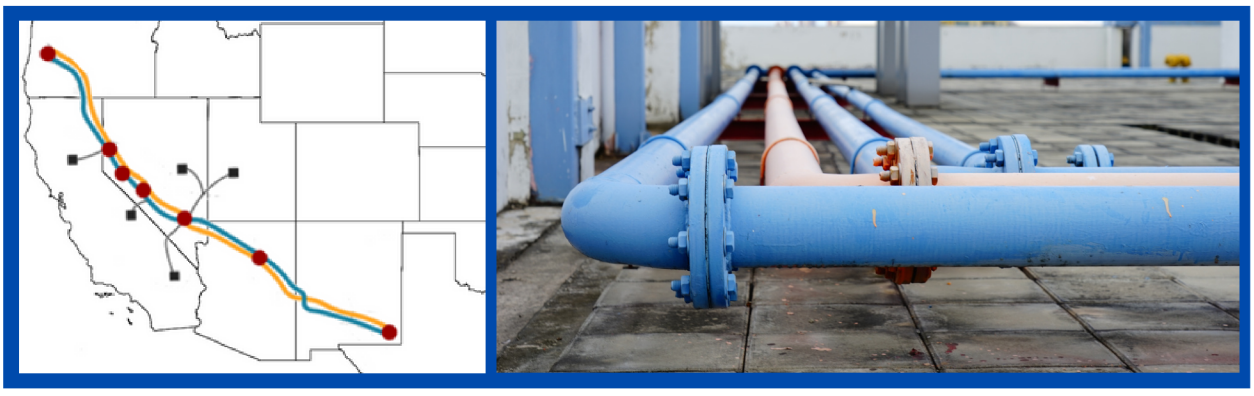
Operational Resilience Framework
Acme Pipeline Example

Executive Summary:

This document is a brief, high-level walkthrough of an Operational Resilience Framework (ORF) scenario involving Acme Pipeline, a fictional organization on the west coast of the United States. Acme Pipeline operations mirror those of the pipeline company that experienced a ransomware attack in May 2021. The company responded by proactively shutting down its pipeline system, resulting in significant disruptions to consumers and airlines while it worked to restore operations to pre-event levels.

Acme Pipeline, at steady state, delivers 45% of all fuel consumed in the Southwestern US, approximately 100 million gallons per day of various refined petroleum products to 12 primary distribution terminals, including some third-party terminals. Acme has implemented traditional business continuity (BC) and disaster recovery (DR) plans and, as a result, has approximately 30 days of product on hand at each distribution terminal. Acme's primary oil products are gasoline, diesel and jet fuel. It also ships more than 20 other petroleum and petrochemical products in small amounts. Its direct customers and end users include terminals/tankage parties, shippers, suppliers/consignees, businesses and consumers within 500 miles of the distribution locations.

For this scenario, the Acme organization responsibility chart will be simplified to include leadership as follows:C-Suite, Business Leaders,Contingency Planners and Technology Leaders.The involvement of the various parts of the organization will be tracked via a RACI (Responsible, Accountable, Consulted, Informed) chart and the remainder of the scenario will be organized by steps in the ORF. Through several rounds of analysis, an operational resilience plan is developed to determine how and when to deliver products from the onsite reserves to increasingly few and higher priority customers as the magnitude of disruption is realized from any event that may significantly impact operations.



1	RACI
A	C-Suite
R	Operational Resilience Exec
R	Business Leaders
I	Contingency Planners
R	Technology Leaders
I	Implementation Team

Step 1 : Build the Foundation

In the weeks following the Colonial Pipeline incident, the C-Suite of Acme Pipeline gathered to discuss operational resilience using the ORF. First, in consultation with their technology leaders, Acme Pipeline confirmed they had matured their implementation of ITIL and NIST CSF over many years. This satisfied one of the foundational requirements for ORF: to have industry recognized IT and cybersecurity controls implemented. Next, Acme's C-Suite selected a leader to become the Operational Resilience Executive (ORE). They provided sufficient resources based on the recommendation of relevant parties and gave the ORE the directive to implement the ORF in a sustainable way while keeping them informed on progress.

Acme Business Functions

2	RACI
I	C-Suite
A	Operational Resilience Exec
R	Business Leaders
C	Contingency Planners
I	Technology Leaders
C	Implementation Team

Step 2 : Understand the Ecosystem

In the second step, Acme's goal was to understand the ecosystem supporting and consuming their external services. At the direction of the ORE, Business Leaders assembled a comprehensive list of business services, identifying them as Operations Critical or Business Critical. They also identified, grouped and prioritized the customers and business partners that depend upon Acme's services. For Acme, the physical delivery of petroleum products is the singular service that would significantly impact external parties if disrupted. That means the elements supporting this service, including the data, system images and configurations of OT and IT systems, must be immutably backed up regularly and stored in multiple locations.

With an understanding of the ecosystem, the ORE worked with Business Leaders and Contingency Planners to determine the priority level for product delivery to each defined customer group.

Acme Customer Groups

From their analysis of past incidents, shortages in Commercial Gas Stations could cause systemic supply chain issues in many sectors, and consumers would be vulnerable to shortages and prone to panic, as seen during the pipeline incident in May 2021. To avoid widespread economic impacts, both customer groups were categorized as a high priority. Airports were categorized as a medium priority because of their large stores of fuel, ability to fly in new fuel, and ability to reroute planes, taking short hops to refuel elsewhere before long international flights. Airports would be inconvenienced by disruption but would be able to continue their operations in an impaired state for a long period of time. All other customers were found to have large product stores and were rated low priority.

