

## Digital Sandbox Whitepaper

### Establishing Effective Risk Management For The Long Haul

Risk has become the watchword of Homeland Security. The conversation has changed from “is it necessary?” to “what are the best practices for implementing a world class risk management program for my jurisdiction?” Despite the compelling case for risk management, it has been a challenge for state and local agencies to move forward as there have been few standards and best practices to guide implementation. Digital Sandbox (DBS) has been leading the development of these standards, best practices and the systems to implement them for over 10 years. This white paper discusses the essential requirements for building a robust analysis capability and provides a template for a proven implementation approach. Ultimately, a risk management system must generate meaningful and updated risk analysis data; transform the data into information and insight; and create operational policies and procedures to ensure that steps the organization is taking (and has taken) are properly aligned with the risks it faces.

---

#### **A proper risk analysis capability must provide flexibility and a clear path for updating and continuous improvement**

Establishing a risk analysis capability is an essential undertaking, and organizations must focus on how analysis is going to support their strategy and programs when setting up the capability. There is no “one size fits all” risk analysis capability so organizations should consider an aggregate approach: people (insiders and outsiders), processes and technologies combined into a risk capability that provides the answers they need on demand. This risk analysis capability should have two primary attributes for long-term success: **flexibility** and a successive path for **continuous updating and improvement**.

**Flexibility** is critical in a risk analysis capability for two reasons:

##### **1. Your need for risk analysis is predicated on changing business requirements**

Risk analysis is not an end to itself. It is meant to inform *risk management* actions such as investment justifications, resource allocation, and operational prioritization. Each management action that is taken will typically require subtly different analyses both in the context of the analysis and the depth of the drilldown into risk data. For instance, a high-level analysis of risk may be sufficient for a Homeland Security Grant Program Investment Justification, but not of a sufficient detail to drive grant fund allocation down to a County level. Additionally, a high-level

analysis may be only a point of departure for a deeper dive into a specific sector such as Agriculture or specific events such as a major NFL game or state fair.

In any given 12-month span, a Homeland Security organization must accomplish many things including updating its strategic plan, evaluating candidate investments, applying for funding (using a risk justification), apportioning received funding, and answering multiple Federal data calls (Tier II data call, State Preparedness Report, Special Events data call, etc.). In a risk management strategy, all of these strategic planning and resource allocation functions require different views and slices of the risk analysis results. In addition, these same organizations cannot always predict what other analytic requirements they are going to need. For instance, when a major event like a terrorist attack or natural disaster happens in the Nation or internationally, they are often called on to provide information quickly to elected officials on exactly what they are doing about a certain hazard/threat, or a certain type of infrastructure in their own jurisdiction. These kinds of data calls and ad hoc requests require an ability to actively mine through data and often require a deeper dive into risk and a specific area of threat, vulnerability, or consequence.

## **2. The way you choose to analyze risk is an expression of policy – which can change and evolve**

While risk analysis tends to combine a set of factors that most can agree on, the way in which these factors are combined, the weight each factor is given, and the way results are displayed all have policy implications. For instance, a typical risk analysis will consider four areas of consequence: health and human effects (H), economic impact (E), mission impact (M), and psychological impact (P). These factors (H-E-M-P) are typically combined mathematically, but the relative contribution of each variable is not typically considered equal (typically H and E are weighted more heavily than M and P). How they are weighted is an expression of the decision maker's policy based on their belief about the relative severity of certain kinds of consequence. Weighting can also stress the *asset risk* (the risk due to the presence of critical infrastructure and key resources) vice the *population risk* (risk due to densities of population) in a risk analysis, or vice versa.

There are many judgments and policies that can be “baked” into a risk algorithm based on the goals of analysis and intended use of the results – even if the same data is used in each variation of analysis. These judgments and policies are always subject to re-examination and it is important to ensure that risk analysis is flexible enough to accommodate changing policy. It is also important to have an analytical capability that is robust enough to show decision makers the effect that their proposed policies and judgments may have on the analytic risk results.

The other attribute to consider when building a risk analysis capability is a **path for continuous updating and improvement**. It is not sufficient to generate one analysis and then rely on that analysis for long stretches of time. Each individual analysis should be considered a snapshot in time based on the best

data and judgments available at that time. Over-relying on a single snapshot should be strictly avoided for the following two reasons:

### 1. Risk is Dynamic

Risk is driven by three primary elements: Threat, Vulnerability, and Consequence. These drivers are subject to change and many of these changes are beyond the control of your organization. Using threat as an example, it is clear to see how the likely occurrence of various threat scenarios changing depends on national/international events, or the intent of various entities to conduct said threats. New threat scenarios can emerge which also must be accounted for in your risk analyses. Additionally, changes to your infrastructure profile, development of new infrastructure, shifts in population, and special events are examples of jurisdictional characteristics that can shift and change over time – altering your picture of risk.

