SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Resilience >

Vendor Resilience Questionnaire

Created by the Security Executive Council

Your business continuity plan should identify which vendors provide significant services and products to your organization and rank their criticality to your operations. It should consider your organization's regulatory, reputational, and operational risks should each vendor suffer a supply chain disruption that impacts you, and at what point the disruption becomes critical.

How prepared are your key vendors to quickly and effectively manage disruptions to their operations that could impact you? If you haven't asked, now is the time.

This vendor resiliency checklist is a starting point. When you expand and revise it to meet your needs, avoid including "Yes" or "No" questions. You're looking for useful information that will help you evaluate their resilience. Don't be too broad; keep your questions relevant to the goods and services the vendor provides to you. Also, where possible, build in a way for you to verify the vendor's answers.

Vendor Resiliency Questionnaire

1. What documented recovery plans do you have in place for the goods and services you provide us and for the key facilities from which they are provided?

2. What types of failures and disruptions do your plans consider, and what is the expected recovery time?

3. How do your plans account for your critical interdependencies within your organization and with your key vendors?

4. Who is in charge of executing, updating, testing and planning your business continuity plan? (single individual, several individuals across functions, a dedicated team of Business Continuity leaders, external provider, e.g.)?

5. How does your critical incident management plan deal with internal and external communications? How would you notify us in the event of a critical incident or disruption, and within what timeframe?

6. What is your data recovery strategy? Do you have backup locations offsite and who maintains or monitors those?

7. Can your backup facilities work at the same capacity as your primary facility? If not, what is their capacity percentage? For how long?

8. What is your workplace recovery strategy? From where will employees work in the event of a critical incident that disrupts your ability to deliver your goods/services to us?

9. How often do you test your Business Continuity plan?

10. What were the results of your most recent test?

11. Which components of your infrastructure or systems are tested, and how are tests audited?

12. When was your Business Continuity Plan last updated, and how often do updates occur?

Visit the Security Executive Council website for other resources in the Program Best Practices: Resilience series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website: https://www.securityexecutivecouncil.com/

