Business Continuity Readiness Checklist

Use this checklist to evaluate your organisation's current operational resilience and continuity preparedness.

Check each item that accurately reflects your current business practices.

Operational Awareness

☐ 1. Our organisation has identified its most critical business operations.

☐ 2. We understand which systems and services are essential for daily operations.

☐ 3. Key operational responsibilities are documented clearly.

☐ 4. We understand major operational dependencies and single points of failure.

☐ 5. Leadership understands continuity planning priorities.

Communication Preparedness

☐ 6. Internal communication procedures exist for operational disruptions.

☐ 7. Backup communication methods are available if primary systems fail.

☐ 8. Customer communication expectations are defined during service interruptions.

☐ 9. Vendor and partner communication procedures are documented.

☐ 10. Employees understand escalation and reporting procedures during disruption.

Cyber Resilience

☐ 11. Important systems and data are backed up regularly.

☐ 12. Backup recovery procedures are tested periodically.

☐ 13. Multi-factor authentication (MFA) is used on important systems.

☐ 14. Employees receive phishing and cybersecurity awareness guidance.

☐ 15. Cybersecurity incidents are included in continuity planning discussions.

Remote Work and Operational Flexibility

☐ 16. Remote employees understand secure communication expectations.

☐ 17. The organisation can continue operating remotely if necessary.

☐ 18. Critical information remains accessible during disruption.

☐ 19. Cloud service dependency risks have been considered.

☐ 20. Alternative workflows exist for critical operations when systems fail.

Testing and Continuous Improvement

☐ 21. Continuity plans or procedures are reviewed periodically.

☐ 22. The organisation performs continuity discussions or tabletop exercises.

☐ 23. Lessons learned from incidents are documented and reviewed.

☐ 24. Vendor continuity risks are evaluated periodically.

☐ 25. Leadership supports operational preparedness and resilience planning.

SCORING YOUR RESULTS

Strong Maturity: 20–25 Checked Items

Your organisation demonstrates strong operational resilience awareness and continuity preparedness.

You likely maintain:

- operational visibility,
- communication discipline,
- cyber resilience,
- and adaptable recovery capability.

Your next step is continuing regular reviews, improving testing maturity, and strengthening long-term resilience culture.

Moderate Exposure: 12–19 Checked Items

Your organisation has implemented some important continuity protections but may still have operational gaps.

Common risks at this level include:

- unclear recovery priorities,
- inconsistent communication planning,
- untested backups,
- or limited vendor risk visibility.

Your next step is improving documentation, testing procedures, communication planning, and operational awareness across teams.

High Vulnerability: 0–11 Checked Items

Your organisation may currently face significant operational disruption risk.

Potential exposure areas may include:

- recovery confusion,
- undocumented processes,
- communication breakdowns,
- weak backup readiness,
- and heavy dependency on individual employees or systems.

Your next step is establishing foundational continuity procedures, clarifying operational priorities, and strengthening communication and cyber resilience planning.