3-2-1-1 Framework Checklist

A Professional Photographer's Cloud Storage & Backup Guide

The 3-2-1-1 Strategy Explained

The industry standard 3-2-1 rule has evolved. For professional photographers, we now use the **3-2-1-1** framework to protect against hardware failure, theft, and modern ransomware.

- **3 Copies of Data:** Original + 2 Backups.
- **2 Different Media:** e.g., Internal SSD + External HDD/NAS.
- **1 Offsite Copy:** Cloud storage for disaster recovery.
- **1 Immutable Copy:** Offline or "Locked" cloud backup that cannot be deleted or modified.

1 Phase 1: Immediate Post-Shoot (On-Site)

☐ **Dual Slot Capture:** Shoot to two cards simultaneously in-camera (Primary + Overflow/Backup).
☐ **Checksum-Verified Ingest:** Use software (e.g., Hedge, OffShoot, or Lightroom Import with verification) to copy files from cards to local storage.
☐ **Immediate Preview:** Open a sample of RAW files from the local storage to verify integrity before formatting cards.

2 Phase 2: Local Redundancy (The "2" in Media)

☐ **Primary Working Drive:** High-speed SSD (NVMe preferred) for active editing.
☐ **Local Mirror (Clone):** Create an exact replica of the working drive to a secondary HDD or NAS.
☐ **Automation Setup:** Use software like Carbon Copy Cloner or Time Machine to mirror files hourly or daily.

3 Phase 3: Offsite Protection (The "1" in Cloud)

☐ **Automated Cloud Sync:** Set up a background service (e.g., Backblaze Computer Backup or Carbonite) to upload all local drives.
☐ **High-Speed Connection:** Verify upload speeds are sufficient for large RAW files and 4K video.
☐ **Selective Sync for Keepers:** Use a secondary cloud service (Google Drive/Dropbox) specifically for "Selects" and delivered JPEGs for client sharing and quick access.

4 Phase 4: Data Security & Immutability (The Final "1")

☐ **Cloud Object Lock:** Enable "Immutable Storage" (Object Lock) in professional cloud tiers (e.g., Backblaze B2, AWS S3, or Wasabi) to prevent ransomware from deleting backups.
☐ **Offline "Cold" Storage:** Alternatively, perform a monthly backup to an external HDD that is physically disconnected from the network after use.
☐ **Two-Factor Authentication (2FA):** Enable hardware-based 2FA (e.g., YubiKey) on all cloud storage accounts.

5 Monthly Maintenance & Health Check

☐ **The Restore Drill:** Pick one random folder from the cloud and restore it to a new location to ensure it works.
☐ **Disk Health Scan:** Run ”First Aid” or SMART checks on all physical local drives.
☐ **Account Review:** Audit storage usage and upgrade plans before you hit 90% capacity.

”Your data is not safe until it exists in at least three places, one of which is the cloud.”