Below is a **professional, sentence-by-sentence breakdown** of the document titled **“Backup Schemes Notes”**, fully aligned to the **CompTIA A+ 220-1102 (Core 2) – Objective 4.3: Backup and Recovery Methods**. This study guide is formatted for easy copy-paste into Word with proper bullet points, numbered sections, and minimized spacing for professional readability.

**📚 Study Notes: Backup Schemes and Rotation Strategies**

**Document: “Backup Schemes Notes”** **Mapped to: CompTIA A+ 220-1102 Objective 4.3**

**1. Introduction to Backup Schemes**

* Understanding backup types (full, incremental, differential, synthetic) is foundational before designing a **backup scheme**.
* A **backup scheme** defines **how**, **when**, and **where** backups are conducted.
* Key factors in designing a backup scheme include:
  + **Frequency of backups**
  + **On-site vs off-site** storage
  + **Rotation strategies**, such as:
    - **Grandfather-Father-Son (GFS)**
    - **3-2-1 Backup Rule**

**2. Backup Frequency**

* **Frequency** refers to how often backups are performed.
  + **Or period between backup jobs.**
* Example: A full back up every 24 hours = backup frequency of **24 hours**.
* Frequency must align with **business tolerance for data loss**.
  + Some businesses may tolerate up to **24 hours** of data loss.
  + Others may tolerate no more than **1 hour** of loss.
* Your system architecture must support the chosen frequency.
  + A 1-hour tolerance = backups must be taken **every 60 minutes**.
  + A failure to meet this would result in potentially **hours of data loss**.

**3. High-Frequency Backup Alternatives**

* When data needs to be backed up **every minute or second**, traditional full/incremental systems may not be viable.
* **RAID arrays** become useful for real-time fault tolerance.
  + Example: **RAID 5** allows one disk to fail without data loss.
* Even RAID should be backed up nightly to external storage in case of complete array failure.
* Example: **Time Machine (macOS)**:
  + Full backup once per day.
  + Incremental backups every **10–30 minutes**, depending on settings.
  + Enables frequent recovery points without overwhelming storage.

**4. On-Site vs Off-Site Backups**

* **On-Site Backup**:
  + Backup devices (tapes, external drives, NAS) are **in the same building** as the production systems.
  + Pros: **Fast access and recovery** using local network (e.g., gigabit Ethernet).
  + Cons: If a **fire, flood, or natural disaster** occurs, all data (live and backup) may be lost.
* **Off-Site Backup**:
  + Stored at **a different physical location**, separate from production servers.
  + Methods:
    - Manually rotating backup tapes to another location weekly.
    - Using **cloud-based** backup systems.
  + Cloud storage:
    - Offers remote, automated off-site storage.
    - Drawbacks: **Expensive** and **slow upload** speeds for large datasets on slow connections.
    - Example: Cable upload at 30–40 Mbps may struggle with multi-terabyte transfers.

**5. Media Rotation: Tape Backups and Transport**

* Many organizations still use **backup tapes** due to:
  + High capacity (multiple TB per tape).
  + Portability (easy to move off-site).
* Strategy:
  + Perform **daily on-site backups**.
  + Perform **weekly off-site tape rotation**.
* If a **local server fails**, recover from on-site backups.
* If a **major disaster** (e.g., fire) occurs, recover from **weekly off-site tapes**.

**6. Rotation Scheme 1: Grandfather-Father-Son (GFS)**

* A **tape media rotation** strategy organized into **generations**:
  + **Son**: Daily backups (short-term use, rotated often).
    - **Will store most recent data and they have the shortest retention period**.
  + **Father**: Weekly backups (medium-term use).
    - **Middle generation**.
  + **Grandfather**: Monthly backups (long-term retention period).
    - **Oldest Generation**.
* Example setup:
  + **Sons**: 5 tapes (Mon–Fri) reused weekly for daily incremental backups.
    - **One for Each Day**.
  + **Fathers**: 5 weekly tapes for full backups each Friday.
    - **One for Each Week**.
  + **Grandfathers**: 12 tapes, one full back up each month.
    - **One for Each Month**.
* **Total tapes needed**: 22 (5 sons + 5 fathers + 12 grandfathers).
* GFS is flexible and can be **customized** for business needs.
* **Off-site transport** is commonly done with **father or grandfather tapes**.

