protiviti®
Face the Future with Confidence

Understanding Changes in Resilience Risks from Technology Advancements

How resilient is our organization? How do we track our organization's change in resilience? Those are two of the most common questions posed by boards on the topic of resilience. The proper responses to these seemingly abstract questions require a firm understanding of the organization's ability to recover important services and functions, as well as the ability to benchmark resilience, either on a comparative basis or using an organizational baseline.

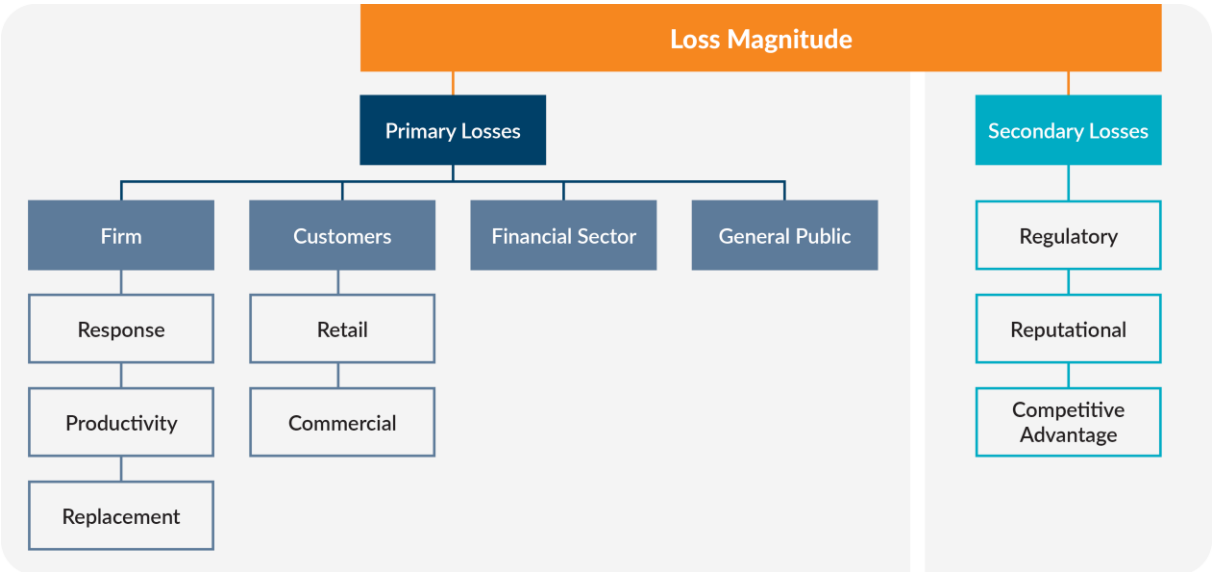
Due to the uniqueness of financial firms, comparative recovery analysis on competitors is prone to assumptions and errors, and ultimately may be too weak as a usable reference. Rather, to understand resilience, organizations must create a baseline recovery metric and map the change in recovery abilities (reduction in resilience risk) as policies and technologies are enhanced.

A common reaction to understanding recovery is to challenge recovery against established recovery time objectives (RTOs). This process can be prone to errors. When not mandated by regulation, RTOs are often used as abstract time periods developed through the qualitative assumptions of business heads who naturally have a bias to their businesses. RTO does not contemplate service or process-level recovery; meaning, the RTO of one system may not accurately reflect the time period required to begin a service or process after a resilience event. Additionally, regulators are moving towards requiring a cost or harm component against the time factor to understand what downtime means to an organization and its stakeholders, and to define the degree of downtime that will cause irreparable harm to an important business service or process. This move does not align well with the concept of RTO.

Factor Analysis of Information Risk (FAIR), a method created to quantify unknown cybersecurity risks, can be used to measure resilience and derive significant organizational benefits and savings. Open source and industry-accepted, FAIR can be used to break down the cost of downtime to organizational stakeholders. All types of harm can be measured using this detailed process. Most important, the net aggregation of the output can be used to quantify an organization's important services and processes, baseline resilience and impact tolerance, as proposed by the UK supervisory authorities.

