ASIS FOUNDATION™

OPERATIONAL RESILIENCE

THE CRITICAL CONTRIBUTION OF SECURITY TO OPERATIONAL RESILIENCE

Prepared by Tracy Hatton, Joanne Stevenson, and Erica Seville

EXECUTIVE SUMMARY

In partnership with

ResOrgs
Resilience
& Risk Experts

Get Involved:
ASIS Foundation

EXECUTIVE SUMMARY

THE EVOLUTION OF OPERATIONAL RESILIENCE

Organizations face an unprecedented convergence of threats—from sophisticated cyberattacks and supply chain disruptions to climate events and geopolitical instability. When critical services fail during these events, the consequences extend beyond immediate financial losses to include damaged reputation, regulatory scrutiny, and eroded customer trust. In response, operational resilience has emerged as an essential capability that enables organizations to deliver critical services even during significant disruptions.

Operational resilience represents an organization's ability to maintain critical services through disruption by proactively reducing risks, preparing systems and people, responding effectively when incidents occur, and recovering quickly to acceptable performance levels. While many organizations have components of resilience in place, such as business continuity plans or incident response protocols, these efforts often operate in isolation, limiting their effectiveness during complex, fast-moving disruptions. Operational resilience is not just a policy—it's a practice. It must be tested, refined, and embedded in how people and systems operate together during both business-as-usual and times of stress.

Operational resilience

The ability to maintain delivery of critical services in the face of disruption.

Applied definition for security practitioners

Ensuring that protective, detection, and response capabilities are enablers of continued critical service delivery.

Security has a central role in operational resilience: enhancing the preparedness and response of organizations in the face of disruption. Security functions can connect different parts of an organization, provide early insight into emerging risks, and support fast, coordinated responses. Embedding the security function into resilience efforts will strengthen an organization's ability to manage disruption effectively. The applied definition of operational resilience for security practitioners is: Ensuring that protective, detection, and response capabilities are integrated across the organization to safeguard the delivery of critical services during disruption.

This report, commissioned by the ASIS Foundation, examines how security functions can strengthen their contribution to operational resilience. Drawing on a global literature review and interviews with 20 senior practitioners across multiple sectors and continents, our findings reveal that security is already performing critical operational resilience work. However, there is an opportunity to improve the depth and maturity of engagement in broader resilience strategies and governance structures to enhance the impact of the function.

KEY RESEARCH FINDINGS

Security's Strategic Role

Security teams contribute essential capabil-

ities to operational resilience daily: they provide real-time situational awareness, identify emerging threats, manage physical and cyber risks, and support incident response. Security professionals are uniquely positioned as boundary spanners within organizations. With visibility across operational activities and strategic priorities, they can bridge critical gaps between threat intelligence and business impact, technical controls and operational requirements, and day-to-day management and crisis response. Despite this, security professionals and functions are not currently well integrated into broader resilience planning. There is a significant opportunity to enhance the awareness and role of security professionals in operational resilience more systematically.

Four Phases of Resilience—An Integrated Framework

The value of security professionals to operational resilience can be articulated across the four interconnected phases of resilience:

1. **Reduction** – Detecting, evaluating, and mitigating risks proactively before disruptions occur.

2. **Readiness** – Preparing systems, people, and processes to absorb stress and respond effectively.

3. **Response** – Implementing coordinated actions during disruptions to contain impacts.

4. **Recovery** – Restoring functionality quickly to acceptable performance levels.

Security plays a vital role in all four phases—from intelligence gathering and threat detection to incident containment and post-event analysis—but must coordinate with other functions to maximize effectiveness.

This framework provides a common language for cross-functional teams. It can be used to clarify how security integrates with other operational resilience functions, such as business continuity management. It provides a clearer understanding of where security professionals can contribute to resilience and how they can beneficially coordinate with others.

EXECUTIVE ENGAGEMENT AND GOVERNANCE

Executive-level commitment and governance are essential for embedding resilience into the organization's culture. When security is positioned as a strategic enabler and integrated into high-level decision-making, it enhances operational resilience outcomes. Regular oversight from governance bodies ensures that resilience remains a priority and that resources are appropriately allocated. Effective governance structures should include representatives from all key functions to ensure that resilience strategies are coordinated and aligned with organizational objectives.

