Good Practice Guide for Improving Resilience

Version 1 | July 2025

Introduction

Resilience is defined as the ability for an organization to resist and recover quickly from adversities. It is an emergent property derived from the interrelationships of various capabilities within an organization, equipping it to navigate disruption. The COVID pandemic has demonstrated how different organizations react to a major global shock through problems in supply chain, acute shifts in consumer preferences, and the change in lifestyle. Faced with significant challenges from climate change, extreme events, rising insurance premiums, disruptive technologies and geopolitical conflicts in an increasingly connected global environment, organizations are finding themselves navigating evermore complex risks, which also accompany emerging opportunities. It is increasingly clear that resilience is a differentiator for performance, particularly for organizations that rely on assets to deliver services. Those that can practice a good resilience will have a significant advantage in today's business context because they are better able to seize these opportunities.

At a minimum, the need to maintain continuity of business operations is a key driver of resilience efforts in asset-owning organizations. However, there are many other reasons for the pursuit of resilience and some of these are highlighted below.

Protecting Operations and Business from Natural Hazards

With the increasing frequency of natural hazards, exposed assets are expected to suffer increasing losses and disruptions in the decades ahead. The City of Toronto suffered flash floods in 2013 and 2024, with water exceeding the 100-year flood level. Both events incurred an insured loss of more than one billion dollars, with major damage to the subway system, large sections of the urban highway, both airports, and an electricity transmission station, which caused more than 10 hours of outage for thousands of customers. Similarly, Hurricane Sandy devastated the port of New York and flooded the city's subway system. During the storm however, Goldman Sachs' headquarters in New York remained operational due to extensive flood defenses, while neighbouring buildings suffered significant damage. This capability to withstand disruptions ensures continuity and builds investor and customer confidence. There is also the famous story of the Anheuser brewery in Van Nuy California which survived the 1994 Northridge earthquake unscathed due to a comprehensive seismic defence upgrade completed before the event. It gained a large market share from its competitor after the event, amounting to roughly 30 times the initial capital investment.

Funding for Infrastructure
Governments and international bodies are increasingly allocating funds to mitigate the risk of climate change. Organizations with a decision framework and associated capabilities for embedding climate resilience are better positioned to access this funding due to their readiness to implement robust infrastructure projects with well-defined climate goals. For example, the Investing in Canada Infrastructure Program (ICIP) is a federal initiative that mandates climate assessments for funded projects to ensure alignment with Canada's climate objectives. Similarly, the European Regional Development Fund offers grants to projects that invest in climate resilience. The cities of Toronto and Copenhagen have obtained funding from each program, respectively, to implement major stormwater management projects. In the US, the Department of Transportation's Rebuilding American Infrastructure with Sustainability and Equity (RAISE) Grants fund transportation projects that prioritize climate resilience, sustainability, and equitable community impact. These projects include resilient roadways, transit systems, and ports, all designed to withstand extreme climate conditions. Additionally, the Promoting Resilient Operations for Transformative, Efficient, and Cost-saving Transportation (PROTECT) program, established under the Bipartisan Infrastructure Law in 2021, provides $8.7 billion over five years to fortify US transportation infrastructure against natural hazards and climate change impacts.

Gaining Better Access to Insurance
Insurers are becoming increasingly selective and favour resilient organizations due to their lower risk profiles, translating into better access to insurance and reduced premiums. For instance, Zurich Insurance offers incentives for companies that adopt resilience-enhancing measures. Many insurers offer 10%-15% premium reductions for resilience measures such as leak detection and automatic shutoff devices. With increasing extreme weather disasters across the globe, this preference will become more pronounced. For instance, record-breaking tropical storms and wildfires in Florida and west coast North America in the first few years of the 2020's has led to a mass exodus of insurers in these markets, where many residents and businesses are no longer able to purchase insurance. Endeavour Energy in Sydney has responded to escalating bushfire risks by implementing comprehensive strategies to mitigate potential damages and manage rising insurance premiums. Their approach includes rigorous vegetation management, regular maintenance of power lines, and the adoption of advanced technologies to monitor and respond to fire threats. By proactively reducing the likelihood of bushfire-related incidents, Endeavour Energy not only enhances the safety and reliability of its services but also positions itself as a lower-risk entity in the eyes of insurers. This proactive stance involves a change from past policies and approaches by multiple jurisdictional parties, and is instrumental in securing more favourable insurance terms and controlling premium costs.

Accessing Alternative Risk Transfer Models
Traditional insurance may not offer the best protection for geospatially spread and complex portfolios of assets. Organizations that understand their risk and are proactive in becoming resilient are better able to access alternative risk transfer tools such as parametric insurance, which allows the insured maximum freedom to control when and how much payout is made by the insurer based on measurable parameters. In many cases, parametric insurance provides cost savings, simplifies claims and provides coverage that more accurately reflects the asset owner's risk.

Accessing Market Capital More Effectively
Resilient organizations better attract investors who prioritize sustainability and risk management as they can be assured of the long-term viability of the business. BlackRock, the world's largest financial

asset manager, has emphasized investing in companies with strong resilience and sustainability practices. For example, Tesla received substantial investment due to its focus on sustainable and resilient energy solutions. The Public Utilities Board in Singapore is internationally recognized for its resilient water infrastructure and has secured significant international investment through vehicles such as green bonds.

Gaining Ground in Competitive Markets

In many sectors, there is a consumer market-driven preference for organizations and businesses that demonstrate resilience. In Japan, a seismic rating system has been implemented in its real estate property market for decades where consumers prefer and pay a premium for more earthquake-resilient housing. Rotterdam's port has invested heavily in climate resilience, securing its position as a leading global logistics hub despite rising sea levels. BXP, the largest publicly traded real estate investment trust in the US, has incorporated climate resilience practice into its development and management practice, making it a preferred choice for businesses seeking secure and sustainable office spaces.

Maintaining Property Values

Numerous case studies from the Urban Land Institute indicate that properties with resilience features, such as flood defences and energy-efficient systems, have higher market values and lower operational costs. The Rockefeller Foundation's 100 Resilient Cities initiative has supported cities like New York and San Francisco in implementing resilience strategies that have preserved property values and spurred economic growth.

The IAM has long considered resilience a key element in asset management. The IAM Subject Specific Guidance 32 (SSG32) [1] outlines good asset management practice for resilience analysis and contingency planning, which are critical asset management capabilities within the IAM Anatomy that deal with the response to major shocks, and how to plan for operational recovery. Figure 1 shows the current 10-box model in the IAM Anatomy. The capabilities "Contingency Planning and Resilience Analysis" reside in the "Strategy & Planning" box, along with "Shutdown & Outage Strategy & Planning", as well as "Asset Costing and Valuation". The move of "Contingency Planning and Resilience Analysis" from the "Risk and Review" box in the previous 6-box model reflects the key role that resilience plays at the strategic level. However, it does not mean that resilience is not relevant to risk anymore. In fact, resilience should be considered across all the boxes in the model (this is backed up by the results from a previous survey by the IAM Resilience Group).

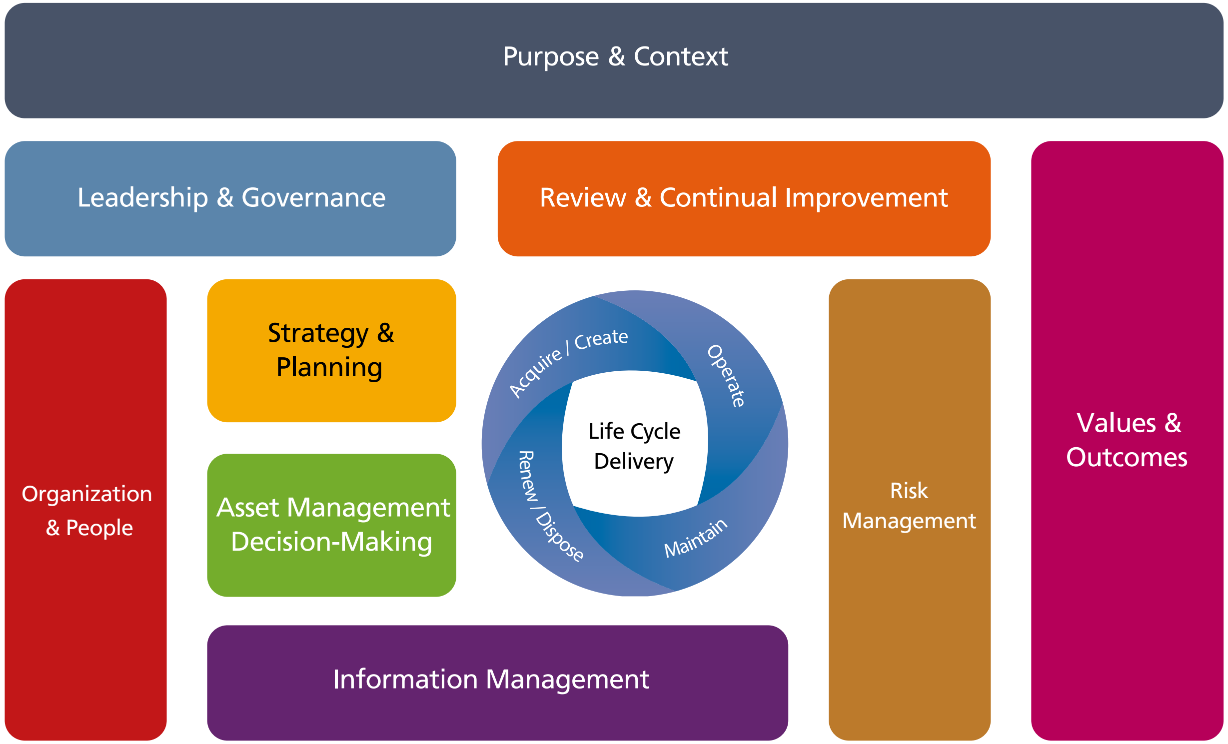


Figure 1 IAM 10-box Model

Other capabilities that clearly impact the resilience of an organization include capital and maintenance investment decision-making, outage strategy, asset information systems management, supply chain management, as well as strategic planning. The difference between resilience and resilience analysis is widely recognized. The recently updated GFMAM landscape document [2] clearly recognizes resilience as an emergent property that manifests through resilience-building capabilities in different parts of the asset management process, from risk management to contingency planning, to operations, to regulatory compliance, to leadership and decision-making. Many of the elements that are critical to the resilience of an organization have been identified in a paper by the IAM resilience group [3].

To help organizations achieve resilience, it is helpful to think about resilience not only as a collection of capabilities, but also how each is related in a business context. A common framework that can illustrate the relationships between different asset management activities is derived from emergency response, where organizational activities that impact its resilience are presented as a cycle beginning with the identification and **assessment** of threats, **planning** and **preparing** through implementing measures to resist and absorb disruptions.

A resilient organization is able to **monitor** and identify events when they occur, deploy effective **responses**, and rapidly **recover** and possibly adapt to a new normal. Presenting resilience in this manner highlights the logical and temporal connections between various asset management activities. This concept is illustrated in Figure 2, along with capabilities found in the IAM Anatomy labelled using the same colour code.

Beyond the critical capabilities of resilience assessment and contingency planning covered in the SSG32, the activities in the resilience cycle are closely tied to strategic goals and stakeholder management. Key activities include risk assessments, capital and maintenance planning, supply chain management, incident response and management, recovery and adaptation to new operating contexts, as well as asset repurposing and disposal.

Additionally, the capabilities shown in Figure 2 should also be guided by sound leadership and policies using a rational decision framework. Many of these activities are covered by IAM SSGs. Regardless of the existence of a SSG, there is a need to present practical implementation aspects of the activities in Figure 2 in the context of achieving resilience.

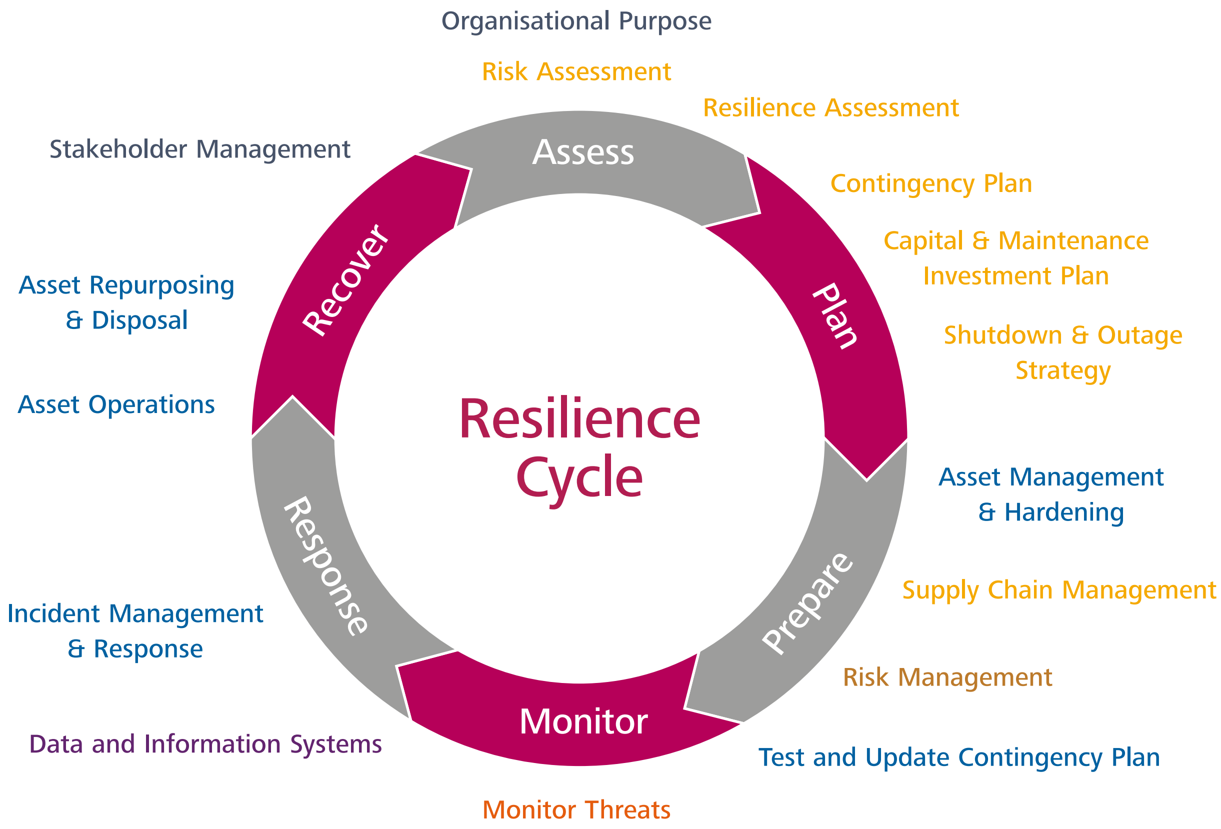


Figure 2 Resilience Cycle

There are many asset management competencies that are required for an organization to achieve resilience. This does not mean that each capability is equally important to all asset classes. The relative importance of these competencies varies greatly depending on the asset class and the organizational context defined by its value chain, tolerance for risk, level of service (LOS), and the relative importance of asset and operations in providing the required LOS. For instance, water infrastructure needs to ensure the quality and reliability of water delivery and the robustness of wastewater systems during extreme events. Resilience likely involves the capability to detect problems and to maintain the conditions of physical components like pipelines, treatment plants, and storage facilities through preventative maintenance and selective asset hardening to achieve a minimum risk of disruption in water delivery to customers. Resilience for power and telecommunication infrastructure may accept a certain number of outages, and focus on minimizing the duration of outages caused by natural hazards, cyber-attacks and equipment failure due to other threats. For transportation infrastructure, asset hardening and improved management of traffic flow through better operational procedures and incident response can be key elements. For facilities and buildings, protection of key components that enable service delivery to tenants and stakeholders, management of the supply chain, and developing response plans are all key ingredients for improving resilience. Given the diverse nature of asset-owning organizations, it is impossible to provide a generalized prescriptive approach to resilience. Rather, the key is to ensure there is a clear definition of resilience that aligns with the organizational goal, and that data, knowledge, procedures and decision-making practices are developed in a way to advance this goal.

