SUNGARD

MANAGING OPERATIONAL RISK IN THE 21ST CENTURY

White Paper Series

"Inside of a ring or out, ain't nothing wrong with going down. It's staying down that's wrong."

– Muhammad Ali

In today's competitive and ever-changing business climate, organizations are constantly dealing with the demand to do more with less. The resources required to manage and operate the business, let alone to invest in new initiatives, are always at a premium.

Most organizations have developed business continuity and disaster recovery plans for many years. Can you verify with 100% certainty that these plans are:

- fully functional and actionable, or;
- integrated into an organization's specific risk appetite and identified exposures

This uncertainty is often the result of an inadequate understanding of operational risk. To improve that understanding, risk and resilience management must be supported by transparency around risk and, more specifically, a clear understanding of the organization's risk appetite.

What is risk appetite? A function of organizational culture, risk appetite is the view an organization takes toward managing its risk. It is a careful balance between the achievement of business objectives and of continuous compliance with regulatory requirements.

When an organization gains a transparent view of the risk it is willing to accept versus the risk it desires to mitigate or remove, it is positioned to move from merely managing risk to achieving a state of operational resilience.

WHAT IS OPERATIONAL RESILIENCE?

Many organizations forego investing in true operational resilience. They see risk management as a challenge that resides solely at the enterprise level — and not one that must be addressed at the service and functional area level, as well. While a holistic view of risk is essential to the resilience of an organization, increasingly complex operational environments often cause top-down approaches to fail. This is usually because there is:

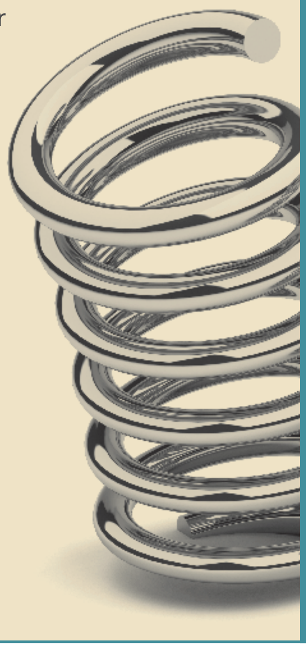
- a lack of convergence between operational risk activities
- a lack of common language to communicate about risk
- an overreliance on governance, risk, and compliance (GRC) software and other technological approaches
- no means to measure managerial competency
- and an inability to confidently predict outcomes during times of stress or disruption

Achieving operational resilience requires an effort both at the enterprise level and across the organization.

Operational Resilience: A Conceptual Definition

Resilience: An ability to recover from or easily adjust to change.

Operational Resilience:
The emergent property of an organization that can continue to carry out its mission in the presence of operational **stress** and **disruption** [CERT-RMM]



Where do the stress and disruption come from?

Risk.

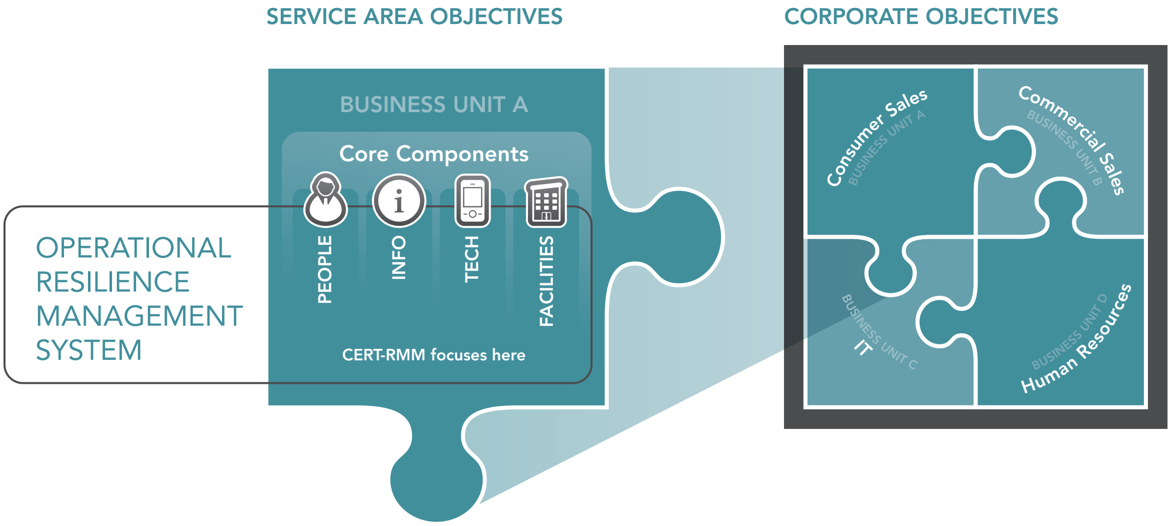
THE CHALLENGE...

