

# ThreatModel for Amazon Simple Storage Service (Amazon S3)

## ***Introduction***

Read the blog: [The last S3 security document that we'll ever need.](#)

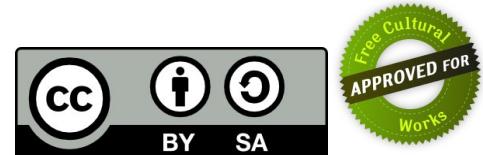
## ***Content***

This publication includes:

- overall data flow diagram of Amazon S3
- overview of the Mitre ATT&CK matrix for Amazon S3
- prioritized list of all threat scenarios
- list of all the control activities and testing procedures
- control mappings to PCI DSS [other frameworks available]
- risk-based prioritized list of control implementation

## ***License Agreement***

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](#). This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.



## ***Source***

The latest version of this work is hosted on [GitHub](#).

## ***Contact***

If you have any questions, please contact [chatbot@trustoncloud.com](mailto:chatbot@trustoncloud.com).

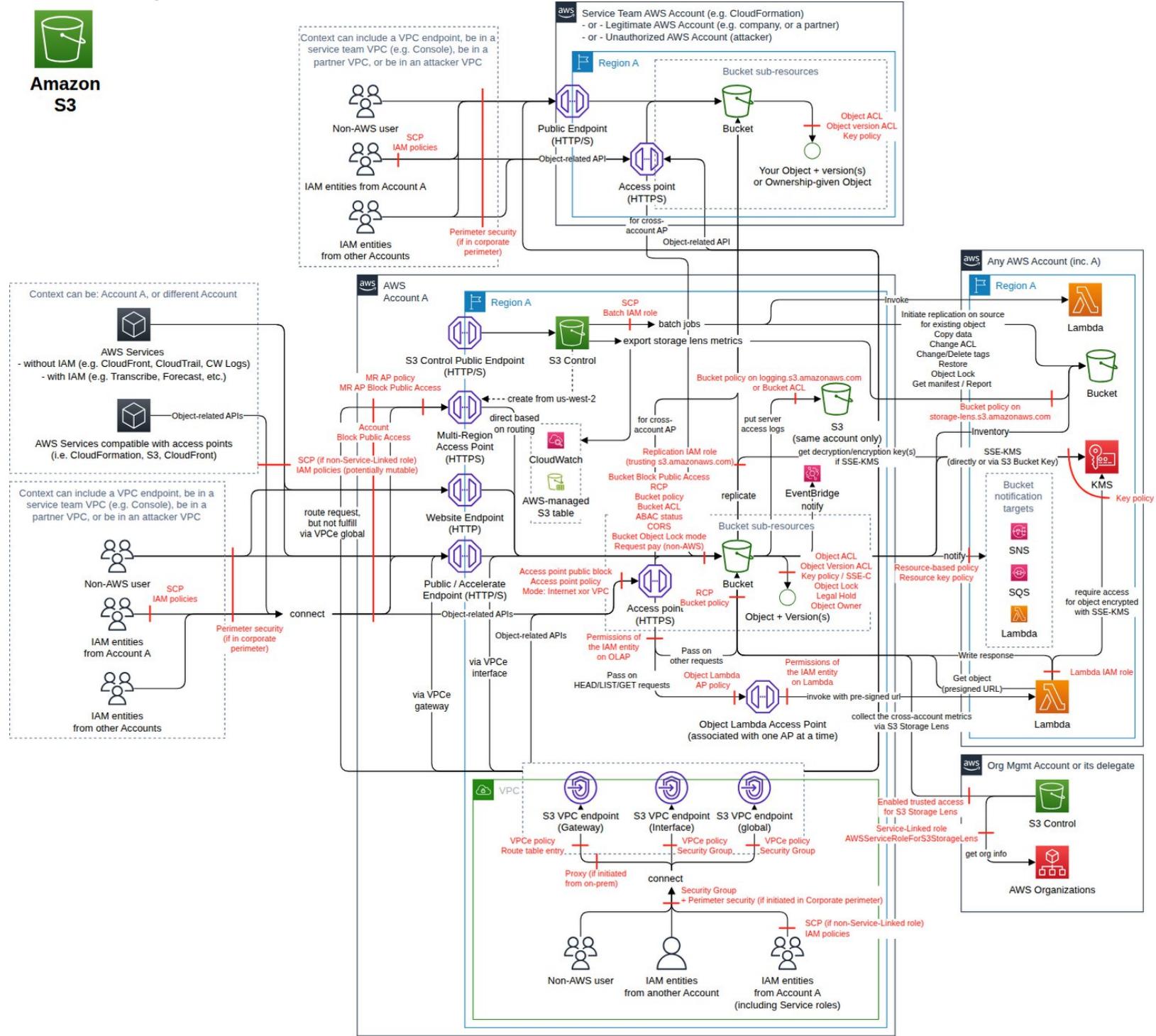


## Amazon Simple Storage Service (Amazon S3)

### Data Flow Diagram



**Amazon  
S3**



## Security Scorecard

### Security in the Cloud

Number of Actions*	194
Identity management	AWS IAM, bucket ACL, object ACL
Number of IAM permissions*	170
Resource-based policy	Bucket
Tag-based ABAC	Yes
CloudTrail Coverage for APIs	100.0%
Number of CloudTrail Event names*	161
CloudWatch Events	Events, via CloudTrail
VPC endpoint	Yes (Interface + Gateway)
VPC endpoint policy	Yes
Network filtering	No
Encryption-at-rest	Yes (SSE-KMS, SSE-S3, SSE-C)
Encryption-in-transit (inc. endpoint protocol)	Yes, but HTTP supported
CloudFormation	6

\* See details in Appendices

## Mitre ATT&CK matrix for Amazon Simple Storage Service (Amazon S3)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Recon of AWS root account emails using the email ACL grantee feature [S3.T19]	Increase bill by creating incomplete multipart uploads [S3.T40]	Use a bucket to upload malware or modify an object to include malware [S3.T14]	Embed client-side script malware in a bucket website [S3.T15]	Uncontrolled change in IAM-managed policies [S3.T57]	Gain access by modifying or deleting important object tags [S3.T33]	Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing its object ACL [S3.T6]		Recon on the security boundaries and resource names through detailed access denial messages [S3.T62]		Bucket takeover to gather data [S3.T1]	Use of less secure or old S3 features [S3.T35]	Unauthorized access to data or loss of control of SSE-C encrypted data via bucket replication [S3.T2]	Grant unauthorized access to a private bucket by changing its bucket ACL [S3.T4]
Recon on valid AWS accounts or IAM principals [S3.T24]	Increase the bill by restoring a large amount of data [S3.T47]				Reduce bucket security by deleting the bucket policy [S3.T38]	Use CloudFront to access a private bucket [S3.T20]				Unauthorized upload of a private object to an accessible (e.g., public) bucket you do not own [S3.T5]		Exfiltrate your data hosted on an external bucket by using compromised IAM credentials accessed over the Internet [S3.T3]	Files encrypted for ransomware [S3.T16]
Recon on the AWS Region of a bucket [S3.T32]					Privilege escalation by enabling ABAC on general purpose buckets [S3.T64]	Exfiltrate data stored on S3 via AWS services [S3.T21]				Move prod data into a non-prod environment [S3.T11]		Exfiltrate data to an attacker bucket via a public endpoint [S3.T7]	Destroy or modify primary data [S3.T17]
						Object made public or accessible in a private bucket you own by changing its object ACL [S3.T36]				Intercept data in transit to an external bucket [S3.T12]		Exfiltrate data by using an S3 VPC endpoint to upload data to an attacker's bucket using an internal IAM entity [S3.T8]	Increase S3 costs by hotlinking or excessive downloading [S3.T22]
						Grant unauthorized access to a private bucket by changing its bucket policy [S3.T37]				Intercept data in transit on an S3 website endpoint [S3.T13]		Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints [S3.T9]	Delete objects by using lifecycle [S3.T25]
						Evade detection by disabling S3 access logs via a bucket ACL change [S3.T51]				Phishing using trademarks [S3.T23]		Exfiltrate data by using the public endpoint to upload data to an attacker's bucket, using external credentials [S3.T10]	Disrupt workflow by manipulating ETag [S3.T27]
						Reduce bucket security by modifying the bucket's Public Access Block [S3.T52]				Unauthorized collection of data by swapping access points [S3.T28]		Exfiltrate data by using tags [S3.T18]	Clickjacking on S3 website [S3.T29]
						Reduce bucket security by modifying the account's Public Access Block [S3.T53]				Use AWS services to access data in S3 [S3.T30]		Unauthorized object restored into an unauthorized bucket [S3.T26]	Loss of ownership of an object [S3.T43]
						Grant unauthorized access to a bucket by changing or deleting one of its access points' policies [S3.T54]				Intercept data in transit to an internal bucket [S3.T34]		Upload to an authorized external bucket but in an incorrect AWS account [S3.T31]	Exfiltrate, modify, or delete objects using Batch [S3.T44]
						Grant unauthorized access to buckets by changing the				Gain unauthorized access to buckets trusting all Multi-		Exfiltrate data by using compromised IAM credentials	Affect data protection by removing versioning

						Multi-Region Access Point policy [S3.T55]				Region Access Points [S3.T56]		from the Internet [S3.T39]	[S3.T48]
						Evade detection by disabling S3 access logs via bucket policy change or removal [S3.T58]						Exfiltrate data via event notification [S3.T41]	Affect data protection by removing replication [S3.T49]
						Evade detection by modifying S3 access logs [S3.T59]						Exfiltrate data via inventory [S3.T42]	DoS by blocking traffic using bucket ACL [S3.T50]
												Hijack a connection with an Object Lambda [S3.T46]	Increase costs and compliance risks by enabling S3 Object Lock in compliance mode [S3.T61]
												Create an exfiltration vector via cross-account access point [S3.T60]	Disrupting object writes by disabling customer-managed encryption on a bucket using SSE-C [S3.T63]
													Disrupting access by switching the object encryption type or its KMS key [S3.T65]

## Feature Classes

Amazon Simple Storage Service (Amazon S3) has the following feature classes and subclasses (i.e. dependent on the usage of its class) that can be activated, restricted, or blocked using AWS Identity and Access Management.

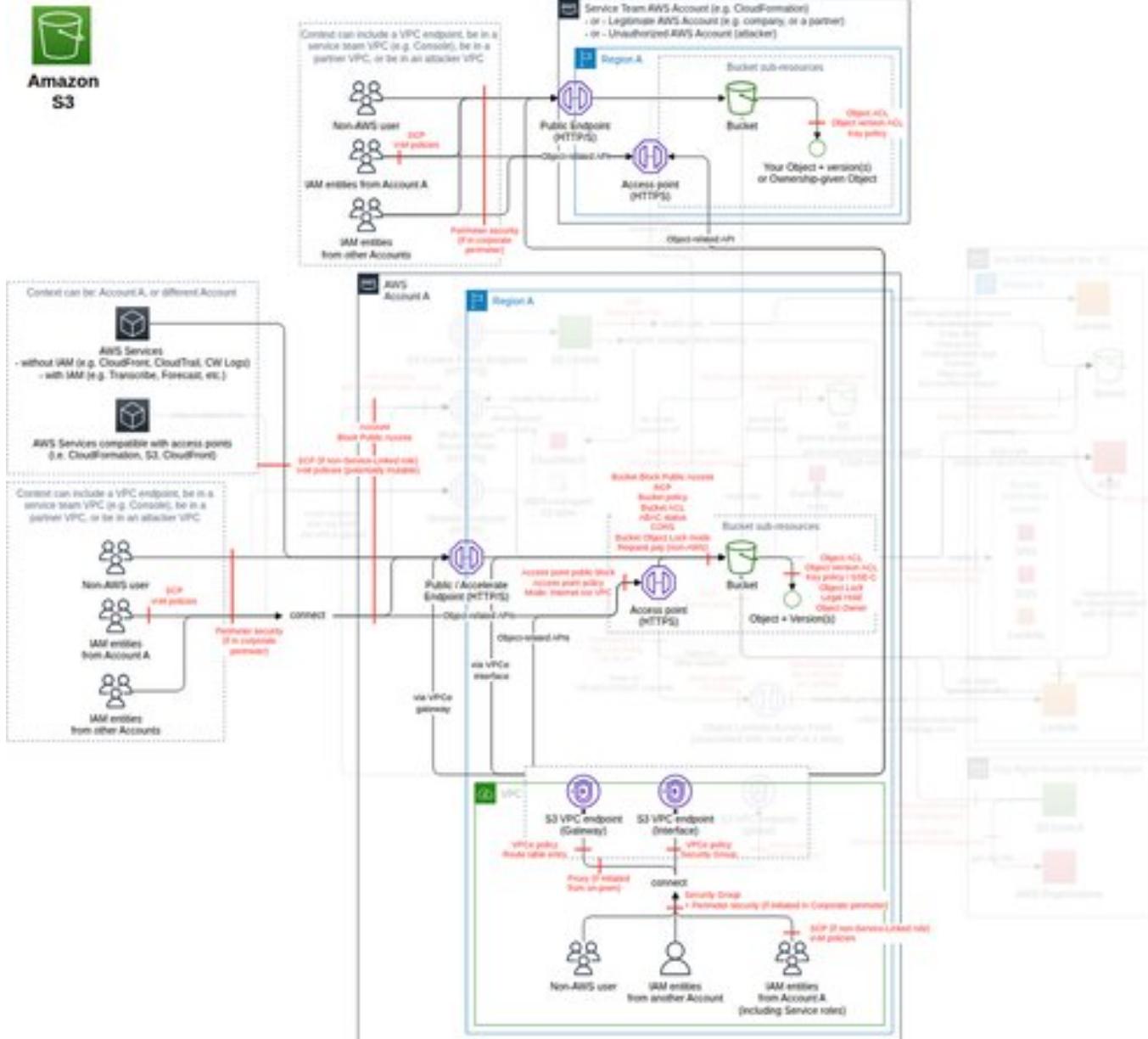
Feature	Relation	Description
Object operations <small>(FC1)</small>	class	You can upload, download, and delete virtually any number of objects to an external S3 bucket for which you are authorized.
Bucket <small>(FC5)</small>	subclass of Object operations	To upload your data into your AWS account, you must create an S3 bucket in one of the AWS Regions.
Bucket tag <small>(FC7)</small>	subclass of Bucket	You can tag buckets ( <a href="#">ref</a> ).
Bucket ACL <small>(FC8)</small>	subclass of Bucket	Amazon S3 Access Control Lists (ACLs) enable you to manage access to buckets ( <a href="#">ref</a> ).
Bucket policy <small>(FC10)</small>	subclass of Bucket	For your bucket, you can add a bucket policy to grant other AWS accounts or IAM users permissions for the bucket and the objects in it. Any object permissions apply only to the objects that the bucket owner creates.
S3 access logging <small>(FC19)</small>	subclass of Bucket ACL/Bucket policy	Server access logging provides detailed records of the requests made to a bucket.
Analytics <small>(FC11)</small>	subclass of Bucket	You can analyze storage access patterns to decide the storage class ( <a href="#">ref</a> ).
Inventory <small>(FC12)</small>	subclass of Bucket	You can create a report on your storage, including object metadata or versions ( <a href="#">ref</a> ).
Lifecycle <small>(FC13)</small>	subclass of Bucket	You can manage the lifecycle of your data to reduce storage costs ( <a href="#">ref</a> ).
Metrics <small>(FC14)</small>	subclass of Bucket	You can configure metrics to get additional insights into your usage ( <a href="#">ref</a> ).
Website <small>(FC16)</small>	subclass of Bucket	You can host a static website on Amazon S3. On a static website, individual web pages include static content. They might also contain client-side scripts ( <a href="#">ref</a> ).
S3 Object Lock <small>(FC17)</small>	subclass of Bucket	You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model ( <a href="#">ref</a> ). Creating a bucket with S3 Object Lock will enable versioning even without permissions.
Legal hold <small>(FC29)</small>	subclass of S3 Object Lock	A legal hold provides the same protection as a retention period but has no expiration date. S3 Object Lock must be activated on the bucket.
Transfer Acceleration <small>(FC18)</small>	subclass of Bucket	You can use Transfer Acceleration to improve the performance of long-distance transfers ( <a href="#">ref</a> ).
Notification <small>(FC20)</small>	subclass of Bucket	You can receive notifications when certain events happen in your bucket.
CORS <small>(FC22)</small>	subclass of Bucket	You can create a CORS configuration with rules that identify the origins you will allow to access your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information.
Bucket default encryption <small>(FC23)</small>	subclass of Bucket	You can set default encryption on a bucket so that all new objects are encrypted when stored in the bucket.
Public Access Block (bucket) <small>(FC24)</small>	subclass of Bucket	S3 Block Public Access (bucket) provides controls at the individual S3 bucket level to ensure objects never have public access.
Public Access Block (account) <small>(FC25)</small>	subclass of Bucket	S3 Block Public Access (account) provides controls across an entire AWS account to ensure objects never have public access.
Access point <small>(FC26)</small>	subclass of Bucket	Access points are named network endpoints that are attached to buckets, which you can use to perform S3 object operations.

S3 Object Lambda <small>(FC32)</small>	subclass of Access point	S3 Object Lambda enables users to apply their custom code to process the output of a standard S3 request by automatically invoking a Lambda function.
S3 Storage Lens <small>(FC31)</small>	subclass of Bucket	S3 Storage Lens provides a single view of object storage use and activity across your entire S3 storage.
Tagging (for Storage Lens group only) <small>(FC34)</small>	subclass of S3 Storage Lens	When you configure your Storage Lens group, you can optionally add AWS resource tags to the group.
Multi-Region Access Points <small>(FC33)</small>	subclass of Bucket	S3 Multi-Region Access Points provide a single global endpoint to access a dataset that spans multiple S3 buckets in different AWS Regions or in different AWS accounts.
FIS actions <small>(FC35)</small>	subclass of Bucket	In AWS Fault Injection Service, the action <code>aws:s3:bucket-pause-replication</code> can pause S3 replication from the experiment AWS Region to the destination AWS Region for the targeted buckets. Review FIS ThreatModel for more information.
S3 Object Ownership <small>(FC30)</small>	subclass of Bucket, used by Object operations	S3 Object Ownership enables bucket owners to automatically assume ownership of objects uploaded to their buckets by other AWS accounts.
Object tagging <small>(FC2)</small>	subclass of Object operations, used by Bucket	You can tag objects ( <a href="#">ref</a> ).
Attribute-based access control (ABAC) for general purpose buckets <small>(FC36)</small>	subclass of Object tagging/Bucket	ABAC for general purpose buckets is an Amazon S3 feature that allows access decisions to be made based on matching attributes such as tags between IAM principals and S3 buckets.
Object versioning <small>(FC3)</small>	subclass of Object operations, used by Bucket	You can version your objects ( <a href="#">ref</a> ).
Bucket versioning <small>(FC6)</small>	subclass of Object versioning/Bucket	Versioning is a means of keeping multiple variants of an object in the same bucket ( <a href="#">ref</a> ).
Replication <small>(FC15)</small>	subclass of Bucket versioning	Replication enables the automatic and asynchronous copying of objects from one bucket to another bucket ( <a href="#">ref</a> ).
ACL on versioned objects <small>(FC9)</small>	subclass of Object versioning/Bucket ACL	Amazon S3 Access Control Lists (ACLs) enable you to manage access to object versions ( <a href="#">ref</a> ).
Tag on versioned objects <small>(FC4)</small>	subclass of Object tagging/Object versioning, used by Bucket	You can tag each version of an object ( <a href="#">ref</a> ).
Torrent <small>(FC21)</small>	subclass of Object operations, used by Bucket	You can use the BitTorrent protocol to retrieve objects ( <a href="#">ref</a> ).
Batch <small>(FC27)</small>	subclass of Object operations, used by Bucket	S3 Batch Operations performs large-scale Batch Operations on Amazon S3 objects.
Other uses <small>(FC28)</small>	class	Others can use their S3 service to impact you in some way.

# Object operations (class, FC1)

You can upload, download, and delete virtually any number of objects to an external S3 bucket for which you are authorized. Amazon S3 Access Control Lists (ACLs) enable you to manage access to objects. Each object has an ACL attached to it as a sub-resource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to ensure the requester has the necessary access permissions ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

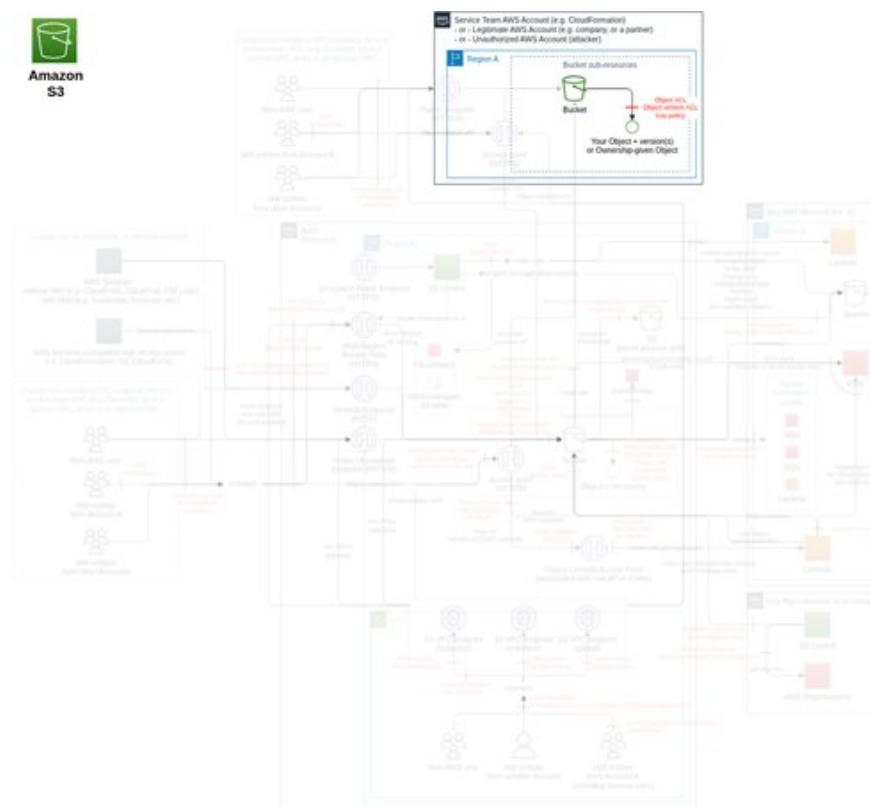
Action	IAM Permission
Deletes an object permanently (non-versioned bucket) or inserts a delete marker (versioned bucket).	s3>DeleteObject
Retrieves an object from Amazon S3.	s3:GetObject
Adds an object to a bucket.	s3:PutObject
Sets the Access Control List (ACL) permissions for an object. You must have WRITE_ACP permission to set the ACL of an object.	s3:PutObjectAcl

## Threat List

Name	CVSS
Loss of ownership of an object	<a href="#">High (7.1)</a>
Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints	<a href="#">Medium (6.2)</a>
Destroy or modify primary data	<a href="#">Medium (6.1)</a>
Exfiltrate data stored on S3 via AWS services	<a href="#">Medium (5.8)</a>
Exfiltrate your data hosted on an external bucket by using compromised IAM credentials accessed over the Internet	<a href="#">Medium (5.7)</a>
Exfiltrate data to an attacker bucket via a public endpoint	<a href="#">Medium (5.7)</a>
Unauthorized upload of a private object to an accessible (e.g., public) bucket you do not own	<a href="#">Medium (5.7)</a>
Exfiltrate data by using an S3 VPC endpoint to upload data to an attacker's bucket using an internal IAM entity	<a href="#">Medium (5.5)</a>
Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing its object ACL	<a href="#">Medium (5.2)</a>
Intercept data in transit to an external bucket	<a href="#">Medium (4.6)</a>
Unauthorized object restored into an unauthorized bucket	<a href="#">Medium (4.3)</a>
Upload to an authorized external bucket but in an incorrect AWS account	<a href="#">Medium (4.0)</a>
Recon on the security boundaries and resource names through detailed access denial messages	<a href="#">Low (3.5)</a>
Exfiltrate data by using tags	<a href="#">Low (3.3)</a>
Use of less secure or old S3 features	<a href="#">Low (1.9)</a>

## Loss of ownership of an object

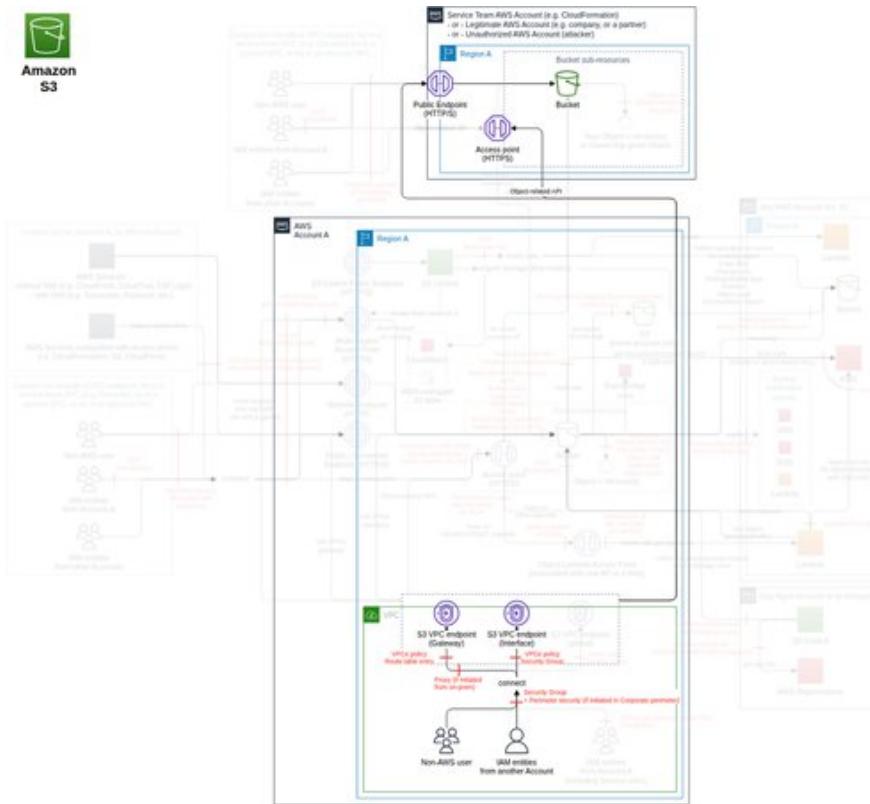
<b>Threat Id</b>	S3.T43
<b>Name</b>	Loss of ownership of an object
<b>Description</b>	S3 Object Ownership enables a bucket receiver to convert a bucket-owner-full-control ACL into an ownership transfer (for a new object); additionally, a bucket can convert all the objects to be owned by the bucket owner. An attacker can modify the receiver bucket to remove your object ACL control on an object and remove your access to this object.
<b>Goal</b>	Data manipulation
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1531</a>
<b>CVSS</b>	<a href="#">High (7.1)</a>
<b>IAM Access</b>	{ "OPTIONAL": "s3:PutBucketOwnershipControls" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO37 - Disabling ACLs for all buckets</b> C152 - Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023). C153 - Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Very High	1	1	-
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b> C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C114 - For all external buckets with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, block the PutObject with any ACL (e.g., using IAM or SCP and a deny on the condition "StringLike": {"s3:x-amz-acl": "*"}). It should be called via PutObjectAcl. C115 - For all external buckets with bucket-owner-full-control ACL requirements but without S3 Object Ownership handover, monitor that the PutObject operation does not include the ACL header.	Very High	1	1	1
<b>CO12 - Enforce secure SDLC processes</b> C113 - When transmitting an object to an external bucket with bucket-owner-full-control ACL requirements but without S3 Object Ownership handover, use 2 separate APIs (PutObject and PutObjectAcl) instead of the built-in object ACL operation in PutObject.	High	1	-	-

## Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints

<b>Threat Id</b>	S3.T9
<b>Name</b>	Exfiltrate data by uploading it to an attacker bucket using a non-authenticated user or an unauthorized external IAM entity via one of your S3 VPC endpoints
<b>Description</b>	VPC endpoints for S3 allow any entity to connect from a VPC to any S3 bucket without an Internet Gateway. An attacker can exfiltrate data to an external S3 bucket via one of your VPC endpoints, using an unauthenticated user or their own external IAM entity. Note that some external IAM entities might be authorized if provided by one of your business partners.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010, T1537</a>
<b>CVSS</b>	<a href="#">Medium (6.2)</a>
<b>IAM Access</b>	{}

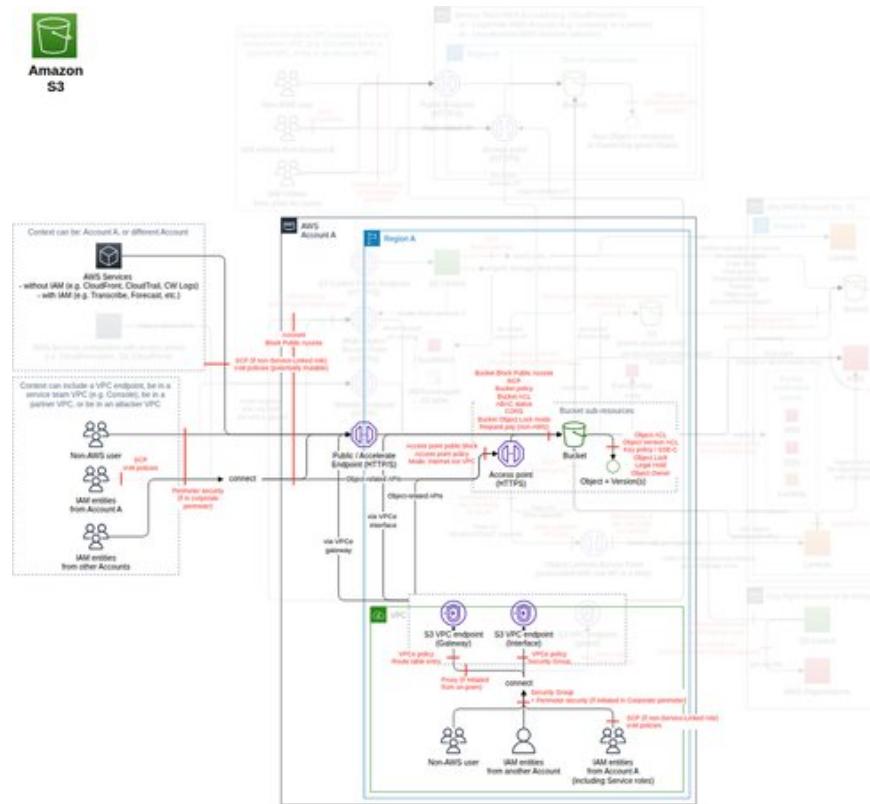


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C105 - Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy.	Very High	1	1	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO7 - Limit and monitor access via S3 VPC endpoints</b> C17 - For each VPC, maintain a list of AWS Organizations, OUs, and/or AWS accounts where IAM entities are authorized to access S3. C18 - For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g., <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ). C19 - Block any IAM entity not belonging to an authorized AWS Organization, OU, and/or AWS account from calling S3 from your VPCs by adding a deny statement in the S3 VPC endpoint policy for each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org IDs, as those are globally unique. C21 - Enable <a href="#">VPC DNS query logging</a> in all VPCs. C22 - Maintain a list of authorized S3 and S3 access points (and their respective AWS accounts) to be accessed for each VPC. C23 - Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g., using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use a specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points). C25 - Monitor VPC DNS query logs to ensure only authorized S3 buckets and S3 access points are being queried in each VPC (e.g., using VPC DNS query logging) and protect them using Route 53	Very High	5	2	1

ThreatModel. C124 - Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoint controls.				
<b>C05 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C15 - Request access via an S3 access point on a bucket you don't own, if compatible with your interaction with the bucket (e.g., not through an unsupported AWS service).	High	2	-	-
<b>C03 - Enable S3 data events in AWS CloudTrail</b>  C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b>  C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Destroy or modify primary data

<b>Threat Id</b>	S3.T17
<b>Name</b>	Destroy or modify primary data
<b>Description</b>	S3 provides high durability by design (11 9s). However, data can still be deleted by the customer. An attacker (or someone by negligence) can use their access to destroy (or modify) primary data located on S3, affecting the ability of the business to operate (for example, <a href="#">Code Spaces</a> ).
<b>Goal</b>	Disruption of Service
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1485</a>
<b>CVSS</b>	<a href="#">Medium (6.1)</a>
<b>IAM Access</b>	<pre>{   "AND": [     {       "OR": ["s3&gt;DeleteObject", "s3:PutObject"]     },     {       "OPTIONAL": {         "OR": ["s3&gt;DeleteObjectVersion", "s3:BypassGovernanceMode", "s3:PutObjectLegalHold"]       }     }   ] }</pre>

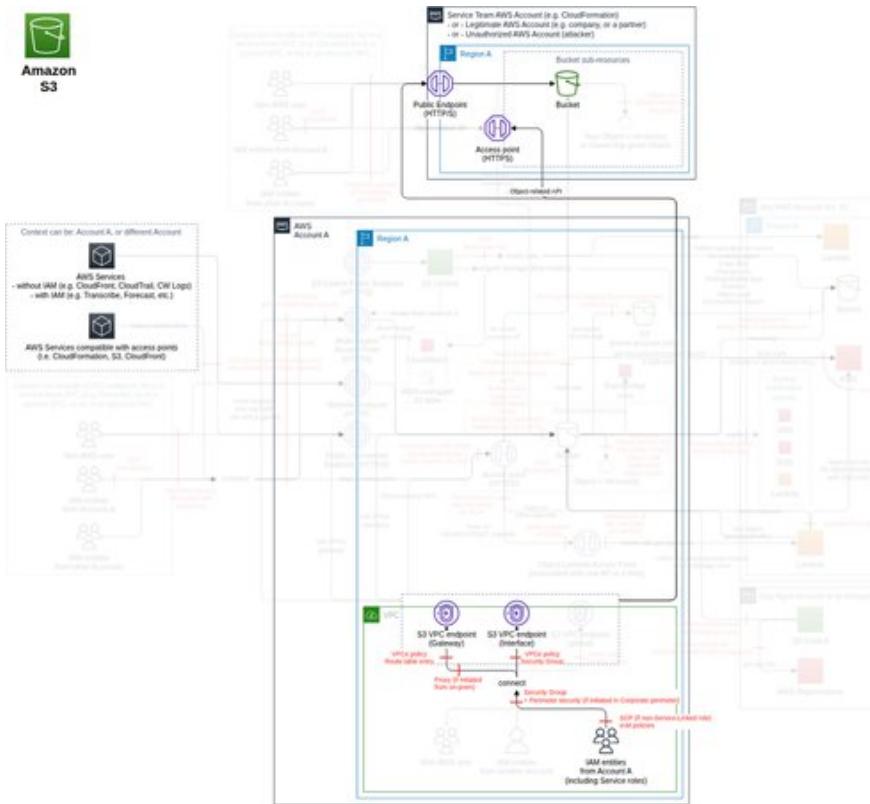


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO29 - Limit access from only authorized VPCs</b> C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpc" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Very High	1	1	-
<b>CO16 - Enforce encryption at rest</b> C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C63 - Use KMS ThreatModel to protect the KMS keys used for S3 (e.g., using encryptionContext on the policy of each KMS key). C64 - Implement an authorized default encryption key on each bucket; enable S3 Bucket Key if not using DSSE-KMS and if CloudTrail events are not required for KMS encrypt/decrypt (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings). C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key).	Very High	4	1	-
<b>CO17 - Protect primary data against loss</b> C69 - Enable versioning on buckets holding primary data. C71 - Back up primary data in a secure location under a different security authority (e.g., in an <a href="#">AWS data bunker account</a> via replication, or using AWS Backup for Amazon S3).	Very High	2	-	-
<b>CO20 - Protect data integrity using S3 Object Lock</b>	Very High	-	2	-

C74 - Implement the authorized default S3 Object Lock on buckets requiring WORM (note: Amazon S3 evaluates and applies bucket policies before applying the bucket default S3 Object Lock settings). C76 - Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on buckets requiring WORM (e.g., using their bucket policy and centrally in an RCP applied to the OU or the AWS account with a deny statement on PutObject and PutObjectRetention if the condition "s3:object-lock-mode" exists and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration).				
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	High	2	-	-
<b>CO12 - Enforce secure SDLC processes</b> C44 - Ensure the integrity of stored objects ( <a href="#">ref</a> ), using "x-amz-checksum" from the <a href="#">object metadata</a> instead of ETag (e.g., using the compute checksum functionality in S3 Batch Operations). If ETag is used, make sure to properly account for its different definitions ( <a href="#">ref</a> ).	Medium	1	-	-
<b>CO19 - Have a process to apply legal holds</b> C73 - Create a process to apply a legal hold to any S3 bucket whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.	Medium	1	-	-
<b>CO18 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Low	1	-	-

## Exfiltrate data stored on S3 via AWS services

<b>Threat Id</b>	S3.T21
<b>Name</b>	Exfiltrate data stored on S3 via AWS services
<b>Description</b>	A number of AWS services use S3 for storage, including cross-account S3 buckets. Services with IAM roles (e.g., SageMaker) will give ownership to the target AWS account, removing ownership protection. An attacker can use those services to exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (5.8)</a>
<b>IAM Access</b>	{ "OPTIONAL": "s3:PutObjectAcl" }

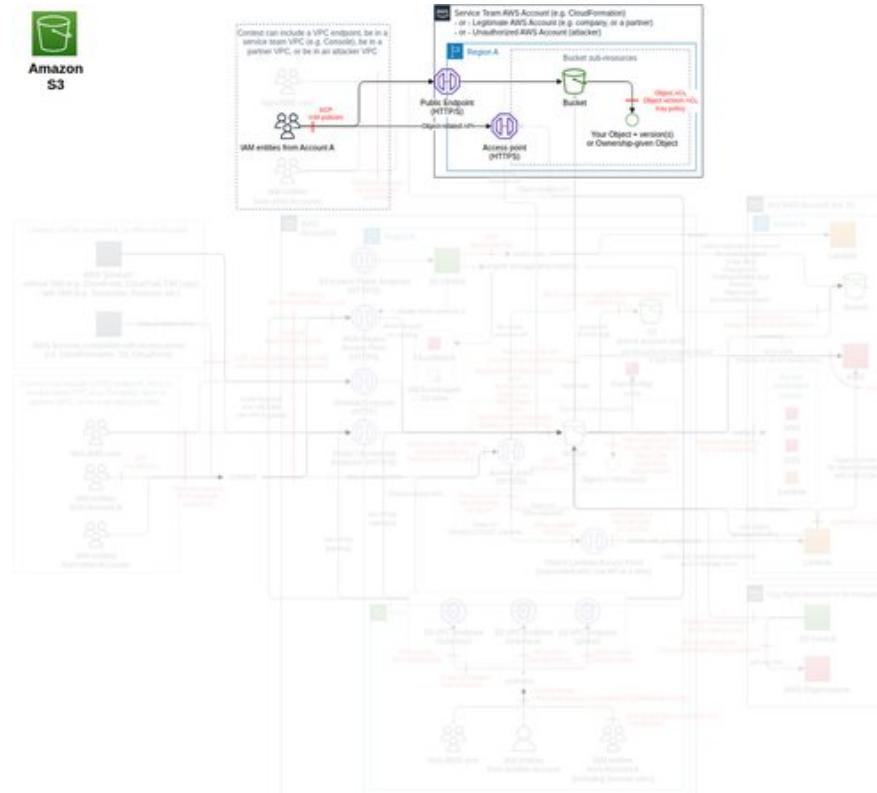


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b> C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C13 - Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	High	1	-	1
<b>CO6 - Model the threats on all AWS services accessing S3</b> C16 - Analyze and protect all AWS services accessing S3 (e.g., via ThreatModel). Enforce use in VPC only, whenever possible.	High	1	-	-
<b>CO3 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to	Medium	2	-	-

review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.				
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

**Exfiltrate your data hosted on an external bucket by using compromised IAM credentials accessed over the Internet**

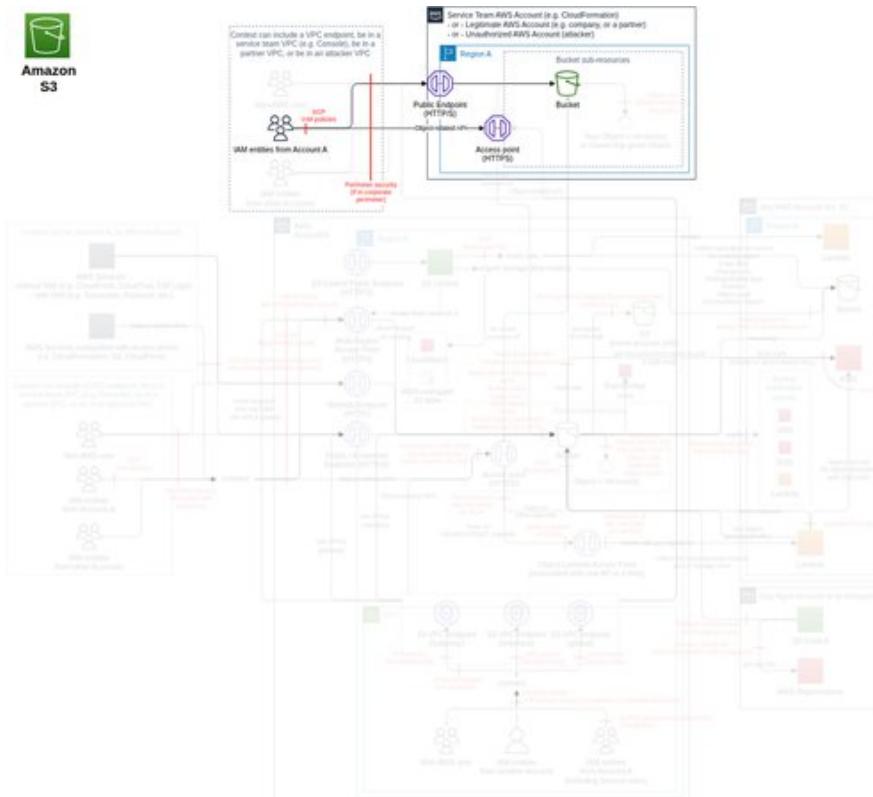
<b>Threat Id</b>	S3.T3
<b>Name</b>	Exfiltrate your data hosted on an external bucket by using compromised IAM credentials accessed over the Internet
<b>Description</b>	IAM credentials can be compromised. An attacker can use a compromised but authorized credential to download your object from an external bucket via the public endpoint or their VPC endpoint.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1567</a>
<b>CVSS</b>	<a href="#">Medium (5.7)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:GetObject" }



Control Objectives		# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b> C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel).	High	1	-	-
<b>CO12 - Enforce secure SDLC processes</b> C46 - Ensure all S3 buckets interacted with are in the correct AWS account (e.g., using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner).	Medium	1	-	-
<b>CO4 - Monitor S3 with Amazon GuardDuty and Macie</b> C10 - Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective).	Low	1	-	-
<b>CO18 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Very Low	1	-	-

## Exfiltrate data to an attacker bucket via a public endpoint

<b>Threat Id</b>	S3.T7
<b>Name</b>	Exfiltrate data to an attacker bucket via a public endpoint
<b>Description</b>	S3 allows IAM entities to upload data to a bucket in other AWS accounts if they have the necessary IAM permissions. An attacker can use one of your IAM entities to upload data to one of their buckets. If the attacker does not control the object ACL, they can use the names of objects (1 KB).
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1537</a>
<b>CVSS</b>	<a href="#">Medium (5.7)</a>
<b>IAM Access</b>	{ "AND": ["s3:PutObject", { "OPTIONAL": "s3:PutObjectAcl" }] }

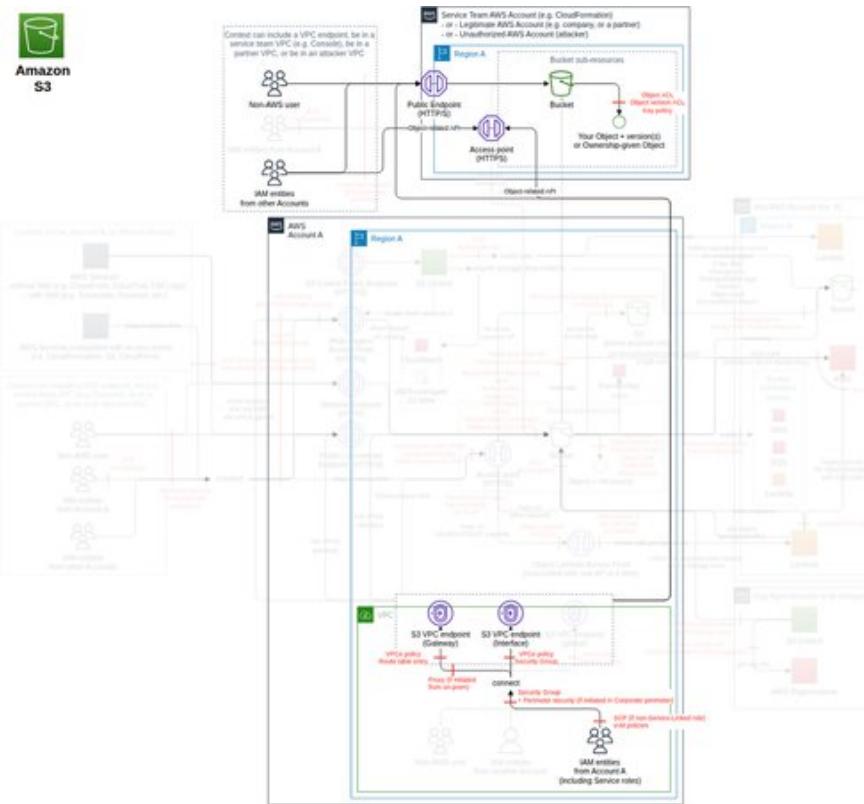


Control Objectives		# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO2 - Block S3 endpoints in your corporate perimeter security</b>  C8 - Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Very High	1	-	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b>  C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO32 - Restrict access point access to VPCs when in use</b>  C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C105 - Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy. C106 - In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn". C107 - Block the creation of non-VPC S3 access point "s3>CreateAccessPoint" (e.g., using IAM policies and SCPs with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}). C108 - Block all traffic from Internet-configured S3 access points (e.g., in their bucket policy, or centrally in an RCP applied to the OU or AWS account, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}). C112 - Block any <a href="#">object-related operations</a> access to S3 buckets not through an access point (i.e., IAM policy, SCP, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on the condition "ArnNotLike": {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountID:accesspoint/*"}).	Very High	1	5	-

<b>C05 - Identify and ensure the protection of all external buckets hosting your objects</b> C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C13 - Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	High	1	-	1
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>C03 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C016 - Enforce encryption at rest</b> C162 - Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse"). C163 - Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Low	-	1	1
<b>C018 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Low	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Unauthorized upload of a private object to an accessible (e.g., public) bucket you do not own

<b>Threat Id</b>	S3.T5
<b>Name</b>	Unauthorized upload of a private object to an accessible (e.g., public) bucket you do not own
<b>Description</b>	S3 buckets can be public for a legitimate reason. An attacker (or someone by negligence) can upload sensitive data to an accessible bucket (e.g., public) you do not own to make it accessible to exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1074</a>
<b>CVSS</b>	<a href="#">Medium (5.7)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutObject" }

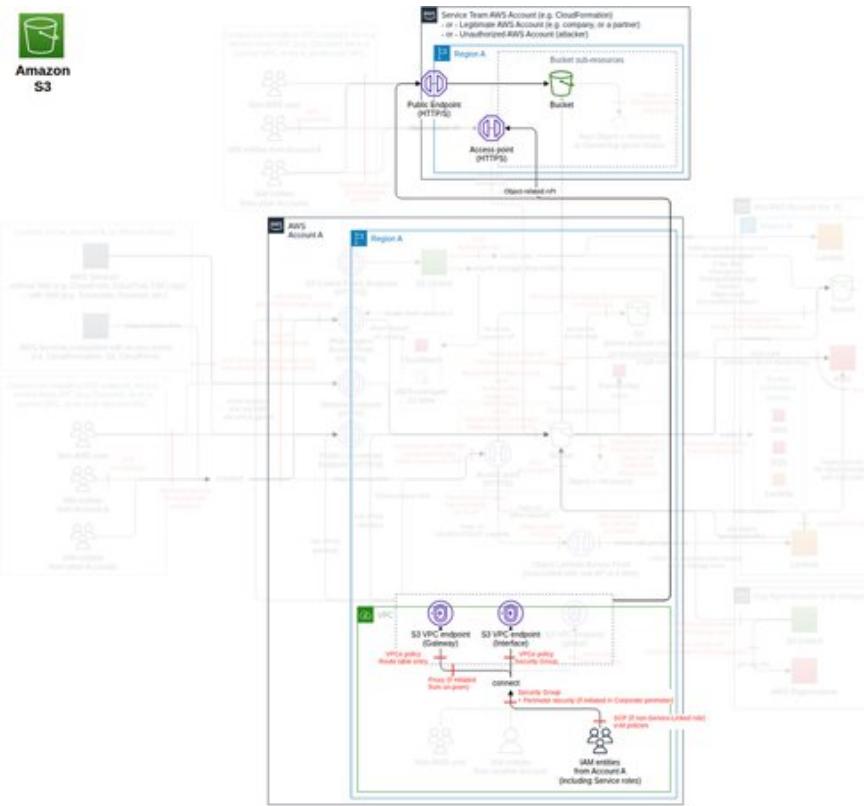


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> <small>C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a>.</small>	Very High	1	-	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> <small>C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").</small>	Very High	1	1	1
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b> <small>C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C12 - Allow only authorized ACLs on objects for buckets you don't control (e.g., using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a>). C14 - Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g., using Macie).</small>	High	2	1	-
<b>CO3 - Enable S3 data events in AWS CloudTrail</b> <small>C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.</small>	Medium	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> <small>C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.</small>	Medium	1	-	-

<b>C016 - Enforce encryption at rest</b> C162 - Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse"). C163 - Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Low	-	1	1
<b>C018 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Low	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Exfiltrate data by using an S3 VPC endpoint to upload data to an attacker's bucket using an internal IAM entity

<b>Threat Id</b>	S3.T8
<b>Name</b>	Exfiltrate data by using an S3 VPC endpoint to upload data to an attacker's bucket using an internal IAM entity
<b>Description</b>	VPC endpoints for S3 allow IAM entities to connect from a VPC to any S3 bucket without an Internet Gateway. An attacker can exfiltrate pre-collected data to an external S3 bucket via a VPC endpoint, using an internal IAM entity they control. If the attacker does not control the object ACL, they can use the names of objects (1 KB).
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010, T1537</a>
<b>CVSS</b>	<a href="#">Medium (5.5)</a>
<b>IAM Access</b>	{ "AND": ["s3:PutObject", { "OPTIONAL": "s3:PutObjectAcl" }]} }

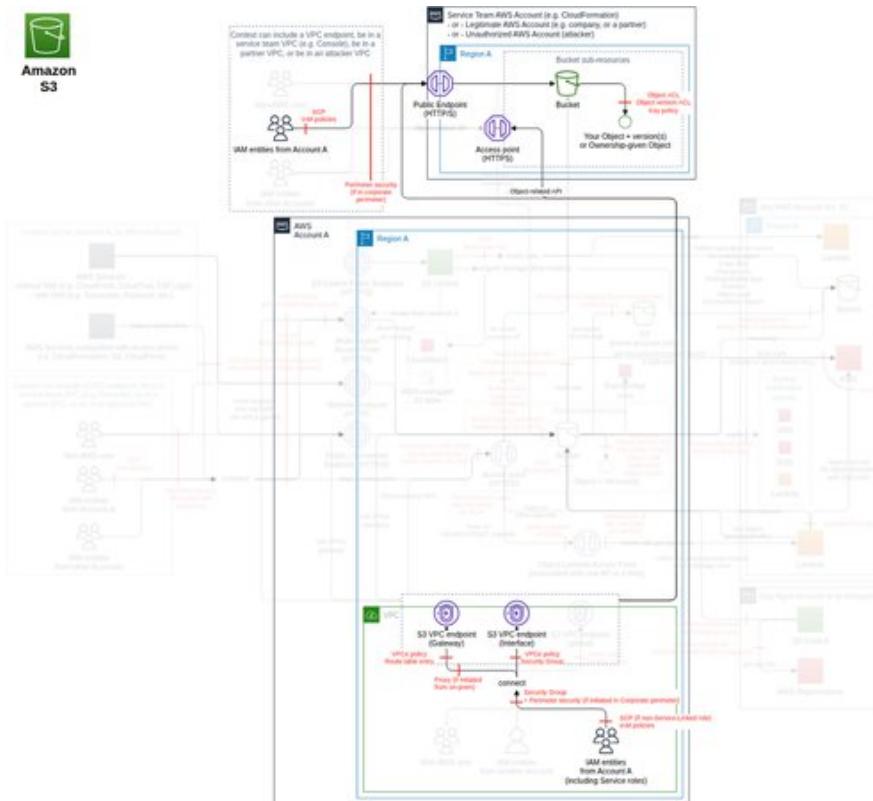


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO7 - Limit and monitor access via S3 VPC endpoints</b> C21 - Enable <a href="#">VPC DNS query logging</a> in all VPCs. C22 - Maintain a list of authorized S3 and S3 access points (and their respective AWS accounts) to be accessed for each VPC. C23 - Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g., using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use a specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points). C25 - Monitor VPC DNS query logs to ensure only authorized S3 buckets and S3 access points are being queried in each VPC (e.g., using VPC DNS query logging) and protect them using Route 53 ThreatModel. C124 - Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoint controls.	Very High	3	1	1
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b> C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C15 - Request access via an S3 access point on a bucket you don't own, if compatible with your interaction with the bucket (e.g., not through an unsupported AWS service).	High	2	-	-