This document consolidates the key elements relevant for the practical implementation of resilience in a general asset management context, and provides directional guidance to decision-makers at all levels of the organization, as well as parties involved in delivering infrastructure. Specifically, this guide aims to help decision-makers better understand the relevance and value of these resilience elements to the organization's mission and identify existing resources and best practices for integrating them into the broad asset management context. There are six practical aspects that are identified in this document for embedding resilience within an organization's asset management process. Each of these may relate to one or several capabilities in the IAM Anatomy. Starting from **Horizon Scanning**, which is an important step for understanding the established practice from different professional spheres, an organization must understand how resilience fundamentally **Aligns with Organizational Value and Level of Service**. Once alignments are identified, strategic goals, metrics and a **Decision-making** framework that incorporates resilience should be developed and communicated to the stakeholders in the organization. From here, a systematic approach to implement effective **Risk Management, Interdependency Mapping,** and **Incident Response and Recovery** are the critical capabilities for achieving these strategic goals in a measurable and transparent way. Each of these elements is discussed in a separate section in this document, with useful resources being included in the Appendices.

Horizon Scanning

Horizon scanning is often the first activity that is undertaken to develop an organizational-appropriate framework for resilience. This section provides an overview of horizon scanning, which is a strategic process aimed at identifying emerging trends, opportunities, and threats that may shape the future of an organization. Horizon scanning does not seek to develop full solutions to resilience, but rather, it helps in gathering existing insights from peers to support informed decision-making and adaptation to changing environments. Unlike traditional forecasting, which aims to predict a single outcome, horizon scanning explores multiple possible futures, broadening the organization's perspective on plausible threats and opportunities. By incorporating horizon scanning into the resilience assessment process, organizations can proactively identify and prepare for potential disruptions, ultimately enhancing their ability to adapt and thrive in the face of uncertainty. Horizon scanning can be conducted in an organization, sector, or system for various purposes, such as:

- Identify and monitor trends and drivers that could impact resilience by looking for trends in technology, regulation, social attitudes, or environmental factors that might threaten an organization's ability to recover from disruptions.
- Anticipate emerging threats (e.g., cyberattacks, climate change events, supply chain disruptions) and assess their potential impacts on operations.
- Explore various "what-if" scenarios to understand how different disruptions might unfold and test the effectiveness of existing resilience plans.
- Inform resilience planning and decision-making by identifying gaps in resilience strategies and prioritize investments in areas that will best prepare an organization for future challenges.
- Stimulate dialogue and collaboration on resilience capability building by engaging stakeholders across different departments to build a shared understanding of potential threats and foster collaboration on resilience capability building initiatives.
- Identify opportunities to enhance resilience by revealing new technologies, strategies, or partnerships that can strengthen resilience capabilities within an organization.
- Stress test existing resilience plans by uncovering vulnerabilities in current plans with consideration of diverse future scenarios and making adjustments before facing a real-world disruption.
- Promote a culture of preparedness by fostering a proactive mindset within an organization, encouraging continuous improvement of resilience strategies.

Horizon scanning can be conducted using a variety of methods and tools to identify emerging issues and assess their potential impact on resilience. These methods include:

1. **Desk research:** Analyze existing literature, data, and reports to identify trends and early warnings of potential disruptions.
2. **Expert consultation:** Engage with specialists and stakeholders to gather insights on future challenges and opportunities related to resilience.
3. **Workshops and seminars:** Facilitate interactive discussions and exercises with experts and stakeholders to explore emerging issues and their potential effects on resilience.
4. **Delphi method:** Conduct anonymous surveys with experts over multiple rounds to gather diverse perspectives and reach a consensus on potential future risks and opportunities impacting resilience.
5. **Cross-impact analysis:** Evaluate how identified trends and drivers might interact with each other, cascading effects that could strengthen or weaken resilience.
6. **Scenario analysis:** Construct plausible future narratives based on identified trends and their uncertainties. This allows exploration of how different scenarios might impact resilience.
7. **SWOT analysis:** Identify an organization's, sector's, or system's strengths, weaknesses, opportunities, and threats related to emerging issues to assess overall resilience.
8. **PESTLE analysis:** Analyze the political, economic, social, technological, legal, and environmental factors that could influence resilience.
9. **STEEP analysis:** Similar to PESTLE but emphasizes the social aspect over the political. Both frameworks provide a structured approach to identifying external factors with potential impact on resilience.
10. **Social Media Intelligence (SOCMINT):** Analyze social media data to identify emerging trends, public sentiment, and potential threats related to resilience.
11. **Human Intelligence (HUMINT):** Gather information through human sources with specialized knowledge of specific sectors or regions, providing insights into potential disruptions and opportunities.

By employing these methods together, horizon scanning helps equip organizations and systems with an understanding of their operating environment. Depending on the purpose, available resources, and level of maturity of the organization, horizon scanning can be conducted at different levels of scope and depth. Specifically, the scope and depth can be influenced by the following:

- **Geographic Scale:** Global trends can be analyzed for broad impact, while local scanning focuses on specific regions or communities.
- **Topic Focus:** Scanning can be broad, covering a wide range of potential issues, or specific, targeting a particular sector or technology.
- **Frequency and Duration:** Continuous scanning provides ongoing awareness, while periodic scans offer in-depth assessments at specific points in time.
- **Structure and Rigour:** Formal scanning utilizes defined methods and expert input, while informal approaches might involve brainstorming sessions or casual data gathering.
- **Source and Participants:** Internal scanning leverages internal data and expertise, while external scanning incorporates external data sources and stakeholder participation.

This tailored approach to horizon scanning aligns perfectly with the intelligence cycle, which involves systematic collection, analysis, and dissemination of information to inform decisions as described by scholars like Heuer (1999) in The Psychology of Intelligence Analysis. By collecting, analyzing, and disseminating insights from different levels of scanning, organizations can gain a comprehensive understanding of their internal and external environment. When applied to resilience assessments, horizon scanning produces valuable outputs that inform decision-making and future preparedness. The key deliverables of this process include:

1. **Reports and Presentations:** These concise summaries communicate the key findings of the scanning process, highlighting potential disruptions and their implications for resilience.
2. **Databases and Dashboards:** These interactive tools provide a central repository for collected information and indicators, enabling ongoing monitoring and analysis of trends relevant to resilience. By integrating GIS data, they enhance spatial context and allow for more informed decision-making.
3. **Visualization Tools:** Maps, matrices and GIS storyboards effectively visualize the identified trends and drivers. These tools not only clarify relationships between factors and their potential impacts on resilience but also leverage GIS capabilities to provide dynamic, location-based insights, reinforcing the central role of GIS in the resilience strategy.

4. **Scenario Narratives:** Developing plausible future scenarios based on identified trends helps explore various possibilities and their consequences for resilience. GIS-driven models can be incorporated into these narratives, adding a spatial dimension to the exploration of potential resilience outcomes.
5. **Actionable Recommendations:** Based on the scanning process, prioritized recommendations or action plans outline specific steps needed to build and strengthen resilience.
6. **Enhanced Awareness and Mindset:** Horizon scanning fosters a culture of anticipation. By understanding future uncertainties and opportunities, organizations become better equipped to navigate change and remain resilient.

These outputs work together, providing a comprehensive picture of the evolving landscape and guiding strategies to build a more resilient future. The table below illustrates how horizon scanning can be applied for resilience assessment across various sectors (such as Water Utility, Transportation, and Healthcare) by following a "Scan → Assess → Scenarios → Planning → Stakeholders" framework which is adopted from well-known strategic foresight frameworks such as Horizon Scanning (UK Government Office for Science), Futures Thinking & Scenario Planning (OECD Strategic Foresight Unit), and Resilience Assessments (ISO 31000).

By applying horizon scanning, organizations can proactively assess their resilience to future challenges and make informed decisions to ensure long-term sustainability.

Stage	Application Across Sectors
Scan	Identify trends and drivers affecting resilience, such as climate change (water utilities), technological advancements (transportation), or demographic shifts (healthcare).
Assess	Anticipate opportunities and threats, like regulatory changes (water utilities), emerging mobility trends (transportation), or new medical standards (healthcare).
Scenarios	Develop and analyze future possibilities, such as water shortages (water utilities), autonomous transport (transportation), or increased patient demand (healthcare).
Planning	Inform strategic decision-making by aligning resilience strategies with future needs, such as infrastructure investments (water utilities), smart mobility plans (transportation), or telemedicine expansion (healthcare).
Stakeholders	Foster collaboration among key stakeholders, including regulatory agencies, technology providers, and community organizations, to align expectations and resilience efforts.

Impact to Organizational Value and the Level of Service

A fundamental driver for decisions within an organization is the creation of value. Resilience has its benefits, but may also require substantial effort and investment to achieve. Hence, one of the first questions that an organization must ask is what the benefits of being resilient are and what level of resource and investment is appropriate given the benefits. Only then, is it possible for the organization to determine an outcome-based strategy for resilience.

To address this question, leadership in an organization must start from why the organization exists, what are its core values, and what value creating steps are necessary to support that existence. [Partick Lencioni's "The Advantage" and "Four Obsessions of an Extra Ordinary Executive"] [4] [5]. Organizations exist to provide value to their customers. Organizations create value in a chain-like series that can be illustrated in a least common denominator format, such as in Figure 3. This model includes primary (supply chain logistics, operations, outbound logistics, promotion, service) and support (risk management, human resources, asset management, asset technology, procurement, and infrastructure) activities.

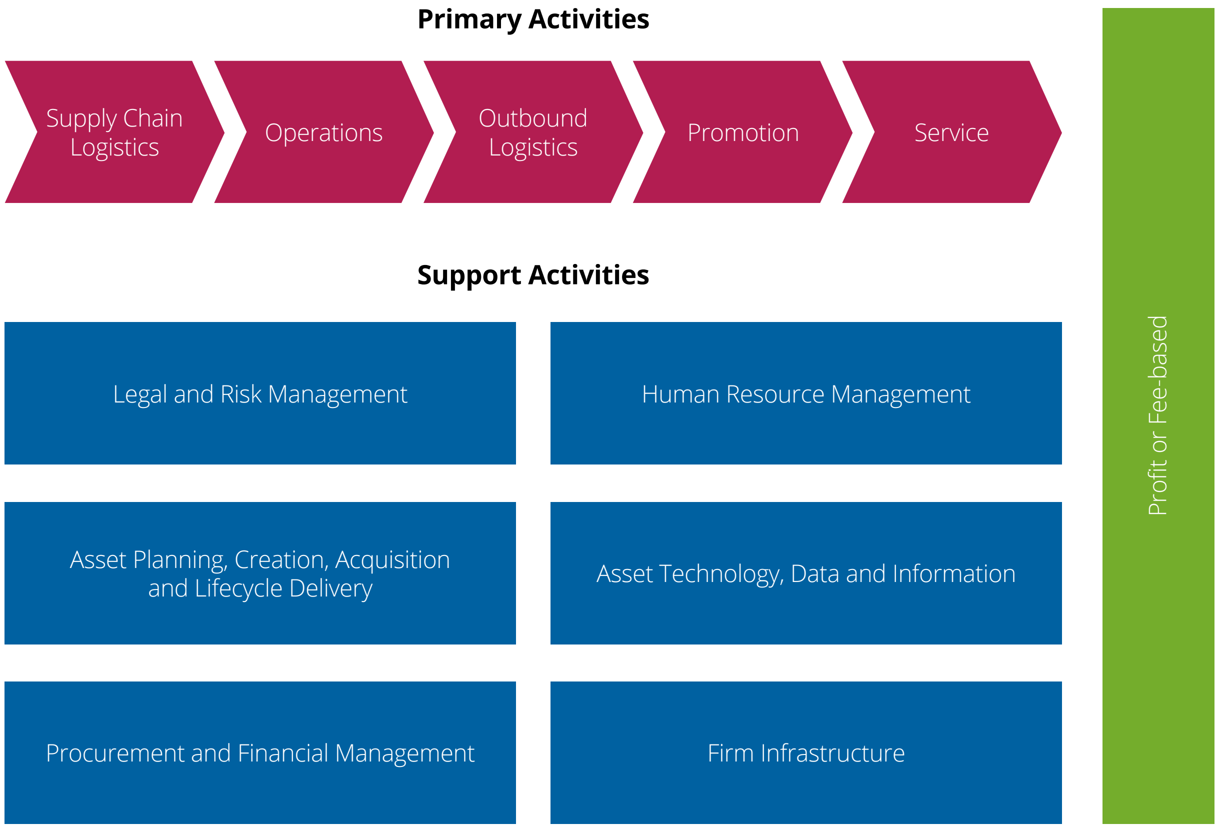


Figure 3 Value Chain Adopted From [M Porter] [6]

Examples may include a series of steps within manufacturing, pharmaceutical, petroleum, food processing and other similar private sector corporate production. Non-profit organizations, like municipal agencies, have infrastructure that provides services and value to customers in a way that justifies its cost. In both cases, the value of assets is reflected in their ability to produce financial and non-financial values across the organization's value chain. Asset management activities and other administrative processes are value streams that support the value chain proposition. Once the least common denominator approach exposes the true value chain, then the value stream of processes and asset activities on asset infrastructure or facilities closest to the customer can be identified.

In asset-intensive organizations with high customer demand, having an asset management framework that includes policy, strategic and tactical asset management plans is a key to delivering the required level of service in the operational value chain. A hallmark of large and mature organizations, therefore, is a well-established asset management framework including a well-defined level of services context. Less mature organizations, and perhaps those who may be in the beginning stages of implementing asset management, may be served by a basic asset management plan with a level of service identified for their customers. Depending on the maturity of the organization, different tools and methods may be more appropriate.

A key value of resilience is that organizations can avoid and reduce the impacts to the business value chain when disruptions occur. Hence, understanding the causes of these disruptions is essential for defining the value of resilience in a given organizational context. There are many methods for identifying critical business processes for the required level of service, and the impacts when such processes are disrupted. Similar to an asset management plan, the tools or methods employed may differ depending on the maturity of the organization. Generally, speaking, more mature organizations are more proficient in integrating strategies with risk management activities, and use data and quantitative metrics in decision-making. Hence, they may seek quantifiable information in more structured ways. On the contrary, organizations with lesser levels of maturity may opt for options that are more qualitative and descriptive in nature, which are easier and less resource intensive to obtain.

Often, a good place to start for understanding value chain impacts is a structured interview or a facilitated workshop with key stakeholder groups or business units which can collect the information required to assess individual business processes and their inter-dependencies at a level sufficient for identifying the type and approximate extent of impacts. Appendix B of this document provides guidance on this type of stakeholder engagement. Interdependencies can then be mapped using a variety of tools, many of which are relatively low effort and low cost, to develop an understanding of potential values gained by having more resilience operations and business processes. The section on Interdependencies provides further detail on the existing resources to guide this process.

For more mature organizations with needs to define not only the type of disruption, but also details pertaining to recovery plans involving physical systems and staff, a Business Impact Analysis (BIA) should be considered. BIA is a widely used tool for identifying the impacts to the business from an event or unforeseen occurrence that disrupts one or more of the value chain areas. A BIA is useful for developing resilience because it identifies the critical functional requirements and operational or organizational processes that must take place to meet the required level of service, and map their dependencies with each other, as well as with the assets and human resources. A BIA can be conducted for the delivery of products or services, and for the level of service to the organization itself or for its customers. When done properly, a BIA is able to identify the weak links in the business process and the impacts that a business can suffer if these links are disrupted. Without this knowledge, an organization will risk "flying blind" amidst unforeseen disruptions. A BIA however, requires relatively high effort and cost compared to the simpler procedures described above.

Depending on the threat, the nature of the incident, and the individual organizational context, there will typically be very large uncertainty related to the exact magnitude of the disruption. A sound understanding of its value chain and supporting value streams, therefore, becomes a crucial bridge for identifying how these disruptions translate into impacts that affect how the organization should conduct itself. This is entirely context dependent and different types of organizations may measure the value of resilience in vastly different ways and find impacts in different value stream areas. For instance, a commercial real estate owner or property manager may view resiliency as a means to reduce the cost of ownership for assets that are exposed to natural hazards through insurance and repair savings. Having more resilient assets may also prevent important anchoring tenants, which may make up a large proportion of its profit, from switching to competitors when the property is offline for a prolonged period of time due to a natural or manmade incident and cannot recover quickly enough to retain the tenant. Furthermore, resilience assets can be used to attract higher profile tenants. A port authority may see resiliency as a quality that allows them to better deliver critical services to avert supply chain disruption affecting gross domestic product, local and regional economies, quality of life and reputation. Similarly, slow recovery can also lead to permanent shifts in shipment routes and customers, which may have a devastating impact on the value chain and organizational existence. A municipal government may find value in resilience because it leads to the equitable well-being of its residents under chronic or acute disruptions. The lack of it, as many examples of post-disaster recovery efforts in urban and rural economies show, can mean a permanent loss of population, which can severely hinder economic development.

