# Why Resilience Needs To Be On Your Radar

Version 1 | February 2024

# Summary

This paper highlights elements of resilience that should be integral within the asset management system to maximize the value derived from assets. It is intended to serve as a basis for spurring wider interest across the subject of resilience and for developing future IAM guidance for practitioners in asset management.

A key question asked by peers is whether resilience is only relevant when considering abnormal incidents or should be considered across the organization's activities. An IAM survey conducted in early 2021 strongly suggests that resilience should be considered at every stage of an organization's operations or asset life cycle. This is because the environment within which an organization and its assets operate may change over time, so to maintain acceptable levels of function, a full awareness of the critical points of an organization's operations, planning, strategy, and its assets must be captured.

**Resilience is an all-encompassing word with many definitions depending on what industry you operate in and your role within your organization. For this paper, we are going to take it as meaning the ability of a system or organization to withstand and recover from adversity, manage crises and disruptions to operations, or manage day-to-day challenges.**

Any organization will have a range of credible potential threats that could cause disruption, damage, or loss. These events, which can come from internal or external sources, may impact assets, people, and the environment.

While resilience and sustainability are often considered alongside each other, resilience differs from sustainability, which the United Nations defines as 'meeting the needs of the present without compromising the ability of future generations to meet their own needs'.

# Introduction

The key driver behind building an organization's resilience is to ensure the continued operation of services and/or products and create conditions for a speedy recovery when faced with any disruption, no matter how remote or substantial. If an organization is resilient, the risk of disruption, damage, or loss to operations is lessened.

The resilience of systems that constitute assets is initially established during asset creation using systems, risk, and reliability engineering. The IAM Conceptual (6-box) model includes resilience[1] as part of the Risk & Review group; however, it is evident from recent worldwide disruptions that resilience needs to be considered within all six groups of the Conceptual model.

We know from recent global events, such as the supply chain impact of the Suez Canal incident in March 2021 and the COVID-19 pandemic's impact on the economy, that many organizations did not consider their planning beyond the "obvious" risks to operations.

Creating organizational resilience means developing the processes and systems to ensure an organization can continue to operate its assets, delivering a suitable level of service in the event of an adverse occurrence while maintaining the safety and integrity of the assets. Decision-makers need to have a sufficient understanding of this, including effective identification and quantification of impacts and likelihoods to be able to act effectively given the organizational context.

[1] Subject 32: Contingency Planning & Resilience Analysis

# Threats Change Over Time

Threats to organizations may happen quickly or slowly, sporadically or intermittently, or may develop over time. How quickly and comprehensively threats are identified will impact how fast an organization is able to respond. An example of this time-based threat is climate change. How does an organization change asset operation caused by the increasing likelihood of extreme events? In 2021, the IAM published a paper on climate emergency planning, which directly responds to two of the COP26 goals of mitigation and adaptation. In it, the IAM provides definitions and guidance on how to include these in your asset management planning[2].

The physical effects of climate change on infrastructure (such as extreme weather and rising tides) and other adverse conditions on an organization means a business needs to consider the following factors:

## Internally;

- Assess risk exposure against risk appetite and tolerance
- Building redundancy into their systems,
- Diversity of both the workforce and the responses to new stress,
- Trial and error analysis to allow for differences in response,
- Analyze organizational mitigation measures (physical, insurance, and operational),
- Access to capital for recovery, and as a business under emerging resilience requirements in the financial industry,
- Opportunity costs of being less resilient compared to competitors.

Modularity of a system allows for individual elements to fail without affecting the whole system. If an organization finds a particular stage of the system is repeatedly failing, they could investigate methods to remove the point of failure, such as through design, especially if the module at risk of failing is one on which the whole system is dependent. This can be considered as both mechanical systems for making a product and within the personnel structure of an organization. Consider, does a certain department have a process that adds a lot of time to the daily functioning of an organization? Can this be changed?

## Externally;

- Government policies and compliance requirements,

[2] https://theiam.org/media/3356/icep-white-paper-climate-emergency-action-planning-v1o1.pdf

- Geo-political issues,
- Potential supply chain disruptions.

