DTE-I Self-Assessment Checklist: Availability & Resilience

Organizational Maturity Assessment - Availability & Resilience Module

Document Information

- Version: 1.0
- Date: August 2025
- Author & Owner: Abed Al Rahman Naboulsi, CISSP / DTE-I Framework Initiative
- Validity: 12 months from assessment date

ASSESSMENT INSTRUCTIONS

Rating Scale:

- **0** = Not Implemented: No formal process or control exists
- **1** = Ad-hoc: Informal practices exist but lack documentation or consistency
- **2** = Defined: Formal processes documented and generally followed
- **3** = Optimized: Mature processes with continuous improvement and measurement

Alternative Rating: You may use **+** (Satisfactory), **-** (Needs Improvement), or **N/A** (Not Applicable)

Completion Guidelines:

1. Involve multiple stakeholders (IT Operations, Risk Management, Business Continuity) for comprehensive assessment
2. Provide evidence or examples for ratings of 2 or 3
3. Use "N/A" only when the control is genuinely not applicable to your organization
4. Document specific examples and improvement plans in the Notes section

AVAILABILITY & RESILIENCE ASSESSMENT (6 Items)

1. Backup and Recovery Validation

Assessment Item: Regular backups are performed and tested for all critical data and systems

What this means: Systematic backup procedures with regular restoration testing to ensure data can be recovered when needed, covering both data integrity and system functionality.

Evidence to look for:

- Documented backup schedules for all critical systems and data
- Regular backup integrity testing and restoration verification
- Recovery testing results documented with lessons learned
- Backup storage redundancy (onsite and offsite/cloud)

- Automated backup monitoring and alerting for failures

Frameworks alignment: ISO 27001 (A.12.3 Information backup), ISO 22301 (Business continuity), NIST CSF 2.0 (Recover-RP)

Maqasid perspective: Life preservation (ensuring critical data availability), wealth protection (preventing data loss costs)

Rating (0-3 or +/-/N/A)	Notes/Evidence

2. Recovery Objectives Definition and Testing

Assessment Item: Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are defined and regularly tested

What this means: Clear, measurable recovery targets based on business impact analysis, with regular validation that these objectives can be met during actual recovery scenarios.

Evidence to look for:

- Documented RTO/RPO for each critical system and business process
- Business Impact Analysis (BIA) supporting recovery objectives
- Regular testing demonstrating achievement of stated RTO/RPO
- Recovery objectives aligned with human impact and business criticality
- Executive approval and regular review of recovery targets

Frameworks alignment: ISO 22301 (Business continuity planning), NIST CSF 2.0 (Recover-RP), ISO 27001 (A.17.1)

Maqasid perspective: Justice (fair allocation of recovery resources), life preservation (prioritizing critical services)

Rating (0-3 or +/-/N/A)	Notes/Evidence

3. Disaster Recovery and Business Continuity Management

Assessment Item: Disaster Recovery (DR) and Business Continuity Management (BCM) plans are up-to-date and regularly exercised

What this means: Comprehensive, current plans that address various disaster scenarios, with regular exercises to validate effectiveness and train personnel in emergency procedures.

Evidence to look for:

- Current DR/BCM plans covering various disaster scenarios
- Annual or bi-annual plan exercises with documented results
- Plans updated based on exercise outcomes and business changes
- Clear roles and responsibilities during disaster response
- Communication plans for stakeholders during incidents

Frameworks alignment: ISO 22301 (Business continuity management), ISO 27001 (A.17 Business continuity), NIST CSF 2.0 (Recover function)

Maqasid perspective: Life preservation (ensuring service continuity), dignity preservation (maintaining stakeholder communications)

Rating (0-3 or +/-/N/A)	Notes/Evidence

4. Continuous Monitoring and Capacity Management

Assessment Item: System capacity and performance are continuously monitored to ensure availability

What this means: Proactive monitoring systems that track performance metrics, predict capacity issues, and alert on availability threats before they impact users.