<b>C03 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-
<b>C016 - Enforce encryption at rest</b> C162 - Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse"). C163 - Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Low	-	1	1

**Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing its object ACL**

<b>Threat Id</b>	S3.T6
<b>Name</b>	Unauthorized modification of an object to become public or accessible in a private bucket you do not own by changing its object ACL
<b>Description</b>	Bucket authority only prevails over object ACL when the object access is explicitly denied ( <a href="#">ref</a> ). An attacker (or someone by negligence) can change the object ACL to make it public or accessible to themselves.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (5.2)</a>
<b>IAM Access</b>	{ "OR": ["s3:PutObjectAcl", "s3:PutObjectVersionAcl"] }

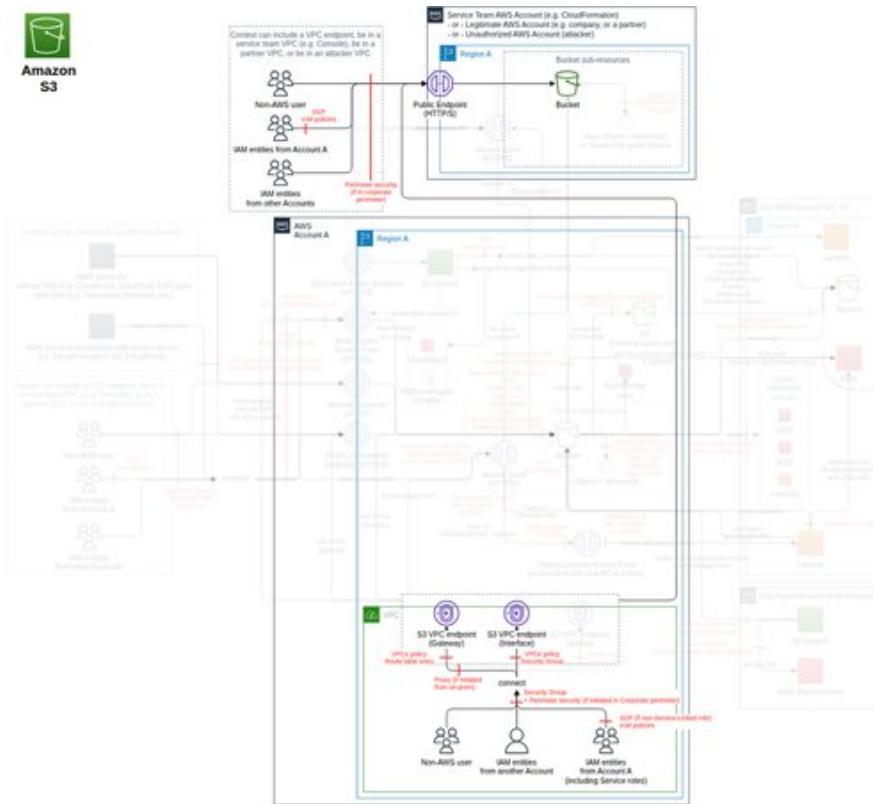


Control Objectives	Priority	# of associated Controls			
		Directive	Preventative	Detective	
<b>CO10 - Block changes to make an object public via object ACL</b>  C34 - Deny requests to change object ACL to public (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy with a deny statement on PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups "http://acs.amazonaws.com/groups/global/AllUsers" and "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"). C35 - Monitor ObjectACL changes (or tentative changes) to public using CloudTrail S3 data events.	Very High	-	1	1	1
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-	-
<b>CO37 - Disabling ACLs for all buckets</b>  C152 - Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023). C153 - Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Very High	1	1	1	-
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C12 - Allow only authorized ACLs on objects for buckets you don't control (e.g., using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> ).	High	1	1	1	-
<b>CO3 - Enable S3 data events in AWS CloudTrail</b>  C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-	-

<p><b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b></p> <p>C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.</p> <p>C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.</p>	Medium	2	-	-
<p><b>C039 - Enforce S3 server access logging on buckets</b></p> <p>C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.</p>	Low	1	-	-

## Intercept data in transit to an external bucket

<b>Threat Id</b>	S3.T12
<b>Name</b>	Intercept data in transit to an external bucket
<b>Description</b>	S3 allows communication over HTTP. An attacker can intercept the traffic you send to an external bucket to read or modify the data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1557</a>
<b>CVSS</b>	<a href="#">Medium (4.6)</a>
<b>IAM Access</b>	{}

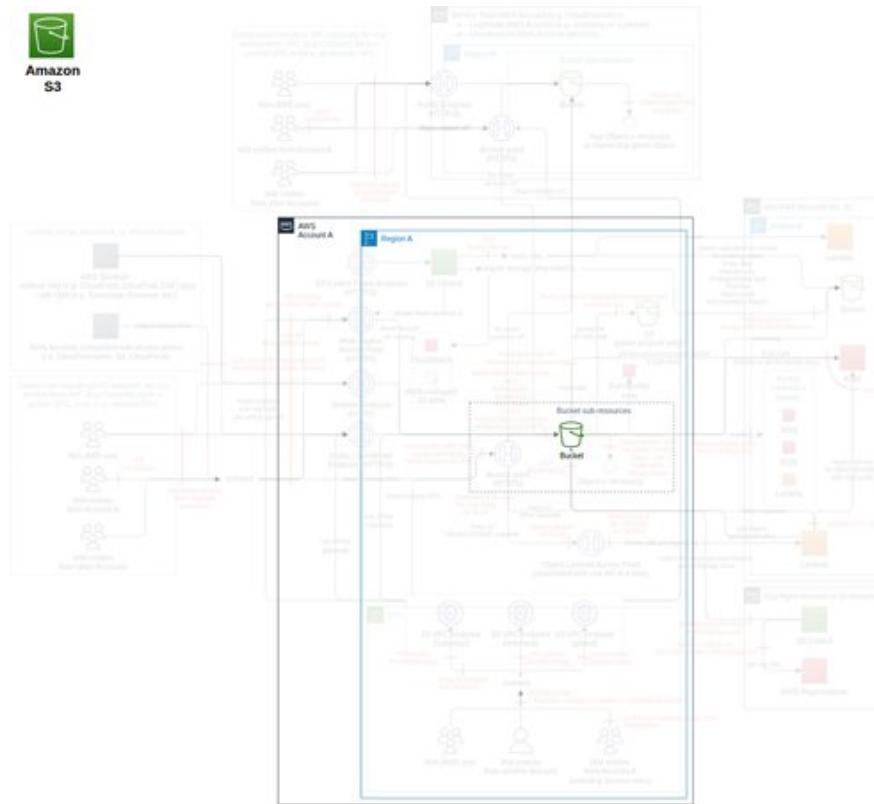


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO1 - Enforce encryption in transit</b> C1 - Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g., by denying all unencrypted requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , using an SCP on your AWS Organization root node). C3 - Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the VPC endpoint policy). C4 - Monitor and investigate all requests made with HTTP (e.g., via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite). C119 - Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org) (e.g., considering <a href="#">quantum-resistant encryption</a> ).	Very High	1	2	1
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO18 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Medium	1	-	-
<b>CO3 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>CO2 - Block S3 endpoints in your corporate perimeter security</b> C8 - Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Low	1	-	-
<b>CO39 - Enforce S3 server access logging on buckets</b>	Low	1	-	-

C166 - Enable [server access logging](#) in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.

## Unauthorized object restored into an unauthorized bucket

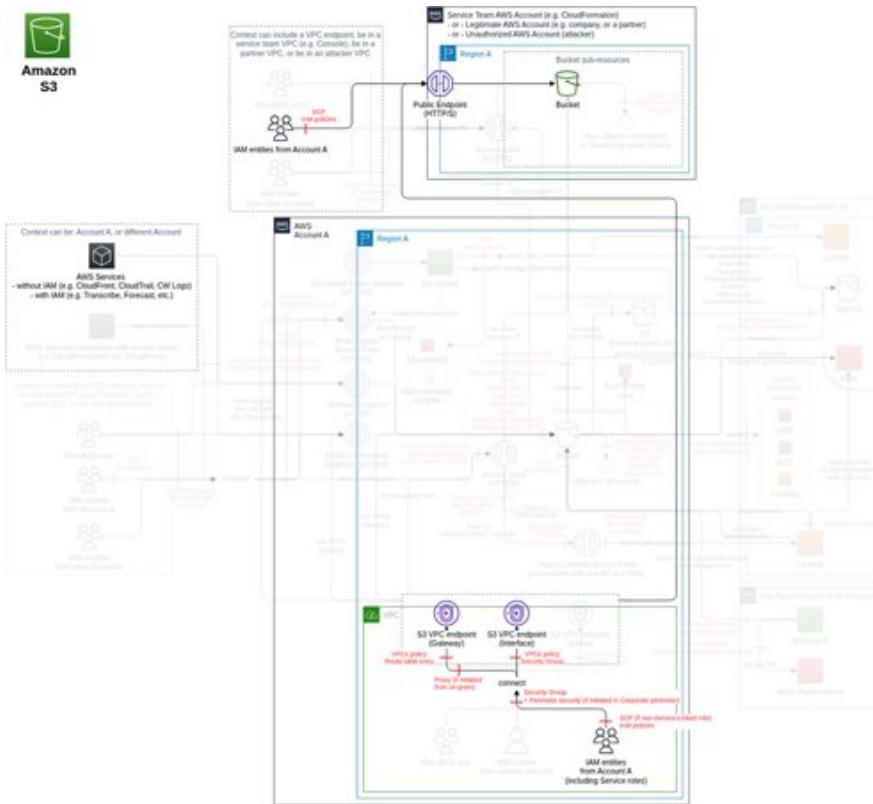
<b>Threat Id</b>	S3.T26
<b>Name</b>	Unauthorized object restored into an unauthorized bucket
<b>Description</b>	Objects can be stored in S3 Glacier. An attacker can restore an object to an unauthorized S3 bucket to collect or exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1020</a>
<b>CVSS</b>	<a href="#">Medium (4.3)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:RestoreObject" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Upload to an authorized external bucket but in an incorrect AWS account

<b>Threat Id</b>	S3.T31
<b>Name</b>	Upload to an authorized external bucket but in an incorrect AWS account
<b>Description</b>	Bucket names are globally unique. An attacker can take over a legitimate external bucket and deceive you into sending data to their bucket.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1537</a> , <a href="#">T1567</a>
<b>CVSS</b>	<a href="#">Medium (4.0)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutObject" }

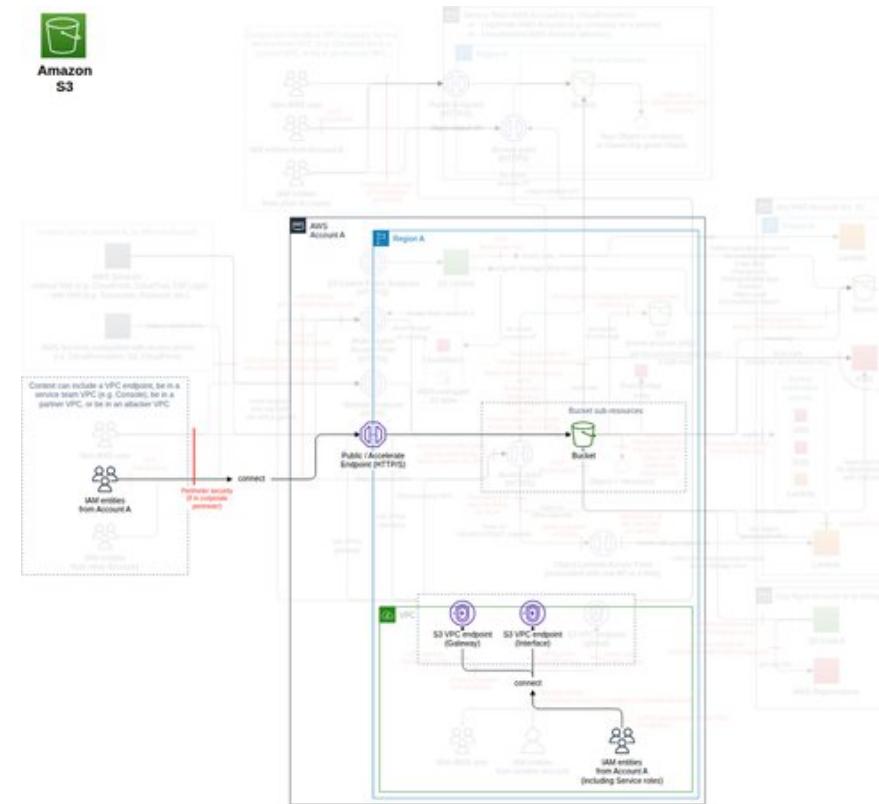


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C13 - Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified. C15 - Request access via an S3 access point on a bucket you don't own, if compatible with your interaction with the bucket (e.g., not through an unsupported AWS service).	Very High	2	-	1
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b>  C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO3 - Enable S3 data events in AWS CloudTrail</b>  C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>CO16 - Enforce encryption at rest</b>  C162 - Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse"). C163 - Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Low	-	1	1

<b>CO18 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Low	1	-	-
<b>CO39 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Recon on the security boundaries and resource names through detailed access denial messages

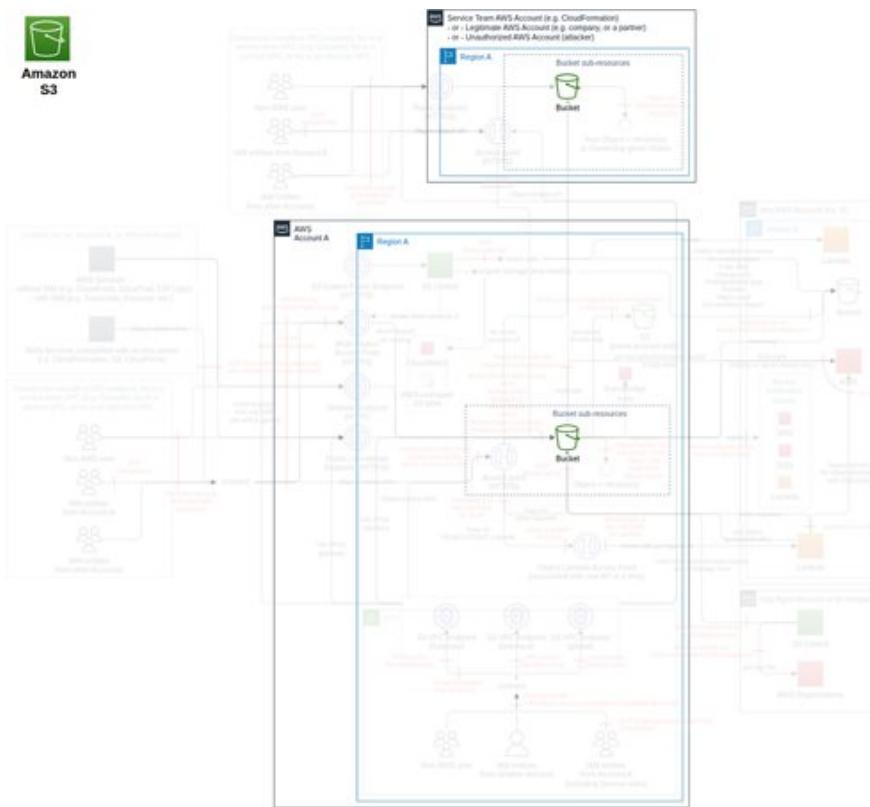
<b>Threat Id</b>	S3.T62
<b>Name</b>	Recon on the security boundaries and resource names through detailed access denial messages
<b>Description</b>	Enhanced access-denied messages include detailed response fields about which condition or permission prevented access. They are available only within the same AWS account or within AWS Organizations. An attacker can repeatedly attempt to access buckets with different parameters or identities and gather specific reasons for denial or existing resource names (using the presence or absence of the enhanced access-denied messages), leading to the discovery of deployed security configurations and buckets in AWS Organizations.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0007</a> , <a href="#">T1518</a> , <a href="#">T1580</a> , <a href="#">T1619</a>
<b>CVSS</b>	<a href="#">Low (3.5)</a>
<b>IAM Access</b>	{ "UNIQUE": "any:any" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO7 - Limit and monitor access via S3 VPC endpoints</b> C17 - For each VPC, maintain a list of AWS Organizations, OUs, and/or AWS accounts where IAM entities are authorized to access S3. C18 - For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g., <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ). C19 - Block any IAM entity not belonging to an authorized AWS Organization, OU, and/or AWS account from calling S3 from your VPCs by adding a deny statement in the S3 VPC endpoint policy for each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org IDs, as those are globally unique.	Very High	2	1	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

## Exfiltrate data by using tags

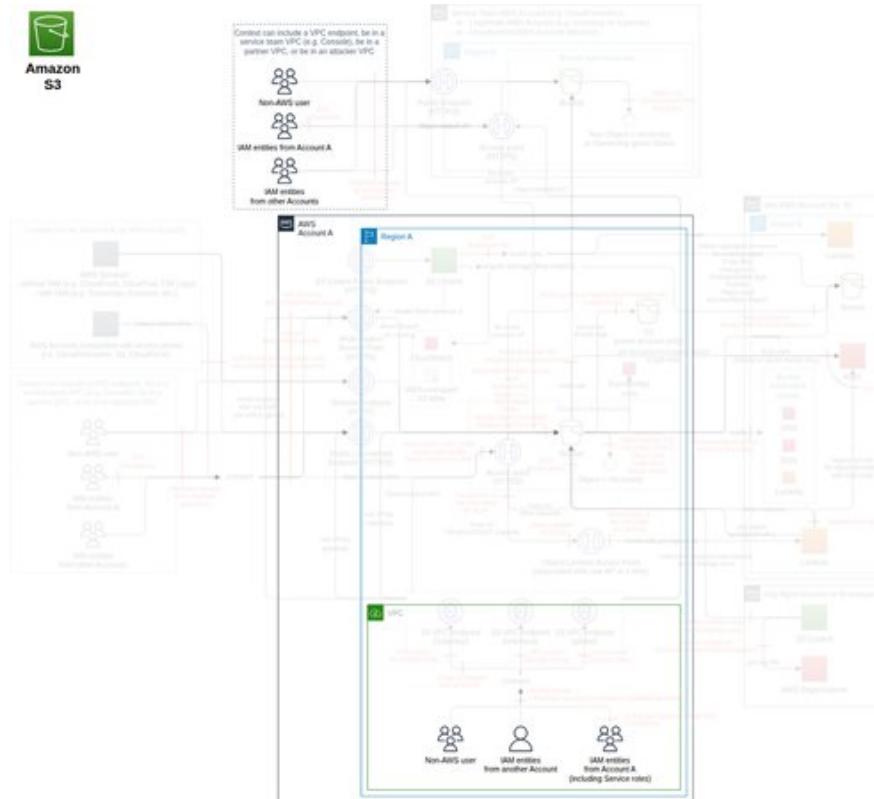
<b>Threat Id</b>	S3.T18
<b>Name</b>	Exfiltrate data by using tags
<b>Description</b>	Objects and buckets can have tags. An attacker can use these features to exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1020</a>
<b>CVSS</b>	<a href="#">Low (3.3)</a>
<b>IAM Access</b>	<pre>{   "AND": [     {       "OR": ["s3:GetObjectTagging", "s3:GetObjectVersionTagging", "s3:PutBucketTagging"]     },     {       "OR": ["s3:PutObjectTagging", "s3:PutObjectVersionTagging", "s3:GetBucketTagging"]     }   ] }</pre>



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO2 - Block S3 endpoints in your corporate perimeter security</b> C8 - Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Medium	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## **Use of less secure or old S3 features**

<b>Threat Id</b>	S3.T35
<b>Name</b>	Use of less secure or old S3 features
<b>Description</b>	S3 was launched in 2006, and its features have evolved. An attacker can use older features that have been proven less secure by AWS (e.g., certain API configurations, <a href="#">SigV2</a> , path-style model), but are still maintained for retro-compatibility.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0011</a> , <a href="#">T1102</a>
<b>CVSS</b>	<a href="#">Low (1.9)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:deprecated" }



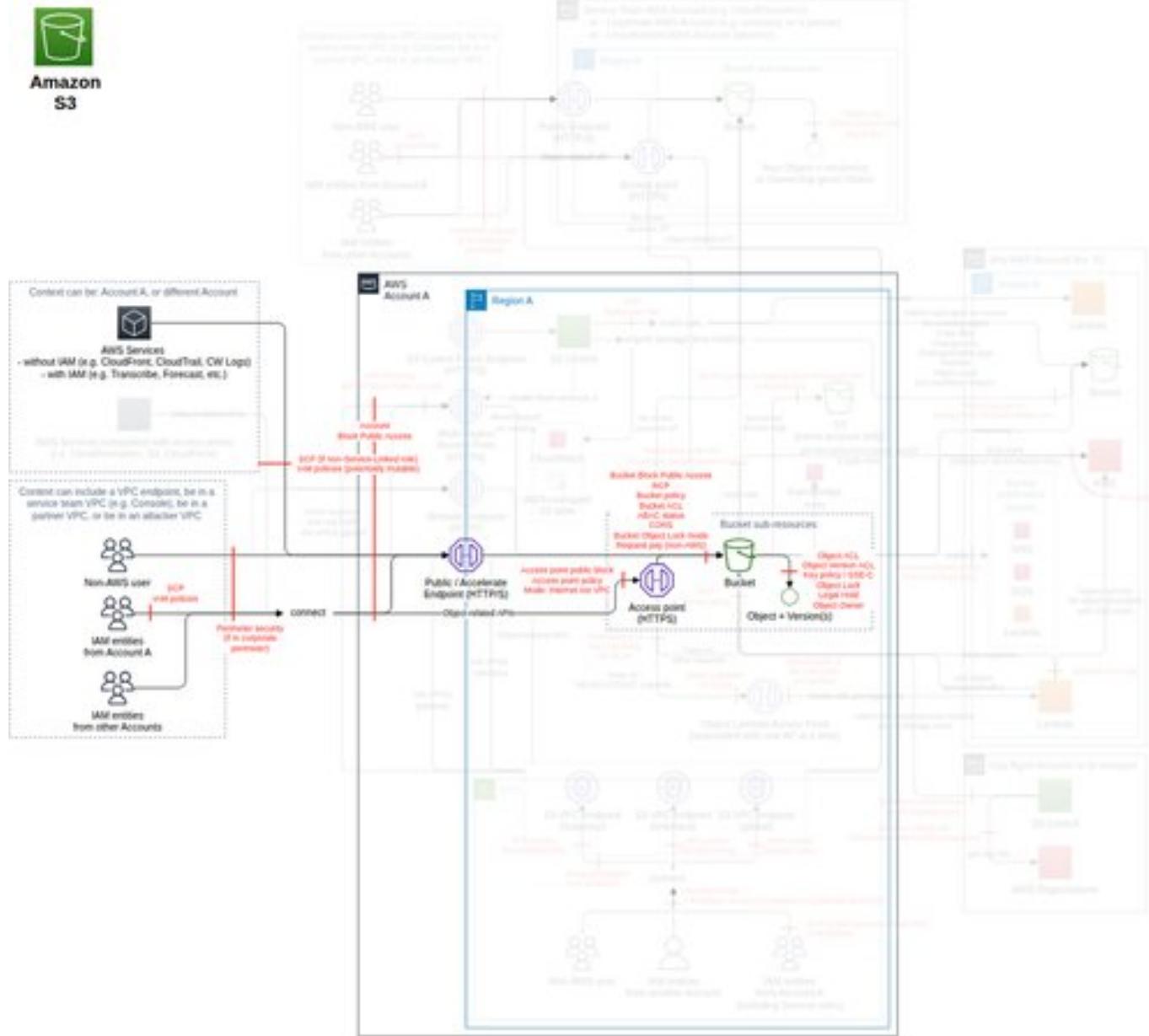
Control Objectives		# of associated Controls		
		Directive	Preventative	Detective
<b>CO12 - Enforce secure SDLC processes</b>  C42 - When connecting to S3 endpoints, use the virtual-hosted model ("my-bucket-name.s3.amazonaws.com" or "my-bucket-name.my-s3-regional-endpoint.amazonaws.com") instead of the path-style model ("s3.amazonaws.com/my-bucket-name" or "my-s3-regional-endpoint.amazonaws.com/my-bucket-name") (see <a href="#">ref</a> ). All the latest SDKs make use of domain style by default. C43 - Monitor that all S3 connections are made with the virtual-hosted model (e.g., via CloudTrail S3 requestParameters.Host).	Very High	1	-	1
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO23 - Enforce SigV4 on all requests</b>  C81 - Block all requests not using SigV4 (e.g., using an SCP, bucket policies, or centrally in an RCP applied to the OU or AWS account on all buckets with deny on "StringNotEquals": {"s3:signatureversion": "AWS4-HMAC-SHA256"}). C82 - Monitor and investigate any requests not using SigV4 (e.g., via CloudTrail S3 when the additionalEventData.SignatureVersion is different from "SigV4"). C83 - Use SDK with SigV4 enabled ( <a href="#">ref</a> ).	Very High	1	1	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	High	2	-	-
<b>CO22 - Block deprecated actions</b>  C80 - Block deprecated S3 actions using IAM ThreatModel and the S3 actions list.	Medium	1	-	-

<b>C03 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

# Bucket (*subclass of Object operations, FC5*)

*To upload your data into your AWS account, you must create an S3 bucket in one of the AWS Regions.*