An external event can impact organizations differently, such as the 2011 Japanese tsunami, which dramatically impacted the worldwide availability of computer processing chips. If an organization were to embed a supply chain or look to develop its own manufacturing processes, it might not find its operations as affected by outside influences. This type of step obviously requires cost and risk balancing.

Knowing when to take action and what to do should be documented within a Business Continuity Plan, but how do you know when conditions are right to activate the plan? Situational awareness with respect to threats is very important, and unless you plan to activate your strategies based on gut feeling, you need a decision process based on facts.

# Adaptability Will Help With Black Swan Events

Asset Management is a risk-based discipline, and our approach to understanding and managing resilience must be linked to the potential impact on delivering corporate objectives.

Risk management can mitigate various threats to an organization’s operation. However, it is no longer enough to rely on anticipating known and predictable events, which has shown itself to be inadequate considering COVID-19 and other worldwide incidents.

Improved situational awareness, when coupled with stress testing and risk analytics, creates better opportunities for earlier identification of ‘unknown unknowns’ - sometimes referred to as ‘black swan’ events. Uncertainty must be considered at a strategic and operational level; it is crucial for an organization to know how to deal with uncertainty and how uncertainty is considered during decision-making.

There is an analogy here with risk and the impacts of high-consequence, low-likelihood events, and high-likelihood, low-consequence events, whereby it is often tempting to focus on the high-impact scenarios but frequently occurring low-impact events take a toll and can be just as important over time. An organization may address these sorts of issues with engineering or service changes and continuous improvement methods instead of contingency planning.

While the nature of all threats may not be known, the vulnerabilities exposed may be common to multiple threats, so focusing on how to mitigate those vulnerabilities is important, and this is where resilience is important. Suppose unanticipated events result in mitigation not previously planned for. In that case, organizations that have proactive resilience planning and mitigation of structural risk from their supply chains are the ones that cope better than others. Note that modern organizations can have many business and technology partners and complex supply chains, and optimizing one piece of that ecosystem may not help if the others break down. Thus, the holistic vision for the organization should be enforced from the top down, considering all relevant business units and management buy-in. This provides the vision needed to understand where adaptability can help, and adaptability is a core capability for resilient organizations.

# Value Chain Analysis

The term 'value chain' refers to the various business activities and processes involved in creating a product or performing a service. A value chain can consist of multiple stages of a product or service's life cycle, from design to end-of-life 'disposal'. Value chain analysis is a means of evaluating each of the activities conducted by an organization to understand where opportunities for improvement lie. Conducting a value chain analysis prompts an organization to consider how each step adds or subtracts value from the final product or service.

Engaging the whole value chain shows what matters to whom and that resilience matters to everyone, but for different reasons. This can also be an element to strongly consider within an organization's strategy, meaning that you should plan considering the whole value chain and not solely that associated with internal critical assets. Resilience should be viewed from a service continuity perspective instead of from an asset or business unit perspective and should be referred to within an organization's strategy and objectives.

It is important to note that a value chain is more than a collection of independent activities. Rather, these activities make up an interlinked system. When an organization conducts value chain analysis, there are usually two levels to consider: Primary supporting activities are anything that directly impacts the input, output, or distribution of products or services. These activities include inbound/outbound logistics, which is the receiving, storing, and distributing of products, goods, and services; operations; sales & marketing; and services from customer support to your finance team, anything that is required to maintain quality control and quality assurance during and after a sale. Secondary supporting activities take into account research and development, procurement, and human resource management, which are all processes and systems relating to managing the people in an organization, such as recruiting, training and retention, and infrastructure.

Value chain analysis is a useful strategic management tool that breaks an organization's activities down into strategically relevant pieces so that you can see a fuller picture of the cost drivers and sources of differentiation and then make changes appropriately. An organization needs to consider the internal aspects of its own activities and its interactions with the external stakeholders, building resilience over time, with actions and behaviors being developed in anticipation of crisis and disruption.

# Information As A Strategic Asset And Fundamental To Resilience Planning

Decision-making is essentially information processing, and thus, having information based on facts and rational analysis that support decision-making is critically important to improving resilience, not just for assets but for entire business processes. Climate change and COVID-19 have pressurized different industries to place emphasis on resilience through compliance and transparency requirements. Organizations that adopt a systematic approach based on data, factual evidence, and science-based analysis will gain an advantage as their actions will be better justified under increasing scrutiny and evaluations by investors and the capital market. Furthermore, the data we can gather from sensors and information networks, especially when correlated, offer us the capability to better assess risk and provide threat alerts that enable faster and more effective responses.

