ECOVIS AL SABTI

Great Place To Work. Certified MAY 2024-MAY 2025 KSA

THE DEBATE

Organization Resilience vs Operational Resilience

In today's fast-paced and unpredictable business environment, disruptions are inevitable. Whether it is a cyberattack crippling IT systems, a supply chain bottleneck halting production, or an economic downturn shaking markets, organizations must be prepared to face a wide range of threats. Enter **Organization Resilience** and **Operational Resilience**—two buzzwords that have become essential in the dictionary of modern business strategy. While they sound similar, they serve distinct purposes and address different aspects of an organization's ability to withstand and adapt to challenges. If you have ever wondered how these concepts differ—or how they can work together to future-proof your business—this article will explain the key distinctions, explore their synergies, and provide actionable insights to help your organization not just survive, but thrive in an era of constant change.

DEFINING THE CONCEPTS

Organization Resilience

Organization Resilience refers to the holistic ability of an organization to anticipate, prepare for, respond to, and adapt to disruptions, both incremental and sudden, to sustain operations and achieve long-term success. It encompasses strategic, financial, cultural, and operational dimensions, ensuring that the organization cannot just survive but also thrive in the face of adversity.

The **ISO 22316: 2017** standard, Security and Resilience – Organizational Resilience – Principles and Attributes, provides a comprehensive framework for building organizational resilience. It emphasizes the importance of leadership, culture, and proactive risk management as key enablers of resilience. According to **ISO 22316**, a resilient organization is one that can "absorb and adapt in a changing environment," highlighting the need for adaptability and continuous improvement.

Operational Resilience

Operational Resilience, on the other hand, focuses specifically on the continuity of critical business operations and services during disruptions. It ensures that an organization can withstand and recover from adverse events while minimizing impact on customers, stakeholders, and regulatory compliance.

In the financial services sector, for example, operational resilience has become a regulatory priority. The Bank of England's Operational Resilience Policy and the European Union's Digital Operational Resilience Act (DORA) mandate that firms identify critical business services, set impact tolerances, and ensure robust incident response capabilities. These frameworks underscore the importance of safeguarding operational continuity in highly regulated industries.

Key Differences Between Organization Resilience and Operational Resilience

While both concepts aim to enhance an organization's ability to manage disruptions, they differ in several key aspects:

Aspect	Organization Resilience	Operational Resilience
Scope	Broad, covering the entire organization	Narrow, focused on critical operations and services
Focus	Long-term sustainability and adaptability	Short-term continuity of critical services
Time Horizon	Strategic and long-term	Tactical and immediate
Key Components	Leadership, culture, strategy, risk management	Critical processes, IT systems, incident response
Regulatory Context	Broader governance and sustainability frameworks	Industry-specific regulations (e.g., financial services)

ECOVIS®
AL SABTI

HOW THEY INTERCONNECT

Operational Resilience is a subset of Organization Resilience. While the former ensures the continuity of critical operations, the latter provides the overarching framework for building a resilient organization. For example, a company with strong operational resilience may successfully navigate a cyberattack, but without organizational resilience, it may struggle to adapt to long-term shifts in the market or industry.

Consider the COVID-19 pandemic: organizations with robust operational resilience were able to maintain critical services, but those with strong organizational resilience were better positioned to pivot their business models, embrace remote work, and capitalize on emerging opportunities.

Building Resilience

A Dual Approach

To effectively manage disruptions, organizations should adopt a dual approach that integrates both Organization Resilience and Operational Resilience. Here are some actionable steps

Adopt International Standards

Leverage frameworks like ISO 22316 for organizational resilience and ISO 22301 (Business Continuity Management Systems) for operational resilience. These standards provide best practices for identifying risks, building capabilities, and ensuring continuous improvement.

Identify Critical Business Services

Conduct a thorough assessment to identify and prioritize critical operations. This is a cornerstone of operational resilience and ensures that resources are allocated effectively.

