (VCC). Both offer critical insights that support business continuity programs, however, whereas VCC has to be bundled with other Everbridge products as part of its Critical Event Management platform, DAE is an open solution that can be integrated into existing risk management frameworks.

Table of Contents

1. What is Enterprise Risk?

Enterprise Risk is also referred to as Integrated Risk or Enterprise Compliance. Despite the seemingly different terms of Enterprise Risk, each refers back to the methods relied on by risk managers to assist them in taking the best course of action in the face of potential threats to their operations or employees. Gartner, a research and advisory company, defines IRM as "a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks."

The six attributes of Enterprise Risk are:
1. Strategy: The structured approach Risk Managers use to optimize business operations, minimizing cost risks.

2. Assessment: The procedure or method Risk managers use to order their priority of risks. It is essential to prioritize risks as fast as possible.

3. Response: the procedures and protocols that are executed to mitigate the impact of a risk.

4. Communication and reporting: Both are critical for updating and informing stakeholders and executives regarding a risk situation.

5. Monitoring: Risks are unpredictable if not continuously tracked. "Risk accountability" includes having full awareness of compliance policies and the outcome of risk decisions made.

6. Technology: Relying on only the expertise of risk management individuals is no longer enough in modern risk management. New technology allows for a more wary and cost-effective risk management. There is a vast overlap and interplay between each IRM attribute. Each is necessary and they must work in concert to build a successful plan. The interplay also ensures that Risk Managers have a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers, and outsourced entities to assist in their high stakes decisions in a limited time.

1

Strategy
Implementation of a framework to improve performance through effective governance and risk ownership

2

Assessment
Identification, evaluation, and prioritization of risks

3

Response
Identification and implementation of mechanisms to mitigate risk

4

Communication and reporting
Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response

5

Monitoring
Identification and implementation of processes that methodically track governance objectives.

6

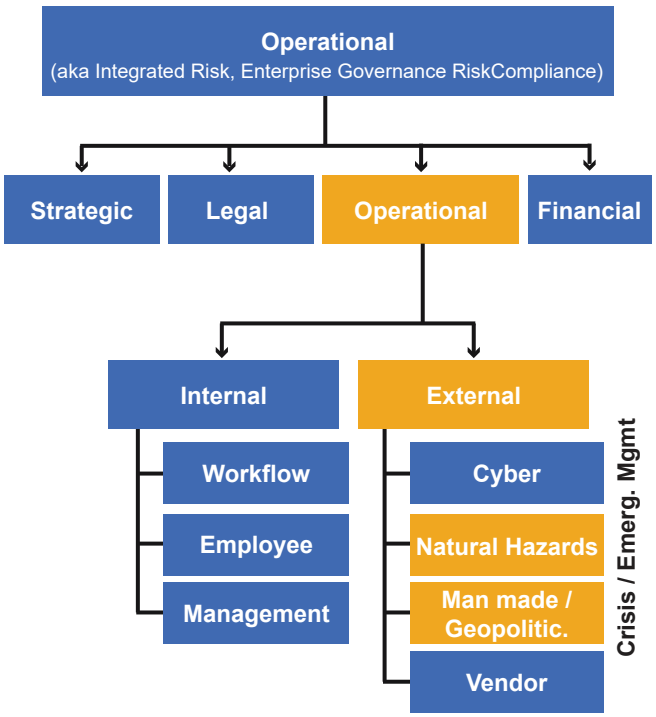
Technology
Design and implementation of an IRM solution (IRMS) architecture

Source: https://www.gartner.com/en/information-technology/glossary/integrated-risk-management-irm

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

DisasterAware Enterprise

2.Types of Corporate Risks



Strategic Risks
These are external macro risks that do not manifest overnight and often disrupt the whole industry. In every fundamental decision made there are risks.

Examples include: *change in the market, customer demands, technological landscape.*

For instance, an automobile company decides to make drastic innovations to their cars to stay ahead of competitors, but the speedy change comes with the risk of consistency and quality issues. (Spacey 2017).

Legal Risks
These are the changes in international or national laws that could adversely affect companies.

Examples include: *employee safety rules, regulatory and compliance laws.*

For instance, the COVID-19 pandemic has forced restaurants, bars, salons and many other industries nationwide to change how they do businesses or risk incurring steep fines or penalties.

Financial Risks
These are the risks that could cause monetary and investment losses.

Examples include: *liquidity risks, funding risks, credit risk with suppliers*

> *Our experience suggests that by improving the efficiency and effectiveness of current risk- management approaches, digital risk initiatives can reduce operating costs for risk activities by 20 to 30 percent.*
>
> **McKinsey**
> Digital risk: Transforming risk management for the 2020s

Operational Risks
The risks that impact day-to-day operations. are the internal risks that can be prevented more proactively as they do not originate from an uncontrollable external source.

