BITSTC TRAINING & CONSULTING

Continuity & Recovery Checklist

A structured readiness review for business continuity, disaster recovery, crisis leadership, and testing.

Mark each item Complete, In Progress, Not Started, or Not Applicable - and assign an accountable owner.

Governance & scope

Readiness item	Status	Owner
Executive sponsor and program owner are named.	_____	_____
Program scope includes business continuity, technology recovery, cyber incidents, crisis management, and third parties.	_____	_____
Policies define roles, review frequency, exercise expectations, and board reporting.	_____	_____
Plans have named owners, alternates, approval dates, and accessible copies.	_____	_____

Business impact analysis

Readiness item	Status	Owner
Critical services, products, and public functions are identified.	_____	_____
Impact categories and maximum tolerable disruption are approved.	_____	_____
People, facilities, technology, data, suppliers, utilities, and communications dependencies are mapped.	_____	_____
Recovery priorities, RTOs, RPOs, and operational workarounds align.	_____	_____

Continuity strategies

Readiness item	Status	Owner
Strategies address loss of people, facilities, technology, suppliers, utilities, and connectivity.	_____	_____
Manual workarounds are realistic, documented, and supported by required data or forms.	_____	_____
Alternate work locations, remote work, and succession arrangements are validated.	_____	_____
External and internal communication plans include current contacts and approval paths.	_____	_____

Technology recovery

Readiness item	Status	Owner
Applications, infrastructure, data, integrations, cloud services, and vendors are prioritized.	_____	_____
Recovery procedures specify dependencies, sequencing, access, credentials, and decision points.	_____	_____
Backups are protected from production compromise and monitored for successful completion.	_____	_____
Recovery tests prove usable data and end-to-end service restoration against business objectives.	_____	_____

Crisis & cyber response

Readiness item	Status	Owner
Crisis leadership and incident response structures are connected.	_____	_____
Escalation criteria, executive authority, alternates, and decision logging are established.	_____	_____
Ransomware scenarios include continuity, containment, recovery, legal, insurance, regulatory, and communications decisions.	_____	_____
Stakeholder messages can be prepared quickly for employees, customers, residents, regulators, partners, and media.	_____	_____

Exercises & improvement

Readiness item	Status	Owner
Annual exercises include executive, operational, technology, cyber, legal, communications, and vendor participants as appropriate.	_____	_____
Scenarios test decisions and operational continuity, not only plan awareness.	_____	_____
After-action findings are prioritized, assigned, funded, and tracked to closure.	_____	_____
Plans are updated after exercises, incidents, organizational changes, system changes, and vendor changes.	_____	_____

Priority actions

01 Immediate risk or decision: _____

02 30-day action and owner: _____

03 90-day improvement and owner: _____

04 Next exercise or test date: _____

Need help validating the checklist? Schedule a BITSTC continuity and recovery review at Claude@bitstc.com.