While FAIR was not developed for this purpose, this expanded use represents a logical extension of its intended use and the math that drives the standard. Clearly, to understand and quantify risks, the harm posed by an event must also be understood. In **Figure 1** below, resilience risk is broken down by primary or secondary loss. The losses can be decomposed further and aggregated at any given level.

Figure 1. A breakdown of losses by primary and secondary losses using the FAIR model.



Using FAIR to Understand Change in Resilience Risk

Technology is a primary tool for enhancing organizational resilience. Software as a service (SaaS). Remote desktops. Public cloud providers. Internet of things (IoT). These technologies have had a significant impact on the ability of an organization to withstand adverse events by, among other things, enabling the decoupling from a desktop, decreasing concentration risk, and providing enhancements in the storage and availability of data. The net effect of these technology advancements, on both the risk to an organization and its ability to recover, cannot be overlooked.

Consider the charts below, which show the loss magnitude of a hypothetical cyberattack based on the following assumptions derived from publicly available data:

- A hypothetical consumer bank with $250 billion in assets
- The bank is the target of a ransomware attack
- A nation state is the sponsor of the attack
- A select number of services at the public cloud service were targeted
- The hypothetical consumer bank maintained robust technology before migrating to the cloud.

Figure 2

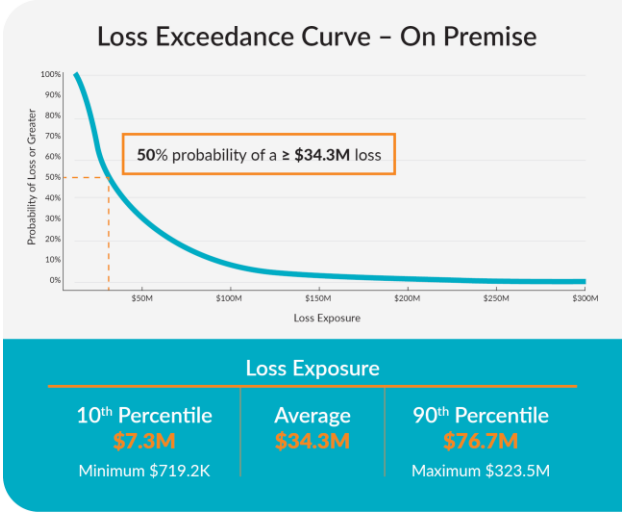
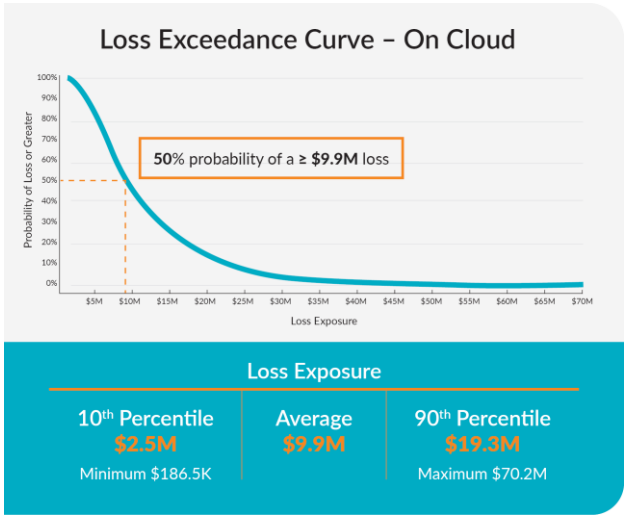