Internal Risks
There are three types of internal risks:
Workflow risks, in which the procedures of day to day operations may not be optimal in the advancement of business objectives.
Employee risks are based on the abilities and competencies of the employee.
Management risks are based on the abilities and actions of those running the organization.
External Risk As previously noted, external risks cannot be prevented and often cannot be

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

maintained by human control such as a Natural Hazard Risk, like a weather-related incident that impacts business operations or the safety of employees.

Cyber risk are breaches to a company's information systems that could see employee private information or closely guarded trade secrets leaked.

Vendor risks are the risk by association and dependency to other vendors. Business operations might rely too heavily on the vendors and have concurrent risks.

Man-made risks are those created by human actions but cannot be controlled. For example, mass shootings, protests, or labor strikes. Sometimes Natural Hazard risks and Man-made risks together can be called "**Global Incidents**" or "**Emergency Crisis**" such as terrorist attacks or man-made wildfire.

3.Pressures to Proactively Manage Risks

Reputation

In the 2000s, risk management meant finding a good insurance plan. These days companies can be scrutinized and lose credibility if risk management isn't done properly. A poor response could lead to poor media coverage or sour relationships with key stakeholders and investors.

Regulation/Standardization

Mandatory regulations and standard procedures in business conduct demand proactive action. This includes **Duty of Care**, in which businesses are legally obligated to continually care for their employee's wellbeing. Companies in high-risk industries face regulations/standards called **Standard of Care**, that demand safety and proper function of employees and business operations. Not meeting these regulations and standards exposes companies to major fines, legal entanglements and potential closure.

Business Credit

Better risk resilience means better business credit, and better business credit allows for better relationships or more opportunities and stability with vendors and finances. "Banks, lenders, and suppliers rely on business credit reports to assess the creditworthiness of a company" Thought of as a "financial reputation" for businesses. *(source)*

Globalization

As companies become larger with globally distributed assets, their risk exposure increases. Rules, regulations, and types of risks vary across jurisdictions.

4.The Need for a Digital Risk Management Approach

It is nearly impossible to manually manage risks. External Operational Risks are too expansive and complex. There's no good enough insurance or effective spreadsheet polling method that can manage such risks. These Operational Risks have specific requirements. The solution is a Digital Risk Management Approach that is:

1. Always running
2. Automated
3. Easily Accessible

5.Types of Risk ManagementSolutions

Risk Management Solutions generally have four aspects:

1. Monitoring
2. Planning
3. Responding
4. Recovering

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

The Types of Solutions include a **Full Stack Solution** and a **Focused Solutions.**

Full Stacks Solutions
A full-stack solution consists of multiple products and services that are integrated with one another. This works as an end-to-end solution but also can be limiting as it locks in the user. *(source)*

Focused Solutions
A focused solution hones in on a specific part of the risk life cycle, by doing so it has the capability to give more insights and relevant information to decision makers.

6.External Operational Risks

Operational risk is one of the most complex forms of risk for organizations to manage. The most damaging are external operational risks such as natural disasters, cyber, vendor, or man-made hazards. These can quickly arise and have a devastating impact on organizations. Insurance as a solution means to accept the loss, but having the capabilities to monitor the external operational risk conditions can help minimize loss.

7.What makes a good Digital Risk Management tool?

Digital Risk Management tools have features that assist in doing risk management from anywhere over any location.

Hazard Coverage
To handle operational risks, Digital Risk Management tools must have a wide range in hazard coverage to manage the organization's multiple locations and risks.

Speed and Accuracy
It is also important to get accurate information as quickly as possible. Otherwise, decisions that are made too late or based on false information may cause costly actions, excessive business and personnel losses.

Asset Focused
The Digital Risk Management tool should be asset focused, based on the company's employees, property, and production. It should provide insights into how assets could be affected by an ongoing risk or hazard in order to protect from potential harm or business operation expenses.

Ease of Use/Set Up
There is no time to waste during a risk event. Operating and integrating a risk management tool into an organization's risk management system should be simple and require minimal training. This allows for quick implementation, fast understanding, and immediate results.

Cloud Deployed
As risks come and go at any time of day, no matter where you are, a cloud-deployed digital risk intelligence tool gives access to users from anywhere in the world. There is no downtime and risk managers can monitor from any device at any time anywhere.

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

DISASTERAWARE ENTERPRISE

8.Focused Solution: DisasterAWARE Enterprise™

DisasterAWARE Enterprise™(DAE) is a risk intelligence software that covers 98.9% of man-made and natural disasters. Through the partnership between Tenefit and Pacific Disaster Center (PDC), DisasterAWARE Enterprise has provided sophisticated risk intelligence and resilience for both the public and enterprises by protecting employees and ensuring the safety of assets and business continuity.

Key Features

Asset focused

DAE provides aggregated information via SmartAlerts of incoming hazards that could potentially harm defined asset locations.

Predictive Impact Models

With PDC's 30 year expertise in research and analysis of potential impacts. DAE presents layers such as Vulnerability Index, Resilience Index, Impacts and Losses, and more that could assist Risk Managers in making difficult decisions.