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

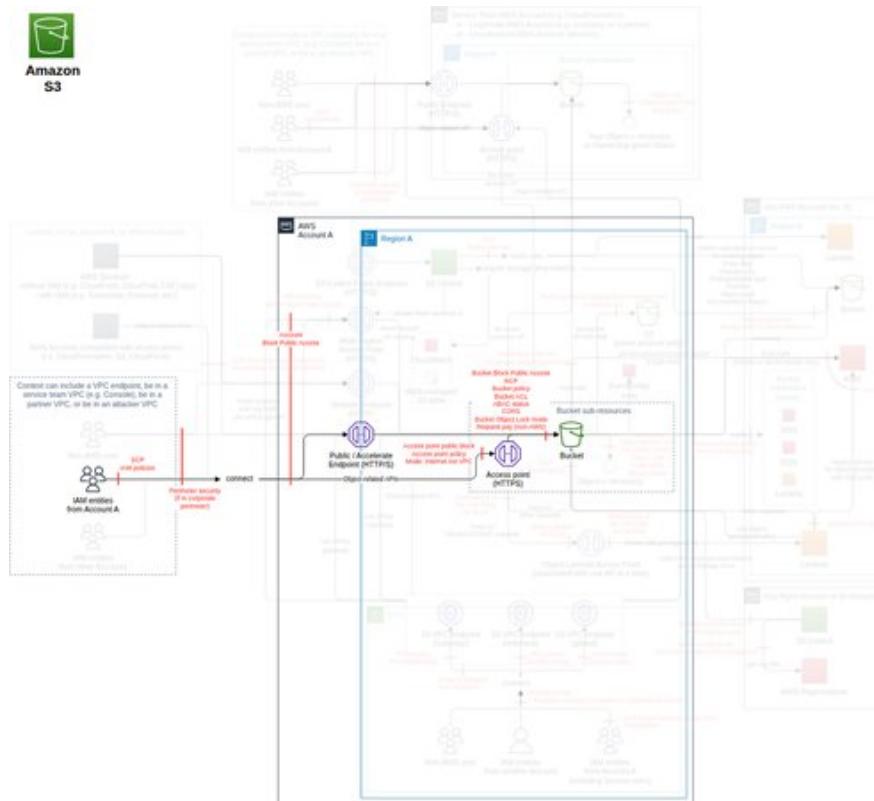
Action	IAM Permission
Creates a new bucket.	s3:CreateBucket

## **Threat List**

Name	CVSS
Exfiltrate data by using compromised IAM credentials from the Internet	<a href="#">High (7.5)</a>
Use a bucket to upload malware or modify an object to include malware	<a href="#">High (7.3)</a>
Files encrypted for ransomware	<a href="#">Medium (6.3)</a>
Object made public or accessible in a private bucket you own by changing its object ACL	<a href="#">Medium (5.9)</a>
Increase S3 costs by hotlinking or excessive downloading	<a href="#">Medium (5.3)</a>
Bucket takeover to gather data	<a href="#">Medium (5.2)</a>
Intercept data in transit to an internal bucket	<a href="#">Medium (4.6)</a>
Use AWS services to access data in S3	<a href="#">Medium (4.4)</a>
Move prod data into a non-prod environment	<a href="#">Medium (4.4)</a>
Increase the bill by restoring a large amount of data	<a href="#">Low (2.4)</a>
Increase bill by creating incomplete multipart uploads	<a href="#">Low (2.3)</a>
Disrupt workflow by manipulating ETag	<a href="#">Low (1.8)</a>

**Exfiltrate data by using compromised IAM credentials from the Internet**

<b>Threat Id</b>	S3.T39
<b>Name</b>	Exfiltrate data by using compromised IAM credentials from the Internet
<b>Description</b>	IAM credentials can be compromised (directly or using <a href="#">presigned URL</a> ). An attacker can use a compromised but authorized IAM credential to download your object from an internal bucket via the public endpoint (using or not their own VPC endpoint).
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1567</a>
<b>CVSS</b>	<a href="#">High (7.5)</a>
<b>IAM Access</b>	{}



Control Objectives		Priority	# of associated Controls		
			Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .		Very High	1	-	-
<b>CO29 - Limit access from only authorized VPCs</b>  C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).		Very High	1	1	-
<b>CO24 - Block all requests not using an HTTP authorization header, if not explicitly authorized</b>  C84 - Block all requests not using HTTP authorization header, i.e., presigned via query strings or POST ( <a href="#">ref</a> ) (e.g., using an SCP, bucket policies, or centrally in an RCP applied to the OU or AWS account on all buckets with deny on "StringNotEquals": {"s3:authType": "REST-HEADER"}). Note that it blocks uploads via the console, as well. C85 - Monitor and investigate all requests that do not use the HTTP authorization header (e.g., via CloudTrail S3 events where the additionalEventData.AuthenticationMethod is different from "AuthHeader").	Medium	-	1	1	1
<b>CO3 - Enable S3 data events in AWS CloudTrail</b>  C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-	-

<b>CO39 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-
--	-----	---	---	---

**Use a bucket to upload malware or modify an object to include malware**

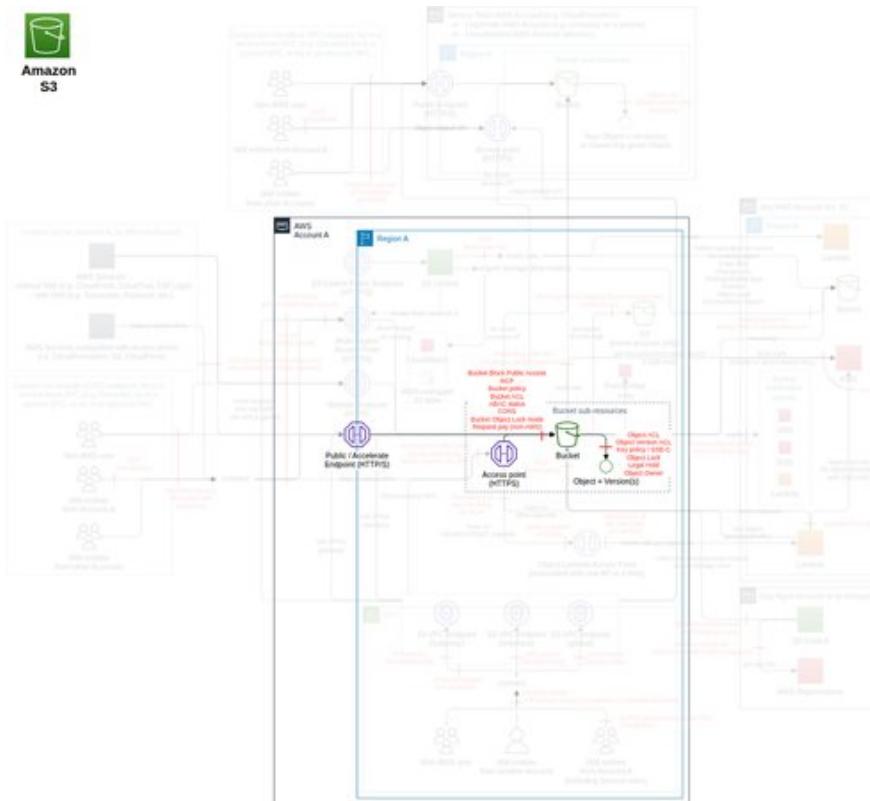
<b>Threat Id</b>	S3.T14
<b>Name</b>	Use a bucket to upload malware or modify an object to include malware
<b>Description</b>	S3 buckets are commonly used to distribute software. An attacker can upload malware to a bucket to better position it for later use or directly change an object to include malware ( <a href="#">example</a> ).
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0001</a> , <a href="#">T1195</a>
<b>CVSS</b>	<a href="#">High (7.3)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutObject" }

Control Objectives	Priority	# of associated Controls			
		Directive	Preventative	Detective	
<b>CO13 - Block direct public access</b>  C47 - Front buckets that are required to be public, using authenticated CDN (e.g., CloudFront) or API Gateway, protected with WAF (e.g., for <a href="#">hotlinking</a> ). C49 - Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C51 - Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023). C53 - Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C173 - Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Very High	5	-	-	
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-	
<b>CO29 - Limit access from only authorized VPCs</b>  C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Very High	1	1	-	
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C14 - Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g., using Macie).	High	2	-	-	
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to	High	2	-	-	

review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.				
<b>C026 - Scan objects used for input/output of a workflow for malware</b> C93 - If the bucket is used as an input or the output of a process, scan the objects for malware (e.g., using <a href="#">GuardDuty Malware Protection for S3</a> , <a href="#">BucketAV</a> , <a href="#">Cloud Storage Security</a> , <a href="#">Trend Micro Cloud One</a> , or <a href="#">your own scanning solution</a> ).	Medium	-	-	1

# Files encrypted for ransomware

<b>Threat Id</b>	S3.T16
<b>Name</b>	Files encrypted for ransomware
<b>Description</b>	S3 provides several types of encryption where the key is not operated by AWS (e.g., SSE-KMS with Bring Your Own Key). An attacker can encrypt all the data stored in S3 to ransom the data owner for the decryption key (blogs: <a href="#">1</a> and <a href="#">2</a> ). Alternatively, an attacker can change the default encryption key, for a similar effect on any new data uploaded.
<b>Goal</b>	Direct Financial Gain
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1486</a>
<b>CVSS</b>	<a href="#">Medium (6.3)</a>
<b>IAM Access</b>	{ "OR": [ "AND": ["s3:GetObject", "s3:PutObject"] ], "s3:PutEncryptionConfiguration" }

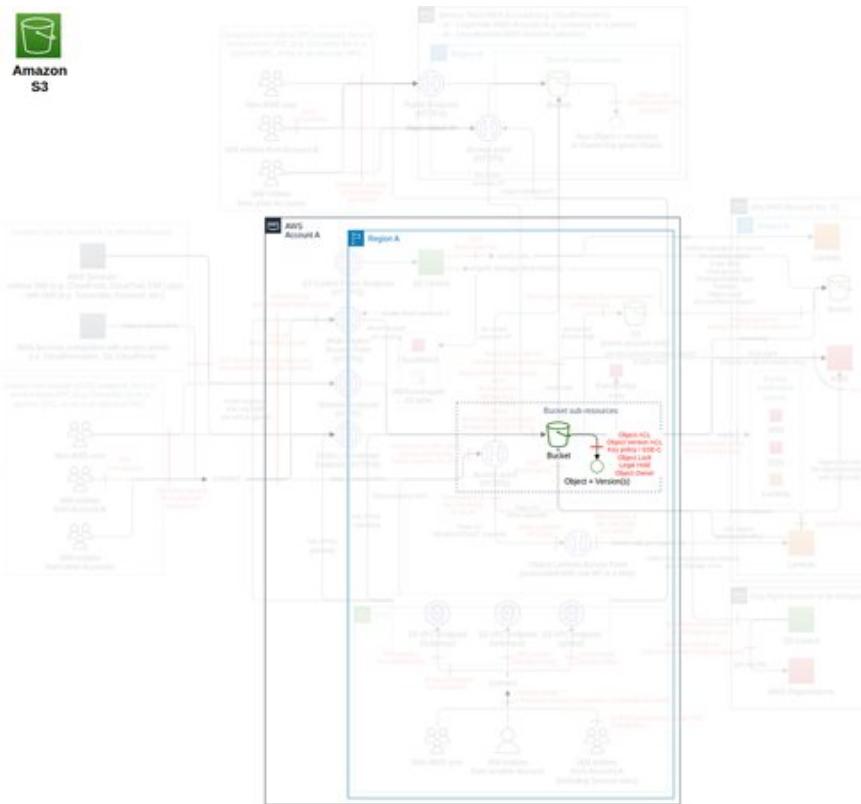


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO16 - Enforce encryption at rest</b> C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key). C68 - Monitor that only authorized KMS keys are used for each bucket (using CloudTrail S3 data events in "requestParameters.bucketName" and "response.x-amz-server-side-encryption-aws-kms-key-id"). C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C). C146 - For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present). C148 - For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in requestParameters.bucketName and response.x-amz-server-side-encryption-customer-algorithm). C167 - Ensure SSE-C is blocked when not required for each bucket [default from April 2026].	Very High	4	2	2
<b>CO17 - Protect primary data against loss</b> C69 - Enable versioning on buckets holding primary data. C71 - Back up primary data in a secure location under a different security authority (e.g., in an <a href="#">AWS data bunker account</a> via replication, or using AWS Backup for Amazon S3).	Very High	2	-	-
<b>CO20 - Protect data integrity using S3 Object Lock</b> C74 - Implement the authorized default S3 Object Lock on buckets requiring WORM (note: Amazon S3 evaluates and applies bucket policies before applying the bucket default S3 Object Lock	Very High	-	2	-

settings). C76 - Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on buckets requiring WORM (e.g., using their bucket policy and centrally in an RCP applied to the OU or the AWS account with a deny statement on PutObject and PutObjectRetention if the condition "s3:object-lock-mode" exists and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration).				
<b>C09 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>C03 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>C04 - Monitor S3 with Amazon GuardDuty and Macie</b> C10 - Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective).	Medium	1	-	-
<b>C019 - Have a process to apply legal holds</b> C73 - Create a process to apply a legal hold to any S3 bucket whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.	Low	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Object made public or accessible in a private bucket you own by changing its object ACL

<b>Threat Id</b>	S3.T36
<b>Name</b>	Object made public or accessible in a private bucket you own by changing its object ACL
<b>Description</b>	Bucket authority only prevails over object ACL when the object access is explicitly denied by the bucket authority ( <a href="#">ref</a> ). An attacker (or someone by negligence) can change the object ACL to make the object public or accessible to themselves to exfiltrate or modify the data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (5.9)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutObjectAcl" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO10 - Block changes to make an object public via object ACL</b>  C34 - Deny requests to change object ACL to public (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy with a deny statement on PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups " <a href="http://acs.amazonaws.com/groups/global/AllUsers">http://acs.amazonaws.com/groups/global/AllUsers</a> " and " <a href="http://acs.amazonaws.com/groups/global/AuthenticatedUsers">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a> "). C35 - Monitor ObjectACL changes (or tentative changes) to public using CloudTrail S3 data events. C37 - Monitor and investigate anonymous requests to objects (e.g., using CloudTrail S3 data events with userIdentity.accountId=ANONYMOUS_PRINCIPAL).	Very High	-	1	2
<b>CO13 - Block direct public access</b>  C49 - Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C51 - Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023). C53 - Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C173 - Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Very High	4	-	-
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO16 - Enforce encryption at rest</b>  C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C63 - Use KMS ThreatModel to protect the KMS keys used for S3 (e.g., using encryptionContext on the policy of each KMS key). C64 - Implement an authorized default encryption key on each bucket; enable S3 Bucket Key if not using DSSE-KMS and if CloudTrail events are not required for KMS encrypt/decrypt (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings).	Very High	5	2	2

C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key). C68 - Monitor that only authorized KMS keys are used for each bucket (using CloudTrail S3 data events in "requestParameters.bucketName" and "response.x-amz-server-side-encryption-aws-kms-key-id"). C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C). C146 - For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present). C148 - For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in requestParameters.bucketName and response.x-amz-server-side-encryption-customer-algorithm).				
<b>CO29 - Limit access from only authorized VPCs</b> C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Very High	1	1	-
<b>CO37 - Disabling ACLs for all buckets</b> C152 - Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023). C153 - Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Very High	1	1	-
<b>CO4 - Monitor S3 with Amazon GuardDuty and Macie</b> C118 - Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	High	1	-	-
<b>CO3 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>CO39 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

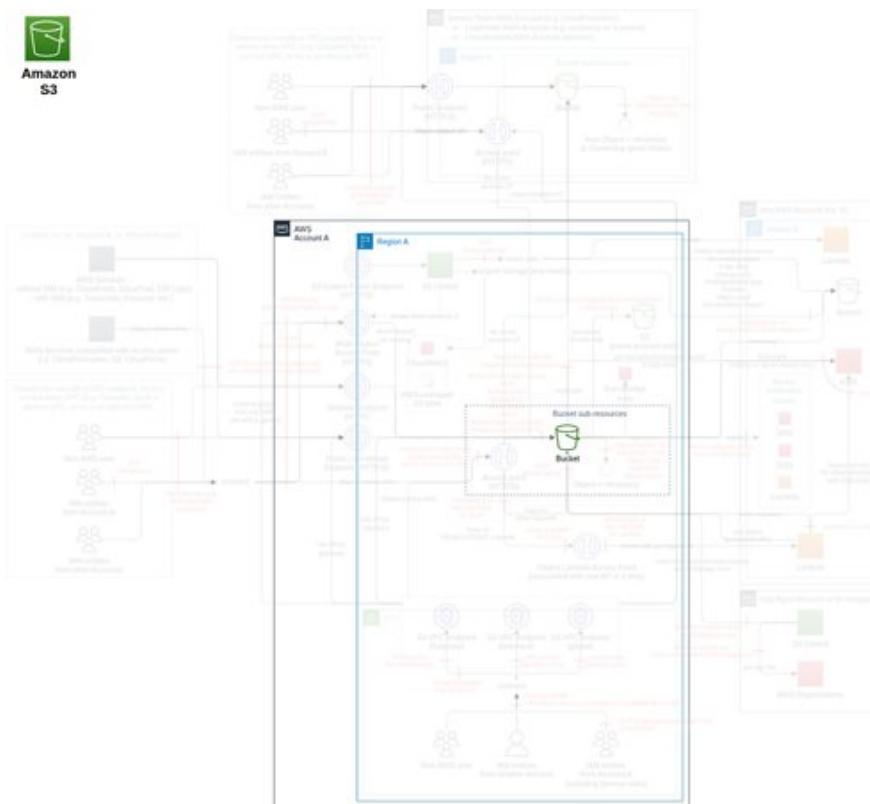
**Increase S3 costs by hotlinking or excessive downloading**

<b>Threat Id</b>	S3.T22
<b>Name</b>	Increase S3 costs by hotlinking or excessive downloading
<b>Description</b>	S3 charges for hosting and data transfer out. An attacker can hotlink your content hosted on S3 on another page to avoid paying the S3 bills ( <a href="#">ref</a> ) or download your public data excessively to increase your bills (especially doing <a href="#">partial downloads on large objects</a> ).
<b>Goal</b>	Financial Drain
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1496</a>
<b>CVSS</b>	<a href="#">Medium (5.3)</a>
<b>IAM Access</b>	{}

Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO13 - Block direct public access</b> C47 - Front buckets that are required to be public, using authenticated CDN (e.g., CloudFront) or API Gateway, protected with WAF (e.g., for <a href="#">hotlinking</a> ).	Very High	1	-	-
<b>CO4 - Monitor S3 with Amazon GuardDuty and Macie</b> C118 - Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	High	1	-	-

## Bucket takeover to gather data

<b>Threat Id</b>	S3.T1
<b>Name</b>	Bucket takeover to gather data
<b>Description</b>	Bucket names are globally unique and can be recreated after 1 hour from deletion in another AWS account. An attacker can recreate the same bucket name of a deleted bucket you used to own to collect any new data uploaded by a non-updated party ( <a href="#">ref</a> ), do a DNS takeover (using a non-deleted CNAME / CloudFront origin to the bucket), or use remaining permissions to exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1586</a>
<b>CVSS</b>	<a href="#">Medium (5.2)</a>
<b>IAM Access</b>	{ "OPTIONAL": "s3>DeleteBucket" }

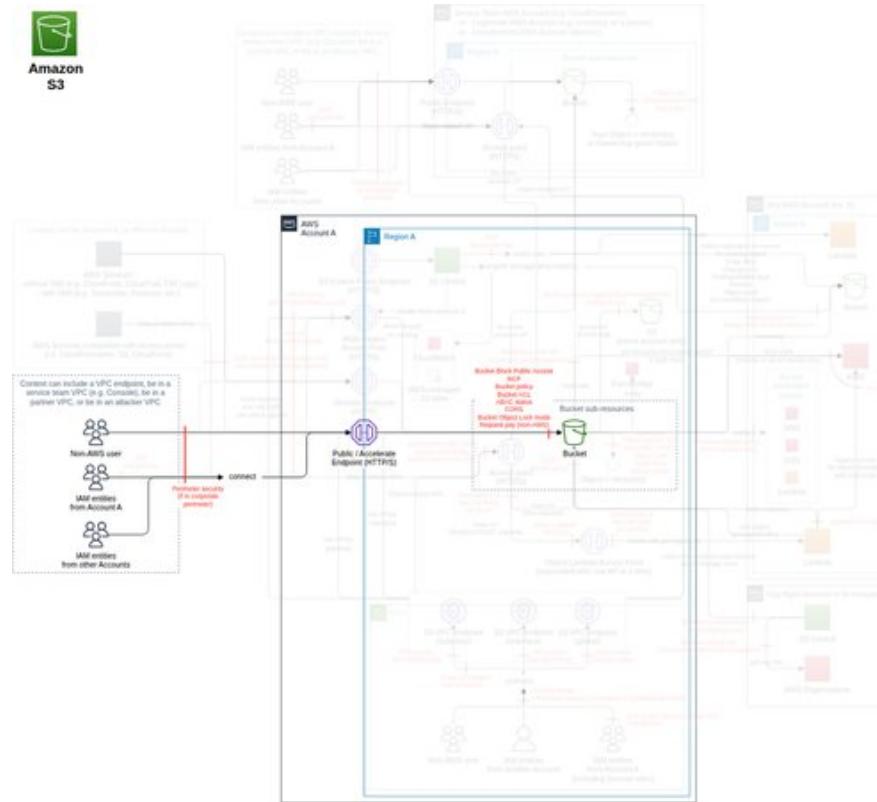


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO11 - Prevent deletion of buckets</b>  C38 - Block the action "s3:DeleteBucket" (e.g., via SCP or in an RCP applied to the OU or AWS account; exemption can be managed by authorizing a SuperAdmin to delete buckets with a certain tag, and with bucket owners able to tag buckets). C40 - Scan your CNAME records (e.g., in Amazon Route 53) and CloudFront origin for deleted buckets.	Very High	-	1	1
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b>  C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C13 - Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	High	1	-	1
<b>CO12 - Enforce secure SDLC processes</b>  C41 - Parameterize the S3 bucket name or S3 access point in your code (no hardcoding). C46 - Ensure all S3 buckets interacted with are in the correct AWS account (e.g., using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner).	Medium	2	-	-

<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>C03 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-
<b>C018 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Very Low	1	-	-

## Intercept data in transit to an internal bucket

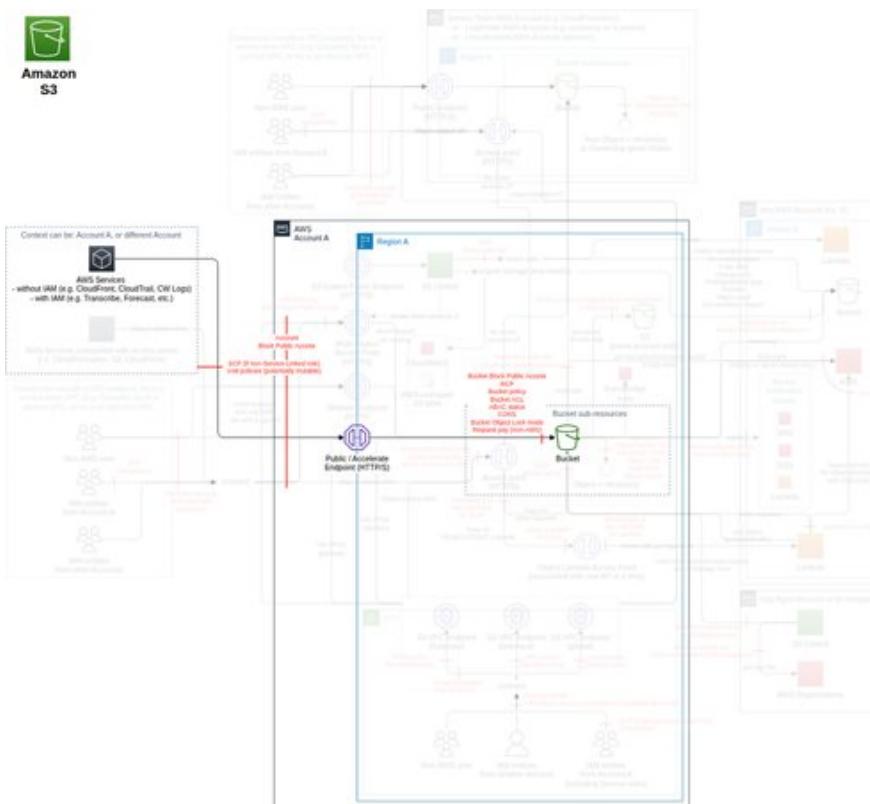
<b>Threat Id</b>	S3.T34
<b>Name</b>	Intercept data in transit to an internal bucket
<b>Description</b>	S3 allows communication over HTTP. An attacker can intercept the traffic you send to an internal bucket in order to read or modify the data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1557</a>
<b>CVSS</b>	<a href="#">Medium (4.6)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO1 - Enforce encryption in transit</b> C1 - Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g., by denying all unencrypted requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , using an SCP on your AWS Organization root node). C3 - Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on the VPC endpoint policy). C4 - Monitor and investigate all requests made with HTTP (e.g., via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite). C6 - Block all unencrypted requests to the buckets you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != <i>authorized TLS version(s)</i> , on their bucket policy or centrally in an RCP applied to the OU or AWS account). C119 - Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org) (e.g., considering <a href="#">quantum-resistant encryption</a> ).	Very High	1	3	1
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO2 - Block S3 endpoints in your corporate perimeter security</b> C8 - Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Very High	1	-	-
<b>CO3 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>CO39 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Use AWS services to access data in S3

<b>Threat Id</b>	S3.T30
<b>Name</b>	Use AWS services to access data in S3
<b>Description</b>	A number of AWS services can access S3 to execute their functions. An attacker can use them to collect data using their service roles or service-linked roles.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1530</a> , <a href="#">T1119</a>
<b>CVSS</b>	<a href="#">Medium (4.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "iam:PassRole" }

