AWS S3 Object Lock: Governance Mode and Compliance Mode

# Overview

AWS S3 Object Lock allows you to prevent objects from being deleted or modified for a fixed amount of time or indefinitely. This is useful for enforcing regulatory requirements or protecting data integrity by ensuring that critical data cannot be altered.  
  
It operates in two modes:   
- Governance Mode   
- Compliance Mode

# 1. Governance Mode

Governance Mode allows users to protect objects from being deleted or overwritten, but IAM users with special permissions, like the root user, can still override these restrictions.

## Key Features:

- Prevent Deletion by Most Users: Files protected under Governance Mode cannot be deleted by most users. This includes IAM users who do not have elevated permissions.  
- Root User/Authorized Users Can Override: Certain users with elevated permissions (such as root users or those with specific permissions) can bypass the lock to modify or delete the objects.  
- Retention Period: You can set a retention period for an object. During this period, deletion attempts by regular users will fail.  
- Legal Holds: Similar to a retention policy, you can place a legal hold on an object, which will prevent deletion, but authorized users can still remove the hold or delete the object.

## Use Cases:

- Internal Governance Policies: Organizations can use Governance Mode to enforce retention policies for regular users while allowing select administrators to bypass the restrictions when necessary.  
- Audit and Compliance: While providing some flexibility, this mode ensures compliance for most users while giving certain users the ability to override when required.

# 2. Compliance Mode

Compliance Mode is the stricter of the two Object Lock modes. In Compliance Mode, no user, including the root user or those with elevated IAM permissions, can modify or delete the object until the retention period expires.

## Key Features:

- Absolute Data Protection: Once the object is locked, it cannot be deleted or overwritten by anyone, including the root user.  
- No Exceptions: Even authorized users or root users cannot modify or delete the objects in Compliance Mode.  
- Retention Period: You can set a retention period, but once in Compliance Mode, it cannot be shortened or bypassed.  
- Legal Holds: A legal hold can be placed on objects for indefinite protection, and no one can remove the hold until the specified conditions are met.

## Use Cases:

- Regulatory Compliance: Industries like healthcare, finance, and legal services often need to meet strict regulatory requirements where data cannot be altered or deleted before a certain period.  
- Litigation: For organizations involved in legal proceedings, Compliance Mode ensures that documents or records cannot be tampered with.

# How to Implement AWS S3 Object Lock:

1. Enabling Object Lock:  
 - Create an S3 bucket with Versioning and Object Lock enabled.  
 - Object Lock can only be applied at the bucket level and for individual objects if the bucket is configured for Object Lock.  
2. Setting Retention Modes:  
 - Upload the object to the S3 bucket.  
 - Navigate to the Object Properties and enable Object Lock for that object.  
 - Select either Governance or Compliance Mode.  
 - Specify the retention period (days, months, or years).  
 - Save the settings.  
3. Attempt to Delete:  
 - For Governance Mode: Authorized users can delete the object.  
 - For Compliance Mode: No one can delete the object until the retention period ends.

# Best Practices:

- Plan Your Retention Policies: Clearly define the retention periods and use the appropriate mode for your organizational needs.  
- Test in Non-Production: Always test Governance and Compliance modes in a non-production environment.  
- Monitor and Audit: Use AWS CloudTrail to monitor and ensure compliance with data retention policies.  
- Use Legal Holds Sparingly: Ensure legal holds are part of a defined legal or compliance process to avoid indefinite data protection.