

# How resilient is your business?

## Let's get you started!

We have created a checklist to help you understand and assess your current business resilience plan, focusing on network resiliency.


**Note:** This checklist is not exhaustive, It is a guide only. Your organisation's specific context should always be taken into account.

Network resilience is about providing and maintaining an acceptable level of service in the face of faults and challenges to regular operation. How would you rank the following areas of consideration for your business

(Please rate 1 to 5 for each question with 1= Haven't considered, 2= Not likely to consider, 3= Might consider, 4=Likely to consider, 5= Definitely consider):

Infrastructure Redundancy - How your business optimises its network redundancy to boost fault tolerance and ensure high availability	1	2	3	4	5
● Data centre redundancy					
● WAN links redundancy					
● WAN provider and technology diversification					
● Additional investment in general hardware redundancy (network, server, and/or storage)					
● Power redundancy and survivability					
● Data backup and offsite storage					
Capacity & Scalability - How your business responds to expected and unexpected increases in application usage as well as the steady growth of application adoption?	1	2	3	4	5
● Visibility into network hardware capacity (max number of remote users, accepted sessions/access ports, etc.)					
● Visibility into traffic prioritisation					
● Visibility into application health					
● Visibility into general hardware utilisation					
● Capacity planning					

Infrastructure Management - The effectiveness of your business in its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.	1	2	3	4	5
● Compliance with industry management best practices					
● Consistency in firmware management					
● Team Skills training					
● Infrastructure automation					
● Overall environment health reporting					
Security - How well your business withstands and recovers from deliberate attacks, accidents, or naturally occurring threats or incidents.	1	2	3	4	5
● Securing from internal threats					
● Bolstering cyber security measures					
● Visibility into security threats					
● Bolstering your business Data against security breaches					
Disaster Recovery - How well your business adapts to and recovers from hazards, shocks, or stresses without compromising long-term prospects for development.	1	2	3	4	5
● Survivability for prolonged outages (network/hardware/power)					
● Mature and tested disaster recovery plans					
● Improving our Recovery Time Objective (RTO)/time to recover after a system goes down					
● Improving our Recovery Point Objective (RPO)/maximum amount of time that we can afford to lose data					


 Congratulations on taking the first step to understand how resilient your network is. If you wish to discuss this further, please forward your completed checklist to Shalini Keyan ([shalkart@cisco.com](mailto:shalkart@cisco.com)).