3	RACI
I	C-Suite
A	Operational Resilience Exec
R	Business Leaders
R	Contingency Planners
C	Technology Leaders
I	Implementation Team

Step 3 : Identify Minimum Viable Service Levels

With the services categorized and customer groups prioritized, the ORE established Minimum Viable Service Levels (MVSLs). The Contingency Planners worked with Business and Technology Leaders to identify potential failure modes and types of service disruptions that could occur, regardless of the root cause. The demand from each customer and partner group was analyzed for the level of impairment that could be tolerated to limit systemic impacts and outrage. The Contingency Planners consulted with Business Leaders, Technology Leaders and Implementation Team to design four increasingly impaired service levels:

1 **Minor impacts to all customer groups to continue services at 80% of normal deliveries for up to two weeks.**

2 **Significant impacts across all customer groups to continue services at >60% deliveries for up to four weeks.**

3 **High and Medium customers receive >50% delivery capacity for up to six weeks. Services to Low priority customers are deprioritized.**

4 **Only High priority customers receive >50% of normal product delivery. Services to Medium and Low customers are deprioritized.**

4	RACI
I	C-Suite
A	Operational Resilience Exec
C	Business Leaders
R	Contingency Planners
C	Technology Leaders
C	Implementation Team

Step 4 : Define Service Delivery Objectives

Once Acme identified its MVSLs and target impaired service levels for the delivery of petroleum products, the Contingency Planners worked with the team to define the Service Delivery Objectives (SDOs) required to achieve those service levels. This required a detailed analysis of the petroleum delivery service, including internal and external dependencies across people, processes, technology, vendors and suppliers. This often requires iteration across Steps 3 and 4, but in this case, the MVSLs and related SDOs were considered practical and achievable by Technology Leaders and the Implementation Team. SDOs included:

1
>80M gal/day through pipeline
Use local reserves and manual processes

2
>60M gal/day through pipeline
Use local reserves and manual processes
Use 3rd party delivery

3
>50M gal/day through pipeline
Use local reserves and manual processes
Use 3rd party delivery
Use overtime and duty reassignment

4
>40M gal/day through pipeline
Use local reserves and manual processes
Use 3rd party and gov't delivery
Use overtime and duty reassignment

Each impaired service level and transition between levels was accompanied by communication plans accounting for Customers, Business Partners, Regulators, Legal Entities and other relevant parties to mitigate the risks and outrage. At each progressively impaired service level, additional actions were documented. In the event of a level4 impairment, Acme would consider assistance from the government, external parties and even competitors to make deliveries to the most important customer groups. By anticipating these delivery challenges, Acme was prepared to make rapid decisions and adapt to changing circumstances.

5	RACI
I	C-Suite
A	Operational Resilience Exec
C	Business Leaders
C	Contingency Planners
R	Technology Leaders
R	Implementation Team

6	RACI
I	C-Suite
A	Operational Resilience Exec
C	Business Leaders
C	Contingency Planners
R	Technology Leaders
R	Implementation Team

7	RACI
I	C-Suite
A	Operational Resilience Exec
R	Business Leaders
R	Contingency Planners
C	Technology Leaders
C	Implementation Team

Step 5 : Preserve the Data

The Technology and Implementation teams then worked to define Data Restoration objectives for Critical Data Sets that enable recovery within the constraints set by the Service Delivery Objectives. The Critical Data Sets included consumer and business data and all other data required to restore Operations Critical services such as applications, system images, networks, core infrastructure services and configurations that must be immutably backed up to enable recovery. Acme considered several options before selecting an effectively immutable cloud storage service and geographically distributed offline backups for Operations Critical Data Sets that enable rapid restoration within hours. In Acme's case, the design included immutable backup of Business Critical Data Sets to similar distributed offline storage, but with lower Data Restoration priorities. Additional design considerations ensured confidentiality, integrity, availability and secure transfers to the archive environment.

Step 6 : Enable Recovery

With its data properly preserved, categorized and prioritized, Acme had to enable the recovery of Operations Critical and Business Critical Services to meet Service Delivery Objectives (SDOs). The Technology Leaders and the Implementation Team worked together to define the recovery procedures, including alternative processes for critical components of the services and new vendor agreements. This enabled switchable configurations for the target service levels depending upon disruption type and level of impairment. Redundancy was built in to prevent single point failures across people, process and technology including cryptographic key and archive access. The architecture and design of recovery environment, systems and processes were reviewed to ensure they met SDOs. Acme designed a separate recovery environment specifically for restoring Operations Critical Services to predesigned impaired levels, so this could be done in parallel with full restoration of all services in the primary recovery environment.

Step 7 : Independently Test

In the final step, Business Leaders and Contingency Planners developed and implemented processes to run tests, train personnel and run exercises to independently verify and validate the Operational Resilience Plan and its ability to meet Service Delivery Objectives and associated business outcomes. They also updated the continuous monitoring and improvement policies to include operational resilience policies, practices and mechanisms.

Conclusion:

After extending their BCM practicesby implementing the ORF, Acme Pipeline ensuredthe needs of customers and business partnerswill be addressed duringcrisis situations. By designing its systems to deliver Operations Critical services in predefined impaired states, regardless of the cause of the disruption, Acme may prevent systemic issues and significant impacts to the ecosystem while working to achieve full restoration. In addition, the ORE ensured continuous improvement and sustainability of the program and infused the principles of operational resilience into existing processes and controls throughout the organization including service design, architecture, application development, data management, third-party and supply-chain risk management, procurement, and more.