Foster a Resilient Culture

Leadership plays a pivotal role in embedding resilience into the organizational culture. Encourage proactive risk management, collaboration, and innovation at all levels.

Invest in Technology and Infrastructure

Robust IT systems, cybersecurity measures, and supply chain redundancies are essential for operational resilience. At the same time, digital transformation can enhance organizational resilience by enabling agility and adaptability.

Test and Refine Plans

Regularly test business continuity and incident response plans to identify gaps and areas for improvement. Simulations and tabletop exercises can help prepare teams for real-world scenarios.

CONCLUSION

In an era defined by volatility and uncertainty, resilience is no longer optional, it is a strategic imperative. While **Organization Resilience** and **Operational Resilience** serve different purposes, they are complementary and essential for building a robust, future-ready organization.

differences and interconnections, leaders can develop a comprehensive resilience strategy that ensures both short-term continuity and long-term success.

As the **World Economic Forum** aptly states*, "Resilience is the capacity to absorb stress, recover critical functionality, and thrive in altered circumstances."* Whether it is navigating a global crisis or adapting to market shifts, organizations that prioritize resilience will be better equipped to turn challenges into opportunities.

REFERENCES

1. ISO 22316:2017 – Security and Resilience – Organizational Resilience – Principles and Attributes.
2. ISO 22301:2019 – Security and Resilience – Business Continuity Management Systems – Requirements.
3. Bank of England's Operational Resilience Policy.
4. European Union's Digital Operational Resilience Act (DORA).
5. World Economic Forum – The Global Risks Report 2023.

By adopting a dual focus on Organization Resilience and Operational Resilience, businesses can not only survive disruptions but also emerge stronger, more agile, and better prepared for the future.

ECOVIS® AL SABTI

PROVEN TRACK RECORD | CUSTOMER FOCUSSED | AGILE & FLEXIBLE | TRUSTED PARTNER | QUALITY FOCUSSED

EXPERIENCED TEAM | VENDOR NEUTRAL | LOCALLY AVAILABLE | INDUSTRY EXPERIENCE | INNOVATIVE SOLUTIONS

Certifications & Accreditations

ISO 20000 | ISO 22301 | ISO 27001 | Great Place To Work. Certified MAY 2024-MAY 2025 KSA

REGISTERED — National Cybersecurity Authority

REGISTERED — FintechSaudi

Our Core Values

Excellence
At ECOVIS, we consistently surpass expectations and deliver exceptional results.

Innovation
We take on challenges to achieve extraordinary outcomes through innovation, constantly pushing the boundaries

Professionalism
Our unbiased, objective-oriented, and diligent approach in all our endeavors embodies professionalism.

Collaboration
ECOVIS is dedicated to nurturing relationships based on mutual trust and respect.

Integrity
We uphold a commitment to honesty, responsibility, and transparency in all our actions.

Our Services

- Business Continuity Management (BCM)
- Governance, Risk & Compliance (GRC)
- Risk Advisory & Internal Audit
- Data Management & Data Privacy
- Enterprise System & Data Analytics
- Technology Consulting
- Cybersecurity Services
- Deal Advisory Services

Contact ECOVIS ALSABTI

Riyadh, Saudi Arabia | Jeddah, Saudi Arabia | Khobar, Saudi Arabia | Manama, Bahrain

920023534 | ecovisalsabti.com

/EcovisAlsabti | /EcovisAlsabti

Noman Khan
Executive Director
+966 500 074 619
noman.khan@ecovisalsabti.com

Muhammad Kashif
Associate Director
+966 553 479 664
muhammad.kashif@ecovisalsabti.com

About Author: Muhammad Kashif is the Associate Director of Business Continuity Management and Resilience Services at ECOVIS ALSABTI, bringing over two decades of experience in resilience and business continuity across the Middle East. He has led large-scale resilience and continuity programs throughout the region, demonstrating his expertise in safeguarding organizational sustainability.