It is not possible to build an impermeable operational risk infrastructure. It is possible to fully understand an organization's people/process/technology infrastructure and map this to a specific risk appetite. We recommend this direct mapping as the essential outcome from any operational risk management program which an organization puts in place. Focusing on the outcome, organizations can more easily predict the performance of business services under uncertain conditions, manage unknown risks, meet its mission under adverse circumstances, and return to normal when the adversity is eliminated.

No matter how resilient an organization considers itself to be, it should look to formalize its approach to managing resilience in order to overcome traditional barriers to implementation and control. One approach to doing so draws on Carnegie Mellon's CERT Resilience Management Model (CERT-RMM).

MEASURING OPERATIONAL RESILIENCE & CERT-RMM

No matter how resilient your organization is today you should consider a formal approach that moves beyond traditional barriers to implementation and control.



The CERT-RMM model describes the essential processes for managing operational resilience, and provides a structure from which an organization can begin process improvement of its Business Continuity/ Disaster Recovery (BCM/DR), IT Security, and other organizational efforts.

Moreover, the CERT Resilience Management Model is the first known model in the security and continuity domain that includes a capability dimension. This provides an organization a means by which to measure its ability to control operational resilience and to consistently and predictably determine how it will perform under times of stress, disruption, and changing risk environments.

CERT-RMM Highlights

- Provides a deep process definition across four categories: enterprise management, engineering, operations management, and process management
- Focuses on four essential operational assets: people, information, technology, and facilities
- Includes processes and practices that define four capability levels for each process area: Incomplete, Performed, Managed, and Defined
- Serves as a meta-model that includes references to common codes of practice such as ISO27000, ITIL, COBIT, and others such as BS25999 and ISO24762
- Includes process metrics and measurements that can be used to ensure that operational resilience processes are performing as intended
- Facilitates an objective measurement of capability levels via a structured and repeatable appraisal method

In plain English, the model creates a formal method in which to execute IT and other tasks. Given the reality that most IT tasks are executed in an ad-hoc manner, the CERT-RMM can be a welcome relief to most organizations. For those organizations that are truly serious about resiliency, serious about security, serious about saving money and being more efficient, this is a model to embrace as the pathway to resilience.

So how do we ensure that investments in operational resilience will increase our confidence that services will continue to meet their mission, even during times of stress and disruption? And by so doing, how are we able to justify such investments to senior managers?

MAKING THE BUSINESS CASE

Positioning operational resilience to build a stronger business is accomplished by articulating the business need and showing how to meet it—in a tangible and measurable way at an affordable cost with a positive return. In the context of operational risk, it is often the answer to the questions of "Where does it hurt the most?" and "What high-impact, high-loss events would put us out of business?" A key step in this process is to identify the senior manager who most cares about the answer to these questions and to make sure he or she is on board as the visible champion and sponsor of operational resilience investments.

In addition, those making the case for operational resilience must be able to demonstrate that investments are subject to the same decision criteria as other business investments such as alignment to business mission, strategic objectives, and critical success factors, which are the basis for determining the high-value services that support the accomplishment of strategic objectives.