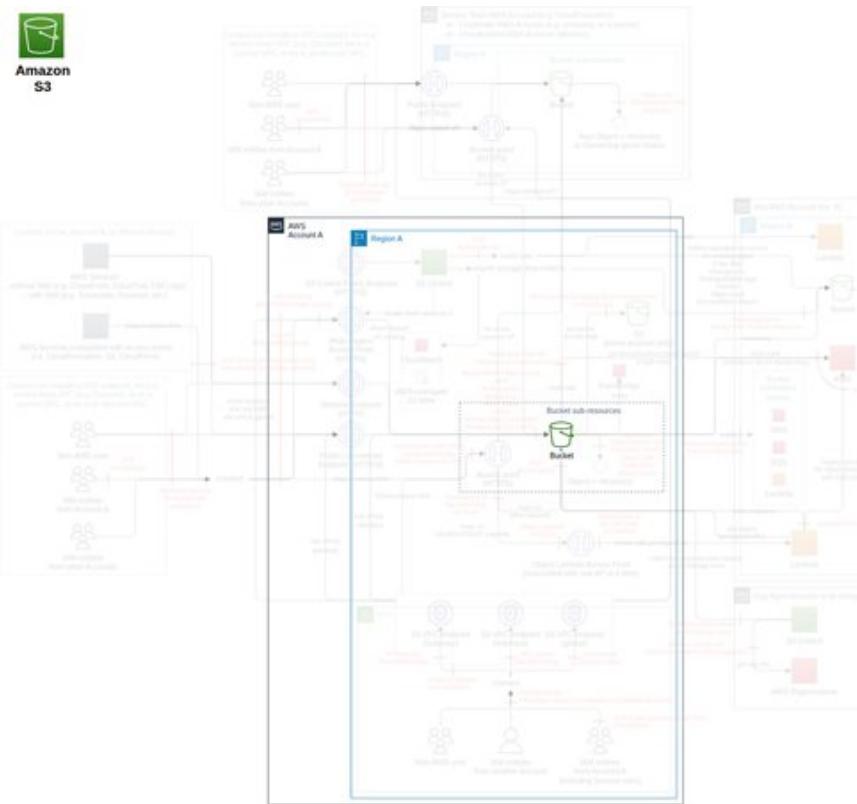


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO16 - Enforce encryption at rest</b>  C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).  C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key.  C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key).  C68 - Monitor that only authorized KMS keys are used for each bucket (using CloudTrail S3 data events in "requestParameters.bucketName" and "response.x-amz-server-side-encryption-aws-kms-key-id").  C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C).  C146 - For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present).  C148 - For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in requestParameters.bucketName and response.x-amz-server-side-encryption-customer-algorithm).	Very High	3	2	2
<b>CO29 - Limit access from only authorized VPCs</b>  C98 - For each S3 bucket, maintain a list of VPCs authorized to access it.  C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpc" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Very High	1	1	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b>  C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account.	Very High	1	1	1

C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").				
<b>C06 - Model the threats on all AWS services accessing S3</b> C16 - Analyze and protect all AWS services accessing S3 (e.g., via ThreatModel). Enforce use in VPC only, whenever possible.	High	1	-	-
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>C018 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Low	1	-	-

## Move prod data into a non-prod environment

<b>Threat Id</b>	S3.T11
<b>Name</b>	Move prod data into a non-prod environment
<b>Description</b>	Multiple types of environments are usually operated in AWS. An attacker can move the data from a secure location (e.g., production) to a less secure location (e.g., dev).
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1074</a>
<b>CVSS</b>	<a href="#">Medium (4.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:GetObject" }

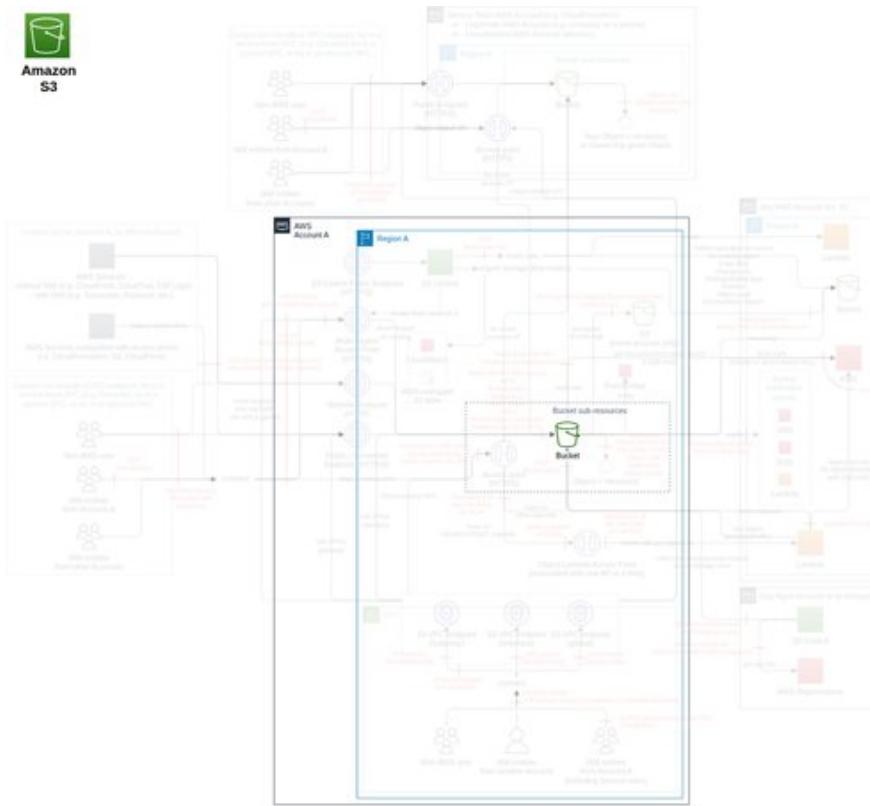


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> . C59 - Use a data discovery tool (e.g., Amazon Macie) to ensure no sensitive data is stored in an unauthorized bucket. C60 - Use a data discovery tool (e.g., Amazon Macie) to ensure the bucket names, object names, tags, and metadata do not contain sensitive data.	Very High	1	-	2
<b>CO16 - Enforce encryption at rest</b>  C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key). C68 - Monitor that only authorized KMS keys are used for each bucket (using CloudTrail S3 data events in "requestParameters.bucketName" and "response.x-amz-server-side-encryption-aws-kms-key-id"). C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C). C146 - For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present). C148 - For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in requestParameters.bucketName and response.x-amz-server-side-encryption-customer-algorithm). C162 - Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse"). C163 - Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Very High	3	3	3
<b>CO29 - Limit access from only authorized VPCs</b>	Very High	1	1	-

C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).				
<b>C09 - Block requests with KMS keys from unauthorized AWS accounts</b>  C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>C032 - Restrict access point access to VPCs when in use</b>  C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C105 - Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy. C112 - Block any <a href="#">object-related operations</a> access to S3 buckets not through an access point (i.e., IAM policy, SCP, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on the condition "ArnNotLike": {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"}).	Very High	1	2	-
<b>C07 - Limit and monitor access via S3 VPC endpoints</b>  C17 - For each VPC, maintain a list of AWS Organizations, OUs, and/or AWS accounts where IAM entities are authorized to access S3. C18 - For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g., <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ). C19 - Block any IAM entity not belonging to an authorized AWS Organization, OU, and/or AWS account from calling S3 from your VPCs by adding a deny statement in the S3 VPC endpoint policy for each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org IDs, as those are globally unique. C21 - Enable <a href="#">VPC DNS query logging</a> in all VPCs. C22 - Maintain a list of authorized S3 and S3 access points (and their respective AWS accounts) to be accessed for each VPC. C23 - Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g., using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use a specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points). C25 - Monitor VPC DNS query logs to ensure only authorized S3 buckets and S3 access points are being queried in each VPC (e.g., using VPC DNS query logging) and protect them using Route 53 ThreatModel.	Very High	4	2	1
<b>C05 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel). C13 - Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	High	1	-	1
<b>C018 - Encrypt or tokenize critical data</b>  C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Medium	1	-	-
<b>C03 - Enable S3 data events in AWS CloudTrail</b>  C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>C039 - Enforce S3 server access logging on buckets</b>  C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## Increase the bill by restoring a large amount of data

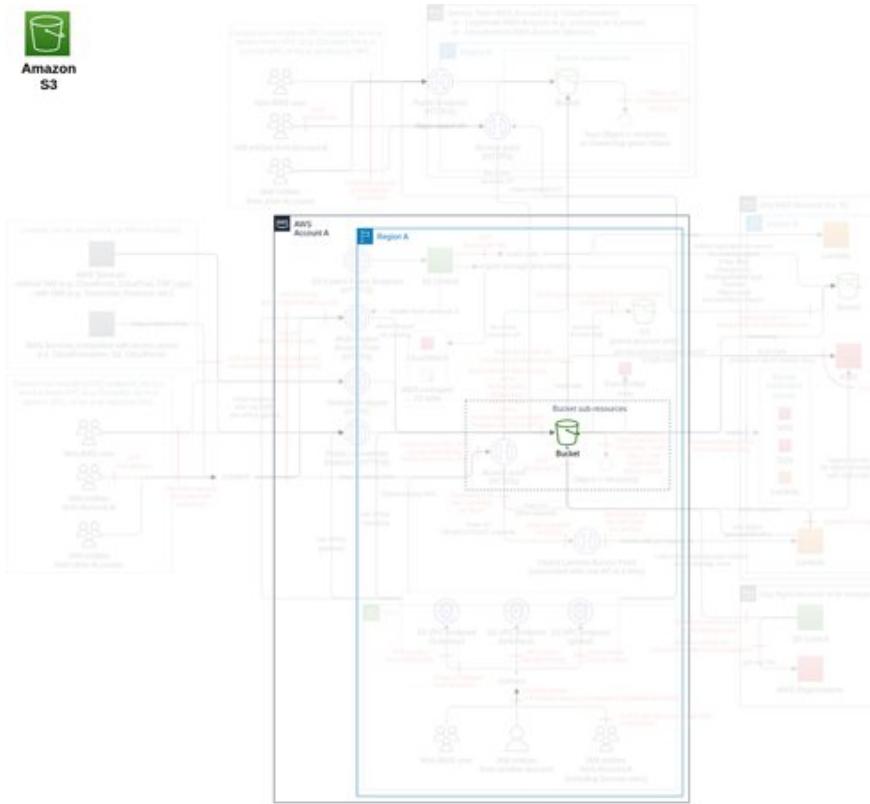
<b>Threat Id</b>	S3.T47
<b>Name</b>	Increase the bill by restoring a large amount of data
<b>Description</b>	Restore costs can be amplified by the size and the type (i.e., expedited). An attacker can restore lots of data to generate costs.
<b>Goal</b>	Financial Drain
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0042</a> , <a href="#">T1586</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:RestoreObject" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

## Increase bill by creating incomplete multipart uploads

<b>Threat Id</b>	S3.T40
<b>Name</b>	Increase bill by creating incomplete multipart uploads
<b>Description</b>	By default, when a multipart upload is initiated but not completed, S3 will keep it ( <a href="#">ref</a> ). An attacker can upload a large amount of data without completing it while being hard to detect.
<b>Goal</b>	Financial Drain
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0042</a> , <a href="#">T1586</a>
<b>CVSS</b>	<a href="#">Low (2.3)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutObject" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO21 - Remove incomplete multipart uploads</b> C78 - Reduce costs related to incomplete multipart uploads by creating a lifecycle policy to remove them after an agreed length of time (e.g., 7 days) ( <a href="#">blog</a> ).	Very High	-	1	-

## Disrupt workflow by manipulating ETag

<b>Threat Id</b>	S3.T27
<b>Name</b>	Disrupt workflow by manipulating ETag
<b>Description</b>	ETags include the MD5 of the file but not consistently and can be used by developers to verify the integrity of a file. An attacker can affect an upload function to change the ETag of a file to disrupt a workflow downstream.
<b>Goal</b>	Data manipulation
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1565</a>
<b>CVSS</b>	<a href="#">Low (1.8)</a>
<b>IAM Access</b>	{}

Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO12 - Enforce secure SDLC processes</b> C44 - Ensure the integrity of stored objects ( <a href="#">ref</a> ), using "x-amz-checksum" from the <a href="#">object metadata</a> instead of ETag (e.g., using the compute checksum functionality in S3 Batch Operations). If ETag is used, make sure to properly account for its different definitions ( <a href="#">ref</a> ).	Very High	1	-	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1

## Bucket tag (*subclass of Bucket, FC7*)

You can tag buckets ([ref](#)).

## **Data Flow Diagram (DFD)**

## ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Adds a set of tags to an existing bucket.	s3:PutBucketTagging

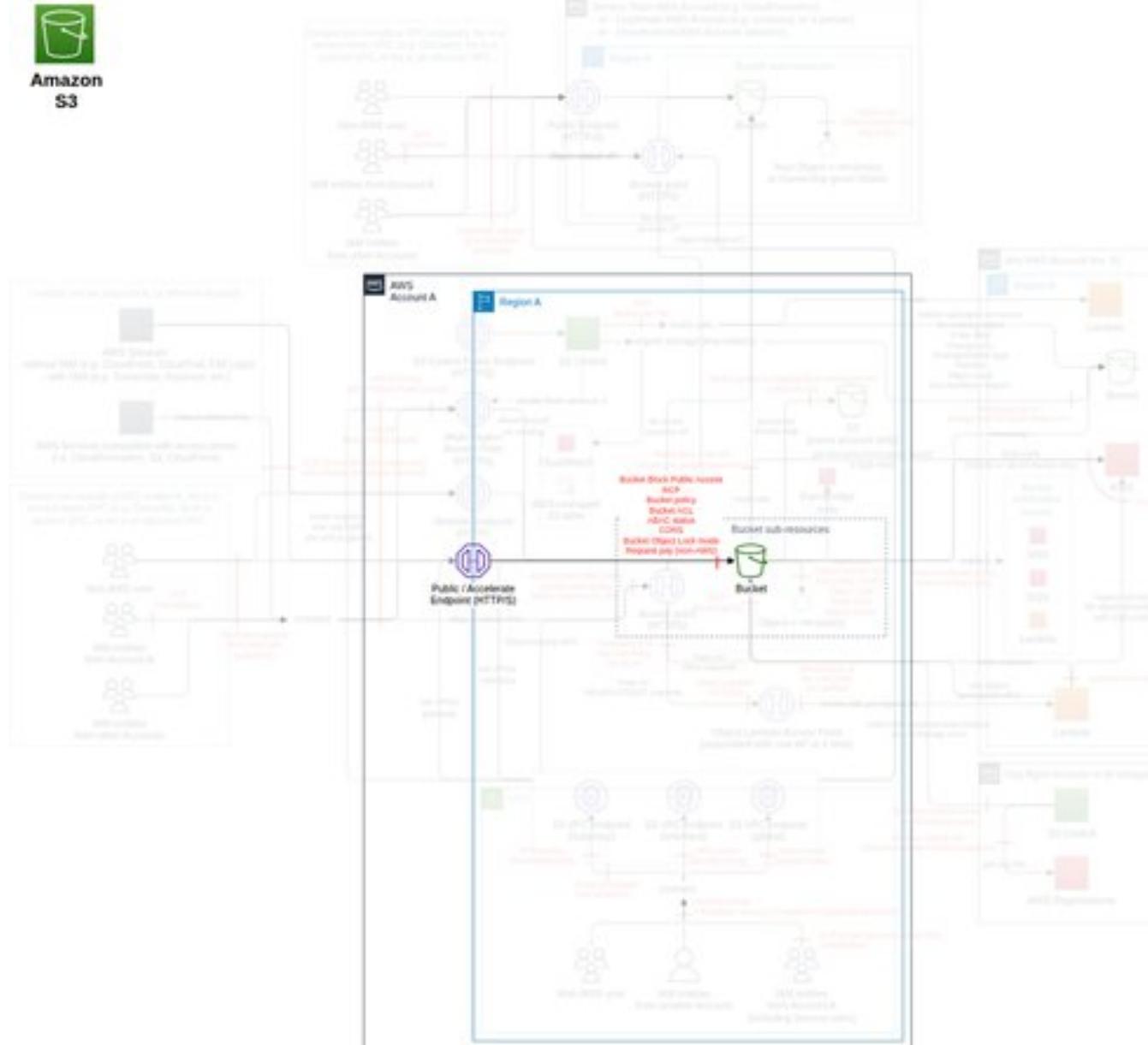
## ***Threat List***

Name	CVSS
None	None

## Bucket ACL (*subclass of Bucket, FC8*)

**[NOT RECOMMENDED]** Amazon S3 Access Control Lists (ACLs) enable you to manage access to buckets. Each bucket has an ACL attached to it as a sub-resource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to ensure the requester has the necessary access permissions ([ref](#)).

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Sets the permissions on an existing bucket using Access Control Lists (ACL).	s3:PutBucketAcl

## ***Threat List***

Name	CVSS
Grant unauthorized access to a private bucket by changing its bucket ACL	<a href="#">Medium (5.2)</a>
DoS by blocking traffic using bucket ACL	<a href="#">Low (2.1)</a>

## Grant unauthorized access to a private bucket by changing its bucket ACL

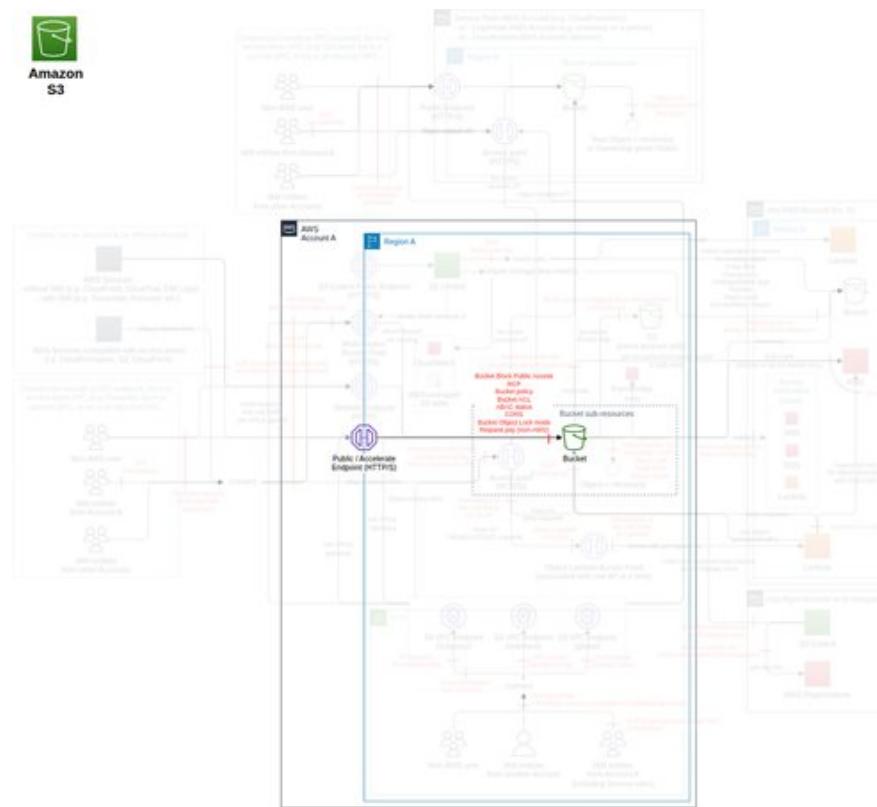
<b>Threat Id</b>	S3.T4
<b>Name</b>	Grant unauthorized access to a private bucket by changing its bucket ACL
<b>Description</b>	Bucket ACL can be used to give access to bucket information, list objects, and overwrite or delete objects. An attacker can change the bucket ACL to destroy or modify data, or exfiltrate data via the object name (1 KB).
<b>Goal</b>	Data manipulation
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1486</a>
<b>CVSS</b>	<a href="#">Medium (5.2)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketAcl" }

Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO13 - Block direct public access</b> C49 - Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C51 - Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023). C173 - Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Very High	3	-	-
<b>CO14 - Block bucket ACL</b> C55 - Deny requests to add an ACL on a bucket (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy, with a deny statement on "s3:PutBucketAcl"). C56 - Monitor changes to bucket ACLs to ensure they stay private (e.g., using the CloudTrail event PutBucketAcl and its field requestParameters.x-amz-acl, which should either be "private" or not exist).	Very High	-	1	1
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO37 - Disabling ACLs for all buckets</b> C152 - Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023). C153 - Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Very High	1	1	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account).	Very High	1	1	1

C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").				
<b>C04 - Monitor S3 with Amazon GuardDuty and Macie</b> C10 - Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective). C118 - Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	High	2	-	-
<b>C03 - Enable S3 data events in AWS CloudTrail</b> C9 - Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Medium	1	-	-
<b>C039 - Enforce S3 server access logging on buckets</b> C166 - Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Low	1	-	-

## DoS by blocking traffic using bucket ACL

<b>Threat Id</b>	S3.T50
<b>Name</b>	DoS by blocking traffic using bucket ACL
<b>Description</b>	Bucket ACL can allow access (e.g., for CloudFront access logs). An attacker can remove an existing permission to deny legitimate access to the bucket.
<b>Goal</b>	Disruption of Service
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1531</a>
<b>CVSS</b>	<a href="#">Low (2.1)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketAcl" }

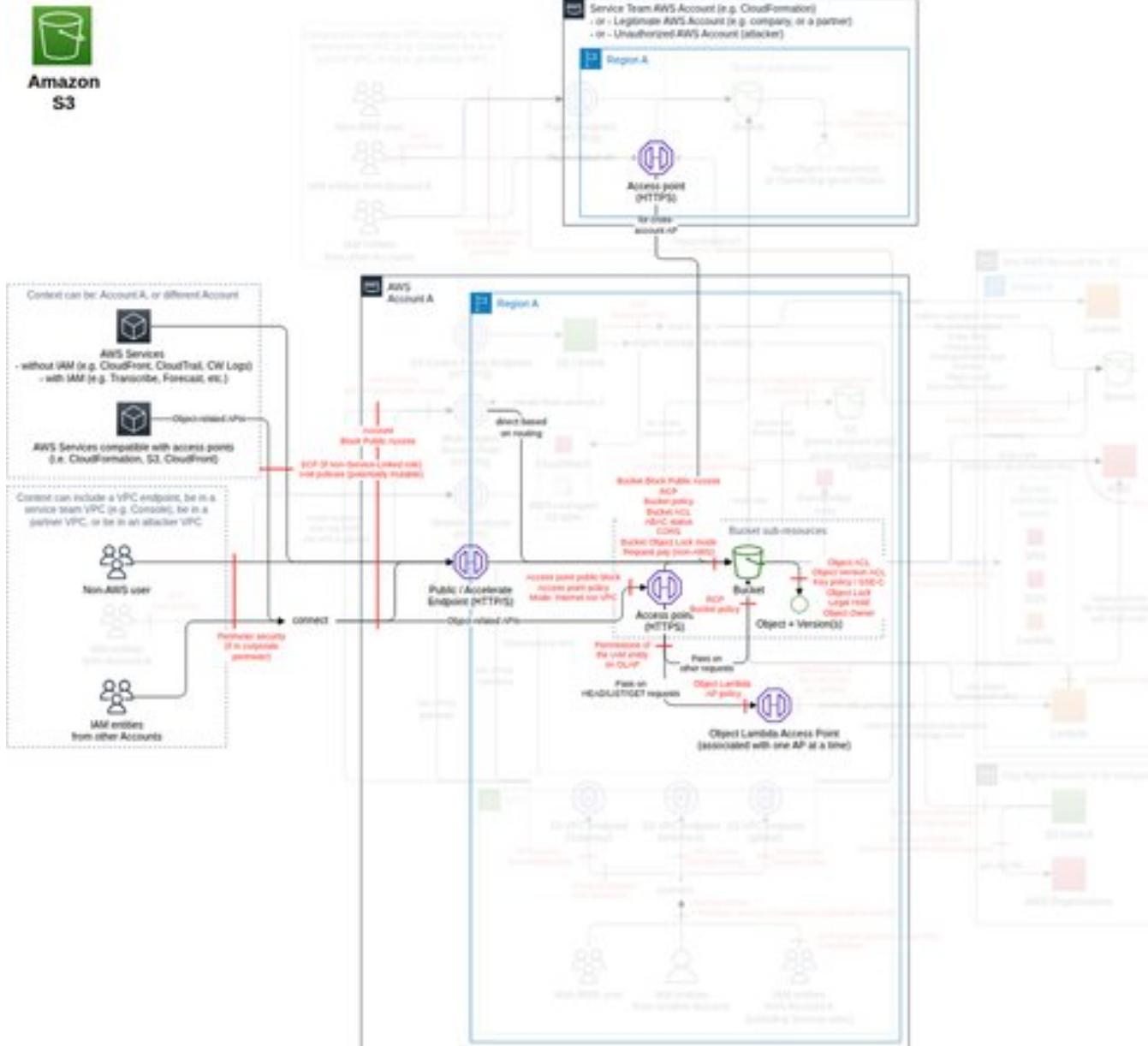


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

# Bucket policy (subclass of Bucket, FC10)

For your bucket, you can add a bucket policy to grant other AWS accounts or IAM users permissions for the bucket and the objects in it. Any object permissions apply only to the objects that the bucket owner creates.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

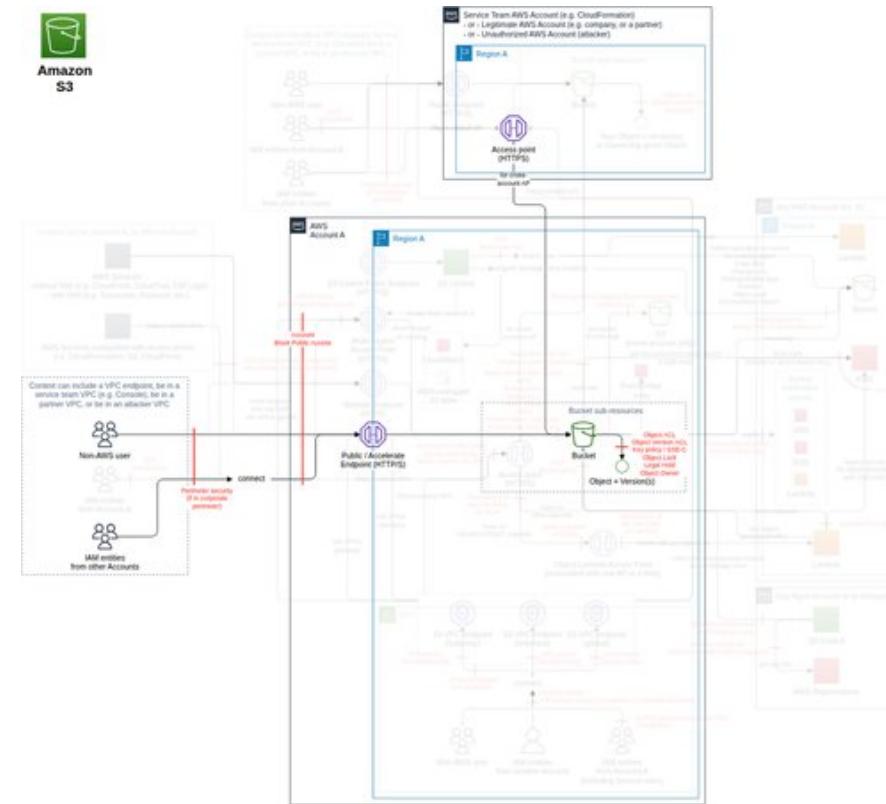
Action	IAM Permission
Adds to or replaces a policy on a bucket.	s3:PutBucketPolicy

## Threat List

Name	CVSS
Grant unauthorized access to a private bucket by changing its bucket policy	<a href="#">Medium (6.9)</a>
Reduce bucket security by deleting the bucket policy	<a href="#">Medium (6.4)</a>
Use CloudFront to access a private bucket	<a href="#">Medium (5.5)</a>

