SUMMIT
CYBERSECURITY & IT SOLUTIONS

Backup & Recovery Readiness Overview

A practical guide to understanding recovery capability, not just backup status

Summit Cybersecurity & IT Solutions
Reports & Guides • Version 1.0 • February 2026

Why Backup Readiness Matters

Many organizations believe they are protected because backups exist. Files are copied, storage grows over time, and backup jobs report success.

Backup readiness, however, is not determined by storage alone. It is determined by whether systems and data can be **restored in a timely and predictable way** when disruption occurs.

This guide is designed to help business owners understand how prepared their environment is for recovery — before recovery is required.

How to Use This Overview

- This document focuses on **recovery capability**, not software features
- It is technology-agnostic and applies to most environments
- Not all items apply equally to every business
- Gaps highlight risk exposure, not failure

The goal is clarity and awareness, not complexity.

Backup Coverage

What Is Being Protected

- ☐ Critical business systems are identified

- ☐ Servers and workstations with business data are included
- ☐ Cloud-based data sources are considered
- ☐ Line-of-business applications are evaluated
- ☐ Backup exclusions are documented intentionally

If something is critical to operations, it should be considered for backup.

Backup Frequency & Retention

How Often Data Is Captured

- ☐ Backup schedules align with business operations
- ☐ Data change rates are understood
- ☐ Retention periods meet business and regulatory needs
- ☐ Short-term and long-term retention are defined
- ☐ Old backups are reviewed and rotated appropriately

Backup frequency should match how much data loss is acceptable.

Storage, Security & Separation

How and Where Backups Are Stored

- ☐ Backup data is encrypted at rest and in transit
- ☐ Backup storage is protected from unauthorized access
- ☐ Backups are isolated from primary systems
- ☐ Credentials for backup systems are restricted
- ☐ Storage access is monitored and reviewed

Backups must be protected from the same threats they are designed to recover from.

SUMMIT
CYBERSECURITY & IT SOLUTIONS

Recovery Expectations

What Recovery Actually Looks Like

- ☐ Recovery priorities are defined
- ☐ Acceptable downtime is understood
- ☐ Acceptable data loss is documented
- ☐ Recovery steps are outlined at a high level
- ☐ Responsibility for recovery is assigned

Recovery expectations should be clear before an incident occurs.

Testing & Validation

Confidence Through Verification

- ☐ Restore testing is performed periodically
- ☐ Test results are reviewed and documented
- ☐ Recovery time aligns with expectations
- ☐ Failures are investigated and corrected
- ☐ Testing scope evolves as systems change

Untested backups create false confidence.

Interpreting Readiness Gaps

Reviewing backup readiness helps identify where assumptions may exist.

- Gaps increase downtime risk
- Recovery delays often impact customers and revenue
- Testing reveals issues early
- Readiness improves decision-making under pressure

Backups are only valuable when recovery works as expected.

Closing Perspective

Effective backup strategy is built around recovery, not storage volume.

Understanding how systems are restored, how long recovery takes, and who is responsible allows businesses to reduce uncertainty and respond calmly when disruption occurs.

This is the perspective Summit applies when designing and managing backup solutions.