Benefits of Operational Resilience

- Lowered or eliminated redundancy and cost by optimizing between protection and sustainability strategies
- Greater compliance as well as improved metrics to demonstrate that compliance
- Lowered operational risks with an enterprise focus
- Improved processes that are measurable and manageable — and thus more effective

REGULATING RESILIENCE

Another key driver for operational resilience can be found in current laws and regulations. Business leaders are increasingly required to focus their attention on investing in operational resilience — to better prepare for and recover from disruptive events, to protect and sustain high-value services and supporting assets (information, technology, facilities, and people) that are essential to meet business objectives and to satisfy compliance requirements.

Current compliance criteria can be defined by the following grouping:

- Regulatory/Legal Compliance — Laws that require organization policies, practices and procedures.
- Commercial/Contractual Compliance — Business agreements between partners, customers, and other organizations.
- Other business agreements committed through contracts and service level agreements (SLAs) can have similar penalties for non-compliance or non-performance.
- Organizational Compliance — Internal controls; often, these are related to Frameworks or Standards in support of the items above.

Viewed from an operational perspective, organizational compliance serves as the foundation upon which the management desires to comply with both legal requirements and commercial agreements can be built. The decision to satisfy regulatory compliance — once approved by the organization's management — is then reflected in the day-to-day operational tasks that are developed, refined and followed by management and staff.

WHO OWNS RESILIENCE?

Neither compliance nor resilience can be outsourced.

In building the business case for operational resilience, it is vital that an organization understands that the decision to choose this business model is independent of, but interrelated to technology decisions. From an operational perspective it is the obligation of business leadership to know what areas of compliance are required by laws or commercial agreements, and to develop sufficient policies and procedures within the normal business operation that help ensure compliance is achieved.

From Model to Practice — Questions to Consider

First, define the discussion by considering the following:

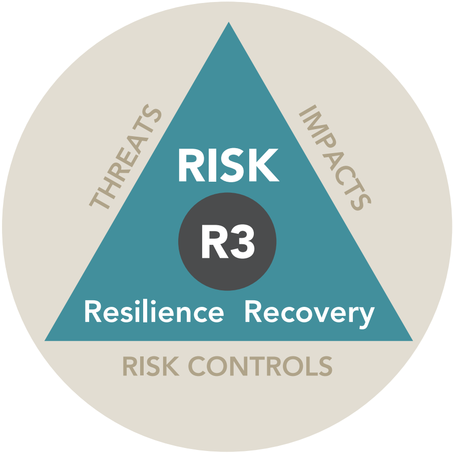
1 Does your organization bring all key operational stakeholders (top management, IT, Security, BC/DR, and business units) together in an integrated program?

2 Do you understand your operational resilience requirements: What standards and regulations inform these requirements? How resilient do you want to be?

3 Have you embedded your organization's risk appetite and tolerance into these requirements, and is there a structured program to assess, prioritize, and manage controls for operational risks?

AN IMPLEMENTATION MODEL TO CONSIDER

Once the organization has defined its current and desired state of resilience they are now ready to develop a roadmap to achieve their resiliency goals. The SunGard R3 Framework takes a holistic approach to operational risk management. R3 starts at the enterprise level to understand the current maturity of the risk management posture, processes and tools of a client organization. This approach provides an organization with useful risk data and analytics to better measure and align operational risk programs across the organization and promotes integration with the businesses broader operational framework.



Key drivers for the R3 Framework are leveraging existing risk data within the client organization and leading with industry ORM-based risk data to reduce the discovery phases that are often associated with such efforts. This results in a tailored, highly repeatable framework of risk management processes that address the dynamics of the client organization and its operational and strategic challenges.

Combining the theory framework of CERT-RMM with the R3 implementation model aligns risk appetite to business objectives and provides a transparent framework for driving operational resiliency and giving the business the tools, training, and guidance it needs to maintain its operations before, during, and after an event that impacts its business.

You can learn more about this solution, as well as all of our consulting services, at www.sungardas.com.

SUNGARD www.sungardas.com

SunGard Availability Services
680 East Swedesford Road
Wayne, PA 19087
Tel: +1-610-768-4120
USA Toll Free: 1-800-468-7483