S3 Security Audit Descriptions

1. *Ensure the bucket ACL does not grant 'Everyone' READ permission [list S3 objects]*

   Severity: Critical

   Control ID: LW_S3_1

   Description:

   The S3 bucket ACL gives 'Everyone' permission to list objects, which allows anyone to list the bucket contents. It is best practice to restrict READ permission to only principals who require it.

   Rationale:

   Granting 'Everyone' READ permission allows anyone, including anonymous users from the Internet, to list all objects in a bucket. Malicious users can use this information to identify and exploit objects with misconfigured ACL permissions.

   Remediation:

   Perform the following to revoke READ permission for 'Everyone':

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of buckets, select the bucket you want to change
   4. Navigate to the permissions tab
   5. Select Access Control List from the permissions tab
   6. Under Public access, uncheck the Group 'Everyone' by clicking the circular button in front of it
   7. Uncheck 'List objects' under 'Access to the objects'
   8. Click 'Save' to remove the permission for 'Everyone'
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

2. *Ensure the bucket ACL does not grant 'Everyone' WRITE permission [create, overwrite, and delete S3 objects]*

   Severity: Critical

   Control ID: LW_S3_2

   Description:

   The S3 bucket ACL gives 'Everyone' permission to create, write and delete objects in the bucket. It is best practice to restrict WRITE permission to only principals who require it.

   Rationale:

   Granting 'Everyone' WRITE permission allows anyone, including anonymous users from the Internet, to create, write and delete objects in the bucket. Malicious users can exploit this permission to alter data, delete data and misuse your resources.

   Remediation:

   Perform the following to revoke WRITE permission for 'Everyone':

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of S3 buckets, select S3 bucket you want to change
   4. Navigate to the permissions tab
   5. Select Access Control List from the permissions tab
   6. Under Public access, Select the Group Everyone by clicking the circular button in front of it
   7. Uncheck 'Write objects' under 'Access to the objects'
   8. Click 'Save' to remove the permission for 'Everyone'
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

3. *Ensure the bucket ACL does not grant 'Everyone' READ_ACP permission [read bucket ACL]*

   Severity: Critical

   Control ID: LW_S3_3

   Description:

   The S3 bucket ACL gives 'Everyone' permission to read the bucket ACL. It is best practice to restrict READ_ACL permission to only principals who require it.

   Rationale:

   Granting 'Everyone' READ_ACL permission allows anyone, including anonymous users from the Internet, to read the bucket ACL. Malicious users can use this information to identify and exploit objects with misconfigured permissions.

   Remediation:

   Perform the following to revoke READ_ACL permission for 'Everyone':

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of buckets, select the bucket you want to change
   4. Navigate to the permissions tab
   5. Select Access Control List from the permissions tab
   6. Under Public access, Select the Group 'Everyone' by clicking the circular button in front of it
   7. Uncheck the 'Read bucket permissions' under 'Access to this bucket's ACL'
   8. Click 'Save' to remove the permission for 'Everyone'
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

4. *Ensure the bucket ACL does not grant 'Everyone' WRITE_ACP permission [modify bucket ACL]*

   Severity: Critical

   Control ID: LW_S3_4

   Description:

   The S3 bucket ACL gives 'Everyone' permission to write [or re-write] the bucket ACL. It is best practice to restrict WRITE_ACL permission to only principals who require it.

   Rationale:

   Granting 'Everyone' WRITE_ACL permission allows anyone, including anonymous users from the Internet, to write [or re-write] the bucket ACL. Malicious users can exploit this permission to change a hidden bucket to a public bucket by granting 'READ' and 'WRITE' permission to 'Everyone' – see LW_S3_1 & LW_S3_2.

   Remediation:

   Perform the following to revoke WRITE_ACL permission for 'Everyone':

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of S3 buckets, select S3 bucket you want to change
   4. Navigate to the permissions tab
   5. Select Access Control List from the permissions tab
   6. Under Public access, Select the Group 'Everyone' by clicking the circular button in front of it
   7. Uncheck the 'Write bucket permission' under 'Access to this bucket's ACL'
   8. Click 'Save' to remove the permission for "Everyone"
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

5. *Ensure the bucket ACL does not grant 'Everyone' FULL_CONTROL [READ, WRITE, READ_ACP, WRITE_ACP]*

   Severity: Critical

   Control ID: LW_S3_5

   Description:

   The S3 bucket ACL gives 'Everyone' total control of the bucket and the bucket ACL. It is best practice to restrict FULL_CONTROL.