Often, the most direct impact of resilience, or lack of resilience, is devastating losses in assets and services levels caused by rare but severe events. This can come in the form of direct physical damage or disruptions in the critical services and business processes (value chain and value streams) caused by cascading impacts due to inherent system

Port of Kobe after the Jan 1995 Great Hanshin Earthquake

interdependencies. A study by the US Federal Emergency Management Agency (FEMA) estimates that 65% of small businesses will fail within one year after a natural disaster. Furthermore, due to competitive market dynamics and the connected global environment, asset and service losses during a major disaster are often irreversible. Before being devastated by the Great Hanshin Earthquake in 1995, the port of Kobe was the world's busiest port by volume in the late 1980s and ranked amongst the top 5 in the early years of the 90s. After the destruction of much of the port's infrastructure, shipping demands in the region shifted to nearby ports such as Busan and Hong Kong. Despite completing its repairs in 1997, the port of Kobe never recovered its lost market share and now falls far behind other major shipping hubs in Asia (Figure 4).

'65% of small businesses will fail within one year after a natural disaster.'

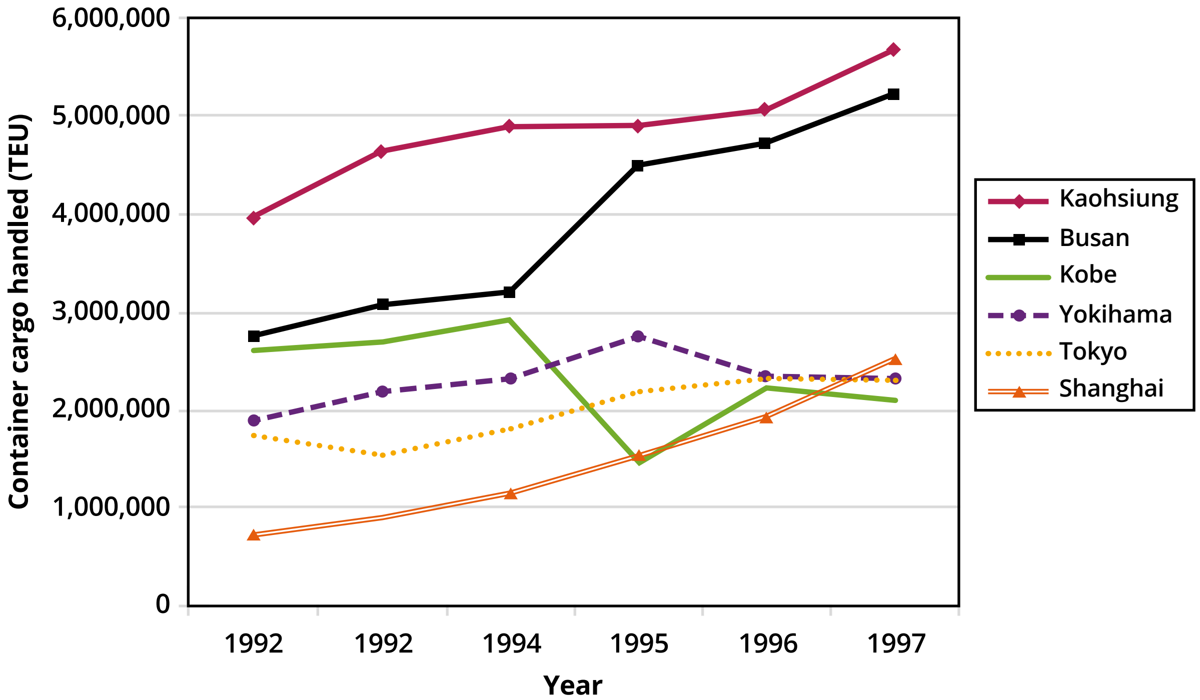


Figure 4 Container traffic through the Port of Kobe and other close by ports prior and after the Hanshin earthquake

Another direct consequence of severe natural hazard events, particularly in the real estate property sector, is the reduced accessibility to insurance due to reduced availability of new insurance policies and the tightening of requirements for purchasing insurance. Under climate change, many of the rare and extreme climate events can become increasingly frequent, leading to multiple years of large losses in the insurance industry that were previously unanticipated. This has a massive impact on the ability to offer insurance, and only organizations that have a demonstrably good record of resiliency would have access to insurance coverage, which is a critical tool in the set of measures available for risk management. The 2022 mass exodus of primary insurers in the hurricane-hit regions of Florida is a perfect example of such an event. Hurricane Ian in 2022 was the latest in the series of destructive billion-dollar hurricanes that occurred in the region in the early years of the decade. Also noteworthy is the widespread damage from the California and other wildfires in the western United States. The insurance market is volatile due to these losses and a flood of fraudulent claims for weather-related damage. As a result, large firms such as AAA and Farmers Insurance in the US have stopped offering coverage for residential owners.

Long-term owners of assets with exposure to climate events will see a growing difference in property values between resilient and non-resilient assets . There are also business practices where disaster resiliency is explicitly priced into rental costs (e.g. US hurricane, Japan earthquake). Both factors produce measurable business impacts, although they are not always measured consistently. Emergent standards for asset resilience assessment may change this in the near future. Just like some markets in the US and Europe, as awareness of transition and physical risk due to climate grows in the public, a resilient asset portfolio and organizational structure, especially when well disclosed and communicated, will strengthen organizational trust and reputation, which can indirectly drive value . This will have a positive impact on access to capital compared to organizations that are less resilient due to emergent regulatory requirements (IRFS, TCFD, OSFI) from the financial sectors. In some instances, market value may also increase as resilient firms are perceived as a better investment.

COVID-19 exposed resource accessibility and supply chain issues with pandemic-related medical and non-medical supplies, generally associated with large-scale centralized manufacturing available in only a handful of developing countries. (See also section on interdependencies). The demand for medical supplies during the COVID pandemic, such as the personal protective equipment (PPE), experienced shortages in many countries and particularly where sharp increases in COVID were experienced in less-developed countries. In this example, global value chain resiliency may have created barriers worldwide related to inequality. Geography, political, third-party ownership, and biological logistics with the production of medical supplies during the COVID pandemic created complexities that also exacerbated the impacts on global value chains. The auto industry has been extremely impacted due to the manufacturing and supply chain limitations in silicon chip technology. There is now a similar situation with the fossil fuel transformation to electrical vehicles (EVs) of which corporate value chains rely on strategies secured by lithium natural resource availability, mining, geopolitical complexities, policies yet to be developed, and healthy supply chains or adequate logistics, well-invested infrastructure, and capacity.

Lessons learned from the pandemic have shifted the thinking from centralized global supply chains amongst a few geolocations and in developed countries to a redistribution of manufacturing that is closest to the demand. In this case, decentralizing the manufacturing process to satellite locations worldwide that are closest to the demand for medical supply needs is a forward-thinking strategy being considered. This strategy creates a rapid response but also a less crippling effect to the entire global process experienced during the COVID pandemic. This also enables inclusivity among several countries for local/personalized participation in different areas of the overall value chain.

This example can be scalable for many asset-intensive industries and organizations, including municipal asset owners. Several factors that are relevant to resilience in the context of municipal assets are listed below:

1. Supplies for resources (materials and products) become more difficult to procure with lengthy construction project delays of new capital infrastructure.
2. Constraints in the labour market, challenging regulatory compliance or adequacy of services to perform asset operational or maintenance activities on infrastructure.
3. Heavy reliance on external contracting resources rather than making the business case for increasing internal staffing capacity.
4. Readiness for multi-faceted or widespread emergencies, for example, flood and fire.

Many organizations, both private and public sectors, have been financially impacted and are experiencing constraints from an historic labour capacity from which they have never fully recovered. Unhealthy labour levels may impede adequate services that forces unintended non-compliance with national rules and laws, let alone an inability to monitor service levels within infrastructure products, such as water and discharging effluent from sanitary sewer collection and cleaning, rendering widespread effects to people and the environment.

Despite efforts made by some [Cockram and Van Den Heuvel 2012, Fragouli et al 2013] [7] [8] to quantify the value of resilience by tracking market values gains and losses as a function of organizational resilience, a universal approach for quantifying the value of resilience, which can be measured in financial or non-financial metrics of avoiding disruptions, does not exist for all organizations due to the large variability in what organizations perceive as value. Rather than direct quantification, it is much easier to identify these values and classify them as tangible (measurable or quantifiable) and intangible. Table 1 provides a non-exhaustive list of outcomes that may be perceived as values of resilience by different asset-owning organizations. It is noteworthy that the basic root of these values of resilience are classified as critical elements in a risk registry whose consequences warrant mitigation measures to avert their effects. The root cause of these examples emphasizes inefficiencies, ineffectiveness, unawareness on desired/capable level of service, disinvestment, and cultural dysfunction that inadvertently causes and action or inaction whose consequences have effects on attaining organizational outcomes. The degree of these causes and consequences marks the severity of the impact to an organization, and hence, its resilience to "bounce back" in the face of adversity.

Table 1 may be used as a starting point when thinking about the reasons an organization may want to enhance resilience. It is important to note that these values must be attached to an appropriate and measurable metric(s) that allow(s) the benefit to be estimated. This is harder for some of the benefits than others, and the organization must determine what these metrics are given the business context and goals. Once the values of resilience are identified, an organization can proceed to evaluate decisions by how they impact value, outcomes, and levels of service.

Tangible	Intangible
• Reduce downtime of critical services	• Improves customer satisfaction
• Reduce insurance cost or increase "book" value	• Enhanced corporate image and reputation
• Improve access to risk transfer options (including insurance)	• Gain strategic advantage as thought leaders
• Reduce likelihood of large property loss	• Create better performance stability amidst changing physical and policy environments
• Reduce likelihood of prolonged functional disruption	• Become more attractive to top talent in the labour market
• Protect property value	• Gain customer loyalty
• Improve access to capital market	• Culture of resilience (culture that fosters effective information sharing, rapid escalation and clear accountability)
• Increase revenue in markets that value resilience	
• Gain market share in a competitive environment	
• Reduce social and environmental impact	
• Regulatory compliance	
• Leverage contingency planning to prepare, response, and recover from low frequency-high consequence events	

Table 1 Potential values of resilience

Decision Making

Asset managers face a variety of decisions at different levels and stages of their work. These decisions have different characteristics, objectives, and challenges, and they require different approaches and tools to support them. This section introduces the main types and stages of decisions for asset managers and provides guidance and recommendations on how to make them effective and efficient.

Strategic decisions: These are long-term, high-level, and often complex decisions that affect the overall direction and goals of the asset management organization. For example, deciding which markets to enter or exit, which products or services to offer or discontinue, or how to allocate resources among different business units. These decisions can impact the level of resilience that an organization needs, or alternatively, organizational resilience may enable access to strategic opportunities. For example, entering into a rental housing market with high hurricane and climate-related extreme event risk presents challenges in property risk management, but also offers access to a market where consumers have a growing awareness and willingness to pay for the benefit of climate-resilient buildings. Strategic decisions involve uncertainty, ambiguity, and multiple stakeholders with diverse interests and preferences. They require a thorough analysis of the external and internal environment, a clear vision of the desired future state, and a sound evaluation of the available options and their trade-offs.

Tactical decisions: These are medium-term, operational, and often routine decisions that support the implementation of the strategic decisions. For example, deciding how to optimize the portfolio composition, how to price the products or services, or how to manage the risks and compliance issues. Tactical decisions involve less uncertainty and ambiguity than strategic decisions, but they still require a good understanding of the market conditions, the client needs, and the organizational capabilities. They require a systematic and efficient process of gathering and processing relevant information, applying appropriate models and methods, and monitoring and adjusting the outcomes. In the example above, making tactical decisions will require an understanding of the availability and cost of hurricane and flood insurance, potential rental disruption times, proactive maintenance measures, and knowledge of local plans for risk mitigation.

Operational decisions: These are short-term, tactical, and often repetitive decisions that deal with the day-to-day activities of the asset management organization. For example, deciding when to buy or sell a security, how to execute a trade, or how to handle a client request or complaint. Operational decisions involve minimal uncertainty and ambiguity, but they require a high level of speed, accuracy, and consistency. They require a well-defined and automated process of applying predefined rules and criteria, using reliable and timely data, and following established procedures and protocols. In the example above, emergency response protocols for weather disasters, arrangements for tenant evacuation and temporary shelter are some of the elements that need to be considered.

The stages of decision making are not fixed and rigid, but rather flexible and adaptive, depending on the type and context of the decision. However, a general framework that can guide asset managers through the decision-making process is:

1. **Define the problem or opportunity:** This stage involves identifying and clarifying the nature, scope, and significance of the decision situation, and articulating the objectives and criteria that will guide the decision-making process.
2. **Analyze the alternatives:** This stage involves generating and evaluating the possible courses of action that can achieve the objectives and satisfy the criteria, and assessing the pros and

cons of each alternative, taking into account the costs, benefits, risks, and uncertainties.

3. **Select the best option:** This stage involves choosing the most suitable and feasible alternative, based on the analysis and evaluation of the previous stage, and justifying the choice with rational and evidence-based arguments.
4. **Implement the decision:** This stage involves executing the chosen option, communicating the decision and its rationale to the relevant stakeholders, and allocating the necessary resources and responsibilities for the implementation.
5. **Review the results:** This stage involves monitoring and measuring the outcomes and impacts of the decision, comparing them with the expected and desired results, and identifying and addressing any gaps or deviations.

By understanding the main types and stages of decisions that asset managers have to make and applying the appropriate tools and techniques for each type and stage, asset managers can improve their decision-making quality and outcomes related to resilience, and achieve their strategic, tactical, and operational goals.

Key Principles and Frameworks for Effective and Ethical Decision Making

Effective and ethical decision-making is a core competency for asset managers, as it affects the performance, sustainability, and reputation of their organizations and stakeholders. To make effective and ethical decisions, asset managers should follow some key principles and frameworks that can guide them through the decision-making process and help them avoid common pitfalls and biases.

1. **Define the problem or opportunity clearly and objectively:** Asset managers should identify the root cause, scope, impact, and urgency of the problem or opportunity they are facing, and avoid jumping to conclusions or solutions without sufficient information and analysis. This is ultimately tied to the value discussed in the last section. Opportunities and benefits should be attached to well-defined and measurable metrics, such as what is the additional capital that can be accessed through resilience efforts, or what is the additional cost for hardening assets.
2. **Identify and evaluate the possible options and alternatives:** Asset managers should generate and consider a range of possible options and alternatives that can address the problem or opportunity, and evaluate them based on their feasibility, effectiveness, efficiency, and alignment with the organizational goals, values, and mission. Again, understanding business impacts at a quantitative level enables decision-makers to weigh the value of improved resilience, whether that is capital investment in asset hardening, additional risk transfer, or increased redundancy of critical staff.
3. **Involve and consult the relevant stakeholders:** Asset managers should involve and consult the relevant stakeholders, such as customers, employees, suppliers, regulators, and the public, who may be affected by or have an interest in the decision. This can help them gain more insights, perspectives, feedback, and support for the decision-making process and outcome. Often, resilience may only be one part of the criteria for decision making, and organizations have constraints, both legal and financial. Hence, compromise is usually inevitable. Stakeholder consulting, when it is done with sound data and analysis that are accessible to all, ensures objectives are clearly communicated across the organization, and allows more effective mobilization of different stakeholder groups towards these objectives.
4. **Apply the ethical principles and standards:** Asset managers should apply the ethical principles and standards that govern their profession, such as integrity, accountability, transparency, fairness, and respect, and ensure that their decisions comply with the applicable laws, regulations, policies, and codes of conduct. They should also consider the ethical implications and consequences of their decisions for themselves, their organizations, and their stakeholders. A key consideration for large asset organizations, particularly public infrastructure owners and operators, is the impact the organization and its operations has on the community resilience. In recent years, there is also a trend towards encouraging other asset-owning organizations, public or private, to consider their impacts on the surrounding community. More guidance on metrics and approaches for incorporating this aspect into decision-making is found in the community resilience resource section in Appendix A.
5. **Choose the best option and communicate the decision:** Asset managers should choose the best option that balances the needs and interests of the stakeholders, solves the problem or exploits the opportunity, and meets the ethical criteria. They should also communicate the decision and its rationale clearly and convincingly to the stakeholders,

and address any concerns or objections that may arise. For decisions relating to resilience, a challenge is that many of the major interruptions cannot be foreseen or anticipated with great accuracy. Hence, reliable asset data and sound analysis of the benefits or the criteria are ever more critical to developing rational and defendable decisions.