Sample Layers:

Vulnerability Index: *a composite measure of the susceptibility of populations to disruptions.*

Vulnerability assesses the contributions of recent disaster impacts and conflicts as well as socio-economic demographic, and environmental dimensions

Resilience Index: *a composite measure of the ability to absorb, respond to, and recover from disruptions to normal function. The Resilience Index is hazard-independent, combining the Vulnerability Index and Coping Capacity Index*

Impacts and Losses (PAGER alerts): *estimated losses trigger the appropriate color-coded alert, which determines the suggested level of response: no response needed(green), local/regional (yellow), national (orange), or international (red)Index*

Ease of Use

There is no lengthy onboarding time, and learning the software capabilities is intuitive. Defining asset locations simply by uploading a CSV file or HR system. DisasterAware Enterprise utilizes Map Services to make the Asset onboarding process very efficient

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

DISASTERAWARE ENTERPRISE

9.DAE and the Operational Risk Management Life Cycle

Monitoring
DAE's is a cloud-based SaaS, constantly monitors, never offline, and works across multiple platforms. DAE's aggregated SmartAlerts and predictive layers allow for real-time, accurate data, allowing informative decision making

Response
With DAE's integration of a mass notification system, Rave Mobile Safety allows for quicker response and communication in an emergency situation

Prepare
Using DisasterAWARE Enterprise's media heatmap users can stay on top of whatever is going on around the world. Traffic and highway cameras also give the ability to check routes for supplies and plan accordingly.

10.DAE vs. Everbridge

Flexibility
DisasterAWARE Enterprise and Everbridge both provide valuable standalone services but diverge in key areas when it comes to customization and flexibility.

Everbridge works as a full-stack solution and its situational risk intelligence solution, Virtual Command Center, is tightly coupled with its other offerings. Conversely, DisasterAWARE Enterprise allows for a greater degree of customization. Management software, for instance, can be integrated into an existing management plan. Both these approaches have their pros and cons, but if flexibility is a priority, then one of the solutions is more appropriate.

DisasterAWARE Enterprise

DAE is a specialized, open risk management solution.
Pros:
- Open solutions allow managers to build their own risk management stack and tailor it to their needs
- Open solutions make it easier to integrate custom data layers
- Open solutions alleviate vendor lock-in

Cons:
- More vendors could require more management for an organization
- More features and vendors mean managing more relationships and potentially less cohesion

Everbridge
Everbridge is a full-stack offering with a Virtual Command Center.
Pros:
- A full-stack offering requires less management as everything comes "out of the box"
- Tighter relationships between risk lifecycle components

Cons:
- Vendor are locked-in or contracted
- Longer set up and onboarding
- Expensive

Everbridge is the more "hands-off" option as less management is required by risk managers. It works as an all-in-one solution but has a higher cost.

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

DISASTERAWARE ENTERPRISE

Data Visualization
DisasterAWARE Enterprise and Everbridge both have man-made and natural hazard “layers” that are used to identify the positions of hazards This information can help in making more impactful decisions.

DisasterAWARE Enterprise’s layers are often more insightful when it comes to population density and vulnerability index. Everbridge categorizes assets so that communication can be streamlined to the correct people depending on their roles and responsibilities (friends, family, officers, employees, etc)

Data Sources
Everbridge and DAE source their data from public sources, but also through their partnerships in other countries.

DAE’s data partnerships:

- 200+ partner countries
- 60 staff and industry experts
- 6 global locations
- Pacific Disaster Center (located University of Hawaii)
- Georgetown University

Everbridge’s data partnerships:

- Everbridge Nixle
- International SOS
- Dataminr
- Anvil DAE’s partnerships and team at PDC include industry experts of over 30 years of experience and insight.

Data Modeling
Both platforms give assets information at locations. However, DAE provides population density, as well as risk and vulnerability indexes based on location or country.

27 Natural and Man-Made disasters

Integration
Capabilities Both have integration capabilities, however as mentioned before, Everbridge has preset stacks, and users are brought into their contract. DAE is a more buildable stack that gives greater control to its user

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com

DISASTERAWARE ENTERPRISE

11.Conclusion

It’s almost impossible to manually manage risks. Risk management tools such as DisasterAWARE

Enterprise and Everbridge can provide invaluable speed and accuracy from anywhere in the world to ensure the safety of employees and business assets. DisasterAWARE Enterprise and Everbridge’s VCC are relatively unique in the risk management software sphere. For those without risk management software already set in place, Everbridge is a one-stop-shop that has everything ready for its user. Everbridge is configurable to be hands-off, but this means lengthy onboarding, a steeper learning curve and vendor-lock in. For more seasoned risk managers or those who value flexibility and wish to assemble their own risk management stack, DAE is a more appropriate fit. DAE’s unparalleled hazard data coverage alongside its advanced data modeling and visualization capabilities provide a solid situational intelligence foundation that is critical to operational resilience. DisasterAware Enterprise has been used extensively by the DOD as well as many other large global organizations.

2107 N 1st St. #660
San Jose, CA 95131
(408) 800-4569
disasteraware.com