## Grant unauthorized access to a private bucket by changing its bucket policy

<b>Threat Id</b>	S3.T37
<b>Name</b>	Grant unauthorized access to a private bucket by changing its bucket policy
<b>Description</b>	Bucket policies can enable access to objects owned by buckets. An attacker (or someone by negligence) can change a bucket policy to make the content of the bucket either accessible (via public endpoints, cross-account VPC endpoints, or cross-account access points) or to block all principals (leading to the need to use root to delete the policy) to impact the availability of any applications using the bucket.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (6.9)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketPolicy" }

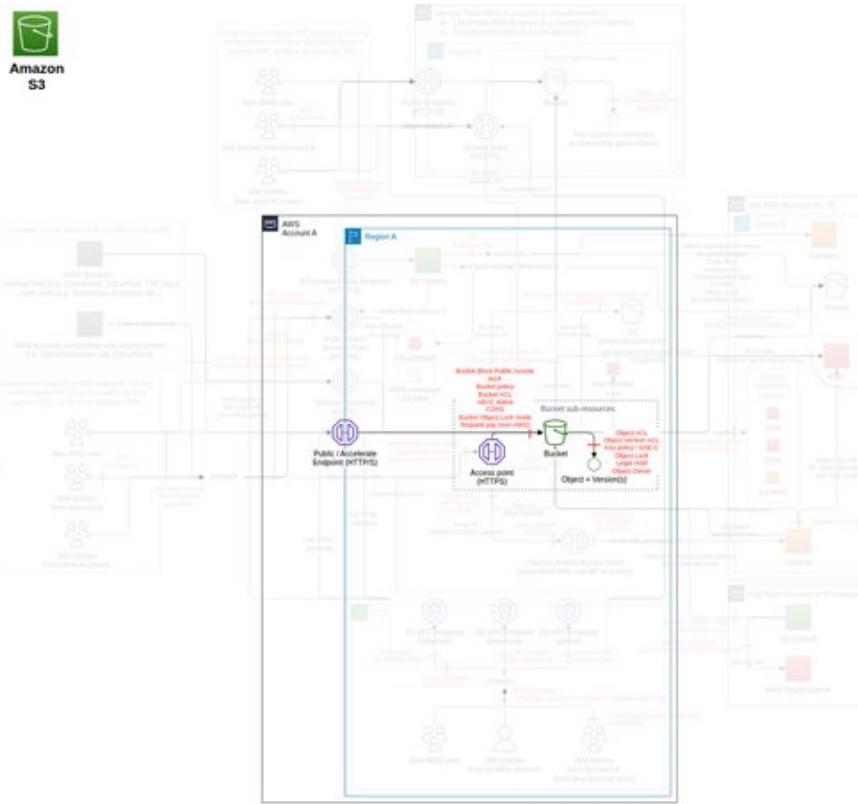


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO13 - Block direct public access</b> C49 - Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C51 - Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023). C53 - Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C173 - Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Very High	4	-	-
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO16 - Enforce encryption at rest</b> C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C63 - Use KMS ThreatModel to protect the KMS keys used for S3 (e.g., using encryptionContext on the policy of each KMS key). C64 - Implement an authorized default encryption key on each bucket; enable S3 Bucket Key if not using DSSE-KMS and if CloudTrail events are not required for KMS encrypt/decrypt (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings). C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key). C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C). C146 - For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present).	Very High	5	2	-
<b>CO32 - Restrict access point access to VPCs when in use</b>	Very High	1	1	-

C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C106 - In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn".				
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account. C149 - For each bucket, maintain a list of authorized IAM principals allowed to access via the bucket policy. C150 - Ensure only authorized IAM principals allowed to access via bucket policy are configured (e.g., using IAM Access Analyzer for reconciliation).	Very High	4	-	-
<b>C04 - Monitor S3 with Amazon GuardDuty and Macie</b> C118 - Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	High	1	-	-

## Reduce bucket security by deleting the bucket policy

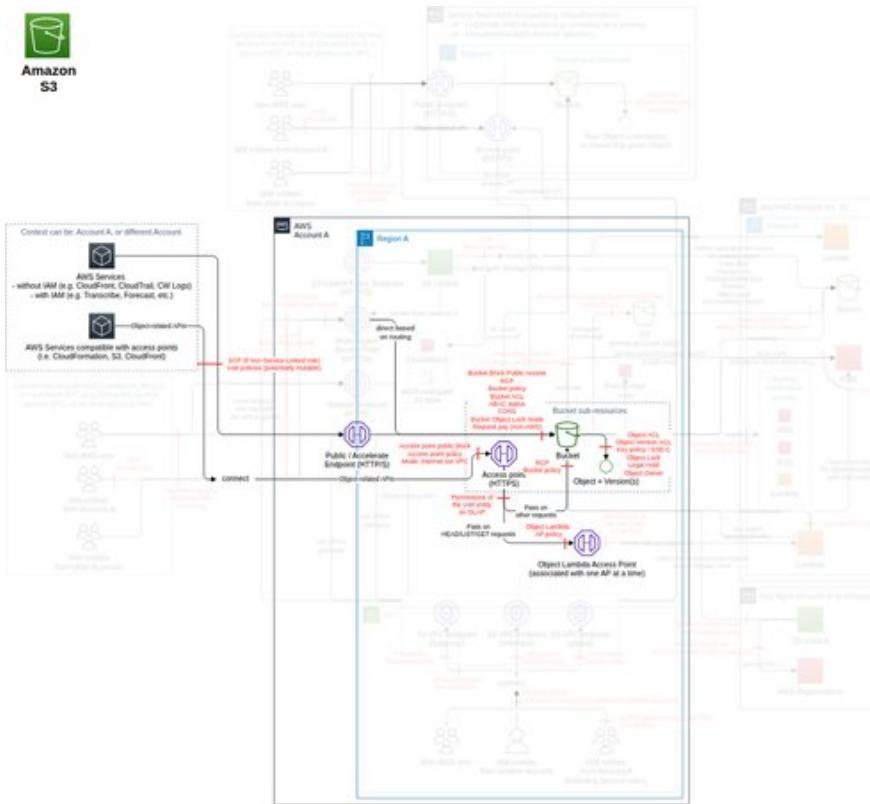
<b>Threat Id</b>	S3.T38
<b>Name</b>	Reduce bucket security by deleting the bucket policy
<b>Description</b>	Bucket policy can deny access to objects, as it supersedes the object's authority. An attacker (or someone by negligence) can delete the bucket policy and make the content less secure.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0004, T1548</a>
<b>CVSS</b>	<a href="#">Medium (6.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3>DeleteBucketPolicy" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO29 - Limit access from only authorized VPCs</b> C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Very High	1	1	-
<b>CO13 - Block direct public access</b> C49 - Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C51 - Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023). C53 - Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true. C173 - Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	High	4	-	-
<b>CO4 - Monitor S3 with Amazon GuardDuty and Macie</b> C118 - Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	High	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	High	2	-	-

## Use CloudFront to access a private bucket

<b>Threat Id</b>	S3.T20
<b>Name</b>	Use CloudFront to access a private bucket
<b>Description</b>	CloudFront distributions can use S3 buckets or access points as their origin. An attacker can connect a CloudFront distribution to a private S3 bucket to gain access to it. Note: S3 resource policies can allow a "cloudfront.amazonaws.com" principal, which could allow any distribution if not restricted.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (5.5)</a>
<b>IAM Access</b>	{ "OPTIONAL": { "OR": ["s3:PutBucketPolicy", "s3:PutAccessPointPolicy", "s3:PutAccessPointPolicyForObjectLambda"] } }

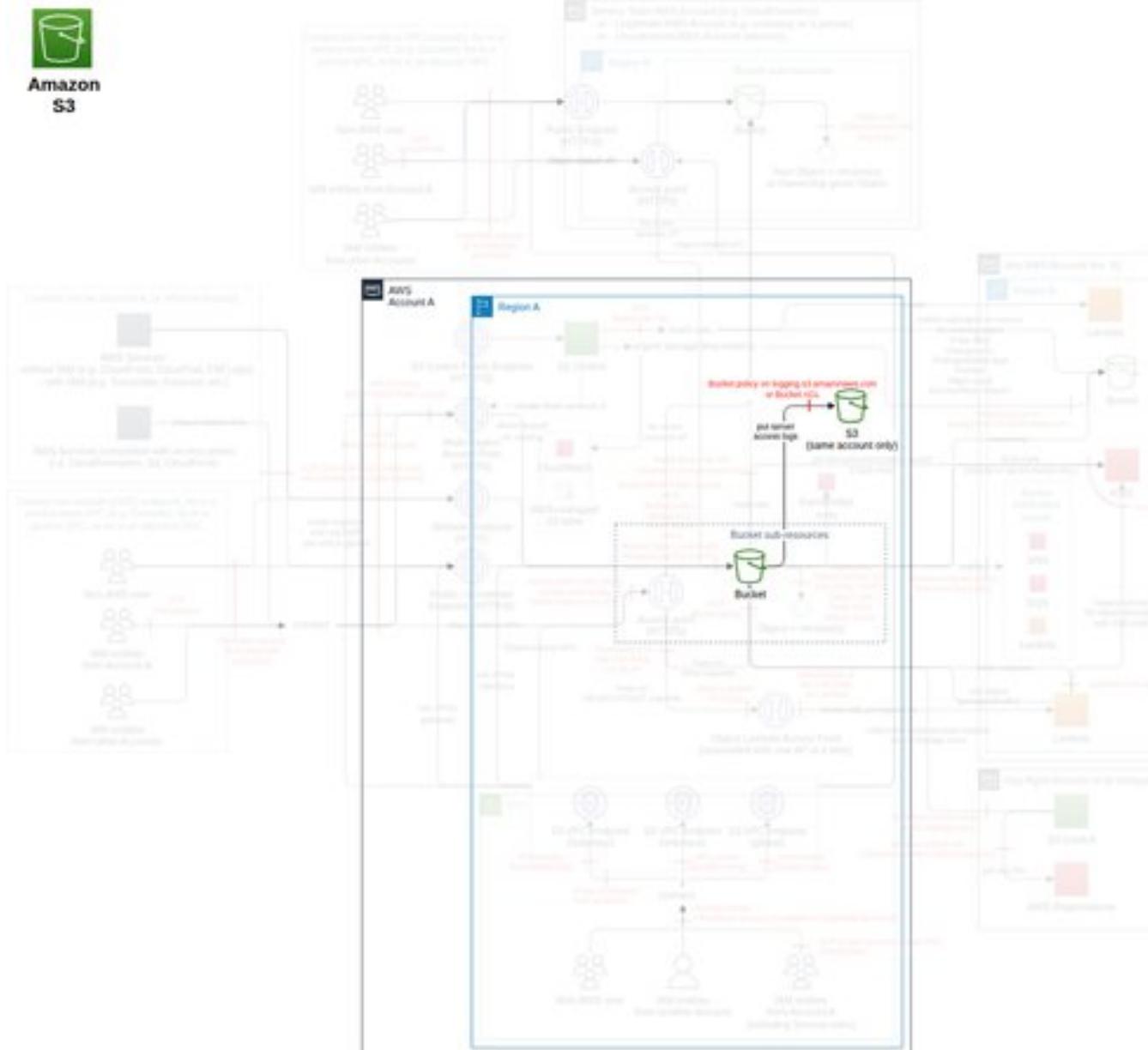


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> <small>C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a>.</small>	Very High	1	-	-
<b>CO16 - Enforce encryption at rest</b> <small>C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption (<a href="#">ref</a>). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C64 - Implement an authorized default encryption key on each bucket; enable S3 Bucket Key if not using DSSE-KMS and if CloudTrail events are not required for KMS encrypt/decrypt (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings). C66 - Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key). C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C). C146 - For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present).</small>	Very High	4	2	-
<b>CO30 - Control CloudFront access</b> <small>C101 - Maintain a list of authorized CloudFront distributions (via Origin Access Control) and associated bucket, access point, and/or Object Lambda Access Point. C137 - Ensure only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa (e.g., using their bucket policy, centrally in an RCP applied to the OU or AWS account, with a deny statement, access point policy, resource policy for an Object Lambda Access Point, limiting the access to only the authorized distribution(s) in the SourceArn).</small>	High	2	-	-
<b>CO18 - Encrypt or tokenize critical data</b> <small>C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.</small>	Low	1	-	-

# S3 access logging (*subclass of Bucket ACL/Bucket policy, FC19*)

Server access logging provides detailed records for the requests made to a bucket. CloudTrail S3 data events are preferred due to the more reliable delivery timing, consistency, supporting KMS encryption, and S3 Object Lock ([full comparison](#)); however, the website endpoint is not recorded on S3 data events, some SIEM modules might be more feature-rich with S3 access logs, and access logging is free besides storage.

## **Data Flow Diagram (DFD)**



## ***Actions and IAM Permissions to deny the feature***

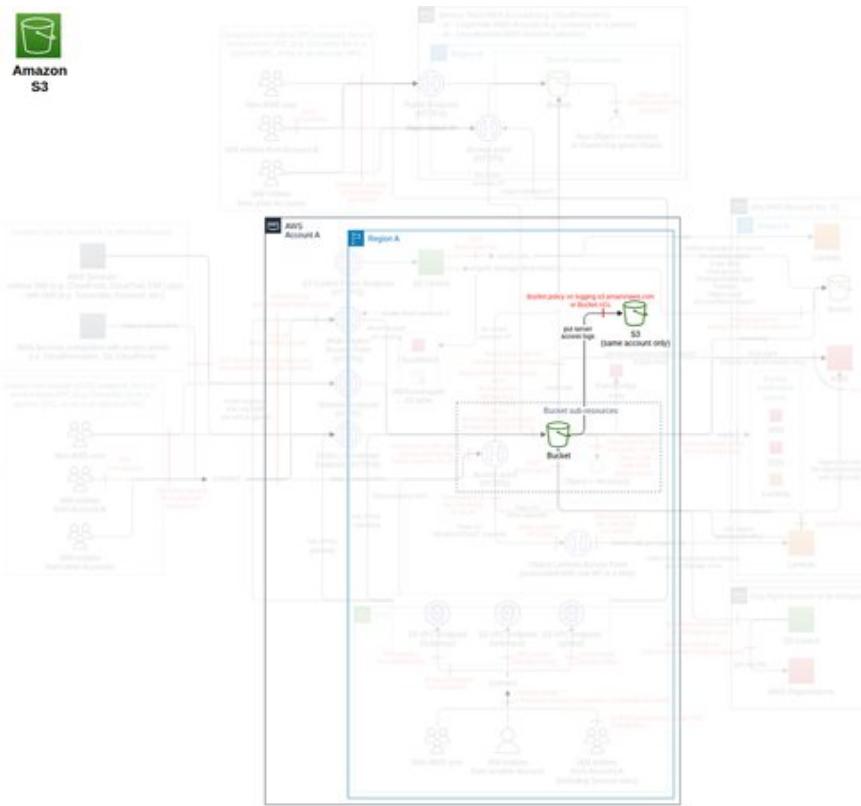
Action	IAM Permission
Sets the logging parameters for a bucket.	s3:PutBucketLogging

## ***Threat List***

Name	CVSS
Evade detection by disabling S3 access logs via a bucket ACL change	<a href="#">Low (2.4)</a>
Evade detection by disabling S3 access logs via bucket policy change or removal	<a href="#">Low (2.4)</a>
Evade detection by modifying S3 access logs	<a href="#">Low (2.4)</a>

## Evade detection by disabling S3 access logs via a bucket ACL change

<b>Threat Id</b>	S3.T51
<b>Name</b>	Evade detection by disabling S3 access logs via a bucket ACL change
<b>Description</b>	S3 access logs can be used by SIEM to detect abnormal behaviors. An attacker can disable S3 access logs via bucket ACL changes on the logging destination bucket to evade detection.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1564</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketAcl" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

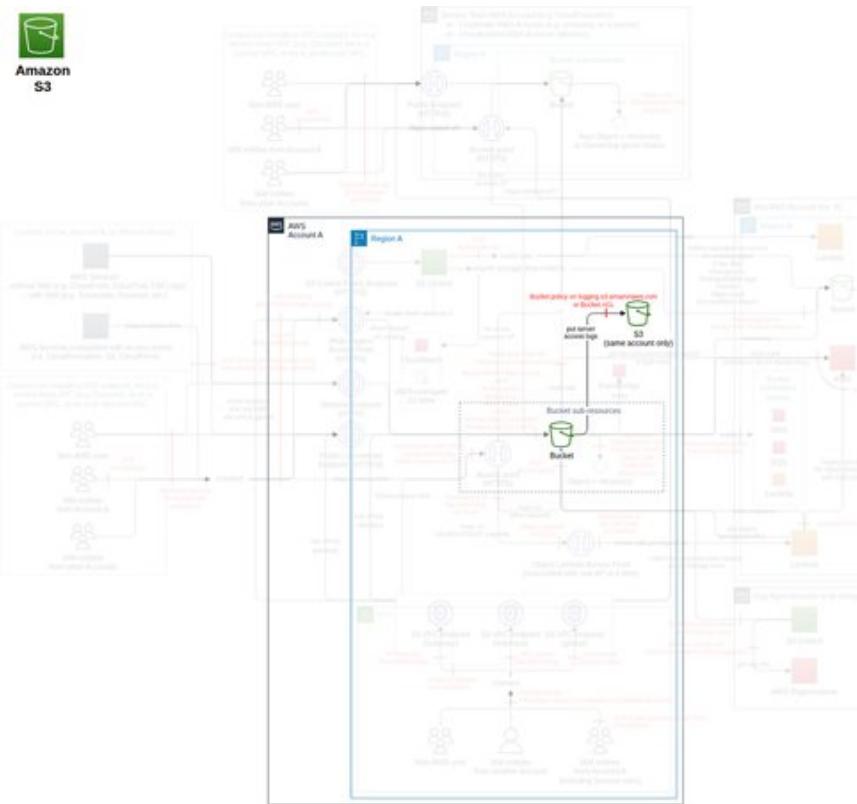
**Evade detection by disabling S3 access logs via bucket policy change or removal**

<b>Threat Id</b>	S3.T58
<b>Name</b>	Evade detection by disabling S3 access logs via bucket policy change or removal
<b>Description</b>	S3 access logs can be used by SIEM to detect abnormal behaviors. An attacker can disable S3 access logs via bucket policy changes on the logging destination bucket to evade detection.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1564</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "OR": ["s3:PutBucketPolicy", "s3>DeleteBucketPolicy"] }

Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO14 - Block bucket ACL</b>  C55 - Deny requests to add an ACL on a bucket (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy, with a deny statement on "s3:PutBucketAcl"). C56 - Monitor changes to bucket ACLs to ensure they stay private (e.g., using the CloudTrail event PutBucketAcl and its field requestParameters.x-amz-acl, which should either be "private" or not exist).	Very High	-	1	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Evade detection by modifying S3 access logs

<b>Threat Id</b>	S3.T59
<b>Name</b>	Evade detection by modifying S3 access logs
<b>Description</b>	S3 access logs can be used by SIEM to detect abnormal behaviors. An attacker can modify or disable S3 access logs to evade detection.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1564</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketLogging" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO39 - Enforce S3 server access logging on buckets</b> C157 - Monitor PutBucketLogging to detect bucket server access logging changes, including deactivation and bucket changes (i.e., using the CloudTrail event "PutBucketLogging" and the "requestParameters.BucketLoggingStatus" field to examine the lack of the "LoggingEnabled" key or an unauthorized bucket in "requestParameters.BucketLoggingStatus.LoggingEnabled.TargetBucket").	Medium	-	-	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

# Analytics (*subclass of Bucket, FC11*)

You can analyze storage access patterns to decide the storage class ([ref](#)).

# **Data Flow Diagram (DFD)**

## ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Adds an analytics configuration (identified by the analytics ID) to the bucket.	s3:PutAnalyticsConfiguration

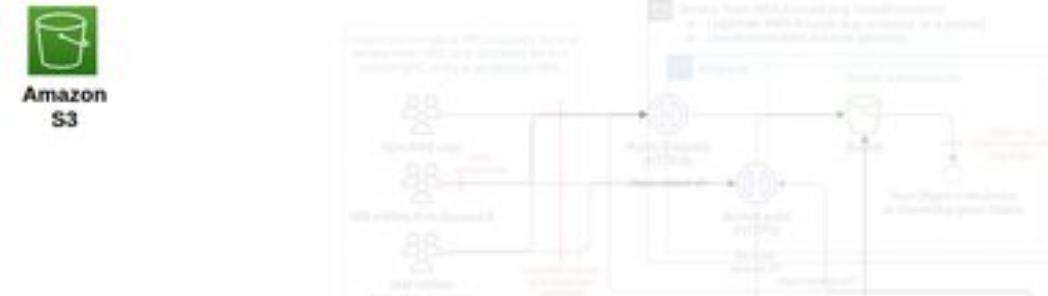
## ***Threat List***

Name	CVSS
None	None

# Inventory (*subclass of Bucket, FC12*)

You can create a report on your storage, including object metadata or versions ([ref](#)).

## **Data Flow Diagram (DFD)**

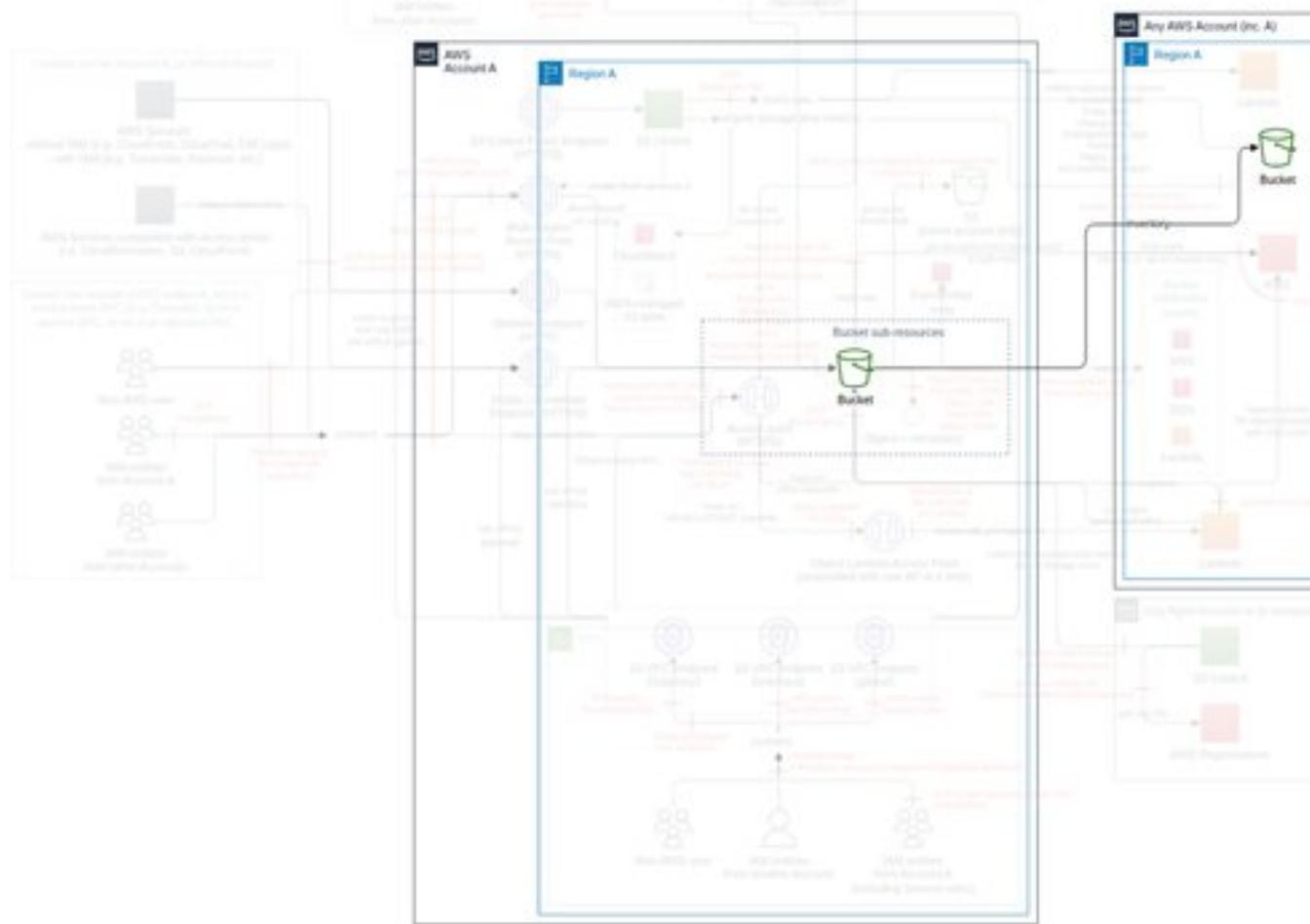


## ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Adds an inventory configuration (identified by the inventory ID) to the bucket.	s3:PutInventoryConfiguration

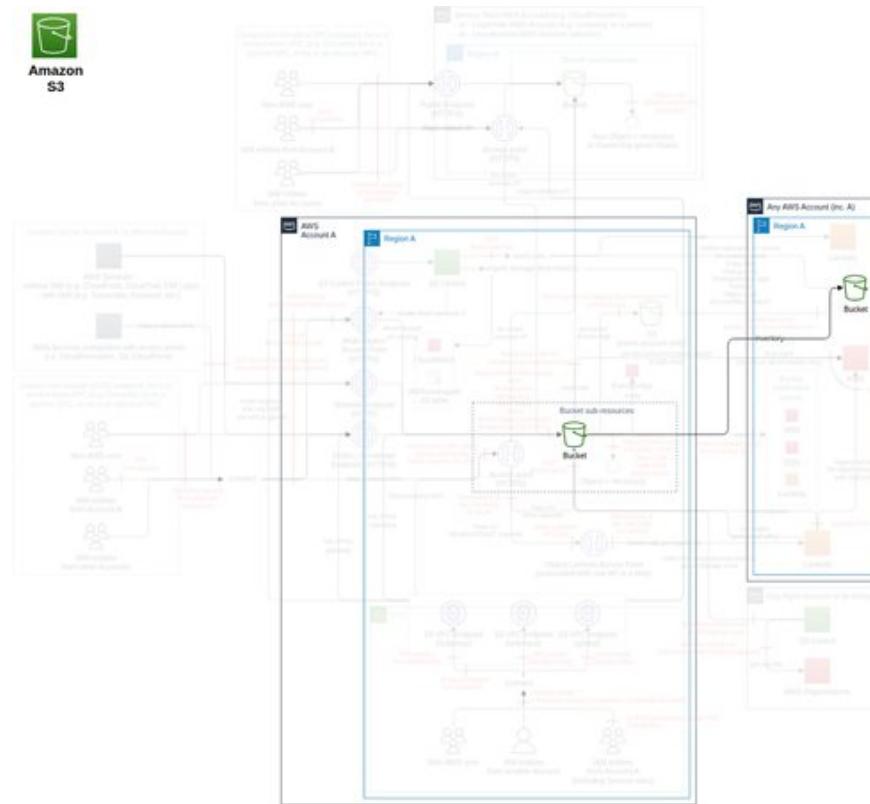
## ***Threat List***

Name	CVSS
Exfiltrate data via inventory	<a href="#">Low (2.4)</a>



## Exfiltrate data via inventory

<b>Threat Id</b>	S3.T42
<b>Name</b>	Exfiltrate data via inventory
<b>Description</b>	Inventory sends the object names (i.e., keys) to any configured S3 bucket or other metadata. An attacker can use the names of objects (1 KB) to exfiltrate data or use the metadata to conduct reconnaissance.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1020</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutInventoryConfiguration" }