Evidence to look for:

- Real-time monitoring dashboards for critical systems
- Capacity planning based on growth projections and usage patterns

- Automated alerting for performance degradation or capacity limits
- Regular capacity reviews and infrastructure scaling decisions
- Performance baseline documentation and trend analysis

Frameworks alignment: ISO 27001 (A.12.1 Operational procedures), NIST CSF 2.0 (Protect-PT, Detect-DE), ITIL Service Operation

Maqasid perspective: Wealth preservation (preventing service disruption costs), life preservation (maintaining critical service availability)

Rating (0-3 or +/-/N/A)	Notes/Evidence

5. Operational Documentation and Procedures

Assessment Item: Runbooks and operational procedures are documented and regularly reviewed for critical systems

What this means: Comprehensive, up-to-date documentation that enables consistent system operations and incident response, regularly validated for accuracy and completeness.

Evidence to look for:

- Step-by-step runbooks for critical system operations
- Incident response procedures with clear escalation paths
- Regular document reviews and updates (at least annually)
- Procedure validation through testing and exercises
- Knowledge management system with version control

Frameworks alignment: ISO 27001 (A.12.1 Operational procedures), ISO 22301 (BCM procedures), NIST CSF 2.0 (Recover-IM)

Maqasid perspective: Intellectual integrity (maintaining operational knowledge), accountability (clear procedural guidance)

Rating (0-3 or +/-/N/A)	Notes/Evidence

6. Crisis Simulation and Response Capability

Assessment Item: Regular simulation exercises (e.g., tabletop exercises) are conducted to test incident response and recovery capabilities

What this means: Structured exercises that test both technical recovery capabilities and human decision-making under pressure, with focus on stakeholder communication and coordination.

Evidence to look for:

- Regular tabletop exercises covering various crisis scenarios
- Full-scale disaster recovery tests with actual system failover
- Cross-functional participation including senior management
- Exercise outcomes documented with improvement action plans
- Communication and decision-making protocols tested during exercises

Frameworks alignment: ISO 22301 (Testing and exercising), ISO 27035 (Incident management), NIST CSF 2.0 (Recover-IM)

Maqasid perspective: Justice (ensuring fair resource allocation during crises), dignity preservation (maintaining stakeholder trust through preparedness)

Rating (0-3 or +/-/N/A)	Notes/Evidence

SCORING SUMMARY

Individual Scores:

1. Backup and Recovery: ___/3
2. Recovery Objectives: ___/3

3. DR/BCM Plans: ___/3
4. Monitoring/Capacity: ___/3
5. Documentation: ___/3
6. Crisis Simulation: ___/3

Total Score: ___/18

Availability & Resilience Maturity Percentage: ___% (Total ÷ 18 × 100)

Maturity Level:

- **0-25%:** Initial - Ad-hoc practices with significant availability risks
- **26-50%:** Developing - Some resilience measures but inconsistent implementation
- **51-75%:** Defined - Systematic approach to availability with room for optimization
- **76-100%:** Optimized - Mature resilience program with continuous improvement

---

RECOMMENDED NEXT STEPS

For scores 0-25% (Initial):

1. Establish basic backup procedures for critical systems
2. Define initial RTO/RPO objectives based on business impact
3. Create simple incident response procedures
4. Implement basic monitoring for critical systems

For scores 26-50% (Developing):

1. Formalize backup testing and validation procedures
2. Develop comprehensive DR/BCM plans
3. Implement automated monitoring and alerting
4. Begin regular tabletop exercises

For scores 51-75% (Defined):

1. Enhance automation in backup and recovery processes
2. Implement predictive capacity management
3. Increase frequency and complexity of DR testing
4. Develop advanced crisis communication procedures

For scores 76-100% (Optimized):

1. Share resilience best practices with industry peers
2. Implement AI-driven predictive maintenance
3. Mentor other organizations in resilience planning
4. Contribute to industry standards for business continuity

Assessment Completed By:	**Quality Review:**
Name: _____	Reviewer Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

DISCLAIMER: This assessment tool is provided for educational and self-evaluation purposes. It does not constitute legal advice or guarantee compliance with any specific regulations. Organizations should consult with qualified business continuity and technical professionals for guidance specific to their circumstances.