

Business Cyber Resilience Checklist

Review your systems, suppliers and recovery arrangements

1. Critical Services

- ☐ Identify critical systems
- ☐ Set recovery priorities
- ☐ Record acceptable downtime
- ☐ Document alternative processes

2. Technology Suppliers

- ☐ Record all key providers
- ☐ Identify administrative access
- ☐ Record emergency contacts
- ☐ Review contract and exit arrangements

3. Access Security

- ☐ Enforce MFA
- ☐ Restrict administrator access
- ☐ Remove unused accounts
- ☐ Review remote-management tools

7. Ask Your IT Provider

- Who can access our systems?
- How quickly would you report an incident?
- Are our backups isolated and tested?
- What happens if your systems fail?
- Which responsibilities remain with us?
- Can we retrieve our data and configurations?

4. Incident Notification

- ☐ Agree notification times
- ☐ Record who must be contacted
- ☐ Define information required
- ☐ Include supplier and subcontractor incidents

5. Backup and Recovery

- ☐ Confirm what is backed up
- ☐ Protect and isolate backups
- ☐ Monitor failures
- ☐ Test restoration
- ☐ Measure recovery time

6. Business Continuity

- ☐ Identify decision-makers
- ☐ Store emergency contacts offline
- ☐ Prepare alternative communications
- ☐ Test a cyber-disruption scenario



Scan for the full guide
itclub.work/knowledge-centre

Know what you depend upon. Prepare for disruption. Test recovery.

IT Club

Technology Intelligence — Plain-English guidance for business owners

<https://itclub.work/knowledge-centre>