Figure 3

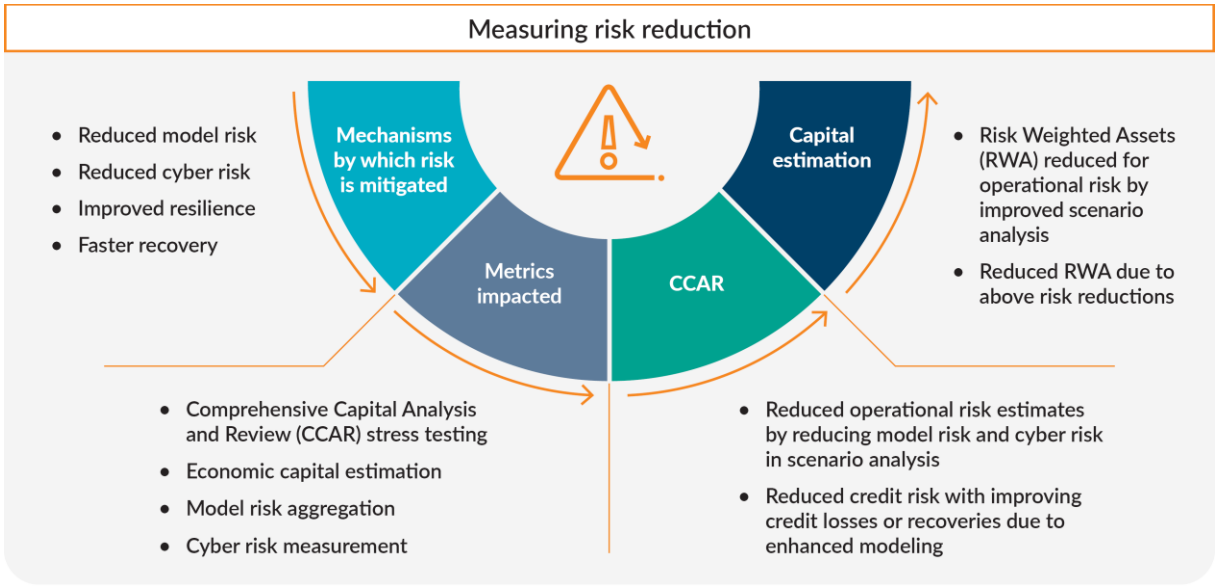


The loss exceedance curves above reflect the impacts of the hypothetical cyberattack in an on-premises environment (**Figure 2**) versus a public cloud environment (**Figure 3**). In the on-premises environment, the probable loss from the cyberattack is 3.5-times greater than in a cloud environment. Additionally, the distribution of loss is wider, with the tenth-percentile loss in the on-premises environment at multiples of the tenth-percentile loss in the cloud environment. Simply put, while there are inherently new risks with migrating to the cloud, the overall resilience risk or overall cost of downtime to the firm is significantly decreased.

The Capital Charge Effect

In the same way cost of downtime before and after implementation of new technology can be calculated using a method like FAIR, it is also possible to calculate the loss exposure reduction resulting from technology implementation – in other words, it is possible to quantify a potential reduction in a component of operational risk. This quantifiable decrease in operational risk can potentially help firms gauge how much capital to hold against operational risk as part of their Comprehensive Capital Analysis and Review (CCAR) and risk-weighted asset calculations.

Figure 4. Robust analytical techniques and measurement processes can be incorporated in stress test scenarios to provide estimates of projected operational risk losses and associated capital needs.