**7. Rotation Scheme 2: 3-2-1 Backup Rule**

* Requires 3 copies of data, including a production copy on servers, two different types of media, and one copy held offline and off-site.
* **Best practice** strategy or solution designed to handle a wide range of disaster scenarios by having **onsite** and offsite **backups**.
* Rule definition:
  + **3** copies of your data:
    - 1 production/live copy
    - 2 backups
  + **2** different media types (e.g., hard drive + tape)
  + **1** copy stored **offline and off-site**
* Real-world application:
  + Web server = 1 copy (live)
  + Local storage array = 2nd copy
  + Backup tape = 3rd copy (taken off-site weekly)

**📘 Example: Implementing the 3-2-1 Backup Rule**

**💡 Rule Definition Recap:**

The **3-2-1 Backup Rule** is an industry best practice that ensures data resilience by requiring:

* **3 total copies** of your data
* **2 different types of storage media**
* **1 copy stored off-site and offline**

**🛠️ Real-World Implementation**

**🎯 Objective:** Protect mission-critical data hosted on a web server from hardware failure, ransomware, or disaster by applying the 3-2-1 rule.

**✅ Backup Breakdown:**

| **Copy #** | **Description** | **Storage Type** | **Location** | **Role in 3-2-1 Rule** |
| --- | --- | --- | --- | --- |
| **1** | Live data on the production web server | Internal hard drive (primary disk) | On-site | **Primary data (live)** |
| **2** | Backup to a local storage array | Storage Area Network (SAN) | On-site | **2nd copy, 2nd media type** |
| **3** | Full backup written to tape weekly | Backup tape | Off-site vault | **3rd copy, off-site and offline** |

**📌 How This Meets the 3-2-1 Rule:**

1. **Three Copies:**
   * Copy 1: Web server’s local drive
   * Copy 2: Local storage array (e.g., SAN or NAS)
   * Copy 3: Backup tape
2. **Two Different Media Types:**
   * Media 1: Hard drive (web server)
   * Media 2: Tape (weekly full backup)
   * *(Bonus: SAN may count as a third distinct type if disk architecture differs)*
3. **One Copy Off-Site:**
   * Backup tapes are transported weekly to an **off-site secure location** (e.g., a disaster recovery facility or secure vault), ensuring recovery even if the main facility is lost.

**🚨 Example Disaster Scenario:**

**Event:**

Fire destroys the primary office building, including web server and storage array.

**Recovery Process:**

* Retrieve the **off-site backup tape**.
* Restore the latest data to a **standby or new web server** at a recovery location.
* **Minimal data loss** (limited to any changes since last backup).

**🧠 Summary:** By implementing the above strategy, the organization is fully compliant with the **3-2-1 backup rule**, achieving redundancy, media diversity, and off-site protection — all essential for reliable disaster recovery.

**8. Combining GFS + 3-2-1**

* GFS and 3-2-1 can be **combined** effectively:
  + Use GFS for **structured media rotation**.
  + Apply 3-2-1 to ensure **diversity of media** and **off-site protection**.
  + Example: Ship **grandfather tapes off-site weekly** to meet 3-2-1’s “1” rule.
* Both schemes are **independent** but **complement each other** well.
* Not mandatory to use both together but doing so increases backup resilience.

**9. Backup Testing and Validation**

* A backup is **not valid** until it’s **tested** and proven restorable.
* **Verify backups** after creation using backup software.
* Conduct **monthly recovery tests** by restoring data to:
  + Lab environments
  + Isolated servers
* Objective: Ensure:
  + Data is readable.
  + Systems can boot.
  + Applications work post-restore.
* Risks of not testing:
  + Media (e.g., tapes) can degrade.
  + Untested backups may fail when needed most.

**10. Backup Testing Best Practices**

* Perform **monthly restore drills** using randomly selected backup media.
* Test:
  + Read/write functionality.
  + Full system recovery.
  + Application integrity.
* Ensures:
  + **Disaster recovery plans are functional**.
  + **Staff are familiar** with recovery processes.
  + Systems can be brought back online effectively during real emergencies.

**✅ Summary of Key Backup Scheme Concepts**

| **Strategy** | **Purpose** | **Key Components** |
| --- | --- | --- |
| **Backup Frequency** | Defines how often backups run | Hourly, daily, every 10 minutes, etc. |
| **On-site Backup** | Fast, local recovery | NAS, local disk |
| **Off-site Backup** | Protection from local disasters | Tapes, cloud storage |
| **GFS (Grandfather-Father-Son)** | Media rotation strategy | 22 tapes: 5 sons, 5 fathers, 12 grandfathers |
| **3-2-1 Rule** | Disaster-resilient backup plan | 3 copies, 2 media types, 1 off-site |
| **Testing Backups** | Validates backup reliability | Monthly test restores, archive bit checks |