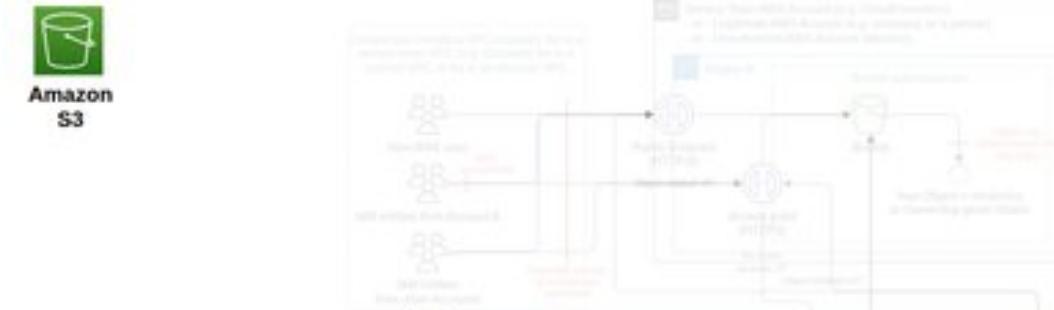


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO12 - Enforce secure SDLC processes</b> C45 - Do not include sensitive data in bucket names, access point names, object names, object metadata, and tags.	Medium	1	-	-
<b>CO28 - Control the data collected and the storage location of the inventory</b> C96 - Maintain a list of authorized S3 buckets to receive the S3 Inventory of each bucket. C136 - Ensure only authorized S3 buckets are configured to receive S3 Inventory for each bucket. C164 - Maintain the list of authorized optional fields allowed to be accessed by each authorized IAM principal. C165 - Prevent the creation of inventories without authorized optional fields (e.g., by using an SCP and/or an IAM policy on "s3:PutInventoryConfiguration" with an allow statement on "s3:InventoryAccessibleOptionalFields" = authorized optional fields only).	Medium	3	1	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

# Lifecycle (*subclass of Bucket, FC13*)

You can manage the lifecycle of your data to reduce storage costs ([ref](#))

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

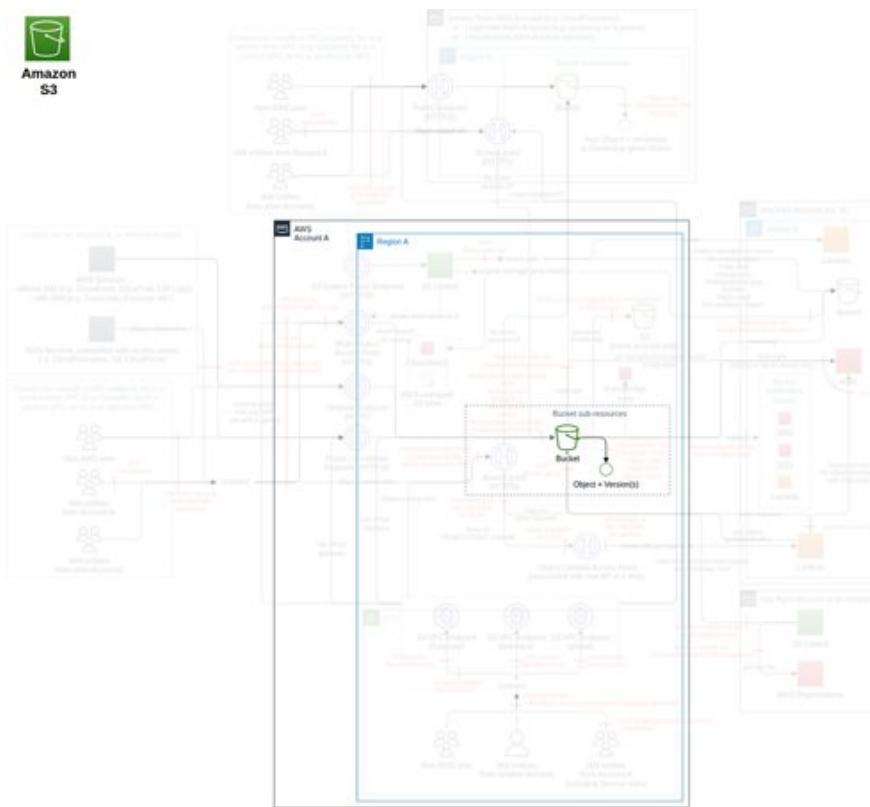
Action	IAM Permission
Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration.	s3:PutLifecycleConfiguration
Puts a S3 Intelligent-Tiering configuration to the specified bucket.	s3:PutIntelligentTieringConfiguration

## **Threat List**

Name	CVSS
Delete objects by using lifecycle	<a href="#">Medium (5.1)</a>

## Delete objects by using lifecycle

<b>Threat Id</b>	S3.T25
<b>Name</b>	Delete objects by using lifecycle
<b>Description</b>	Lifecycle allows you to delete objects after their configured expiry. An attacker can use a lifecycle configuration to destroy data.
<b>Goal</b>	Data manipulation
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1485</a>
<b>CVSS</b>	<a href="#">Medium (5.1)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutLifecycleConfiguration" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO20 - Protect data integrity using S3 Object Lock</b> C74 - Implement the authorized default S3 Object Lock on buckets requiring WORM (note: Amazon S3 evaluates and applies bucket policies before applying the bucket default S3 Object Lock settings).	Very High	-	1	-
<b>CO17 - Protect primary data against loss</b> C71 - Back up primary data in a secure location under a different security authority (e.g., in an <a href="#">AWS data bunker account</a> via replication, or using AWS Backup for Amazon S3).	High	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Metrics (subclass of Bucket, FC14)

You can configure metrics to get additional insights into your usage ([ref](#)).

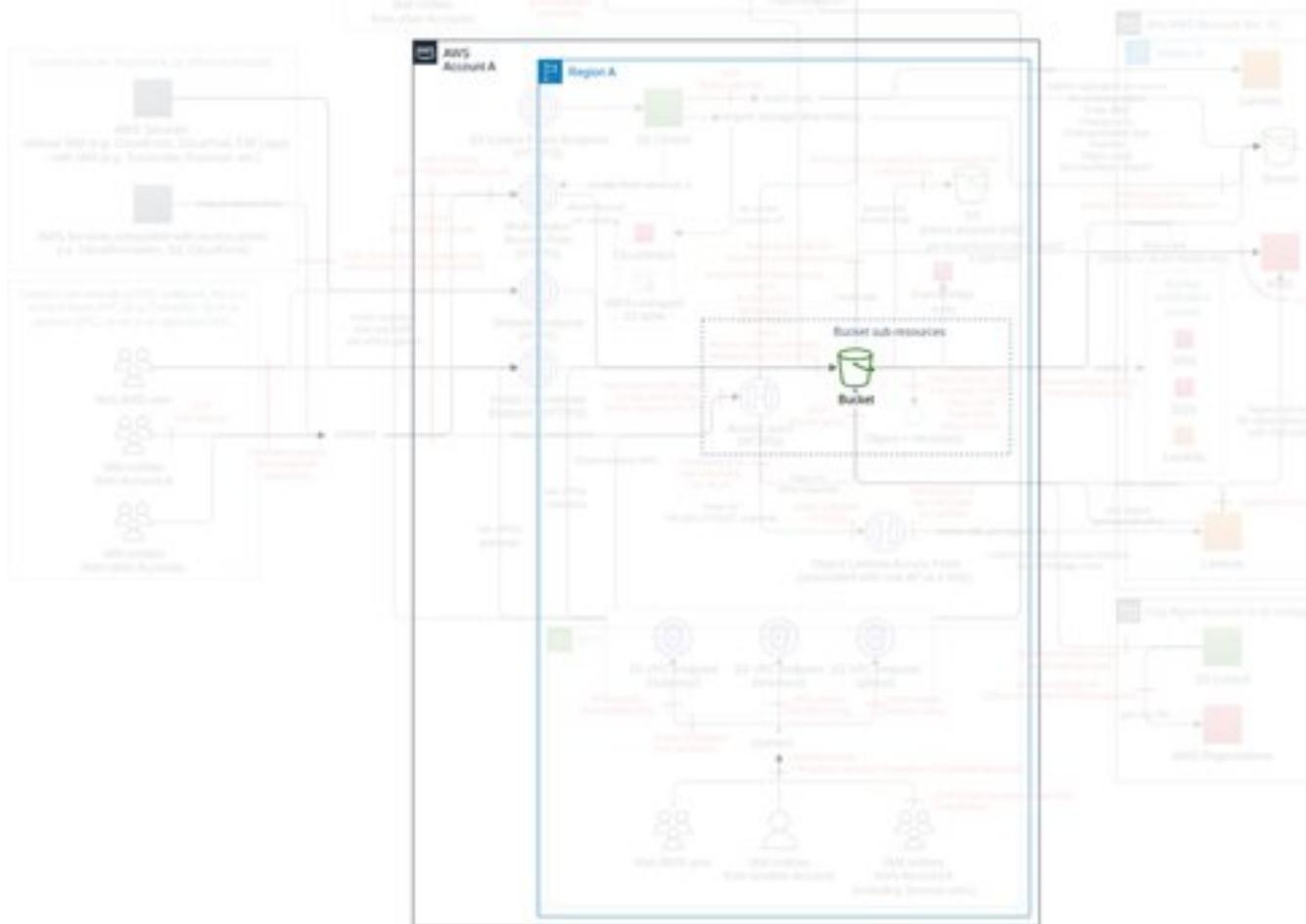
### Data Flow Diagram (DFD)



Amazon S3



S3



### Actions and IAM Permissions to deny the feature

Action	IAM Permission
Sets or updates a metrics configuration for the CloudWatch request metrics (specified by the metrics configuration ID) from the bucket.	s3:PutMetricsConfiguration

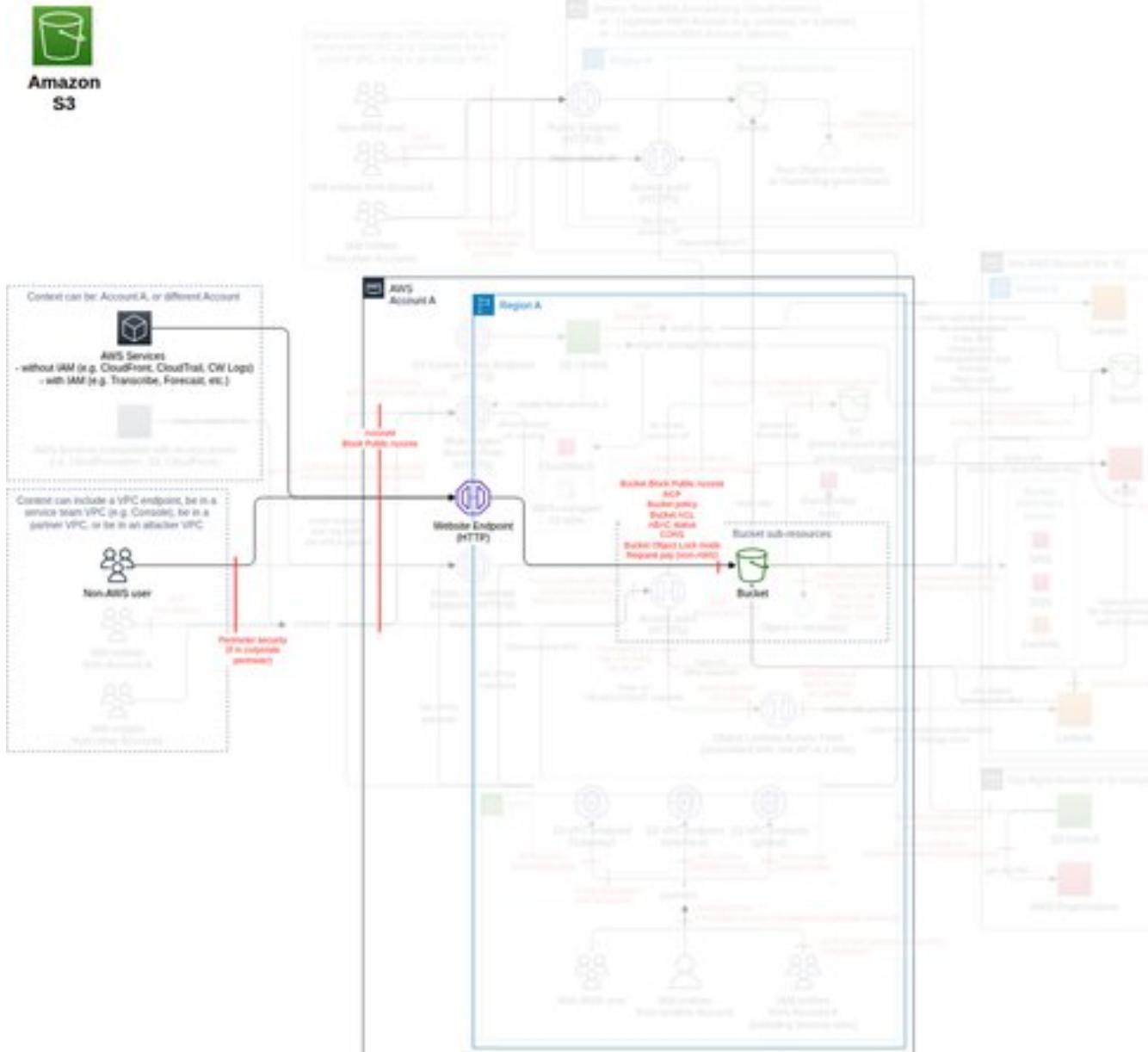
### Threat List

Name	CVSS
None	None

## Website (*subclass of Bucket, FC16*)

You can host a static website on Amazon S3. On a static website, individual web pages include static content. They might also contain client-side scripts ([ref](#)).

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

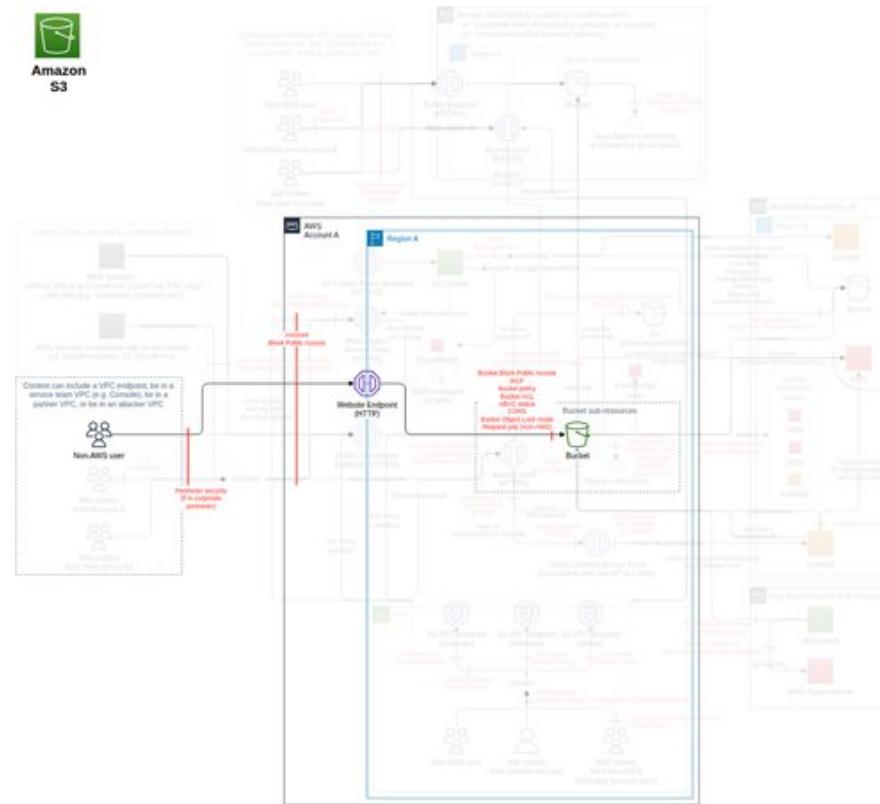
Action	IAM Permission
Sets the configuration of the website that is specified in the website subresource.	s3:PutBucketWebsite

## ***Threat List***

Name	CVSS
Embed client-side script malware in a bucket website	<a href="#">Medium (5.5)</a>
Clickjacking on S3 website	<a href="#">Medium (4.2)</a>
Intercept data in transit on an S3 website endpoint	<a href="#">Low (3.1)</a>

## Embed client-side script malware in a bucket website

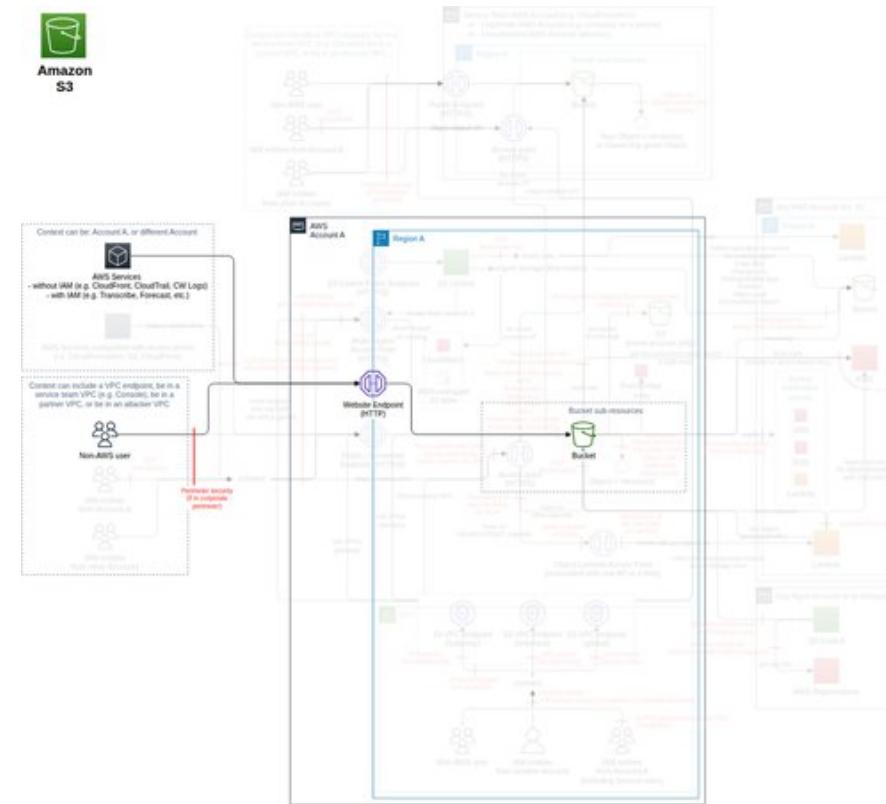
<b>Threat Id</b>	S3.T15
<b>Name</b>	Embed client-side script malware in a bucket website
<b>Description</b>	S3 website enables users to be served client-side scripts (e.g., JavaScript). An attacker can upload a client-side script with malware (e.g., cryptomining) to the visitors.
<b>Goal</b>	Direct Financial Gain
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0002</a> , <a href="#">T1203</a>
<b>CVSS</b>	<a href="#">Medium (5.5)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutObject" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO5 - Identify and ensure the protection of all external buckets hosting your objects</b>  C11 - Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel).  C14 - Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g., using Macie).	High	2	-	-
<b>CO26 - Scan objects used for input/output of a workflow for malware</b>  C93 - If the bucket is used as an input or the output of a process, scan the objects for malware (e.g., using <a href="#">GuardDuty Malware Protection for S3</a> , <a href="#">BucketAV</a> , <a href="#">Cloud Storage Security</a> , <a href="#">Trend Micro Cloud One</a> , or <a href="#">your own scanning solution</a> ).	Low	-	-	1

## Clickjacking on S3 website

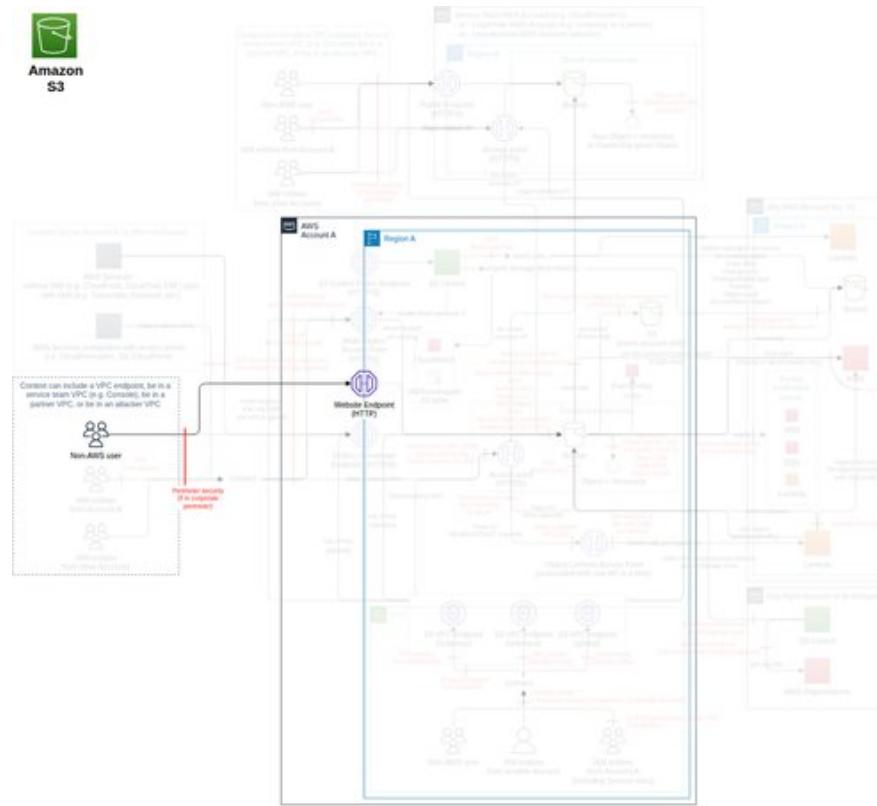
<b>Threat Id</b>	S3.T29
<b>Name</b>	Clickjacking on S3 website
<b>Description</b>	S3 does not enforce certain security headers by default. An attacker can use an iFrame on your website to trick users into interacting with their own scripts.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1496</a>
<b>CVSS</b>	<a href="#">Medium (4.2)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO35 - Deploy only authorized S3 websites and place them behind a CDN</b> C141 - Maintain a list of authorized buckets to be configured as an S3 website endpoint. C142 - Ensure only authorized buckets are configured as an S3 website endpoint. C144 - Ensure S3 website endpoints are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g., CloudFront).	Very High	3	-	-

## Intercept data in transit on an S3 website endpoint

<b>Threat Id</b>	S3.T13
<b>Name</b>	Intercept data in transit on an S3 website endpoint
<b>Description</b>	S3 website endpoint is serving HTTP only. An attacker can intercept the traffic you send to an external bucket to read the data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1557</a>
<b>CVSS</b>	<a href="#">Low (3.1)</a>
<b>IAM Access</b>	{}

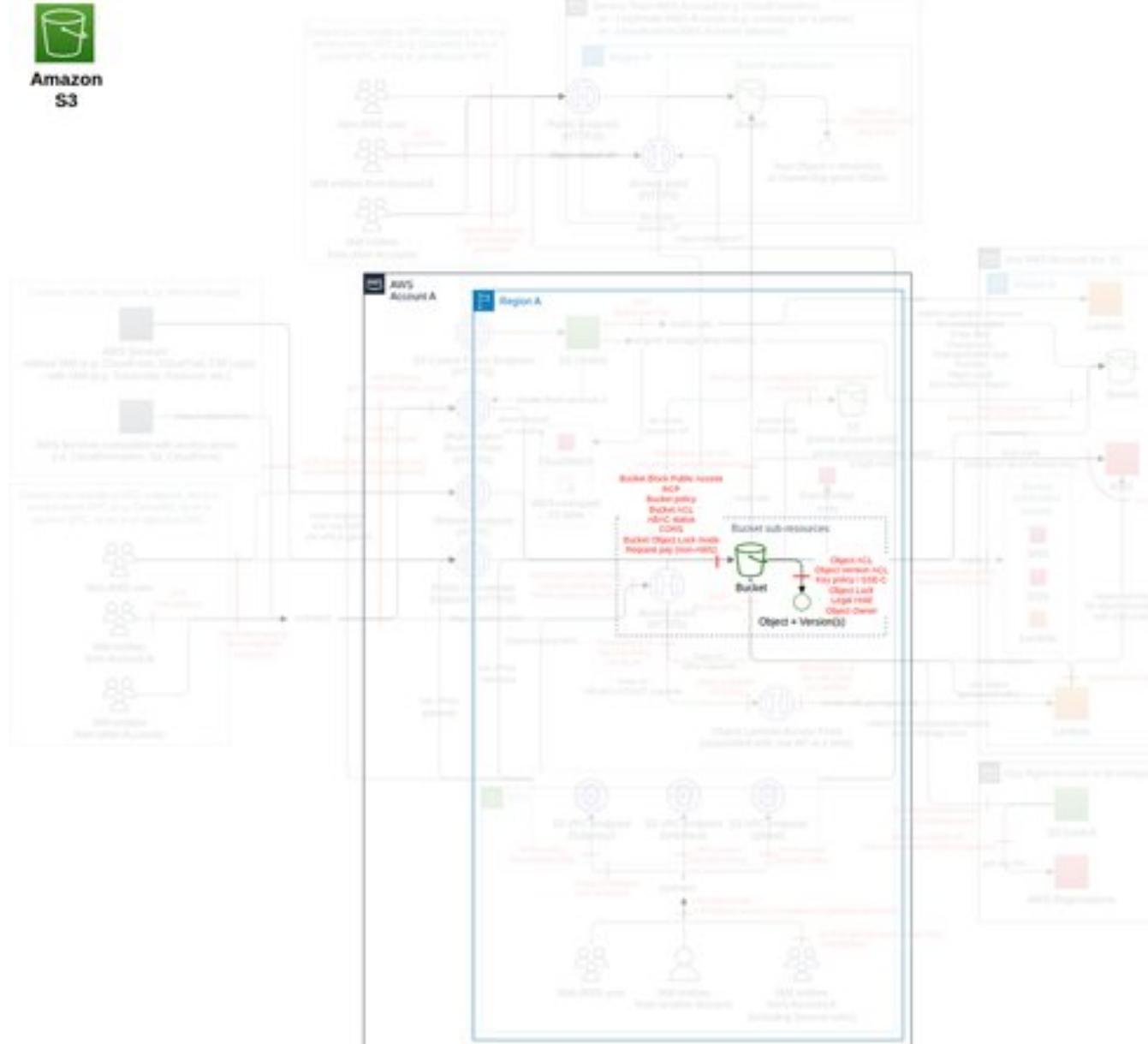


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO13 - Block direct public access</b> C47 - Front buckets that are required to be public, using authenticated CDN (e.g., CloudFront) or API Gateway, protected with WAF (e.g., for <a href="#">hotlinking</a> ).	Very High	1	-	-
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO35 - Deploy only authorized S3 websites and place them behind a CDN</b> C141 - Maintain a list of authorized buckets to be configured as an S3 website endpoint. C142 - Ensure only authorized buckets are configured as an S3 website endpoint. C144 - Ensure S3 website endpoints are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g., CloudFront).	Very High	3	-	-
<b>CO18 - Encrypt or tokenize critical data</b> C72 - Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Medium	1	-	-