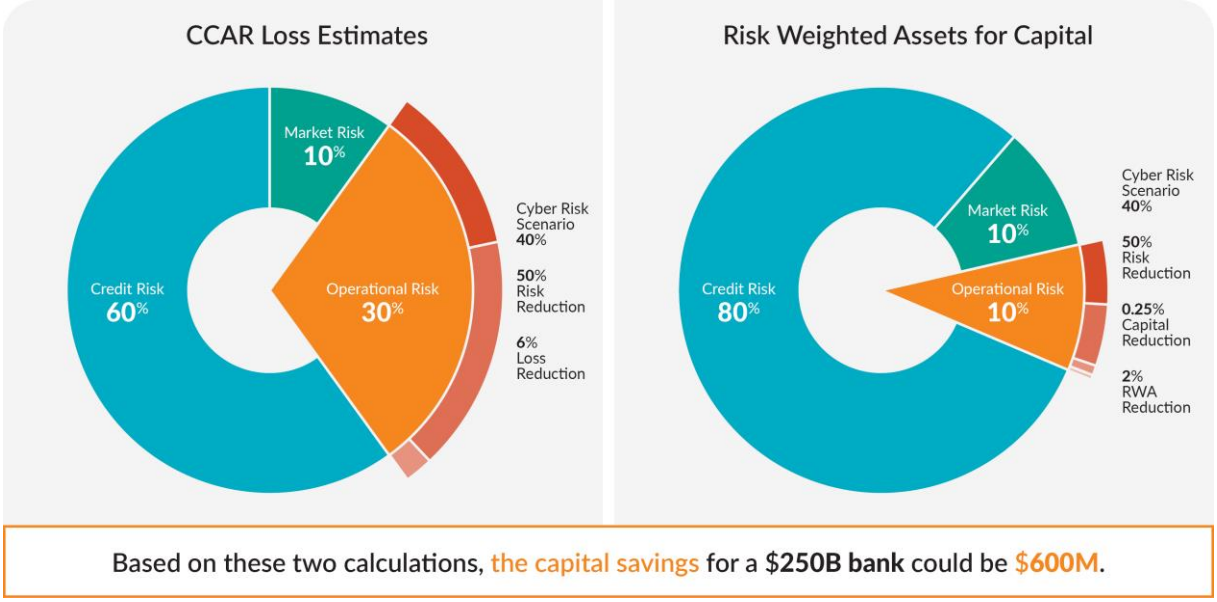
Collectively, large U.S. banks, subject to advanced regulatory capital requirements, hold hundreds of billions of dollars in common equity for operational risk, including regulatory capital minimums and stress testing buffers. For these institutions, it would make sense that a quantifiable net reduction in overall risk would have a substantial effect on their capital charge.

Potential capital reductions may be realized by capturing improvements in operational risk management and loss mitigation during the capital measurement process. The current regulatory capital regime appropriately emphasizes historical operational loss experience, as improvements in operational risk management are expected to reduce losses and lower capital charges over time. However, scenario analysis can reflect changes in operational risk on a timelier basis. Robust analytical techniques and measurement processes around operational risk, as shown in **Figure 4**, can be incorporated in stress test scenarios to provide estimates of projected operational risk losses, and associated capital needs. Increased

use of these measures also would provide a strong incentive for banks to continue to improve operational risk management.

Consider the examples in **Figure 5** below, which uses the same hypothetical $250 billion bank mentioned previously. After migrating from an on-premises computing environment to a cloud environment, the bank successfully reduced its capital charge calculations by 4%. There are many other assumptions which could affect the net reduction, however, the logic behind the capital charge reduction is clear.

Figure 5. Below shows the potential risk mitigation and impact of moving to the cloud for a hypothetical $250 billion bank, based on CCAR loss estimates and RWA for capital.



Stress Testing a Technology Project

There are numerous factors that go into selecting a technology project, however, quantifying resilience as a component of the project selection is not a common consideration. For most organizations, it is a challenge to contemplate the outcome of a project against desired resilience risk reduction. It is also a challenge to validate the success of the project against baseline estimates of the resilience risk reduction versus the anticipated reduction.

FAIR allows users to take numerous projects and stress test their anticipated outcomes. The anticipated effect of a technology project can be realized before and after the project is complete, allowing for a more comprehensive view of:

- Project selection
- Project outcome
- Return on investment.

Why it All Matters

Having a process to keep your board well informed about the organization's level of resilience and how changes to resilience are tracked is critical. It begins with calculating the organization's initial level of resilience using FAIR and reporting that information to the board. With this information, the board can effectively assess the recovery of the organization or an important business service or process and can understand the related potential downtime and cost assumptions. If and when the board asks what the organization is doing to enhance the resilience of the organization, overlaying the reduction of resilience risk from planned projects will provide a simple but effective visual response to the query. Finally, on an ongoing basis, updating resilience risk from completed projects will re-baseline the overall level of resilience, allowing the board to understand the exposure in time and dollars and any changes in exposure to the firm.

Contacts

Douglas Wilbert
Managing Director
+1.212.708.6399
douglas.wilbert@protiviti.com

William Forsell
Associate Director
+1.212.708.6380
william.forsell@protiviti.com