   Rationale:

   Granting 'Everyone' FULL_CONTROL gives anyone, including anonymous users from the Internet, total control of the bucket. Malicious users can exploit this permission to read, delete or steal your data and/or misuse the resources in your account.

   Remediation:

   Perform the following to revoke FULL_CONTROL for 'Everyone':

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of S3 buckets, select S3 bucket you want to change
   4. Navigate to the permissions tab
   5. Select Access Control List from the permissions tab
   6. Under Public access, Select the Group Everyone by clicking the circular button in front of it
   7. Uncheck the 'Read Objects' and 'List objects' under 'Access to the objects' and 'Read Bucket Permissions' and 'Write bucket permissions' under 'Access to this bucket's ACL'
   8. Click 'Save' to remove the permissions for 'Everyone'
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

6. *Ensure the bucket ACL does not grant AWS users READ permission [list S3 objects]*

Severity: Critical

Control ID: LW_S3_6

Description:

The S3 bucket ACL gives any authenticated AWS user permission to list objects, which allows any authenticated AWS user to list the bucket contents. It is best practice to restrict READ permission to only principals who require it.

Rationale:

Granting all AWS uses READ permission allows any authenticated AWS user to list all bucket objects. Malicious users can create temporary AWS accounts and use this permission to identify and exploit objects with misconfigured ACL permissions.

Remediation:

Perform the following to revoke READ permission for all AWS users:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of buckets, select the bucket you want to change
4. Navigate to the permissions tab
5. Select Access Control List from the permissions tab
6. Under Public access, uncheck the Group ‘Any AWS user’ by clicking the circular button in front of it
7. Uncheck ‘List objects’ under ‘Access to the objects’
8. Click ‘Save to remove the permission for ‘Any AWS user’
9. Repeat steps 3-8 for every bucket for which you want to change permissions

7. *Ensure the bucket ACL does not grant AWS users WRITE permission [create, overwrite, and delete S3 objects]*

   Severity: Critical

   Control ID: LW_S3_7

   Description:

   The S3 bucket ACL gives any authenticated AWS user permission to create, write and delete objects in the bucket. It is best practice to restrict WRITE permission to only principals who require it.

   Rationale:

   Granting all AWS users WRITE permission allows any authenticated AWS user to create, write and delete bucket objects. Malicious users can create temporary AWS accounts and exploit this permission to alter data, delete data and misuse your resources.

   Remediation:

   Perform the following to revoke WRITE permission for all AWS users:

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of S3 buckets, select S3 bucket you want to change
   4. Navigate to the permissions tab
   5. Select Access Control List from the permissions tab
   6. Under Public access, Select the Group ‘Any AWS user’ by clicking the circular button in front of it
   7. Uncheck ‘Write objects’ under ‘Access to the objects’
   8. Click ‘Save’ to remove the permission for ‘Any AWS user’
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

8. *Ensure the bucket ACL does not grant AWS users READ_ACP permission [read bucket ACL]*

Severity: Critical

Control ID: LW_S3_8

Description:

The S3 bucket ACL gives any authenticated AWS user permission to READ the bucket ACL. It is best practice to restrict READ_ACL permission to only principals who require it.

Rationale:

Granting all AWS users READ_ACL permission allows any authenticated AWS user to read the bucket ACL. Malicious users can create temporary AWS accounts and use this information to identify and exploit objects with misconfigured permissions.

Remediation:

Perform the following to revoke READ_ACL permission for all AWS users:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of buckets, select the bucket you want to change
4. Navigate to the permissions tab
5. Select Access Control List from the permissions tab
6. Under Public access, Select the Group ‘Everyone’ by clicking the circular button in front of it
7. Uncheck the ‘Read bucket permissions’ under ‘Access to this bucket’s ACL’
8. Click ‘Save’ to remove the permission for ‘Everyone’
9. Repeat steps 3-8 for every bucket for which you want to change permissions

9. *Ensure the bucket ACL does not grant AWS users WRITE_ACP permission [modify bucket ACL]*

   Severity: Critical

   Control ID: LW_S3_9

   Description:

   The S3 bucket ACL gives any authenticated AWS user permission to write [or re-write] the bucket ACL. It is best practice to restrict WRITE_ACL permission to only principals who require it.

