Out-of-Band Communications Resilience Checklist

Could your organisation still coordinate securely if Microsoft 365, Teams, Exchange or Entra ID were unavailable, compromised or untrusted?

Use these questions in a tabletop exercise, continuity review or cyber incident-response planning session.

1	Do we have an agreed communications channel outside our primary Microsoft 365 environment?	☐
2	Can critical users access it if Entra ID or normal corporate authentication is unavailable?	☐
3	Do we maintain the contact information needed to reach critical people independently of the corporate directory?	☐
4	Is access limited to known and verified users?	☐
5	Can teams use secure messaging and voice if required?	☐
6	Are cyber, leadership, continuity and crisis groups already defined?	☐
7	Do incident leaders know exactly when they should move communications to the out-of-band channel?	☐
8	Is the alternative sufficiently independent that compromise or isolation of the Microsoft environment does not create the same failure?	☐
9	Have relevant executives, security, IT, infrastructure, legal, communications and continuity users already been provisioned?	☐
10	Do those users know how to access and use the channel without support during an incident?	☐

saltcommunications.com
info@saltcommunications.com

11	Can the organisation add critical subject-matter experts quickly while still controlling and verifying access?	
12	Can important updates be distributed quickly to the right groups?	
13	Can communications and key decisions be audited after the incident?	
14	Have we tested a switch away from Teams/email as part of a tabletop or resilience exercise?	
15	Is ownership clear for maintaining users, groups, contact data and readiness?	
16	Could we demonstrate to the Board, a regulator or an auditor how critical communications continue if Microsoft services are unavailable?	

Final Scoring

13-16 Yes	9-12 Yes	0-8 Yes
Strong foundations. Keep exercising the process and maintaining user readiness.	Useful capability exists, but there are dependencies or operational gaps worth tightening.	Communications may be a material single point of failure in the incident-response plan.

The Important Question

The issue is not whether Microsoft is reliable in normal operations. It is whether your organisation has somewhere independent, secure and controlled to go when it cannot use or trust that environment.

Next Step:

Book a 20-minute Out-of-Band Communications Resilience Review..