S3 Object Lock: Can you tell the difference between Governance and Compliance mode?

Amazon S3 Object Lock is a feature that helps protect objects from being deleted or overwritten for a fixed amount of time or indefinitely. It's often used to meet regulatory and compliance requirements, especially in industries like finance, healthcare, or legal sectors.

🔐 How S3 Object Lock Works:

When you enable **Object Lock** on an S3 bucket, you can set **retention rules** at the object level:

- **Retention Period**: Specifies how long the object is protected.
- **Legal Hold**: Prevents deletion of the object until the hold is removed (like a legal freeze).
- **Mode**: You can choose between **Governance** or **Compliance** mode.

Governance Mode vs Compliance Mode

Feature	Governance Mode	Compliance Mode
Who can delete?	Users with special IAM permissions (e.g., `s3:BypassGovernanceRetention`) can delete objects	No one can delete the object until the retention period expires—not even the root account
Use case	Internal data protection with some flexibility	Strict regulatory requirements (e.g., SEC, HIPAA)
Retention changes	Can be shortened or removed by privileged users	Cannot be shortened, removed, or bypassed
Legal hold	Supported	Supported

✅ Why We Need It – Real Scenarios

1. Compliance with Government Regulations

Example: A financial services company must retain trading records for 7 years per **SEC Rule 17a-4(f)**.
🔒 Use **Compliance Mode** to lock objects for 7 years, ensuring they're immutable and undeletable by anyone.

2. Ransomware Protection

Example: A healthcare company backs up patient records daily. A ransomware attack might try to delete or encrypt those backups.
Use **Governance Mode** with limited permissions. Even compromised users can't delete backups unless they have `BypassGovernanceRetention`.

3. Accidental Deletion Prevention

Example: A media company stores thousands of video files. An intern accidentally runs a script to delete recent uploads.
🚫 If Object Lock is enabled with a retention period (e.g., 30 days), deletion is blocked — even if the delete API is called.

4. Legal Investigation Hold

Example: A company receives a subpoena and needs to preserve email logs for a legal case.
📌 Apply a **Legal Hold** to relevant objects. This hold stays until explicitly removed, regardless of retention settings.

Object Lock (Governance vs Compliance)

Steps:

1. Create a new S3 bucket → Enable **Object Lock** during creation.
2. Upload a file (`document.txt`).
3. Apply a retention setting:
   - Mode: **Governance Mode**
   - Retention period: 30 days.

✅ Result:

- Normal users **cannot delete** without special permission.
- Admins with "BypassGovernanceRetention" can force delete.

Now, for Compliance Mode:

- Upload another file.
- Set Mode: **Compliance Mode** → 30 days.

✅ Result:

- Absolutely **nobody** can delete or change until 30 days are over.

Which of the following is NOT a feature of S3 Object Lock?

A. Retention period
B. Legal hold
C. Encryption at rest
D. Mode (Governance or Compliance)

✅ **Correct Answer: C**

What happens to versioning when you enable Object Lock on an S3 bucket?

A. It is disabled
B. It must be enabled manually
C. It is automatically enabled
D. It is not required

✅ **Correct Answer: C**

What is the primary purpose of a Legal Hold in S3 Object Lock?

A. To make the object read-only
B. To encrypt the object for legal cases
C. To prevent deletion regardless of retention settings
D. To allow faster access during audits

✅ **Correct Answer: C**

In which Object Lock mode can only users with special permissions override or delete the object during the retention period?

A. Encryption mode
B. Legal hold mode
C. Compliance mode
D. Governance mode

✅ **Correct Answer: D**