6. **Review and learn from the results:** Asset managers should review and learn from the results of their decisions, and assess whether they achieved the intended and expected outcomes and impacts. They should also identify and implement any improvements or corrections that may be needed, and share the lessons learned and best practices with others.

Some of the frameworks that can assist asset managers in applying these principles are:

- The **rational decision-making model** is based on the assumption that asset managers can make optimal decisions by following a logical and systematic process of defining the problem, identifying the criteria, generating and evaluating the alternatives, choosing the best solution, implementing the decision, and monitoring the results. This model can help asset managers to make objective, consistent, and evidence-based decisions, but it may not account for the uncertainties, complexities, and emotions that may affect the decision-making process and outcome.
- The **intuitive decision-making model** is based on the assumption that asset managers can make effective decisions by relying on their intuition, experience, and gut feelings, rather than on formal analysis and evaluation. This model can help asset managers to make quick and flexible decisions, especially in situations where there is limited time, information, or resources, but it may also be influenced by cognitive biases, heuristics, and personal preferences that may impair the quality and validity of the decisions.
- The **ethical decision-making model** is based on the assumption that asset managers should make decisions that are not only rational and intuitive but also ethical and moral. This model can help asset managers to incorporate the ethical principles and standards into their decision-making process and outcomes, and to evaluate the ethical dimensions and impacts of their decisions for themselves, their organizations, and their stakeholders. Some of the steps involved in this model are identifying the ethical issue, gathering the facts, identifying the stakeholders, considering the alternatives, applying the ethical tests, making the decision, implementing the decision, and evaluating the decision.

The common pitfalls and biases that can impair decision making quality and how to avoid them

Major disruptive events are often very difficult to predict. Hence, when making decisions that impact the resilience of an organization, it is important to be aware of the common pitfalls and biases that can impair decision-making quality. One common bias is confirmation bias, where an individual may seek out information that confirms their existing beliefs and ignore information that contradicts them. This can lead to overconfidence and distorted judgment, preventing asset managers from considering alternative solutions or perspectives. To avoid this, it's important to actively seek out information that challenges your assumptions and consider multiple perspectives. A different, but related bias is the optimism bias, which is the tendency for an individual to believe that good things are more likely to happen than bad ones. This is closely tied to resilience as severe threats like natural disasters and a global pandemic tend to be rare and have a long return period. It is very likely that people do not experience such an event within a generation, thus leading them to believe that they are unlikely to experience one ever. The best defence against optimism bias is to make decisions based on data and scientific consensus whenever possible. When data is not available or not reliable, techniques like what-if analysis can prove valuable for gaining insights about these threats. In either case, consulting experts on the relevant subject matter can be explored to support decision-making.

Another common pitfall is anchoring bias, where an individual may rely too heavily on the first piece of information they receive when making a decision, even if it is not relevant or accurate. This can lead to inaccurate estimation and prevent asset managers from updating their beliefs or expectations based on new evidence or information. To avoid this, it is important to consider multiple sources of information and avoid making decisions based on a single data point.

The framing effect is another bias that can impair decision-making quality. This is the tendency to be influenced by the way that a problem or situation is presented or worded, rather than by the actual facts or outcomes. This can lead to inconsistent preferences and biased evaluations, preventing asset managers from assessing the problem or situation objectively. To avoid this, it is important to focus on the facts and outcomes rather than the presentation or wording of the problem or situation. This can be a common problem when metrics for measuring resilience are not defined sufficiently, are difficult to measure, or are too vague to inform decision-making, leading to situations where decisions are based on the way and language a problem is presented rather than the merit of the argument.

Finally, the sunk cost fallacy can also be a pitfall for asset managers. This is the tendency to continue investing in a project or course of action that has already incurred significant costs, rather than cutting one's losses and switching to a more profitable or feasible alternative. This can lead to escalation of commitment and prevent asset managers from maximizing their returns or minimizing their risks. To avoid this, it is important to regularly reassess the costs and benefits of a project or course of action and be willing to make changes when necessary. Again, the availability of reliable data and tractable metrics is paramount.

To avoid or minimize the effects of these common pitfalls and biases, asset managers should adopt some strategies and techniques, such as:

- **Seeking feedback and diverse opinions:** Asset managers should seek feedback and diverse opinions from others, such as colleagues, experts, or stakeholders, who can provide different perspectives, insights, or experiences, and who can challenge or support their assumptions, hypotheses, or decisions. This can help asset managers to reduce their confirmation bias, broaden their horizons, and improve their learning and decision making.
- **Using multiple sources and methods of information:** Asset managers should use multiple sources and methods of information, such as data, statistics, reports, surveys, experiments, or simulations, that can provide reliable, valid, and relevant information, and that can test or verify their hypotheses, estimates, or predictions. This can help asset managers to reduce their anchoring bias, update their beliefs, and enhance their accuracy and confidence.
- **Considering different frames and scenarios:** Asset managers should consider different frames and scenarios, such as positive, negative, neutral, best, worst, or most likely, that can present or describe the problem or situation in different ways, and that can reveal the potential benefits, costs, risks, or opportunities of each option or outcome. This can help asset managers to reduce the framing effect, evaluate their options, and make rational and consistent decisions.
- **Evaluating the opportunity costs and future consequences:** Asset managers should evaluate the opportunity costs and future consequences of their decisions, such as what they are giving up or gaining by choosing one option over another, and how their decisions will affect their short-term and long-term goals, performance, or reputation. This can help asset managers to reduce their sunk cost fallacy, overcome their emotional attachments, and make optimal and ethical decisions.

Decision making is a key skill for asset managers, who need to make complex and high-stakes decisions on a daily basis, such as how to allocate resources, what strategies to adopt, or what risks to take. However, decision making can also be influenced by various cognitive biases, such as confirmation bias, overconfidence bias, or hindsight bias, that can impair the quality and effectiveness of the decisions. Therefore, asset managers need to be aware of these biases and use best practices and tools to overcome them and improve their decision-making skills and outcomes.

Best practices and tools for improving decision-making skills and outcomes

To improve decision making skills and outcomes, asset managers can utilize best practices and tools that enhance critical thinking, problem solving, and judgment abilities. By doing so, they can make more informed, rational, and ethical decisions, which can improve their performance, reputation, and trustworthiness, and create more value for themselves, their clients, and their organizations.

One best practice is seeking feedback and advice from others. Asset managers should seek out colleagues, mentors, experts, or clients who can offer different perspectives, insights, or experiences and who can challenge their assumptions, arguments, or preferences. This can help asset managers to reduce their confirmation bias, broaden their views, and increase their learning and accountability.

Another best practice is setting clear and realistic goals and criteria. Asset managers should define what they want to achieve, why they want to achieve it, how they will measure it, and when they will evaluate it. By doing so, they can guide their decision-making process and align it with their values, mission, and vision. This can help asset managers reduce their overconfidence bias, focus their attention, and enhance their motivation and commitment.

Asset managers can also improve their decision-making skills by reviewing and reflecting on their decisions. This involves assessing the results and impacts of their decisions, identifying what worked well, what did not work well, what can be improved, and what can be learned. By doing so, asset managers can reduce their hindsight bias, improve their adaptability, and foster a growth mindset.

Stakeholder consultation is another key factor that can enhance the decision-making skills and outcomes of asset managers. Stakeholders are the people or groups who have an interest or stake in the decisions and actions of asset managers, such as clients, investors, employees, regulators, or the public. Consulting with stakeholders can help asset managers to understand their needs, expectations, preferences, and perspectives, and to incorporate them into their decision-making process. This can help asset managers to increase the legitimacy, transparency, and accountability of their decisions, as well as to build trust, rapport, and collaboration with their stakeholders. Stakeholder consultation can also help asset managers to identify potential opportunities, challenges, risks, or trade-offs that may arise from their decisions, and to devise strategies to address them. By engaging with stakeholders, asset managers can improve their communication, listening, and negotiation skills, and foster a culture of learning and feedback.

Measuring success is another crucial aspect of decision making that can benefit and improve the skills and outcomes of asset managers. Measuring success involves defining and tracking the indicators and metrics that reflect the progress and performance of the decisions and actions taken. By doing so, asset managers can evaluate the results and impacts of their decisions, and compare them with their goals and criteria. This can help asset managers to identify and celebrate their achievements, acknowledge and learn from their failures, and recognize and address any gaps or discrepancies. Measuring success can also help asset managers to communicate and demonstrate their value and impact to their stakeholders, and to solicit and incorporate their feedback and suggestions. By measuring success, asset managers can foster a culture of continuous improvement and innovation, and enhance their confidence and credibility.

Assessing the impacts of resilience-related decisions is another important factor that can benefit and improve the decision-making skills and outcomes of asset managers. Asset managers need to consider how their decisions can enhance or undermine the resilience of their assets, portfolios, clients, and organizations, as well as the broader social and environmental systems they operate in. By doing so, asset managers can identify and mitigate potential risks, seize new opportunities, and create long-term value. Assessing the impacts of resilience-related decisions can also help asset managers to align their decisions with the UN Sustainable Development Goals and the principles of responsible investing, and to demonstrate their commitment to social and environmental responsibility. By assessing the impacts of resilience-related decisions, asset managers can improve their strategic thinking, scenario planning, and stakeholder engagement skills, and foster a culture of foresight and innovation.

Timing of decision making

One of the important factors that can affect the quality and effectiveness of decision making is timing. Decisions are time-sensitive, meaning that they have to be made within a certain timeframe, depending on the urgency, complexity, and consequences of the situation. Delaying or rushing a decision can lead to suboptimal outcomes, missed opportunities, or increased risks. Therefore, asset managers should consider the optimal timing of their decisions, and balance the trade-off between speed and accuracy, as well as the trade-off between short-term and long-term implications.

A useful way to think about the timing of decision making is to consider different time horizons: short, medium, and long term. Each time horizon has its own challenges and opportunities, and requires different approaches and strategies.

In the short term, asset managers need to make quick and effective decisions in response to changing market conditions, client demands, or operational issues. They need to gather and share relevant information swiftly, and leverage the expertise and insights of others. In large and complex organizations, this may require setting up a type of 'information fusion centre' that can create and disseminate the intelligence and analysis needed for decision making. Also in the short term, asset managers need to prioritize emergency response and crisis management. They need to identify and respond to the most critical and urgent issues that threaten their assets, operations, or reputation. They need to make decisions that can protect their staff, clients, and stakeholders, and minimize the damage or loss caused by unexpected events. They also need to ensure that they have adequate contingency plans, resources, and communication channels to cope with the situation and restore normalcy as soon as possible.

In the medium term, asset managers need to utilize risk management to enhance their control and mitigation of potential threats, uncertainties, or disruptions. They need to monitor and evaluate the performance and impact of their decisions, and adjust them as needed. They also need to communicate and coordinate their actions and expectations with other stakeholders, such as regulators, investors, or suppliers. Also in the medium term, asset managers need to focus on post-incident recovery and learning. They need to analyze the root causes and consequences of the incidents that occurred in the short term, and identify the lessons learned and best practices that can improve resilience. They need to implement corrective and preventive actions that can address the gaps or weaknesses that were exposed by the incidents, and enhance preparedness and response capabilities for future situations. They also need to share their knowledge and experience with other asset managers, and learn from their

The Institute of Asset Management

peers and external sources. By doing so, they can strengthen their organization's reputation and trust, and create value from adversity.

In the long term, asset managers need to enhance their organization's ability to adapt, transform, recover, and anticipate future scenarios and opportunities. They need to conduct holistic assessments of the trends, risks, and strategic priorities that affect their organization, and influence the commercial or regulatory decisions that shape their industry. They also need to foster a culture of innovation, learning, and resilience that can support long-term vision and goals. Also in the long term, asset managers need to align their risk management with their strategic planning and decision making. They need to consider how the organization's risk appetite and tolerance can support or hinder its competitive advantage and value creation in a changing environment. They also need to anticipate and prepare for emerging risks and opportunities that may arise from technological, social, environmental, or regulatory developments. By doing so, they can enhance their organization's agility, flexibility, and responsiveness, and achieve sustainable growth and resilience.

Assessing and Managing Risk

Referring to the resilience cycle in the introduction, assessment of risk is an essential capability that other activities that contribute to the resilience of the organization build on. Risk assessment in turn, informs risk management, which is the way for organizations to implement appropriate measures to deal with risk that include avoidance, mitigation, transfer, acceptance, or any combination of these. In the context of this document, the recovery dimension is considered part of risk, and good risk management practice enables organizations to understand and plan for effective recovery, which is essential for achieving resilience at both the operational and organizational level.

Resilience requires effective risk management, which in turn requires the establishment of a risk management framework and the corresponding risk management process. The former specifies the structure of an organization's operation that identifies, monitors, controls, and governs risk. The latter is the actionable steps by which risk is identified, assessed and managed. As a starting point, good general guidance for establishing a risk framework can be found in:

- ISO31000 standard [9]
- IAM Subject Specific Guidance 31 – Risk Assessment [10]

The same references also provide guidance on establishing a risk management process, which covers risk identification, risk analysis, risk evaluation and risk treatment. Rather than discussing risk assessment in general, this section offers further context and introduces issues in the risk assessment process that are related to achieving resilience.

Metrics and Levels of Resolution in Risk Assessment

Risk deals with uncertainty, and uncertain events, especially extreme ones that occur infrequently but can jeopardize the organization's viability, are difficult to assess, let alone forecast. Therefore, decision-makers should understand the spectrum of risk assessment approaches and identify ones that produce appropriate level of information commensurate with the decision-making need for achieving resilience. This means that there should be a clear set of metrics for measuring and comparing risk, as well as criteria for selecting methodologies that provide the required level of resolution. Some examples of common risk metrics that can be used to inform decisions are given below.

Direct Financial Cost: This includes the direct and indirect financial impact caused by the hazards being evaluated. Examples of direct impacts include property damage requiring repair and replacement, loss of rental income due to downtime. Examples of indirect financial impacts include potential litigations, loss in stock prices, loss of market share or loss of opportunities to access capital.

Disruptions: Loss of operations cannot always be captured by financial metrics. Critical facilities like emergency response, hospitals and data centres cannot tolerate disruptions, even very short-duration ones. For instance, a slight disruption to life-support systems can jeopardize patient well-being, or even result in a hospital casualty.

Downtime: Downtime measures the duration required for service to return to an acceptable level. This can be highly relevant for industrial manufacturing and distribution facilities, transportation facilities, and utilities. In many cases, downtime can be measured using metrics for the service provided such as cost from lost operational income and ridership for transit systems. However, not all impacts caused by downtime can be measured this way. Impact to organizational reputation or loss of customer trust is an example of an impact that cannot be captured this way, but is nonetheless important to many organizations.

Safety: Injury or loss of life are usually used as metrics for safety. Other proxies such as meeting certain codes or accepted standards can be used. The latter is often preferred for assets that have been designed and engineered following accepted standards of practice. For legacy assets where this may not be true, explicit estimates of injury or loss may be necessary if safety is a concern.

Environmental: For certain assets, it may be important to measure environmental costs. Examples of this include CO2 or other greenhouse gas emissions, energy consumption, and levels of biodiversity. These metrics can be highly context dependent, but may be important when an organization operates under regulations and climate-change driven compliance requirements such as carbon caps.

Social: Public infrastructure and asset owners may need to measure impacts to social aspects in a community. Some examples include population displacement, access to essential services (water, electricity, heat), access to shelter. In some cases, long-term socioeconomic well-being may be of concern.

Selecting metrics for risk assessment is highly business-context dependent and there is no "one-size-fits-all" approach that can be applied. Another important factor for selecting the risk assessment approach is the organization's need to understand risk, including the post-event impacts, at different scales of breadth (more or less assets, longer or shorter time horizon) and depth (more or less resolution). If the purpose of an assessment is to identify potential risk and prioritize, there is likely more need for a wider, but shallow screening of risk to come up with indicators. Screening checklists designed for specific hazards are common tools for these purposes. It is also possible to use risk matrices with a scoring system that summarizes the likelihood and consequence of individual events. References for some of these methodologies are provided in Appendix A. On the other hand, for the development of business cases for capital decisions related to specific assets where impacts need to be evaluated in the specific asset and business context, quantitative assessments with high resolution and accuracy are more suitable. Some of the methods referenced in Appendix A may be used, and owners should consider reaching out to experts in this area for support. Organizations with a lot of assets may find it easier to invest in relatively high-level assessments that cover a lot of breadth first, before developing a progressively more refined understanding around a subset of the assets. This process of successive refinement should reduce uncertainties and provide more reliable information for action since they are expected to be supported by increasingly more accurate information, higher effort and cost. However, care is required that consistent risk assessment methods and assumptions are made for different stages of assessment during this process.