There are also factors that can change that are within your control and must be accounted for in risk analyses. For instance, as you develop your capabilities (“capabilities” here refers to the National Preparedness Goal Target Capabilities List), and put in place risk mitigation measures, your risks will change. Some of these changes will have a direct impact on one or more specific risk scenarios (access control systems in all government buildings), while others (interoperable communications) can have a broad risk mitigation impact. Any snapshot analysis will be based on the risk mitigation measure in place at the time of the analysis.

### 2. Over time, the inputs you use for a risk analysis will change and grow

As Homeland Security programs mature, new sources of data are typically uncovered and efforts are made to obtain a better picture of risk through assessments, data calls, and private sector engagement. Most organizations are constantly performing security/vulnerability assessments that reveal more specific and granular data about risk factors to critical infrastructure. It is important to feed this increasing base of information into your risk analysis, ensuring that the best information available is always being used. Limitations in risk results often point out areas where further information gathering is needed so that the collection and analytical processes can be considered an iterative cycle. Furthermore, generating risk results over time using increasingly granular and reliable data can be a valuable inducement to stakeholders to participate in the data collection effort to ensure their interests are being portrayed accurately in risk analyses. Even if the results of the risk analysis don’t change dramatically as new information is used, having an ongoing feedback loop of collection and analysis creates **strong incentives for stakeholder participation** and builds transparency in the process that **enhances confidence in the risk results**.

## **A recommended implementation approach: create a high-level snapshot to start, then build and expand over time**

Most organizations wanting to implement a risk analysis capability already feel pressure to get started quickly with the process of linking analysis to management actions, but they also feel pressure to “get it right.” These competing pressures must be managed with the focus on driving risk management processes, not on analysis methodology or systems. Therefore, it is not a wise strategy to embark on a long-lead-time analysis of requirements, followed by a “waterfall” development approach that takes months or years to yield results. This leads to a “paralysis of analysis,” while risk management information requirements continue to go unmet. Many organizations have stalled using this approach because there is always another source of data to be considered, another pet risk methodology, or an additional IT system to think about.

**Homeland Security organizations should consider a dynamic risk analysis approach** that is designed to provide early, usable results, but also set the stage for a longer-term risk management program. In this approach, an organization has useable risk results early (within weeks of getting started) and then sets up dynamic processes to ensure the analysis is (1) constantly improving, and (2) always available to support Homeland Security decision making. This successive process borrows from the proven “spiral development process” used in software development and other disciplines and comprises the following steps:

- *Create an initial snapshot based on most critical infrastructure and high-level, expert inputs* – the goal is to provide good risk results that are immediately useable, but also to help identify areas for further data collection and analysis. This process is designed to produce results using reasonable inputs on a short turnaround.
- *Expand the scope and depth of the analysis through ongoing data collection and increasingly sophisticated analytic methods* – the goal is to set up processes for data collection and expert elicitation that continuously improve the scope, quality, and flexibility of your analyses. Processes are put into place to produce tailored risk results on demand, ensuring that best possible analytic results drive critical decision making and business processes. This is an ongoing process, year over year.

In a risk management program, you will be using analyses to drive important programmatic, operational, and strategic decisions. The need for these decisions is ongoing – with each requiring risk analyses that have different data inputs, different policy judgments, and different analysis outputs to support the decision maker. Therefore, the best strategy for risk-informed decision making is to ensure your risk analysis capability is dynamic enough to support a broad set of business functions, considers the best data available at the time, and can be executed quickly when the situation dictates. By producing

results early, and communicating your long-term vision for expanding the analysis capability, you will generate buy-in for your program and build confidence in the results you are generating.

---

**Questions? Comments? Let us know.**

[sales@dsbox.com](mailto:sales@dsbox.com)

1-877-442-4553

---

Digital Sandbox has been developing and deploying leading software and service-based risk management solutions since 1998.

We specialize in providing government agencies at every level – Federal, state, and local – with the strategic insight, technical support, and quantitative analysis they need to optimize investments for the risks they face.

Digital Sandbox offerings provide rigor and repeatability for risk and capability assessment and situational awareness, helping customers effectively plan and budget, advocate for, and deploy risk mitigation resources. Our solutions allow government agencies to maximize mission success by minimizing risks to our nation’s citizens, operations, and infrastructure.