On the other hand, in today's world, data itself has become a strategic asset, and the soon-to-be-published ISO 55013 recognizes that information resilience and longevity should be included in all resilience plans.  Despite their increasing importance, data and information assets may be amongst the most fragile and temporal of all assets, and yet they are perhaps the hardest to quantify in terms of value to an organization. Each organization needs to develop an information resilience framework that outlines the capabilities and requirements needed to ensure the resilience of information throughout its life cycle during creation, use, storage, reuse, preservation, and destruction. New technology can improve situational awareness of an organization's assets and the environment within which they operate; however, it also increases the attack vectors for cyber-attacks.

To have an effective cybersecurity plan, an organization needs to identify the capabilities and requirements of process, technology, and people as well as their interdependencies since information vulnerabilities are often caused by exploiting the weakest link, which in many cases is the people.

# People Do Asset Management

As noted in Asset Management – an Anatomy, people do asset management. Organizations are comprised of people, so organizational resilience is also a factor in the ability of people to recover from major setbacks. People are creatures of habit, and disasters disrupt culture, so responding to a disaster is not just about having backup IT systems, alternate work locations, and processes and ensuring staff are well equipped to do their jobs but also ensuring they are mentally prepared for adversity. For instance, many large earthquake-prone metropolitan areas, such as San Francisco, Tokyo, and Vancouver, organize ShakeOut exercises annually to help people develop lifesaving habits during the few seconds of opportunity before the shaking becomes too severe to protect themselves.

The essential elements of resilient management are purely human ones: continuing to operate under less-than-ideal conditions, maintaining good communications, and having the courage to make tough decisions, etc. Without the ability to make and communicate decisions and changes to initial post-disaster modes of operation, all else may fail. A good business continuity program that is tested through exercises and maintained regularly will address these human issues during times of crisis. Being aware of a threat and taking action depends on how personalization of the risk is perceived, even for a large organization. Studies have found significant correlations between risk perceptions and the willingness to adopt adjustments. Therefore, personal reluctance to face the possible impacts of an event may jeopardize organizational preparations. Hence, there should be an emphasis on the systematic and scientific assessment of risk and impacts, as well as the clear communication of potential implications these have on the organization to help decision-makers justify actions, both within and without the organization.

# Conclusions

The IAM Conceptual model currently includes Resilience as part of the Risk & Review group. However, due to the impact of recent global events (where many organizations didn't take their planning beyond obvious high-impact risks), it is evident that consideration of resilience can have a positive impact within all six groups of the Conceptual model and also at every stage of an organization's operations or life cycle.

As resilience applies to all types of events, impacting both the asset system and the humans within the organization, a holistic view of asset life and how the personalization of the risk is perceived by the organization's community is needed – including for digital assets. It's no longer enough only to consider the high-value, high-impact risks when day-to-day your personnel are dealing with the disruptions deemed 'low-value.' Rather, there is a need to consider quantifiable risk and impact metrics, which cover a comprehensive range of event frequencies and impacts, from frequent to rare occurrences, in order to enable rational decision-making. Organizations need to consider the importance of robust scenario planning, which identifies plausible or unlikely future events with the view to develop plans to address them.

As the environment within which an organization and its assets operate may change over time, so too should the acceptable levels of resilience planning. There should be full awareness of the critical points of an organization's operations, planning, strategy, and its assets, as well as considering the interconnected nature of the business unit. Using data and fact-driven analyses that consider the full life cycle of assets and operations under the context of the value chain that flows into the operation will help decision-makers better understand risk exposures and more effective protection measures. Organizations that approach resilience systematically and holistically will be able to better position themselves against their competitors in a rapidly changing business environment and capital market.

# Acknowledgements

**Lead Authors**

- Charlotte Connelly
  *Leonardo Helicopters*
- Mark Knight
  *1898 & Co.*

**Editing**

- The IAM Resilience Group

With thanks to our IAM Patrons whose support is greatly appreciated

The Institute of Asset Management
PATRON

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