A general description of different levels of assessments in terms of the effort and outcome is provided below. While it is impossible to provide exact scopes and level of effort due to the large variability in organizational context, in industry norm and capability, these levels provides a baseline for asset managers to think about the optimal solution in specific business contexts.

Hazard screening deals only with hazard identification and indicative information about trends of hazards. This type of assessment is usually very low cost, low effort and may only take a few days to perform because it relies mainly on desktop studies. It can be useful for identifying assets that do not have any exposure, allowing for very cost-efficient prioritization. It will generally not provide information on risk unless the hazard is found insignificant.

Risk screening combines information on hazard and asset vulnerabilities to develop a view of risk, often qualitative, but sometime rough quantitative estimates are also given. These assessments are relatively low cost and can vary in technical details between different hazards. These assessments often involve checklists, proxies and simple scoring systems to characterize risk and may take days to weeks to complete. The level of uncertainty in the quantitative results can be expected to be high. Often these are suitable for preliminary planning and prioritization for large asset portfolios.
Risk assessment defines the standard level of effort and accuracy required for everyday planning activities related to asset management. Some asset-specific information such as condition reports, design documents and high-level asset data such as year of construction, floor area and occupancy may be required to support the assessment. When quantitative results are given, the level of uncertainty is expected to be moderate.

Comprehensive risk assessment tends to deal with very specific hazards and very specific groups of assets, possibly identified from previously completed screening studies. There can be substantial effort required to collect relevant data such as drawings, design documents, expert interviews, on-site inspections and tests to support the more sophisticated analyses. These types of studies can take weeks to months and are expected to provide quantitative estimates of risk with lower uncertainties to inform decisions related to specific scoping and budgeting of capital projects, or for very important property transactions. The results are highly specific to the target assets and usually cannot be generalized to other assets.

Risk Assessment Methods

When assessing risks for infrastructure or facilities exposed to extreme events, there are three common approaches, each with their merit and drawbacks. 1) Checklists based on proxies, 2) ISO31000-based methodologies, 3) Quantitative probabilistic assessments.

Checklists Based on Proxies: Checklist based assessment can be deployed with low cost and effort. These types of assessments are generally suitable for screening large number of assets or portfolios of assets without a comprehensive review of existing information. The checklists are often developed by technical authorities targeting a specific type of asset and/or specific types of hazards. The forms are typically filled out by experience operations personnel, or a hired consultant who has experience with the type of assessment involved. In practice, they are used for in a wide range of public and private sector asset owners, and they are one of the standardized tools used by insurance risk consultants to evaluate properties.

The level of information provided by this type of assessment is generally sufficient to develop priority lists amongst different types of assets, and in many case can suggest mitigation options. Figure 4.1 shows two examples of checklist based assessments. Figure 4.1a shows a cyber security screening tool with simple yes/no answers used for self-assessment. Figure 4.1b shows an example of a rapid visual screening form for earthquake risk in buildings. The form needs to be filled out by a licensed engineer, and it provides a proxy score that can be used for risk prioritization.

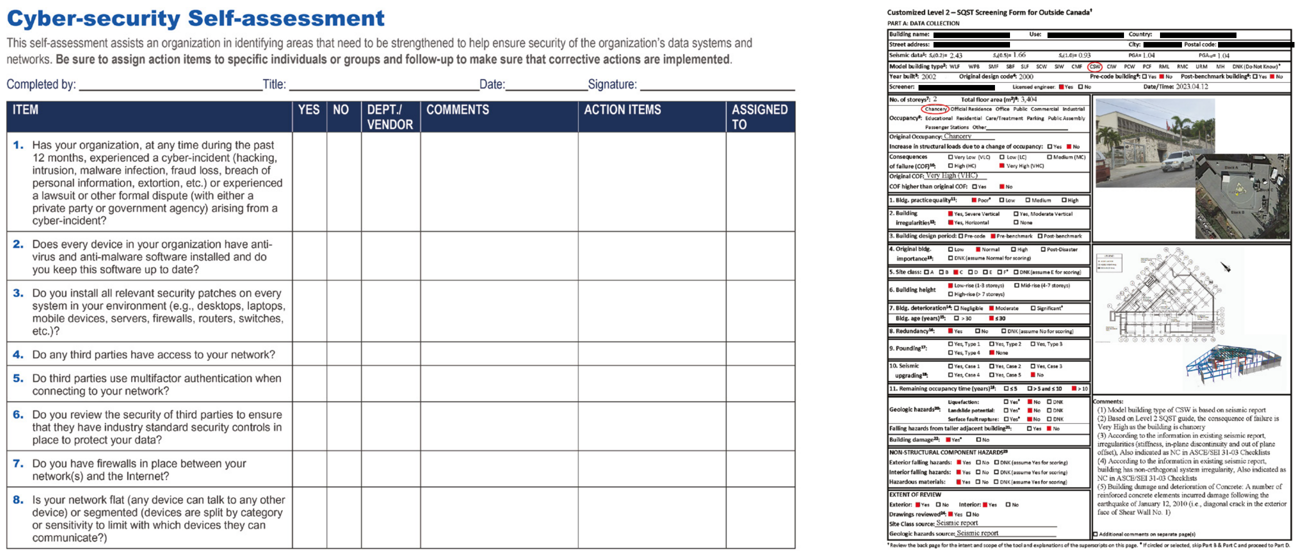
ISO31000-Based Methodologies:
This approach incorporates the principles outlined in ISO31000, which involves scoring risks based on the likelihood and consequence of individual events. This type of assessment can systematically cover a very large breadth of hazards and asset classes and it typically starts by identifying the types of undesirable events that are plausible, and then assigning each with a likelihood score

and a consequence score (e.g. 1 to 5 or 1 to 7). Depending on the specific methodology, the risk and likelihood scores are then combined in some way (usually multiplied) to get a risk score for the event of interest. The risk scores can be used to prioritize and identify vulnerabilities.

A team consisting of qualified risk professional, subject matter experts and key stakeholders is required to perform these assessments. Often, the likelihood and consequence scoring are done based on expert judgement, although in some cases, technical analysis may be performed to support the score assignments. The reliance on technical expert judgement means the cost and time required to undertake this type of analysis may be substantial and will scale with the scope of the assets and hazards of interest. Additionally, the use of discrete numeric scores to represent the extent of probability and consequence can lead to misinterpretation of risk if the user is not careful. This is because different hazards may involve likelihood and consequences that cannot be adequately characterized by a common set of scales. As an illustrative example, a likelihood score of 1 in a 5-point likelihood scale may represent very rare events that have less than 1% annual exceedance probability. By this definition, this threshold cannot differentiate the likelihood of a 100 year flood and 200 year flood, which can lead to the wrong characterization of risk. Due to these reasons, it may be difficult to derive quantitative metrics that support decision making from this type of assessment because the outputs are inherently qualitative as the scores do not measure observable and objective metrics in reality, or they are highly event-specific, or both.

Despite these limitations, the ISO31000 framework has been widely adopted into assessment standards for many different types of risk due to its versatility. Examples of standards for specific

a) b)



Cyber-security Self-assessment

This self-assessment assists an organization in identifying areas that need to be strengthened to help ensure security of the organization's data systems and networks. **Be sure to assign action items to specific individuals or groups and follow-up to make sure that corrective actions are implemented.**

Completed by: ____ Title: ____ Date: ____ Signature: ____

ITEM	YES	NO	DEPT./ VENDOR	COMMENTS	ACTION ITEMS	ASSIGNED TO
1. Has your organization, at any time during the past 12 months, experienced a cyber-incident (hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.) or experienced a lawsuit or other formal dispute (with either a private party or government agency) arising from a cyber-incident?						
2. Does every device in your organization have anti-virus and anti-malware software installed and do you keep this software up to date?						
3. Do you install all relevant security patches on every system in your environment (e.g., desktops, laptops, mobile devices, servers, firewalls, routers, switches, etc.)?						
4. Do any third parties have access to your network?						
5. Do third parties use multifactor authentication when connecting to your network?						
6. Do you review the security of third parties to ensure that they have industry standard security controls in place to protect your data?						
7. Do you have firewalls in place between your network(s) and the Internet?						
8. Is your network flat (any device can talk to any other device) or segmented (devices are split by category or sensitivity to limit with which devices they can communicate?)						

Customized Level 2 – SQST Screening Form for Outside Canada

PART A: DATA COLLECTION

Figure 4.1 Sample screening checklists a) cyber security self-assessment form b) visual screening form for seismic risk

risk include the ISO27005, NIST SP800-30, and the European Union Agency assessment framework for cyber risk, as well as ISO14091, Climate Lens Assessment Framework and PIEVC protocol, and the European Commission's ADAPT Platform for infrastructure risk under climate change. Figure 4.2 shows an example of a risk matrix, which summarizes the risk scores for each plausible combination of hazard event and exposed asset, and it is a typical outcome of a ISO31000-based evaluation.

Quantitative Probabilistic Assessment

This approach employs a fully probabilistic formulation to quantify the likelihood and impact of various hazards, usually through model simulations. In most cases, developing these assessments will require consulting with experts in the field. Compared to the ISO31000 risk scoring framework, this approach is used more often for specific hazards, particularly infrequent ones that require a high level of scientific expertise to forecast. Its main advantage is the ability to capture the physics and causal relationships behind asset damage and consequences under different types of hazards, and enables determining financial, downtime and other loss metrics that are directly relevant for asset management decisions. Since a computer model is typically employed for performing the risk calculations, the cost scales less with the size of the asset portfolio for quantitative analysis, which makes it an attractive option for large portfolios of assets. This approach is commonly applied to natural hazard risk forecasting and risk pricing in the insurance industry. Public asset owners also employ these methodologies for evaluating regional risk due to natural hazards. The HAZUS methodology produced by the Federal Emergency Management Agency (FEMA) in the US, is one popular tool that can be used to assess regional

Sample - Laboratory Facility Climate Risk Assessment (Change in Risk)	Extreme Heat			Higher Average Temp			Wildfire (smoke)			SDHI storm			Drough			Intense Rainfall			100 yr Riverine Flood		
	L	C	R	L	C	R	L	C	R	L	C	R	L	C	R	L	C	R	L	C	R
Scientific content and Evidence Room Content	2	2	4	2	2	4	1	2	2										2	3	6
Roof & Roof Structure	2	3	6							1	4	4				1	4	4			
Foundation and walls																1	2	2	2	4	8
Cladding & Siding & Insulation							1	1	1	1	4	4				1	2	2	2	4	8
Windows and doors	2	3	6				1	1	1	1	4	4				1	3	3	2	5	10
Walls										1	1	1				1	1	1	2	3	6
beams																1	1	1			
columns																1	1	1	2	3	6
slab																1	1	1	2	3	6
Roof Mounted Equipment	2	3	6													1	3	3			
HVAC (heaating, cooling, AHU)	2	4	8				1	3	3							1	3	3			
Pipes / Valves / Pumps																					
Interior & Exterior Lighting																					
Access & Security																					
Emergency Systems																			2	2	4
Building Automation System and Controls							1	1	1										2	3	6
Electrical System	2	4	8				1	1	1										2	4	8
Potable Water Services	2	2	4										2	3	6						
Wastewater Handling Systems																			2	4	8
Stormwater sewers, drain																			2	4	8
Road & Path Systems																			2	3	6
Parking																			2	3	6
Elevators							1	1	1										2	5	10
Natural infrastructure, ecosystem and biodiversity	2	5	10	2	4	8							2	4	8						0
Power	2	3	6				1	1	1												
Natural Gas service																					
Water service																			2	4	8
Sewage service																					
Telecommunication Systems																			2	5	10
Operations, Maintenance & Staff	2	4	8				1	4	4				2	3	6				2	5	10
Programming & Users	2	3	6				1	2	2										2	5	10

Sample - Laboratory Facility Climate Risk Assessment (Change in Risk)	100 yr Overland Flooding			Heavy Snowfall			Lightning /Hail			High Winds			Extreme Cold			Winter Freeze Thaw			Tornado		
	L	C	R	L	C	R	L	C	R	L	C	R	L	C	R	L	C	R	L	C	R
Scientific content and Evidence Room Content	1	1	1	-1	1	-1	1	2	2	1	1	1									
Roof & Roof Structure				-1	4	-4	1	3	3	1	4	4	-1	2	-2	-1	3	-3	1	5	5
Foundation and walls	1	3	3													-1	3	-3			
Cladding & Siding & Insulation	1	3	3	-1	2	-2										-1	2	-2	1	5	5
Windows and doors							1	3	3	1	3	3	-1	3	-3				1	5	5
Walls																			1	3	3
beams																			1	2	2
columns																			1	2	2
slab																			1	2	2
Roof Mounted Equipment				-1	3	-3	1	4	4	1	3	3				-1	3	-3	1	5	5
HVAC (heaating, cooling, AHU)													-1	4	-4						
Pipes / Valves / Pumps													-1	4	-4	-1	2	-2			
Interior & Exterior Lighting										1	2	2				-1	1	-1			
Access & Security																-1	1	-1			
Emergency Systems	1	2	2							1	1	1									
Building Automation System and Controls	1	2	2																		
Electrical System	1	3	3																		
Potable Water Services																					
Wastewater Handling Systems	1	2	2																		
Stormwater sewers, drain	1	2	2																		
Road & Path Systems	1	2	2	-1	2	-2										-1	4	-4			
Parking	1	2	2													-1	4	-4			
Elevators	1	4	4																		
Natural infrastructure, ecosystem and biodiversity																-1	3	-3			
Power				-1	3	-3				1	4	4									
Natural Gas service																					
Water service																					
Sewage service																					
Telecommunication Systems	1		0							1	5	5									
Operations, Maintenance & Staff	1		0							1	2	2									
Programming & Users	1		0																		

Figure 4.2 Example risk matrix from a climate change infrastructure risk assessment

earthquake, flood and hurricane risk for buildings and infrastructure. Other similar tools include FRAT developed by the Environment Agency in the UK for assessing flood risk, and the RiskScape developed in New Zealand for multiple hazards.