   Rationale:

   Granting all AWS users WRITE_ACL permission allows all AWS users to write [or re-write] the bucket ACL. Malicious users can create temporary AWS accounts and use this permission to change a hidden bucket to a public bucket by granting 'READ and 'WRITE' permission to 'Everyone' – see LW_S3_1 & LW_S3_1

   Remediation:

   Perform the following to revoke WRITE_ACL permission for all AWS users:

   1. Sign in to the AWS Management Console
   2. Open the S3 Service - https://console.aws.amazon.com/s3/
   3. From the list of buckets, select the bucket you want to change
   4. Navigate to the permissions tab
   5. Select 'Access Control List' from the 'Permissions' tab
   6. Under Public access, Select the Group 'Any AWS user' by clicking the circular button in front of it
   7. Uncheck the 'Write bucket permission' under 'Access to this bucket's ACL'
   8. Click 'Save' to remove the permission for 'Any AWS user'
   9. Repeat steps 3-8 for every bucket for which you want to change permissions

10. *Ensure the bucket ACL does not grant AWS users FULL_CONTROL [READ, WRITE, READ_ACP, WRITE_ACP]*

    Severity: Critical

    Control ID: LW_S3_10

    Description:

    The S3 bucket ACL gives any authenticated AWS user total control of the bucket and the bucket ACL. It is best practice to restrict FULL_CONTROL.

    Rationale:

    Granting all AWS users FULL_CONTROL gives any authenticated AWS user total control of the bucket. Malicious users can create temporary accounts and exploit this permission to read, delete or steal your data and/or misuse the resources in your account.

    Remediation:

    Perform the following to revoke FULL_ACCESS permission for all authenticated AWS users:

    1. Sign in to the AWS Management Console
    2. Open the S3 Service - https://console.aws.amazon.com/s3/
    3. From the list of S3 buckets, select S3 bucket you want to change
    4. Navigate to the permissions tab
    5. Select Access Control List from the permissions tab
    6. Under Public access, Select the Group ‘Any AWS user’ by clicking the circular button in front of it
    7. Uncheck the ‘Read Objects’ and ‘List objects’ under ‘Access to the objects’ and ‘Read Bucket Permissions’ and ‘Write bucket permissions’ under ‘Access to this bucket’s ACL’
    8. Click "Save" to remove the permissions for all AWS users
    9. Repeat steps 3-8 for every bucket for which you want to change permissions

11. Ensure the attached S3 bucket policy does not grant 'Allow' permission to everyone

Severity: Critical

Control ID: LW_S3_11

Description:

The S3 Bucket policy gives 'Allow' permission to everyone. It is best practice to restrict policies to specific principals for whom the permissions are intended.

Rationale:

Bucket policies can be very complex. By restricting principals, unintended policy permissions will be limited to the target audience.

Remediation:

Perform the following to remove permissions for everyone from the S3 bucket:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of S3 buckets, select S3 bucket you want to change
4. Navigate to the permissions tab
5. Click on ‘Bucket Policy’ to view and edit the policy
6. In the policy, check any statement that has the Effect value set to "Allow" with a Principal element set to "*" or "AWS":"*" and no conditions
7. To entirely disable entirely access to the API, remove the statement
8. To limit access to a specific AWS account or AWS IAM user, replace the unrestricted Principal element with the Amazon Resource Name (ARN) of the AWS account or user
9. Click ‘Save’ to remove the unrestricted permissions
10. Repeat steps 3-9 for every bucket for which you want to change permissions

12. Ensure the S3 bucket requires MFA to delete objects

Severity: Medium

Control ID: LW_S3_12

Description:

Objects in the bucket are able to be deleted according to bucket ACL or policy. If objects in the bucket are considered 'permanent', MFA delete can help prevent accidental deletion by requiring a second factor.

Rationale:

If objects are considered 'permanent', MFA helps prevent accidental deletion. Additionally, MFA adds an extra level of security by preventing malicious users from intentionally deleting objects.

Remediation:

MFA delete must be enabled through the AWS CLI. Please see AWS documentation for a complete understanding:
https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html#MultiFactorAuthenticationDelete