Collaboration Structures Support Resilience

Formal collaboration structures, such as secure interorganizational information sharing networks and intraorganizational resilience governance committees, enable organizations to coordinate effectively to advance operational resilience outcomes. These platforms, which are established during business-as-usual, foster opportunities for cross-functional teams to align resilience goals and respond effectively to disruptions. By facilitating structured communication between stakeholders, these platforms help organizations address shared risks and dependencies, enhancing their overall resilience.

STRATEGIC RECOMMENDATIONS

Our findings are grounded in practitioners' experiences navigating real-world disruptions—from ransomware attacks and natural disasters to system failures and supply chain breakdowns. They reflect hard-won lessons that point to specific actions organizations should take now:

For the Security Professional

Security professionals must position themselves as strategic resilience advisors by breaking down silos, improving cross-functional communication, and contributing actively to crisis management and business continuity planning. Developing business acumen and creating standardized metrics to demonstrate security's resilience contribution will help security teams engage leadership effectively and demonstrate their value beyond threat mitigation.

For Organizations

Organizations should integrate security into formal resilience governance structures and establish

Integrated Operational Resilience Framework

OPERATIONAL RESILIENCE
The ability to **maintain delivery of critical services** through disruption

	REDUCTION Reduce operational risks wherever possible	**READINESS** Maintain the capability to respond to impacts effectively	**RESPONSE** Respond effectively and efficiently to operational incidents	**RECOVERY** Enable swift recovery of operations
SECURITY *Physical & Cyber* Keeping the things needed for critical operations safe: people, property/ infrastructure, ICT	Evaluating threat landscape Instigating protective measures	Creating emergency response plans Running emergency response training	Responding effectively to incidents	Adapting practice to the new normal
BUSINESS CONTINUITY MANAGEMENT *Incl. Supply Chain & Crisis Management* Minimizing the impact of disruption on the business, including supply chain	Understanding criticality and vulnerability of key internal and external resources	Ensuring Plan Bs exist and are tested	Ensuring adequate crisis management coordination arrangements and effective training	Implementing Plan Bs

Helping BCM understand what is vulnerable

Helping security understand what is critical

OPERATIONAL RISK MANAGEMENT FRAMEWORK
Making sure to focus on the key risks and manage residual risk effectively

cross-functional collaboration through committees or working groups. Developing shared risk frameworks and conducting regular scenario-based exercises will ensure all functions can coordinate effectively during disruptions and build mutual understanding during normal operations.

For Governance

Board members and executives must champion operational resilience and the role of security within that by establishing clear accountability, providing adequate resources, and regularly reviewing resilience performance. Leadership should foster collaboration between departments, ensure clear roles and responsibilities, and maintain visibility of emerging risks that could impact critical services.

IMPLEMENTATION PRIORITIES

To successfully implement these recommendations, security professionals and the organizations they support should focus on three key areas:

Cultural Change

- Break down professional silos through shared objectives and collaborative incentives.
- Build trust across functions through joint planning and regular interaction.
- Establish common risk terminology to enable clear communication.
- Encourage transparent information sharing while maintaining security.

Capability Development Amongst Security Professionals

- Enhance training programs to develop both technical and business skills.
- Conduct cross-functional exercises to stress-test coordination.
- Integrate technologies that improve visibility across operations.
- Develop meaningful metrics that demonstrate resilience improvement.

Stakeholder Engagement

- Secure executive sponsorship for the role of security in operational resilience with clear accountability.
- Establish board-level oversight linked to organizational strategy.
- Build external partnerships to share intelligence and best practices.
- Gain cross-functional buy-in through demonstrated mutual benefits.

CONCLUSIONS

In today's interconnected environment, disruptions rarely remain isolated—they cascade across systems, supply chains, and geographies. Organizations that continue to manage resilience in silos remain unnecessarily vulnerable.

Security must be part of the solution because it manages critical risks and provides unique visibility across threat landscapes, operational systems, and stakeholder interactions. When fully integrated, security connects emerging threats with organizational impact in ways other functions cannot.

Integrating security with other resilience functions creates essential infrastructure for operating in a world defined by complexity and interconnected risk. As the systems organizations rely on become increasingly interdependent, approaches to resilience must follow suit.

Operational Resilience

The Critical Contribution of Security to Operational Resilience

Prepared by Tracy Hatton, Joanne Stevenson, and Erica Seville

In partnership with

ResOrgs
Resilience
& Risk Experts