Advancements in computational capacity in the recent decades have propelled the application of these quantitative model-based assessments for physical hazards. For many asset classes and hazards, the evaluation will yield specific details about loss and consequences, as well as direct causes for losses and disruptions. Figure 4.3a shows one of the typical outputs produced by quantitative risk assessment, which is a loss exceedance probability curve (EP) that relates the level of loss in a critical distribution facility to the annual probability of exceedance. From the EP curve, the facility's average annual loss can be calculated, which can be used for capital planning, and assessing insurance premiums. Figure 4.3b shows a post-disaster recovery forecast for an important business operation after a major flood, which is an example of the level of detail that quantitative models can produce.

a)

b)

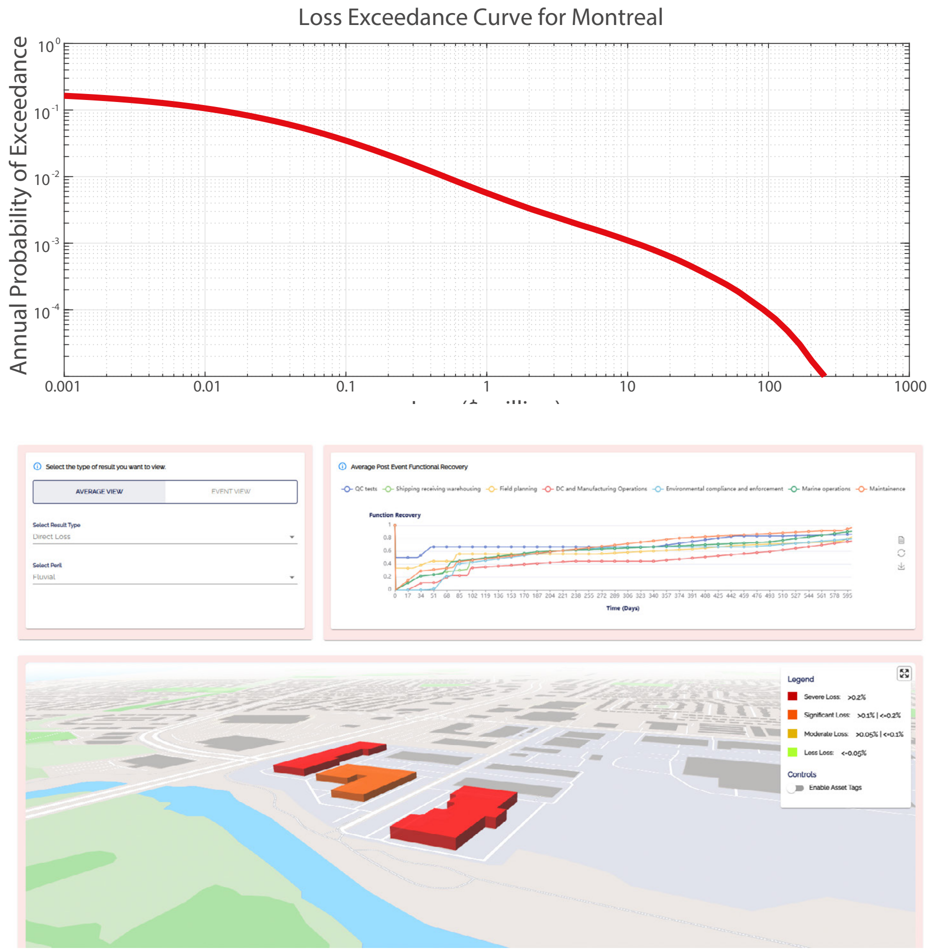


Figure 4.3 Outputs of quantitative probabilitic risk assessment a) example of loss exceedance probability curve b) example of portfolio risk heatmap and recovery time of functions

The Institute of Asset Management

High Impact Low Frequency Events

Leonard J. DeFrancisci

Traditional risk assessment approaches, such as the one outlined in ISO31000, generally identify and quantify known risks based on likelihood and consequence scores. This is a powerful and versatile approach to identify and rank risks based on expert opinions and supported by rational analysis. However, this practice can often overlook, or incorrectly treat events that are unpredictable or have a very low probability of occurrence but has high consequence. Often, it is events like these that will stress the organization and tests its resilience. Major climate and natural disasters like severe hurricanes, flash floods, earthquakes, as well as manmade events like global pandemics, terror attacks and major security breaches are amongst these. Organizations can be more significantly impacted by high-impact-low-frequency (HILF) events because of the low likelihood which can impair people's perception of risk, especially when the solution is complex and/or expensive. Unlike relatively frequent risks that are experienced, understood, and reacted to by many from a first person's perspective, it is likely that personnel in an organization have never experienced a HILF event before it occurs and thus experience is unreliable for dealing with them. In many cases, the impacts of these events are high because of the complex interdependency between assets, business processes and other factors not under the control of the organization that reveals additional vulnerabilities during and after the event. Hence, essential to reducing the impact of HILF events, is the ability to understand these interdependencies at a level that permits informed decisions for managing risk that meet the risk appetite and tolerance requirements. Depending on the complexity and decision-needs, a quantitative analysis may be more appropriate for understanding risk, and it may need to be combined with scenario stress testing to capture the cascading impacts of HILF risk. Regardless of the methods, in order for such an assessment to be effective, organizations should have a silo breaking mindset when dealing with interdependencies, which is further discussed in the next section. To manage HILF risk effectively, a robust combination of risk avoidance, risk mitigation, risk transfer and acceptance measures is often required.

Effective Risk Management

Effective risk management requires decision-makers to align risk assessment with the organizational value chain and clearly define the decision metrics of interest, to the required scope and depth commensurate with the decision needs. To illustrate, consider the risk assessment needs for a residential building owner and an airport authority. The residential portfolio owner may be interested in reducing litigation risk and property loss by identifying and strategically disposing of assets exposed to higher risk due to climate change over 10 years. As a first step, the organization may consider simple climate projections based only on asset locations for sea level rise, flood risk or prolonged days of extreme heat over the next decade to develop indicators of risk for this purpose. On the other hand, the airport authority who must protect and preserve functions of their assets may opt to conduct a detailed quantitative risk study to understand storm surge impacts and develop plans that meets the recovery time objectives of airport operations. The sophistication, time, financial cost and human resource investments required to conduct these two risk assessments can be different by orders of magnitude. In fact, the airport study will likely require more than just assessing damage, but also operational characteristics, including interdependencies as well as how the crew may react to different scenarios that impacts their daily operation. Therefore, it is important to align the assessments with the organizational needs and context so that the output and the level of effort invested are appropriate for supporting the decision needs.

It is also possible that there is insufficient data to support an assessment or that there are no readily available risk assessment solutions that meet the decision-making needs to the degree of reliability that an organization may initially specify. In these cases, the organization's risk appetite and tolerance may need to be revised. Many existing practical risk mitigation standards, such as FEMA extreme weather and earthquake screening guides, as well as emergent standards, such as the ASTM property resilience assessment [11], provides indications on the level of effort required for an assessment versus the expected levels of reliability in the results. A list of these tools are found in Appendix A for reference. Experienced risk professionals can also offer valuable input regarding the available and appropriate assessment approaches for different portfolio sizes and levels of detail.

Understanding risk is a prerequisite for making informed decisions to manage it. Thus, conducting a proper risk assessment is a crucial step for achieving resilience. If not certain about the organization's risk exposure and preparation level, the following list of questions is a good starting point for identifying gaps in knowledge and the type of assessment that is required.

1. Is a resilience and risk assessment required as part of regulatory compliance?
2. How (and why) would resilience outcomes impact the organization's bottom line?
3. What is the purpose of the risk assessment and what are the relevant decision-needs?
4. Has the organization established the metrics for measuring risk and acceptable thresholds in terms of risk appetite and tolerance?
5. Has the organization identified vulnerabilities related to key hazards and assets?
6. Does the organization have data from previous impacts or risks to people and assets?
7. Does the organization currently have a written business continuity or emergency management plan?
8. Has the organization identified any interdependencies to infrastructure systems or nearby assets that impacts the ability for the target asset to provide a desired level of

service? This may be internal interdependencies or external interdependencies.
9. What is the organization's capacity to implement and maintain resilience measures, if recommended?
10. What is the time horizon(s) in which the organization is interested (e.g., number of years, loan term, hold period)?

Once decision-makers have acquired a good understanding of risk, preferably at a quantitative level, a decision must be made whether the risk is acceptable or not by comparing it with the organization's risk appetite. For mature organizations, this risk appetite may be explicitly stated as a threshold of acceptable loss under the worst foreseeable event. A common pitfall for asset owners is to rely on technical regulatory documents such as building codes to determine such thresholds. While this approach certainly protects owners from some liabilities, it usually does very little to protect assets and organization values because regulatory documents are minimum standards for a very narrow set of goals that are usually safety related. While safety is important, it is not sufficient for most organizations. Hence, organizations must understand the risk exposure of their assets and operations rather than relying on codes and regulatory standards, as such metrics are simply outside the scope of these documents.

If the risk is larger than the risk appetite of the organization, then something must be done to reduce the risk (risk mitigation), transfer the risk to another party (insurance or other contractual arrangements) or increase the risk appetite (accept the risk). Each of these actions has financial and operational consequences. Specifically, risk mitigation by asset hardening typically requires upfront investment, which needs to be subjected to a business case analysis to understand if it is worth doing. Certain risk mitigation measures can be in the form of minor business process arrangements. For instance, during COVID-19, many organizations invested in online meeting capacities to enable employees to work from home. This transition is usually inexpensive since most firms already needed a similar capability to conduct regular business prior to the COVID-19 pandemic. Assets that support critical operations such as hospitals may not tolerate even a very small downtime, often in the order of seconds, and in some cases even a fraction of a second for some critical life-support systems. An arrangement for having an emergency maintenance contractor who will always prioritize the owner's call for minor repairs in post-disaster scenarios is very impactful for shortening downtimes. A risk assessment that includes impacts such as downtimes and service loss will identify these options. This aspect is discussed in the Interdependency section of this document.

Risk transfer is typically done through insurance, catastrophe bonds, or other contractual arrangements for hedging risk. Insurance is typically negotiated with a broker who will work with asset owners on optimizing a contract to underwrite risk. This is an area where diligence in understanding risk, and a demonstrable risk management plan can result in win-win situations because these will simultaneously reduce the owner's premiums while reducing the insurer's risk exposure. The owner must also be aware that not all risks are insurable. In fact, some risks that are insurable today may not be insurable tomorrow as exemplified by the aftermath of the 2022 and 2023 hurricane and wildfire seasons in the US where homeowners have been left without coverage after insurers stop offering property coverages for hurricane and fire. Asset owners may transfer some of their risk by passing certain responsibilities to tenants, try to mitigate risk through asset hardening or introducing redundancy, or, choose to accept this additional risk if it makes more sense to do so than to mitigate or eliminate it. This decision should not be made lightly and should be guided by facts and rigorous assessment.

Understanding Interdependency

The key activities in the resilience cycle prior to the occurrence of disruptive events are to assess, plan and prepare. These activities require asset managers to take a comprehensive and integrated approach to risk and resilience assessment, which should include the understanding and explicit consideration for interdependencies.
An interdependency is a situation-based condition where one part of a system is dependent on another and vice versa. Identifying and addressing interdependency is crucial because they can create vulnerabilities and amplify failures in complex portfolios of assets and infrastructure systems that provide essential function to the organization and to society. For example, a power outage can affect not only electricity consumers, but also digital services, transport, water supply, and other sectors that rely on electricity to function. Interdependencies can also lead to emergent outcomes, which are not related to any specific aspect of the system but emerge from all the elements combined, and can be very difficult to foresee without horizon scanning. Asset managers need to understand these interdependencies to ensure that they can maintain the reliability of service.

To understand interdependencies within or outside the organization, the asset manager needs to map out the connections and relationships between its

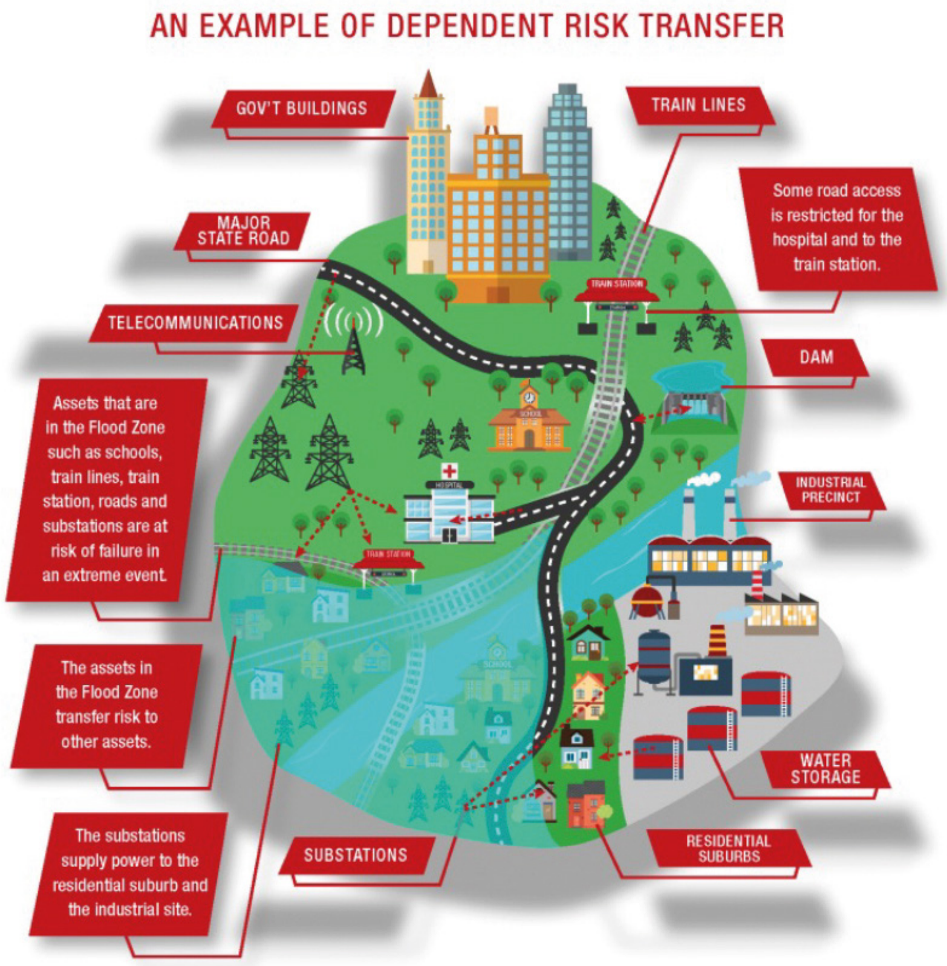


Figure 5.1 Illustration of internal and external dependencies

operations and those of other organizations. This includes identifying critical supply chain partners, customers, and stakeholders, and understanding how disruptions to their operations could impact the organization, as well as who the decision-makers are and how decisions are made during a disruption. This can be challenging, especially with complex asset systems that span different jurisdictions, locations and operating environments. Furthermore, this process can be inherently subject to large uncertainties. Despite these challenges, it is important for organizations to map interdependencies because it is required to assess how to recover. One of the biggest challenges for understanding interdependency in a system recovery context is the difficulty in compiling the relevant information supporting the evaluation, as there is often no standard approach for doing this. This is an issue that can be addressed, at least partially, by having a robust system of storing and updating asset information in the asset management plan. If no such asset information is available or if the information is incomplete, a well-designed stakeholder engagement program is required. More guidance on this is found in Appendix B.

Depending on the types of interdependencies being mapped and the decision needs, the process of compiling relevant information can be very different. The level of detail required is also different. A good contrast is to think of the interdependencies in a hospital complex versus that of the urban rail system. Generally, organizations can have both internal and external interdependencies, as illustrated in Figure 5.1. In the context of the hospital or the manufacturing facilities, the rail and power distribution infrastructure are external dependencies. The operation of the hospital and manufacturing facility require power and rail transport, but the owners of these facilities do not have control over these infrastructure systems. In contrast, these facilities also have internal dependencies that include internal service buildings that receive power, gas and water from the municipality, as well as local roads or machineries that are owned by each facility to serve its stakeholders.

Internal interdependencies are found within assets and operations that an organization has control over. For instance, the operation of an airport can be viewed as an integrated system of different terminal buildings, air traffic control, runway crews, maintenance hangars and freight handling facilities, amongst other assets and operations. Since the airport authority has jurisdiction over all of these assets, their interdependencies are considered internal. Consequently, much of the information related to internal interdependencies is expected to be found within the organization's own records, procedures and archives. Sources of information on interdependencies can include the following:

1. Asset register
2. Asset specifications
3. Planning documents
4. Design or as-built drawings
5. Reports and consulting studies
6. Maintenance records/incident logs
7. Manuals and standardized procedures
8. Operations personnel

Collecting this data for the assessment of risk often involves substantial effort if an organization does not have a system of maintaining and updating this information.

External interdependencies are services and processes that are not under the jurisdiction of the organization but are part of the integrated system that allows the organization to provide the desired level of service. For instance, municipal utilities, suppliers of a manufacturing facility, mutually dependent infrastructure networks are all examples of external interdependencies. External interdependencies are much more difficult to map accurately, so the uncertainty is typically very large. Getting this type of information also requires cross-jurisdictional collaboration, which can become complex and time consuming. Often establishing a framework is required through which groups can be vetted to access such data. For large infrastructure owners, there are often benefits in mapping the interdependencies between asset classes, which improves the level of resilience across the board. The mutual benefits of this information can often be used to justify co-investment. For instance, large investments in infrastructure, such as building access roads and flood defences, can make sense when considering that the cost and risks can be shared amongst the parties who benefit.

Aside from internal and external interdependencies, it is often useful to classify interdependencies as “physical” and “functional”. In this context, **physical interdependencies** refer to systems involving physical assets that were either designed or engineered, such as an assembly line in a manufacturing plant, redundant or backup facilities in a regional distribution network, as well as utility services like power, transportation and telecommunication. Interdependencies of these systems tend to be static and are likely determined at the design or installation of the related physical components. Therefore, information that describes the internal relationship of different physical assets within an interdependent network should be found from engineering drawings, archived design or planning documents, which should be managed according to the asset management plan. For external physical interdependencies, parties involved are often required to share some data with external organizations. A simple and common example of this is the publication of historical downtime statistics of power utility companies that enable individual facilities to prepare for potential outages. More complex interdependencies, such as those between transportation, power and water infrastructure networks in a city, will likely require specific data sharing arrangements between the parties involved.

