



**DuneMount Consulting Services
Resilience**

2023

SERVICES

Chapter 1

Resilience

Resilience(1/2)

In the changing world, it is critical to be able to adapt quickly to changes and to ensure that our company remains as resilient as possible.

Our Resilience Services aim to increase organizations' preparedness and resilience against unforeseen events.

Our services are categorized under four main domains. These are business and information technology continuity, crisis management, physical security and third party management.

All our services and related solutions are based on international best practices and aim to provide the most beneficial service to our customers in line with their needs.

i) Crisis Management

Although organizations try to prevent crises with many efforts, this is not always possible. Unforeseen risks can lead to unforeseen incidents and unforeseen incidents can lead to unforeseen crisis. However, it is possible to reduce the effects of a crisis by taking the right steps and determining a fast and effective response method.

Our Crisis Management services have been developed to provide an end-to-end solution to analyze organizations' internal processes and raise awareness to effectively manage and mitigate the impact of crises.

Critical components and services:

- Crisis preparedness assessment
- Crisis simulations, tabletop simulations and drills
- Crisis scenario design
- Crisis management framework and governance structure design
- Crisis management plan and template development
- Post-crisis assessment

ii) Physical Security

Resilience requires taking precautions not only against digital threats but also against physical threats. In this direction, we offer a wide range of services to our customers in terms of process design, security assessments and physical security solutions.

Critical components and services:

- Physical security assessments
- Physical security framework, policy, standard and procedure design
- Physical site security solutions

Resilience (2/2)

iii) Business and Information Technology Continuity

Business and Information Technology Continuity service is a comprehensive solution designed to ensure the uninterrupted operation of your business and information technology systems even in the face of unexpected disruptions or disasters.

Despite the economic, geographical and cultural barriers in the world, technology and human redundant systems are being built by leading organizations today. In the foreground, we usually see "technology". However, although hardware and software feed the "technology", we should not forget that there are elements such as food, hygiene, electricity and the safety of family members that will "feed" the "human" who will use that technology, both literally and figuratively.

By combining strategic planning, technology resilience and proactive measures, our goal is to offer an approach that is completely independent of the traditional continuity and disaster approach, enabling your organization to maintain critical functions and minimize downtime even in the most difficult events.

Critical components and services:

- Business and IT continuity strategy (compliant with ISO22301), framework, process and document development
- Business and information technology continuity tests, simulations, assessments and gap analysis
- Continuity risk assessments
- Continuity solution support
- Disaster Master Plan analysis and development

iv) Third-Party Resilience

In order to ensure Resilience, organizations need to understand that resilience is not only related to their internal processes but also it is related to their business partners and suppliers. Otherwise, third-party incidents can easily have devastating effects for organizations.

The purpose of Third-Party Resilience is to check whether the third parties you work with are compliant with your organization's operational, security and compliance standards.

Critical components and services:

- Third-Party risk assessment
- Security and compliance controls
- Emergency planning
- Communication channels
- Third-party resilience; framework, process and document development

CONTACT

Contact



Serdar Karaman || CDPSE, ISO27001/ISO22301 LA, D1&D2 LA

DuneMount Founder

Serdar Karaman graduated from the Department of Computer Engineering at Bahçeşehir University in 2011

Over the course of his 14-year professional career, Serdar Karaman has amassed extensive experience in diverse domains, including business continuity, information technology continuity, crisis management, risk management, cyber resilience, cyber security, and information security. Throughout this period, he has offered consultancy services to over 200 companies within these specialized areas.

In the year 2023, Serdar Karaman established DuneMount Consulting Services, a firm exclusively dedicated to providing top-tier security consultancy services.

İletişim

Mobile: 0 555 479 72 31

E-Mail: serdar.karaman@dunemount.com

© 2023 DuneMount . All rights reserved.

DuneMount