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>VersioningState</Status>
  <MfaDelete>MfaDeleteState</MfaDelete>
</VersioningConfiguration>
```

13. Ensure the S3 bucket has access logging enabled

Severity: Low

Control ID: LW_S3_13

Description:

Access logging provides records of requests that are made to a bucket. Access log information is useful in security investigations and may be required for audit purposes. It is good practice review bucket objects and enable server access logging as appropriate.

Rationale:

If the S3 bucket has access logging enabled, you will be able to track every request made to access the bucket. Monitoring this activity can be used to detect anomalies and protect against unauthorized access.

Remediation:

Perform the following to enable server access logging:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. Select S3 bucket you want to change
4. Navigate to the 'Properties' panel
5. Select the 'Server access logging' box
6. Check 'Enable logging'
7. Provide the name of the target bucket where the events will be logged
8. Provide the target prefix to provide a sub-directory within the bucket where the log will be stored
9. Click 'Save' to enable logging
10. Repeat steps 3-9 for every bucket for which you want to audit s3 activity

14. Ensure all data stored in the S3 bucket is securely encrypted at rest

Severity: High

Control ID: LW_S3_14

Description:

When server-side encryption is enabled, Amazon S3 encrypts data as it is written to disk and decrypts it when accessed by users. It is good practice to enable S3 bucket encryption.

Rationale:

Encryption helps protect data from unauthorized users and attacks. Although client-side encryption has advantages, it can be complex to implement. Server-side encryption adds a layer of security if client encryption cannot be enabled.

Remediation:

AWS offers three encryption options:

- Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)
- Use Server-Side Encryption with Customer-Provided Keys (SSE-C)

Please refer to the AWS documentation to understand more and choose which is best for you: https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html

15. Ensure all data is transported from the S3 bucket securely

Severity: High

Control ID: LW_S3_15

Description:

Policies that require requests to use secured transport connections to secure data. It is good practice to enable secure transport.

Rationale:

When S3 buckets are accessed without secured transport connections, bucket data is not encrypted and open to man-in-the-middle attacks.

Remediation:

To determine HTTP or HTTPS requests in a bucket policy, use a condition that checks for the key "aws:SecureTransport".

To comply with the **s3-bucket-ssl-requests-only** rule, create a bucket policy that explicitly denies access when the request meets the condition **"aws:SecureTransport": "false"**. This policy explicitly denies access to HTTP requests.

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. Select S3 bucket you want to change
4. Navigate to the Permissions panel
5. Click on Bucket Policy to review and edit the policy
6. Ensure the following statement is present in the policy

```
{
"Sid": "DenyUnSecureCommunications",
"Effect": "Deny",
"Principal": "*",
"Action": "s3:*",
"Resource": ["arn:aws:s3:::BUCKET-NAME",
            "arn:aws:s3:::BUCKET-NAME/*"
],
   "Condition": {
          "Bool": {
                      "aws:SecureTransport": "false"
          }
   }
}
```

7. Click ‘Save’ to enable secure transport
8. Repeat steps 3-6 for every bucket for which you want to change permissions

16. Ensure the S3 bucket has versioning enabled

Severity: High

Control ID: LW_S3_16

Description:

Versioning enables users to keep multiple versions of an object in a bucket. It is a good practice to enable versioning.

Rationale:

Bucket versioning will allow users to recover objects, which were deleted or changed maliciously or by mistake. For buckets with critical information, versioning can help thwart ransomware attacks.

Remediation:

Perform the following to enable Server access logging:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. Select S3 bucket you want to change
4. Navigate to the 'Properties' panel
5. Select the 'Versioning' box
6. Check 'Enable versioning' [you may have to change any lifecycle rules that you have created to apply any object that becomes a previous version]
7. Click 'Save' to enable versioning

17. Ensure that S3 bucket access is restricted to a whitelist of IP networks

Severity: High

Control ID: LW_S3_17

Description:

S3 bucket access can be restricted to a whitelist of IP addresses. This allows the owners to have greater control over network access to sensitive resources.

Rationale:

Whitelisting IP address access to S3 buckets can mitigate certain attacks and data theft. This practice makes accessing the data in S3 more difficult for an attacker.

Remediation:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. Select S3 bucket you want to change
4. Navigate to the 'Permissions' panel
5. Select the 'Bucket Policy' box
6. Add a conditional statement that allows access from the IP addresses you define such as:

```
   {
  "Version": "2012-10-17",
  "Id": "VPCe and SourceIP",
  "Statement": [{
    "Sid": "VPCe and SourceIP",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": [
      "arn:aws:s3:::awsexamplebucket",
      "arn:aws:s3:::awsexamplebucket/*"
    ],
    "Condition": {
      "StringNotLike": {
        "aws:sourceVpce": [
          "vpce-1111111",
          "vpce-2222222"
        ]
      },
      "NotIpAddress": {
        "aws:SourceIp": [
          "11.11.11.11/32",
          "22.22.22.22/32"
        ]
      }
    }
  }]
}
```

18. Ensure the attached S3 bucket policy does not grant global 'Get' permission

Severity: Critical

Control ID: LW_S3_18

Description:

The S3 Bucket policy gives 'Allow' for global 'Get' permission to everyone. It is best practice to restrict policies to specific actions rather than one global action.

Rationale:

Bucket policies can be very complex. By restricting actions, unintended policy permissions will be limited to the targeted actions.

Remediation:

Perform the following to remove 'Get' permissions for everyone from the S3 bucket:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of S3 buckets, select S3 bucket you want to change
4. Navigate to the permissions tab
5. Click on ‘Bucket Policy’ to view and edit the policy
6. In the policy, check any statement that has the Effect value set to "Allow" with a Principal element set to "*" or "AWS":"*" and no conditions
7. To entirely disable entirely access to the API, remove the statement
8. To limit permissions to specific actions, replace global 'Get' actions with specific 'Get' actions
9. Click 'Save' to remove the unrestricted permissions
10. Repeat steps 3-9 for every bucket for which you want to change permissions

19. *Ensure the attached S3 bucket policy does not grant global 'Delete' permission*

    Severity: Critical

    Control ID: LW_S3_19

    Description:

    The S3 Bucket policy gives 'Allow' for global 'Delete' permission to everyone. It is best practice to restrict policies to specific actions rather than one global action.

    Rationale:

    Bucket policies can be very complex. By restricting actions, unintended policy permissions will be limited to the targeted actions.

    Remediation:

    Perform the following to remove 'Delete' permissions for everyone from the S3 bucket:

    1. Sign in to the AWS Management Console
    2. Open the S3 Service - https://console.aws.amazon.com/s3/
    3. From the list of S3 buckets, select S3 bucket you want to change
    4. Navigate to the permissions tab
    5. Click on ‘Bucket Policy’ to view and edit the policy
    6. In the policy, check any statement that has the Effect value set to "Allow" with a Principal element set to "*" or "AWS":"*" and no conditions
    7. To entirely disable entirely access to the API, remove the statement
    8. To limit permissions to specific actions, replace global 'Delete' actions with specific 'Delete' actions
    9. Click 'Save' to remove the unrestricted permissions
    10. Repeat steps 3-9 for every bucket for which you want to change permissions

20. Ensure the attached S3 bucket policy does not grant global 'List' permission

Severity: Critical

Control ID: LW_S3_20

Description:

The S3 Bucket policy gives 'Allow' for global 'List' permission to everyone. It is best practice to restrict policies to specific actions rather than one global action.

Rationale:

Bucket policies can be very complex. By restricting actions, unintended policy permissions will be limited to the targeted actions.

Remediation:

Perform the following to remove 'List' permissions for everyone from the S3 bucket:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of S3 buckets, select S3 bucket you want to change
4. Navigate to the permissions tab
5. Click on ‘Bucket Policy’ to view and edit the policy
6. In the policy, check any statement that has the Effect value set to "Allow" with a Principal element set to "*" or "AWS":"*" and no conditions
7. To entirely disable entirely access to the API, remove the statement
8. To limit permissions to specific actions, replace global 'List' actions with specific 'List' actions
9. Click 'Save' to remove the unrestricted permissions
10. Repeat steps 3-9 for every bucket for which you want to change permissions

21. Ensure the attached S3 bucket policy does not grant global 'Put' permission

Severity: Critical

Control ID: LW_S3_21

Description:

The S3 Bucket policy gives 'Allow' for global 'Put' permission to everyone. It is best practice to restrict policies to specific actions rather than one global action.

Rationale:

Bucket policies can be very complex. By restricting actions, unintended policy permissions will be limited to the targeted actions.

Remediation:

Perform the following to remove 'put' permissions for everyone from the S3 bucket:

1. Sign in to the AWS Management Console
2. Open the S3 Service - https://console.aws.amazon.com/s3/
3. From the list of S3 buckets, select S3 bucket you want to change
4. Navigate to the permissions tab
5. Click on ‘Bucket Policy’ to view and edit the policy
6. In the policy, check any statement that has the Effect value set to "Allow" with a Principal element set to "*" or "AWS":"*" and no conditions
7. To entirely disable entirely access to the API, remove the statement
8. To limit permissions to specific actions, replace global 'Put' actions with specific 'Put' actions
9. Click 'Save' to remove the unrestricted permissions
10. Repeat steps 3-9 for every bucket for which you want to change permissions