On the other hand, **functional interdependencies** in this context refer to operational relationships required to deliver a given function that involve people as thinking and decision-making agents. For instance, enforcing environmental law in a marine environment involves access to vessels, a command centre, evidence storage and officers. Not only does this function depend on multiple smaller services that are facilitated by different assets, but the people involved in this function can also react to an incident differently, which can lead to different recovery outcomes. The knowledge of functional relationships internal to an organization usually resides within the operational staff themselves and can change dynamically in response to a new situation. Understanding internal functional interdependencies, therefore, requires the collection and maintenance of information from stakeholders and procedural documents that may be used as guides for emergency situations. Exercises can be part of a business impact analysis, which is an essential component for developing an effective business continuity plan. Some of these can be applied at a screening level to help asset owners understand the critical assets and operations within a larger system. External functional dependencies can be much more challenging to characterize. These can range from simple relationships such as the access to contractors and professional services for post-event recovery, to highly complex relationships in a supply chain network. These dependencies involve multiple decision-making agents outside the organization, whose actions can be highly uncertain despite the best efforts to map the interdependencies. For these situations, specialized tools, such as stress testing, and supply chain policies (see Supply Chain SSG) may be required to manage the risks effectively.

A mapping of interdependencies is useful on its own to identify critical points in the organization that are essential to upholding its services. By combining this information with risk assessment on potential hazards, it is possible to determine downtimes for services and identify ways to meet recovery criteria subject to an acceptable level of uncertainty using well-known risk and reliability engineering methods. However, despite best efforts, not all hazard and disruptive events can be predicted and forecasted with current capabilities. Having an up-to-date horizon scanning of credible threats and approaches to addressing them is important (see Horizon Scanning). For threats that are plausible but unpredictable, stress testing a system with interdependencies becomes a crucial tool for assessing the resilience of an organization and its operations. Stress testing is a formal process of asking "what if" questions without determining how likely the scenarios are. It helps organizations understand worst case scenarios that are plausible, although not predictable. Even if likelihoods of events are not established, the adequacy of existing asset conditions and operational policies subject to the worst-case scenario can be established. Stress testing is a practice that initially developed in the financial industry, but has migrated since to other sectors (existing standards such as the UN methodology are listed in Appendix A [12]).

Common approaches for stress testing are listed below. Note that often, these stress testing methods will involve acting out actual scenarios in real life, as many of the measures for recovery require making decisions in real time.

Scenario analysis: This involves developing a range of hypothetical scenarios that could impact the organization and its interdependencies and assessing the potential impact of each scenario.

Sensitivity analysis: This involves testing the impact of changes in key variables, such as interest rates or commodity prices, on the organization and its interdependencies.

Reverse stress testing: This involves identifying a worst-case scenario and working backwards to determine the conditions that would need to be present to cause that scenario to occur.

Network analysis: This involves mapping out the connections and relationships between the organization and its interdependencies and assessing the potential impact of disruptions to any one of these connections.

Monte Carlo simulation: This involves using statistical models to simulate a range of possible outcomes and assess the likelihood and potential impact of each outcome.

Operational risk stress testing: This involves testing the resilience of the organization's operational processes and systems under stress conditions.

Liquidity stress testing: This involves testing the organization's ability to maintain sufficient liquidity under stress conditions.

These stress testing methods can help asset managers or organizations to identify potential weaknesses in their interdependencies and develop strategies to improve resilience and mitigate risks. In order for stress testing to be effective, interdependencies in the systems of interest must be mapped and understood in such a way that allows decision-makers to compare and assess different options for recovery and their consequences. As an example, suppose that an asset manager wants to stress test the interdependency between a power plant and a water treatment plant under future climate scenarios that leads to more drought. The asset manager could use scenario analysis to assess the potential impact of a prolonged drought on the water supply to the power plant.

To undertake this scenario analysis, the asset manager could develop a range of hypothetical scenarios that simulate the impact of a drought on the water supply to the treatment plant, without explicitly evaluating the likelihood of these scenarios. They could then assess the potential impact of each scenario on the power plant's operations, such as the ability to generate electricity, using the mapped interdependencies. For example, the asset manager could simulate a scenario where the water supply to the treatment plant is reduced by 50% for a period of six months. They could then assess the potential impact of this scenario on the power plant's operations, such as the ability to cool the generators.

Based on the results of the scenario analysis, the asset manager could then develop strategies to improve the resilience of the interdependency between the power plant and the water treatment plant. This could include measures such as increasing the capacity of the water storage reservoir or developing alternative sources of water.

Incident Response and Recovery

Incident response and recovery is the final element in resiliency. While resiliency is the "insurance plan" for your business, incident response and recovery are the "coverage limits" of your plan. They are the tools in your toolkit for how one prepares, responds, and recovers from an impactful event. It is important to use your horizon scanning to proactively inform your escalation level based on the type and nature of the event. Incident response is typically the low frequency-high consequence event that requires massive and highly orchestrated response and recovery. It is easier to "ramp-up" quickly and retract than to respond from a position of knowledge deficit. Asset managers may not be in an organizational position to own the narrative if found reactive. Business continuity and disaster preparation, response, and recovery are interrelated and must be done harmoniously. Also noteworthy, public events like parades, celebrations, protests, and athletic games constitute low probability yet high consequence type of situations where large public-agency resources are consumed across multiple enterprise departments. It may impact a different side of infrastructure not commonly found in a traditional emergency preparation thought or decision-making process.

Incident response and recovery is where the "rubber meets the road" and is embedded in the ability of assets to anticipate, resist, absorb, recover, adapt and transform in the face of a range of future shocks and stresses. Without incident response and recovery, organizations leave their value chain, strategic outcomes, and levels of service highly exposed to hazards.

A key principle in incident response and recovery is to build on existing knowledge, avoiding the need to "reinvent the wheel". Major disasters worldwide have provided valuable lessons, best practices, and structured approaches to resilience. Effective asset managers leverage this accumulated wisdom, adapting proven practices into their own resilience plans. Mature organizations capable of conducting horizon scans (see previous section) should do so to gather experience and evidence from others who have experienced major disruptions. For less mature organizations challenged with where to begin, scanning the horizon may be your best tool to help answer these basic questions:

- Who might have already experienced a business disruption or event similar to our organization's concerns for which we can learn how to prepare, respond, and recover?

For example, our organization may be strategically planning to avoid business continuity impacts to our community's infrastructure from flooding, hurricane, wildfire, drought, climate change, or other similar events.

- What was their event and ensuing experience from the event?
- What lessons did they learn?
- Did they have an AMP, SAMP, or are they developing one as a result?
- Did they prepare a BIA and understand the impacts to their value chain and level of service?
- What local, state, or federal emergency action or incident response and recovery guidance is available?
- What Incident Response & Recovery is available from other organizations (e.g. private "for-profit", public "non-profit")?

Private sector response and recovery may present unique challenges depending on the type of organization and their consumer or customer base. For example, the Pfizer warehouse facility in Rocky Mountain, North Carolina was severely damaged from an EF3 tornado placing medical supplies as risk. Similar disruptions occurred after the Great Hanshin Earthquake of 2011 and the more recent 2024 Taiwan earthquake, which impacted the global automotive and computer chips supply chains, respectively.

As part of the recovery solution, an organization needs to understand if sound insurance and asset management strategies are being deployed. Note that although these are not replacements for a business continuity plan, both are part of the overall competence of the organization for managing the impacts of disruptive events. Specifically, an effective insurance strategy allows an organization to gain access to potentially significant upfront capital required to cover the repair and replacement of damaged assets, temporary provisions for migrating operations, as well as lost income. A good understanding of the available insurance coverage limits, triggering criteria and adjustment process, therefore, is vital to the recovery. Despite having insurance coverage, asset owners will also have exposure to risk of damage or disruption, sometimes even significant exposure, that is not covered by insurance or is uninsurable. Understanding what these limitations to coverage are, and implementing strategies to protect the related assets and operations through maintenance and capital investment, or more redundancies in operational procedures should be part of the asset management plan. It is also prudent for asset managers and leadership to understand that even if funding is available and even if damage is controlled, there will be other factors that will delay recovery following a major event. These factors must be considered in the incident response and business continuity plans. A non-exhaustive list of common factors outside of the control of asset owners that causes delays in recovery can be found below:

Utility Disruption: Loss of power, water, telecommunication, and any vital capabilities required for operation due to a regional event such as a hurricane or earthquake.

Transportation: Severance of critical roads, bridges and routes facilitating other modes of transportation can lead to a partial or total halt in operation if employees cannot get to work.

Accessibility Restriction: Some sites can be inaccessible following an event even when no property damage is triggered. For example, the presence of flood water can cut off access as it can be a life safety hazard if the water is sufficiently deep or if there is a risk of electrocution. Cordoning of urban areas by city officials due to disease outbreaks or earthquakes can also restrict access to a site.

Health and Safety: Some events can trigger evacuations of buildings and sites due to life safety concerns, which may not be covered under insurance. Reduced quality of air due to wildfire smoke is one example. Release of harmful substance like asbestos in an older facility is another.

Staff Shortage: Many disruptive events are regional and impact many people's homes and loved ones. The availability of staff may fall short under these circumstances, leading to further disruptions.

Shortage of Professional Services: Recovering from a regional event that requires professional services, such as inspectors, engineers, finance professionals, legal professionals, and/or trades people, may experience delays due to surges in demand from other organizations/businesses in the same region that were impacted.

Shortage of Supplies: Similar to services, replacement of certain parts or supplies that are not usually stocked (e.g. elevator, large chillers, or special equipment) can present challenges due to a temporal surge in demand.

In addition to these factors, organization-specific context, such as in the example of Pfizer, TSMC and the automotive industry in Japan, can give rise to other challenges that must be considered when planning for recovery. Public organizations also have their own context specific considerations, which depend on local policies and culture, and can be very different from a private organization. For instance, in the United States and for public agencies or widespread disaster preparation, response, and recovery, the Federal Emergency Management Agency under the Department of Homeland Security has developed unified incident response and recovery systems. FEMA's toolkit is scalable and adaptable to various-sized public agencies and disaster types; hence, "one size" does not "fit all". Reference 1 lists examples of actions and unified management systems involved with incident response and recovery.

It is important to note that incident response management and asset management are both management systems. Both are necessary to coordinate an emergency event. Incident response and recovery become an interdependency between emergency management and asset management. Without SAMPs and AMPs and an understanding of an organization's value chain and levels of service, navigating incident response and subsequent recovery of assets becomes "organized chaos" at best. Emergency management and asset management are both structured approaches. The former requires the latter to be already in place for a well-coordinated incident response and recovery. For example, the City of Grand Rapids, Michigan, experienced a near-record flood event from the Grand River through its downtown in 2013. The original flood protection system was a patchwork of public works projects (concrete retaining walls and soil embankments) and private buildings whose basement walls were the flood protection structural element. Most segments of the 16-mile flood protection system dated to the 1850s. Those present in the Emergency Operations Centre did the best they could, based on institutional knowledge, but it was "organized chaos "and reactionary, both in response and communication. Two crucial items were missing:

- Lack of flood protection asset system inventory, condition, risk, and capability assessment.
- Lack of a contingency plan as the city had no means of bolstering flood prone areas against inundating flood waters. In other words, the city had no sandbags available or volunteer operational plan ready to implement.

The easy lesson learned from their incident response was to develop an asset management plan for their flood protection system. The plan identified acceptable levels of risk, service, and floodwall deficiencies against a 100-year flood event. Operation and maintenance plans had to be developed and approved by FEMA for all river stages, including post-flood inspection and evaluation. The city also received emergency management training and certification for all levels of personnel within the organization from FEMA.

It is important to understand who has unified command of the incident response for multi-jurisdictional coordination of assessment, resources, and recovery actions within an emergency management system. Most commonly, police and fire first responders to a public safety emergency event follow a standard protocol called the Incident Command Structure (ICS). This may not be known to the engineering, accounting, finance, and business industries and this type of operating environment can be foreign to the asset manager, yet it is critical to learn how to adapt the asset management system to the ICS. In this case, the ICS will take the lead in more than 90% of the scenarios; however, there are newer operating environments to which the asset manager may be required to adapt. For example, climate change has been discussed since the 1800s in many historical references, yet the data, modelling, politics, and interdependencies are a relatively new environment to which asset managers must learn to adapt. Extreme climate-related events can be devastating and widespread, covering large geographical areas; hence, the asset management system will likely be a smaller but important presence within a large-scale incident response and recovery process.

After the incident, asset management emerges in the forefront when physical, operating, financial, and non-financial assessment of asset damage is required to be recorded and submitted in a standardized format for state or federal financial reimbursement.

Emergency or Contingency Planning is the action for Incident Response and Recovery. This guide offers a list of considerations, as a resource, for asset managers developing the incident response and recovery plan or toolkit:

1. Complete asset management planning with emphasis on asset inventory, risk, and levels of service that may be impacted.
2. Identify existing insurance coverage, understand limits, conditions and deductibles. Assess the risk exposure factoring the existing insurance coverage.
3. Identify relevant factors that may contribute to disruptions, including damage and operational disruptions caused directly by the event, as well as those that are indirectly caused by an event. For organizations having many external interdependencies, work with related parties to map interdependencies. Appendix A contains a list of existing resources for community and infrastructure resilience, with concrete approaches to conduct interdependency mapping between different asset-owning organizations.
4. Identify the national, regional, or local ICS and Emergency Operations Centre/Administrator to discuss the structured approach to emergencies. Discuss the integration of the asset management system or other systems that may be integrated like risk management, facility management, and financial management
5. Develop adequate capability and capacity for incident response and recovery. Significant resources may be consumed (personnel, materials, equipment, volunteers, and funding), which may have a considerable impact on normal business operations, business revenues, and organizations and the

community's ability to recover. Hence the importance of the BIA and horizon scan (see previous sections). Also, the importance of competency improvement.

6. Clarity of roles and responsibilities. Everyone will be impacted at some level. Clear roles and responsibilities to execute any contingency plan for response and recovery is essential. The SSG on Asset Management Leadership will contain attributes for asset managers in leadership positions responsible for lead roles during emergency events. Additionally, assuring respondents are in the proper role based on situational behaviours is crucial. Hence, certain personality profiles and natural talents should be aligned with the appropriate roles and responsibilities expected for incident response and recovery. For example, an individual who acts calm and under control in pressure situations may be a candidate who has a key lead role within an ICS. In a contrary example, damage recovery can be emotionally sensitive for members of the public, therefore, damage assessments may require personnel having high emotional intelligence for awareness of sensitivity amongst those they meet in the aftermath of a disaster.
7. Contingency planning and a 'gameplan' rooted in the S.M.A.R.T principles (Simple, Measurable, Attainable, Realistic, and Timebound). Identify, quantify, and cost the materials and equipment necessary to execute the contingency plan using your asset management plan and activities.
8. List of contractors and consultants with names, contact information, emergency contact numbers, equipment, and materials available. This is considered a live asset inventory and must be assigned and updated annually. Use the assessment of risk and disruption (step 2) to inform if special arrangements, contractual or otherwise, need to be created with certain resources (e.g. special contractors) to prevent a recovery bottleneck caused by the lack of availability of critical persons or services.
9. Documentation. Many recovery operations will involve financial assistance. In the United States, assessing and recording post-disaster events is required using prescribed federal documentation. This is generally one-sided since assessments generally do not involve existing conditions; therefore, significant financial value may be lost. Hence, having asset management plans in place aids in understanding the gap between pre- and post-disaster events. Quantifiable levels of service gaps and impacts to the business from a BIA complete this reimbursement request.
10. Avoid working autonomously, enabling others to do the best they can volunteer or contribute is critical for the general public or the common good.
11. Recognize and participate in your national, regional, or local emergency management operations working group or practice teams.
12. Participate in an equivalent emergency action forum to share common knowledge, best practices, and lessons Learned.
13. Value Realization. When developing any incident response, the horizon scan enables the asset manager to "right-size" incident response and recovery based on being wise stewards of public and private funding while simultaneously minimizing the impact to the business value chain that ultimately sustains the organization to achieve its long-term vision and goals. Without this mindset, the latter will never be realized.
14. Regularly scheduled practice in a department, organization, and interagency. This final element cannot be overstated. Incident response should not be a plan that "collects dust on the shelf". It is a living and breathing document that must stand the time of attrition, political needs, and a changing environment. It must be adaptable.

