Pragmatic GRC™

C-003
Backup Verification Log Guide

Cybersecurity Operations Resource | Version 1.0 | Practical Implementation Guide

Executive Summary

Reliable backups are one of the most important safeguards against ransomware, hardware failure, accidental deletion, and natural disasters. This guide explains how to verify that backups are completing successfully and can be restored when needed.

Document Information

Field	Value
Resource ID	C-003
Resource Family	Cybersecurity Operations
Version	1.0
Related Chapters	6, 8
Related Resources	C-002, C-004, F-001, F-002, G-002

1. Purpose

Document routine verification that business backups completed successfully and remain recoverable.

2. Why Verification Matters

A successful backup job does not guarantee successful recovery. Periodic verification reduces the risk of discovering backup failures during an emergency.

3. Recommended Verification Frequency

Verify critical backups monthly at a minimum and after major infrastructure or application changes.

4. Verification Activities

Confirm backup completion, review job logs, validate storage availability, perform sample restore testing, verify encryption, and document exceptions.

5. Recommended Log Fields

Verification Date, System, Asset ID (F-001), Backup Location, Backup Type, Reviewer, Result, Restore Test Performed, Issues Identified, Corrective Actions, Next Review Date.

6. Escalation Criteria

Escalate failed backups, failed restore tests, storage capacity issues, repeated backup failures, and unauthorized backup configuration changes.

7. Integration with Pragmatic GRC™

Update the Unified System Security Plan (F-002), Business Continuity & Disaster Recovery Playbook (C-002), and Monthly GRC Heartbeat™ (G-002) when significant backup issues are identified.

Backup Verification Workflow

Review Backup Jobs
↓
Validate Completion
↓
Perform Restore Test
↓
Record Results
↓
Correct Deficiencies
↓
Report During Monthly GRC Heartbeat™

Suggested Verification Schedule

Activity	Frequency	Resource
Backup Verification	Monthly	C-003
Restore Test	Quarterly	C-004
BC/DR Review	Annual	C-002
Governance Review	Monthly	G-002

Best Practices

- Verify backups rather than assuming success.
- Periodically perform restore testing.
- Protect backups with encryption and appropriate access controls.
- Maintain offline or immutable backup copies where feasible.
- Investigate and document every failed verification.

Revision History

Version	Date	Author	Description
1.0		Pragmatic GRC™	Initial publication