References

1. **IAM Subject Specific Guidance 32 (SSG32)** – Institute of Asset Management (IAM). (2019). Contingency Planning & Resilience Analysis.
2. **GFMAM Landscape Document** – Global Forum on Maintenance and Asset Management (GFMAM). (2024). Asset Management Landscape v3.
3. **Connelly C., Knight, M.** – Institute of Asset Management (IAM). (2024). Why resilience needs to be on your radar.
4. **Lencioni, P.** (2012). The Advantage: Why Organizational Health Trumps Everything Else in Business. Jossey-Bass.
5. **Lencioni, P.** (2000). The Four Obsessions of an Extraordinary Executive: A Leadership Fable. Jossey-Bass.
6. **Porter, M.** (1985). Competitive Advantage: Creating and Sustaining Superior Performance. Free Press.
7. **Cockram, M., & Van Den Heuvel, M.** (2012). Organizational resilience. Business Continuity Institute.
8. **Fragouli, E., et al.** (2013). Leading in crisis: Leading organizational change & business development. International Journal of Information, Business and Management, Volume 7 (3). 71-90.
9. **ISO 31000** – International Organization for Standardization. (2018). Risk Management – Guidelines.
10. **IAM Subject Specific Guidance 31 (SSG31)** – Institute of Asset Management (IAM). (2016). Risk Assessment and Management.
11. **United Nations Resilience Methodology** – United Nations Office for Disaster Risk Reduction (UNDRR). (2023). Global Methodology for Infrastructure Resilience Review.
12. **ASTM Property Resilience Assessment Guide** – ASTM International. (2024). ASTM E-3429 Standards for Property Resilience Assessment.

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
A Guide to Implementing System-based Approach to Climate Resilient Infrastructure	Voluntary Guidance	Infrastructure resilience	All	Infrastructure	Canada
ASTM Property Resilience Assessment	Voluntary Guidance	Property risk assessment	All	Buildings/Sites	US
Energy Resilience Assessment Methodology	Voluntary Guidance	Infrastructure resilience	All	Power infrastructure	US
European Resilience Management Guideline (ERMG)	Voluntary Guidance	Community resilience	All	Communities	Europe
Marine Transportation System Resilience Assessment Guide	Voluntary Guidance	Infrastructure resilience	All	Infrastructure	US
Methodology for Assessing Regional Infrastructure Resilience	Voluntary Guidance	Infrastructure resilience	All	Infrastructure	US
NIST Community Resilience Planning Guide for Buildings and Infrastructure Systems	Voluntary Guidance	Community resilience	All	Communities	US
Power Sector Resilience Planning Guidebook - A Self-Guided Reference for Practitioners	Voluntary Guidance	Infrastructure resilience	All	Power infrastructure	US
Resolute	Voluntary Guidance	Transportation infrastructure resilience	All	Transportation infrastructure	Europe

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
Federal Highway Administration Vulnerability Assessment and Adaptation Framework	Voluntary Guidance	Infrastructure resilience	All	Transportation infrastructure	US
Climate Vulnerability Assessment Guidance for Nuclear Power Plants	Voluntary Guidance	Infrastructure resilience	Climate	Power infrastructure	US
Developing a Climate Change Adaptation Interdependency Process with Economic Considerations	Voluntary Guidance	Infrastructure resilience	Climate	Transportation infrastructure	Canada
Public Infrastructure Engineering Vulnerability Committee (PIEVC)	Voluntary Guidance	Property risk assessment	Climate	All	Canada
WHO Guidance for Climate-resilient and Environmentally Sustainable Health Care Facilities	Voluntary Guidance	Infrastructure resilience	Climate	Healthcare	International
Measuring the Climate Resilience of Health Systems	Voluntary Guidance	Property risk assessment	Climate	Healthcare	International

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
Primary Protection: Enhancing Health Care Resilience for a Changing Climate	Voluntary Guidance	Property risk assessment	Climate	Healthcare	US
ICAO Climate Change: Climate Risk Assessment, Adaptation and Resilience	Voluntary Guidance	Infrastructure resilience	Climate	Transportation infrastructure	International
ASTM E2026	Voluntary Guidance	Property risk assessment	Earthquake	Buildings	US
FEMA P-154	Voluntary Guidance	Property risk assessment	Earthquake	Buildings	US
NRC Seismic Evaluation Guideline	Voluntary Guidance	Property risk assessment	Earthquake	Buildings	Canada
Climate Resilience Buildings: Guideline for Management of Overheating Risk in Residential Buildings	Voluntary Guidance	Property risk assessment	Extreme heat	Buildings	Canada
Weathering the Storm: Developing a Canadian Standard for Flood-Resilient Existing Communities	Voluntary Guidance	Community resilience	Flood	Communities	Canada

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
National Guide for Wildland-Urban Interface Fires	Voluntary Guidance	Property risk assessment	Wildfire	All	Canada
WUI Virtual Handbook for Property Fire Risk Assessment and Mitigation	Voluntary Guidance	Property risk assessment	Wildfire	Buildings	US
Climate Change: Assessment of the Vulnerability of Nuclear Power Plants and Approaches for their Adaptation	Supporting Information	Infrastructure resilience	Climate	Power infrastructure	International
IAEA Climate Change and Nuclear Power	Supporting Information	Infrastructure resilience	Climate	Power infrastructure	International
ISO 22301	Standard	Business continuity	All	All	International
ISO 31000	Standard	Risk management	All	All	International
ISO37102	Standard	Community resilience	All	Communities	International
ISO37123	Standard	Community resilience	All	Communities	International

The Institute of Asset Management

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
J100-21 Risk and Resilience Management of Water and Wastewater Systems	Standard	Infrastructure resilience	All	Water infrastructure	US
ISO 14090	Standard	Climate risk assessment	Climate	All	International
FEMA P-58	Standard	Property risk assessment	Earthquake	Buildings	US
FEMA P-2062	Standard	Property risk assessment	Wind	Buildings	US
Water Resilience Assessment Framework	Risk Assessment Tool	Infrastructure resilience	All	Water infrastructure	International
ICLR Guides	Risk Assessment Tool	Property risk assessment	All	Buildings/Sites	Canada
ULI Developing Resilience Toolkit	Risk Assessment Tool	Property risk assessment	All	Buildings/Sites	US
UNDRR Quick Risk Estimation	Risk Assessment Tool	Community resilience	All	Cities	International
UNDRR Stress Testing Tool	Risk Assessment Tool	Infrastructure resilience	All	Infrastructure	International
Heath Care Facility Climate Change Resiliency Checklist	Risk Assessment Tool	Property risk assessment	Climate	Healthcare	Canada

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
HAZUS Earthquake	Risk Assessment Tool	Property risk assessment	Earthquake	Buildings/Infrastructure	US
HAZUS Flood	Risk Assessment Tool	Property risk assessment	Flood	Buildings/Infrastructure	US
HAZUS Hurricane	Risk Assessment Tool	Property risk assessment	Wind	Buildings/Infrastructure	US
ENVISION	Rating system	Infrastructure resilience	All	Infrastructure	International
IBHS Fortified	Rating system	Property risk assessment	All	Buildings	US
RELi Rating System	Rating system	Property risk assessment	All	Buildings	US
SuRe Standard	Rating system	Infrastructure resilience	All	Infrastructure	International
REDi Rating System	Rating system	Property risk assessment	Earthquake	Buildings	US
USRC Earthquake	Rating system	Property risk assessment	Earthquake	Buildings	US
USRC Wind	Rating system	Property risk assessment	Wind	Buildings	US

The Institute of Asset Management

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
Resilience Rating System – A methodology for building and tracking resilience to climate change	Rating system	Building project assessment	Climate Change	Buildings	International
Overview of Engineering Options for Increasing Infrastructure Resilience	Supporting Information	Infrastructure resilience	All	Infrastructure	International
The Good Practice Note for Energy Sector Adaptation	Voluntary Guidance	Infrastructure resilience	Climate Change	Power Infrastructure	International
Hydropower Sector Climate Resilience Guide	Voluntary Guidance	Infrastructure resilience	Climate Change	Power Infrastructure	International
Stronger Power – Improving Power Sector Resilience to Natural Hazards	Voluntary Guidance	Infrastructure resilience	Natural Hazards	Power Infrastructure	International
US Climate Resilience Toolkit	Voluntary Guidance	Buildings	Climate Change	Buildings	US
No Broken Link: The Vulnerability of Telecommunication Infrastructure to Natural Hazards	Supporting Information	Infrastructure resilience	Natural Hazards	Telecommunication Infrastructure	International

Appendix A: List of Resources

List of published standards and assessment methodologies for different sectors.

Reference	Type of Document	Topic	Hazard	Asset	Region
Highway Development and Management Model (HDM-4) Dissemination Tools	Risk Assessment Tool	Infrastructure resilience	Natural Hazards	Transport Infrastructure	International
Vulnerability Assessment and Adaptation Framework	Risk Assessment Tool	Infrastructure resilience	Natural Hazards	Transport Infrastructure	International
Resilient Water Infrastructure Design Brief	Voluntary Guidance	Infrastructure resilience	Flood, Drought, Wind	Water Infrastructure	International
Incorporating Climate Change Adaptation in Infrastructure Planning and Design	Voluntary Guidance	Infrastructure resilience	Climate Change	Water Infrastructure	US
IAM Assessment Tools and Methodologies for Climate Resilience Across Sectors	Supporting Information	Infrastructure resilience	Climate Change	Assets (diverse)	International

Appendix B: Stakeholder Engagement

Guidance is provided for internal stakeholder engagement for assessing risk and resilience and external stakeholder engagement for improving understanding of interdependencies across organizations. Users of the Good Practice Guide may use this appendix as a starting point to develop a stakeholder engagement process that aligns with organizational goals for resilience.

Understanding needs for risk and resilience assessment

Internal stakeholder engagement can be carried out as a self-assessment by the business continuity manager, asset managers or organizational leaders or by an external party to help define the organization's need and context for resilience. Key objectives of this assessment are to establish the condition of assets, identify gaps in data, define interdependencies (both internal and external), and establish goals and requirements for assessment. Since resilience should be tied to the value chain and level of service the organization provides, one of the first tasks in stakeholder engagement is to put together the relevant participants whose work influences the value chain and the level of services. This team can include staff from operations, maintenance, asset management, real estate and facility management, HR and payroll services, legal services, as well as compliance. Depending on the organization, additional roles may need to be included in the team. For instance, science program leads from a research facility could be invited.

As a team, the stakeholder group needs to develop a set of baseline resilience goals for each business unit and for the organization as a whole, and evaluate whether this can be achieved based on existing state and knowledge (data) on assets and operations. At a minimum, the following aspects should be explored and confirmed.

1. What is the ownership status of assets critical for the organization and its operation (e.g. leased, owned)?
2. What hazards are you most worried about and is there any known vulnerability of assets and operations to these hazards?
3. Is there an incident log for damaging or disruptive events?
4. Has a hazard and risk assessment been conducted to understand the extent of impact, and the options for managing this risk?
5. Is there property and casualty insurance? Is the coverage adequate?
6. Is there business interruption insurance? Is the coverage adequate?
7. Is there a business continuity or contingency plan? When was the last time it was updated? Has it been tested, and how often is it being tested?
8. Has a business impact analysis been conducted? When was the last time it was updated?
9. Have the critical points of key operations/assets been identified? Do the recovery time and recovery point objectives in the Business Continuity Plan require update?
10. Do you have up-to-date information on the condition of your assets? How is the data managed? How often is it updated? How easily can it be accessed and shared amongst the organization?
11. Has the interdependency of internal assets and operations been mapped? Can root causes be tracked quickly in case of an emergency?
12. Is there any external dependency on infrastructure or nearby assets that impacts the ability to deliver service? To what extent can the organization impact these systems?
13. What are the constraints and limitations on the organization's capability to implement resilience measures, if such are recommended? Common constraints include financial, human resources, technological limitations and legal.

Gaps identified in this engagement process need to be documented clearly to support plans for action. If a risk or resilience assessment is required to develop the necessary evidence to inform action, the requirements for such an assessment should be aligned with the decision need by specifying the deliverables, as well as the appropriate scope and depth commensurate with the level of effort and resources available. Refer to the Assessing and Managing Risk Section for a description of the different types of risk assessment. Some relevant questions that the stakeholder group should explore before engaging in a risk assessment are listed to aid the selection of the appropriate assessment approach.

1. How do the identified hazards impact the organization's ability to operate and provide the required level of service?
2. What are the current decision-needs related to resilience, and what impacts and associated metrics are considered relevant for decision-makers to make these decisions?
3. Is there a time frame of interest associated with the decisions? This can be related to the anticipated remaining life of assets, disposal plan or external changes such as regulatory and environmental (e.g. climate change).
4. How has the organization approached the challenges of resilience before, and what issues and challenges need to be addressed?
5. What are the existing constraints with respect to resilience, which can be physical, financial, organizational and regulatory.
6. Are there available data to support the type of assessment required?
7. What other aspects are important for the assessment?

Understanding interdependencies across organizations

Stakeholder engagement is a multifaceted process that is essential for organizations to navigate the complex web of interdependencies that exist both within their internal structure and with external entities such as other asset managers of critical services. Understanding these interdependencies is crucial because it allows an organization to anticipate how changes in one area can have ripple effects throughout the system. For instance, a decision made by a supplier can impact production schedules, which in turn can affect customer satisfaction. By engaging with stakeholders, an organization can gain insights into these connections, enabling it to manage its assets more effectively and maintain operational stability.
The importance of stakeholder engagement cannot be overstated. It serves as a bridge that connects an organization with the various groups and individuals that it affects and that affect it in return. Through this engagement, an organization can build trust and credibility, which are the cornerstones of a strong reputation. By demonstrating a commitment to transparency and accountability, an organization can foster a sense of goodwill and cooperation among its stakeholders, which is invaluable for long-term success.

Moreover, stakeholder engagement is a proactive means to identify and address the concerns and needs of different groups. By fostering open communication, an organization can prevent conflicts and strengthen its relationships. This dialogue is not just about listening; it is about actively responding and showing stakeholders that their perspectives are valued. Such an approach leads to more informed and inclusive decision-making, ensuring that the organization's strategies are aligned with the needs and interests of those it serves and depends upon.

Incorporating the insights and expertise of stakeholders into decision-making processes enriches the quality of these decisions. Stakeholders often bring a wealth of knowledge and experience that an organization might not possess internally. By tapping into this resource, an organization can make choices that are not only well-informed but also more likely to be accepted by those affected by them.

Furthermore, resilience is a key benefit of stakeholder engagement. Understanding the interplay between different assets and stakeholders allows an organization to identify potential risks and vulnerabilities. With this knowledge, it can develop strategies to manage these risks proactively, enhancing its ability to adapt to change and ensuring the sustainability of its operations.

The process of stakeholder engagement is not linear but rather an ongoing cycle of interaction and adaptation. It begins with the identification of the various groups that have a stake in the organization's operations, ranging from government agencies and infrastructure partners to customers and the general public. Recognizing these stakeholders is the first step in understanding the broader context in which the organization operates.

Once stakeholders are identified, the organization must delve into understanding their specific needs and concerns. This understanding can be achieved through a variety of methods, such as direct dialogue, surveys, or focus groups. The insights gained from these interactions are invaluable for shaping the organization's approach to managing its assets and relationships.

With a clear understanding of stakeholder perspectives, the organization can then craft a tailored engagement plan. This plan outlines the goals, strategies, and actions necessary to effectively communicate and collaborate with each stakeholder group. It addresses how to involve stakeholders in decision-making and how to respond to their concerns in a way that is both strategic and empathetic.

The implementation of the engagement plan requires careful and consistent communication. It's about creating a dialogue that is ongoing and responsive, ensuring that stakeholders are kept informed and that their feedback is not just heard but acted upon. Monitoring and evaluating the effectiveness of these efforts is also critical, as it allows the organization to refine its approach and continuously improve its stakeholder relations.

In essence, stakeholder engagement is about fostering a collaborative environment where trust is built, insights are shared, and resilience is developed. It is a dynamic process that requires an organization to be attentive, responsive, and adaptable to the needs and concerns of its stakeholders, thereby ensuring that it can navigate the complexities of its interdependencies with confidence and foresight.

Acknowledgements

Authors and Reviewers (IAM Resilience Group)

- Ben Kuchta
  National Grid
- Charlotte Connelly
  Lenoardo
- Chris Chen
  Infrastructure Canada
- Jack Guo
  Kinetica Risk
- Kambiz Rasoulkhani
  AMCL
- Mark DeClerq
  Applied Asset Management
- Olu EriOlu
  KPMG

External Reviewer

- Eric Pradeep
  WSP

With thanks to our IAM Patrons whose support is greatly appreciated

Institute of Asset Management
St. Brandon's House
29 Great George Street,
Bristol, BS1 5QT
United Kingdom

T: +44 (0)117 4504990
E: office@theIAM.org
www.theIAM.org

The Institute of Asset Management

the leading professional body
for the asset management community