# S3 Object Lock (subclass of Bucket, FC17)

You can use S3 Object Lock to store objects using a write-once-read-many (WORM) model ([ref](#)). Creating a bucket with S3 Object Lock will enable versioning even without permissions.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

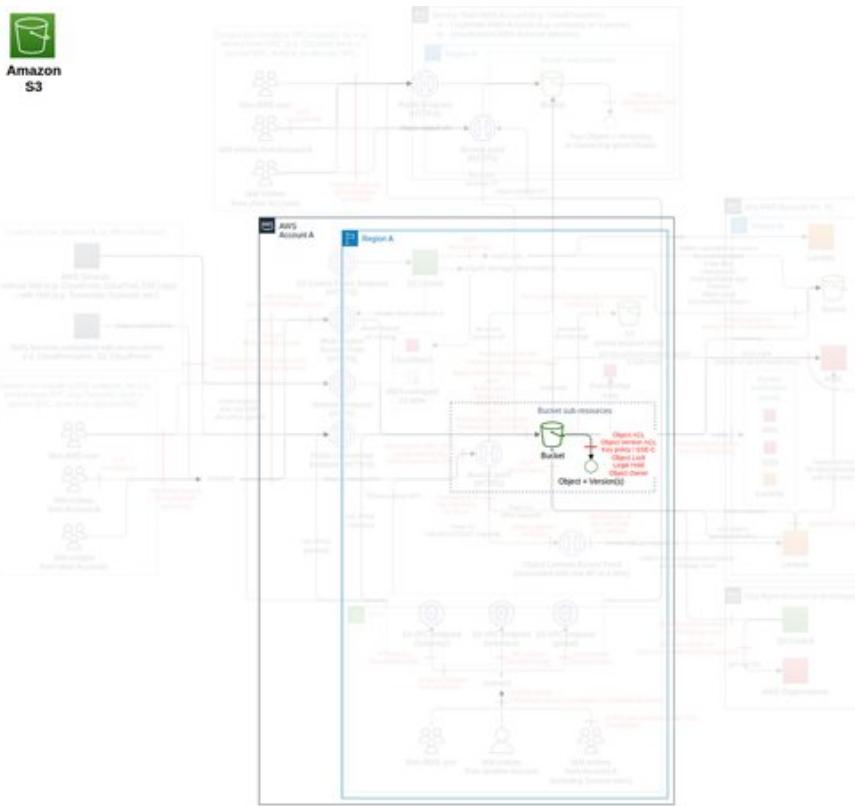
Action	IAM Permission
Grants permission to allow circumvention of governance-mode object retention settings (for DeleteObject, DeleteObjects and PutObjectRetention).	s3:BypassGovernanceRetention
Allows placing a default S3 Object Lock configuration at bucket creation (AWS Support needs to be contacted for existing buckets). It automatically enables versioning, even without permission.	s3:PutBucketObjectLockConfiguration
Puts object retention on a specific object.	s3:PutObjectRetention

## Threat List

Name	CVSS
Increase costs and compliance risks by enabling S3 Object Lock in compliance mode	<a href="#">Medium (4.2)</a>

## Increase costs and compliance risks by enabling S3 Object Lock in compliance mode

<b>Threat Id</b>	S3.T61
<b>Name</b>	Increase costs and compliance risks by enabling S3 Object Lock in compliance mode
<b>Description</b>	Existing objects or buckets can be modified to have S3 Object Lock enabled. An attacker can enable it in compliance mode to lock any existing objects or new objects, increasing costs due to unnecessary data storage and potentially causing compliance risks if data is retained beyond its legally required period.
<b>Goal</b>	Financial Drain
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1586</a>
<b>CVSS</b>	Medium (4.2)
<b>IAM Access</b>	{ "AND": [ {"OR": ["s3:PutBucketObjectLockConfiguration", "s3:PutObjectRetention"]} ], "OPTIONAL": "s3:PutObjectLegalHold" }

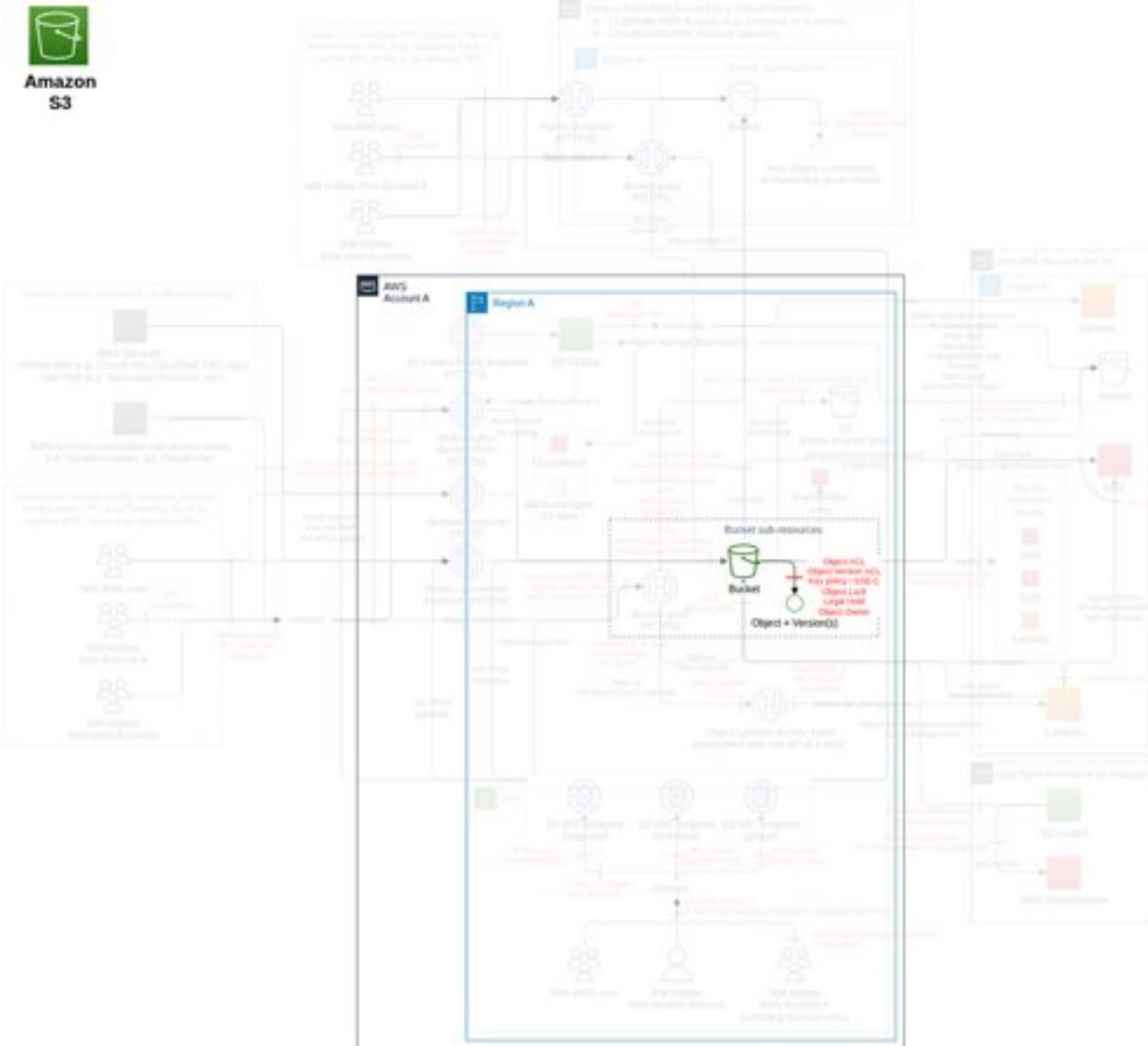


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Very High	1	-	-
<b>CO20 - Protect data integrity using S3 Object Lock</b> C74 - Implement the authorized default S3 Object Lock on buckets requiring WORM (note: Amazon S3 evaluates and applies bucket policies before applying the bucket default S3 Object Lock settings). C76 - Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on buckets requiring WORM (e.g., using their bucket policy and centrally in an RCP applied to the OU or the AWS account with a deny statement on PutObject and PutObjectRetention if the condition "s3:object-lock-mode" exists and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration).	Very High	-	2	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

## Legal hold (subclass of S3 Object Lock, FC29)

A legal hold provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until you explicitly remove it. Legal holds are independent of retention periods.

### Data Flow Diagram (DFD)



### Actions and IAM Permissions to deny the feature

Action	IAM Permission
Puts Object Lock legal hold on a specific object.	s3:PutObjectLegalHold

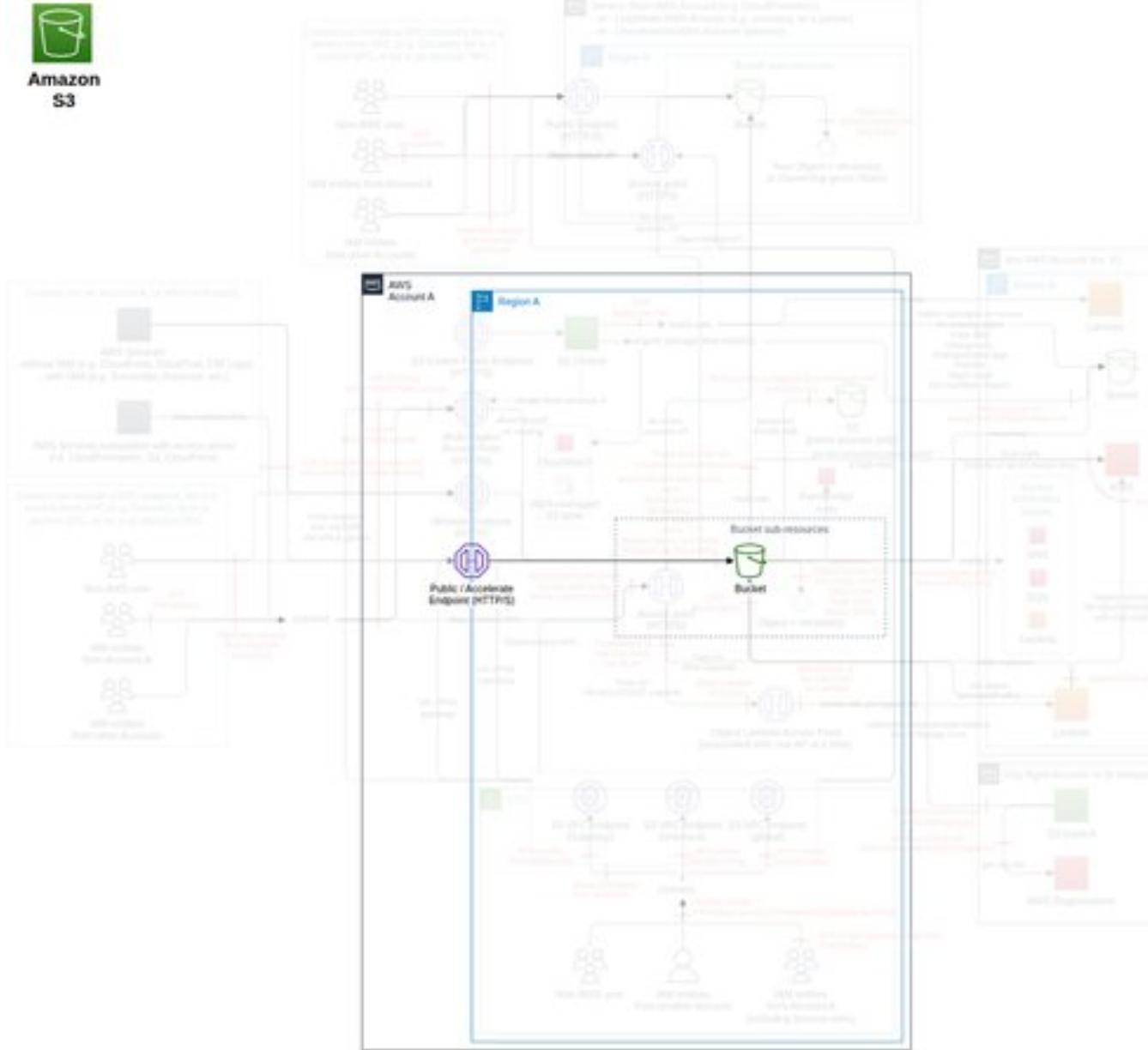
### Threat List

Name	CVSS
None	None

# Transfer Acceleration (subclass of Bucket, FC18)

You can use Transfer Acceleration to improve the performance of long-distance transfers ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

Action	IAM Permission
Sets the Transfer Acceleration state of an existing bucket.	s3:PutAccelerateConfiguration

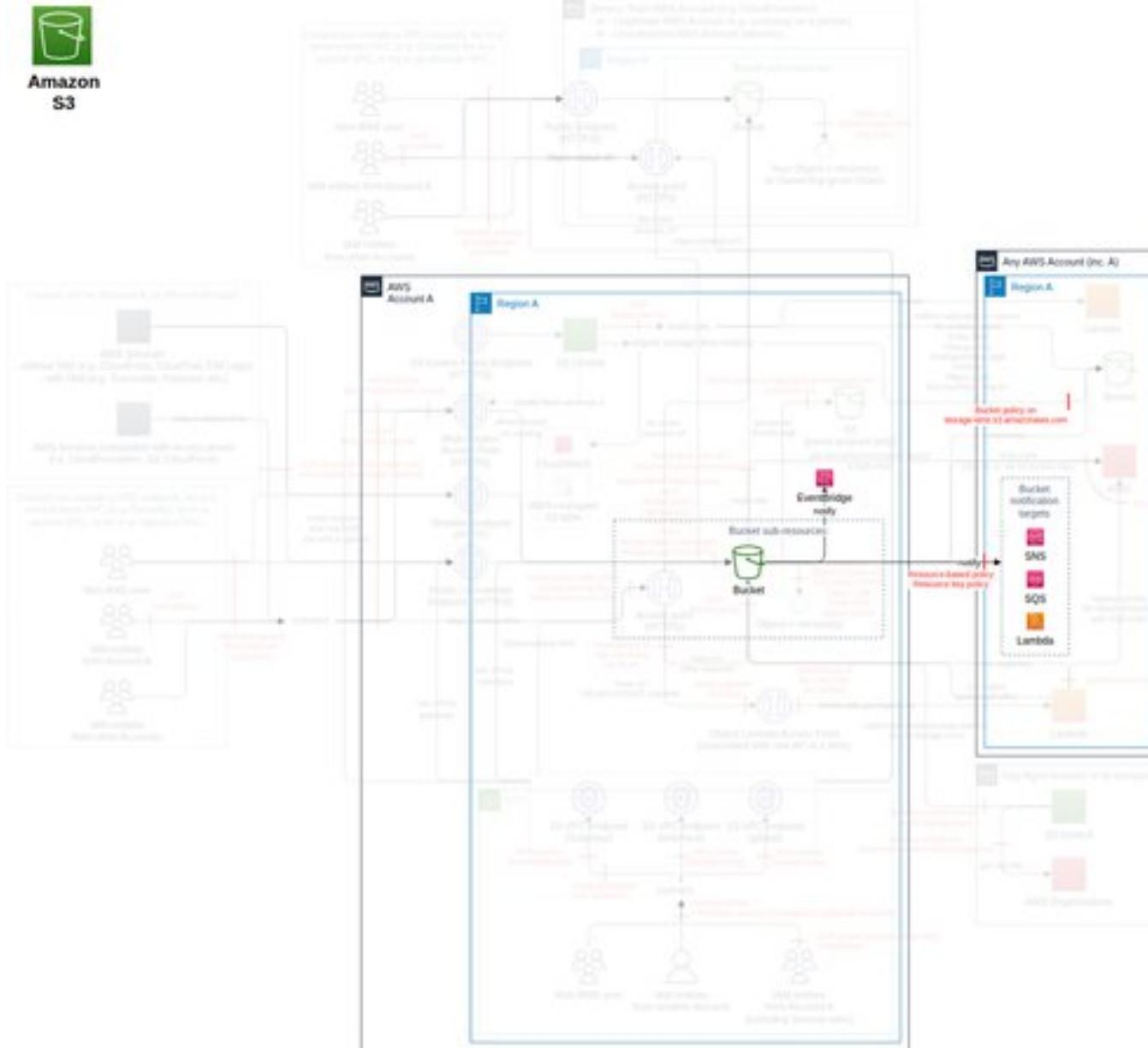
## Threat List

Name	CVSS
None	None

# Notification (subclass of Bucket, FC20)

You can receive notifications when certain events happen in your bucket. Notifications can be sent cross-account ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

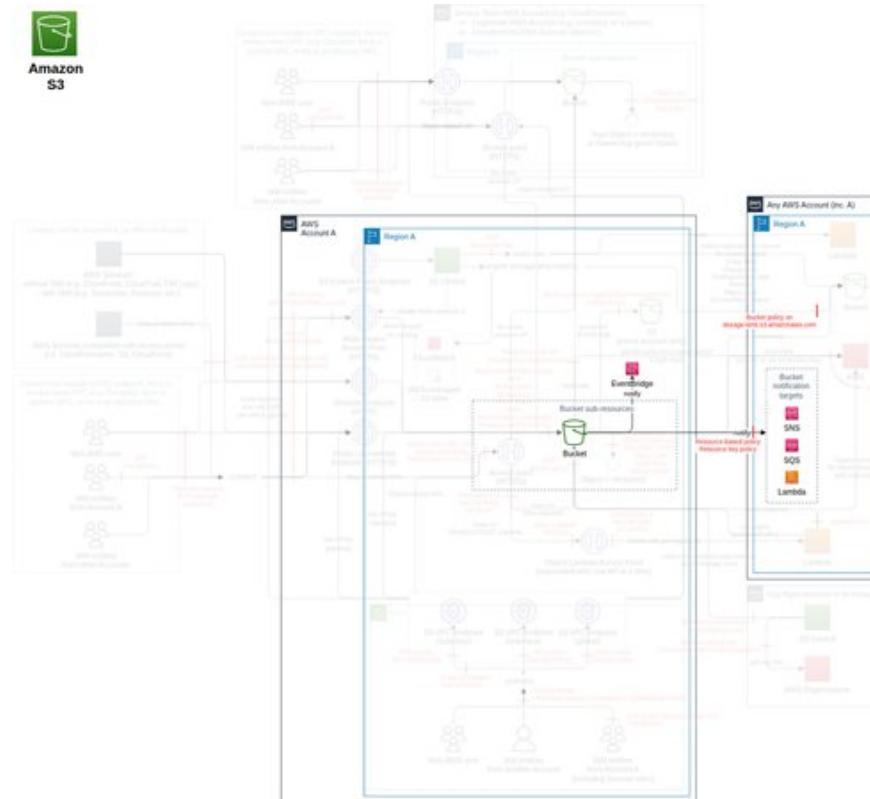
Action	IAM Permission
Enables you to receive notifications when certain events happen in your bucket.	s3:PutBucketNotification

## Threat List

Name	CVSS
Exfiltrate data via event notification	<a href="#">Low (2.4)</a>

### **Exfiltrate data via event notification**

<b>Threat Id</b>	S3.T41
<b>Name</b>	Exfiltrate data via event notification
<b>Description</b>	Event notification sends the key to any configured SQS, SNS, or Lambda (cross-account), or EventBridge (same account). An attacker can use the name of objects (1 KB) to exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1537</a> , <a href="#">T1020</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketNotification" }

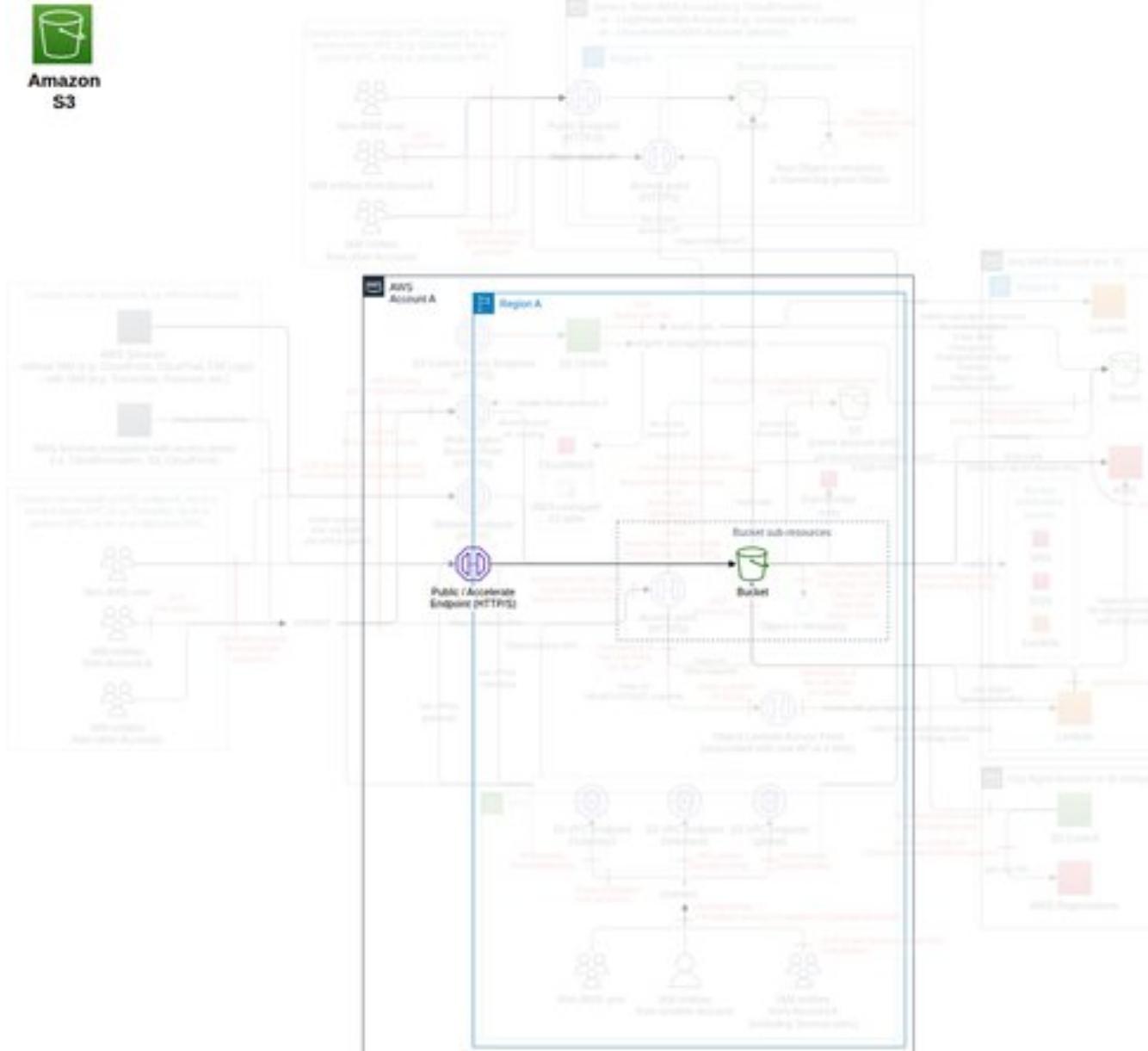


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO27 - Control event receivers</b> C94 - Maintain a list of authorized notification receivers (e.g., SNS topic, Lambda) for each bucket. You might use a simpler approach by using authorized account IDs to ensure all your receivers are in authorized AWS accounts. C135 - Ensure only authorized notification receivers for each bucket are configured.	High	2	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-
<b>CO12 - Enforce secure SDLC processes</b> C45 - Do not include sensitive data in bucket names, access point names, object names, object metadata, and tags.	Low	1	-	-

## CORS (*subclass of Bucket, FC22*)

**[NOT RECOMMENDED]** To configure your bucket to allow cross-origin requests, you create a CORS configuration, which is an XML document with rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) that will support for each origin, and other operation-specific information. This feature class is NOT RECOMMENDED to be activated since it is all HTTP. Prefer the use of CDN (e.g., CloudFront), API Gateway, and/or WAF fronting S3 buckets.

## **Data Flow Diagram (DFD)**



## ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Sets the CORS configuration for your bucket.	s3:PutBucketCors

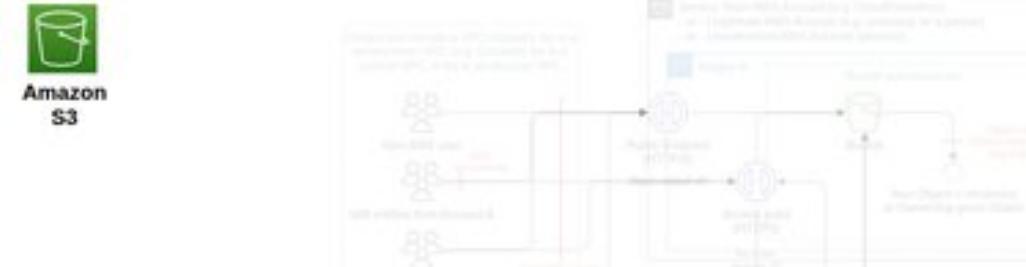
## ***Threat List***

Name	CVSS
None	None

# Bucket default encryption (*subclass of Bucket, FC23*)

You can set default encryption on a bucket so that all new objects are encrypted when stored in the bucket.

## **Data Flow Diagram (DFD)**

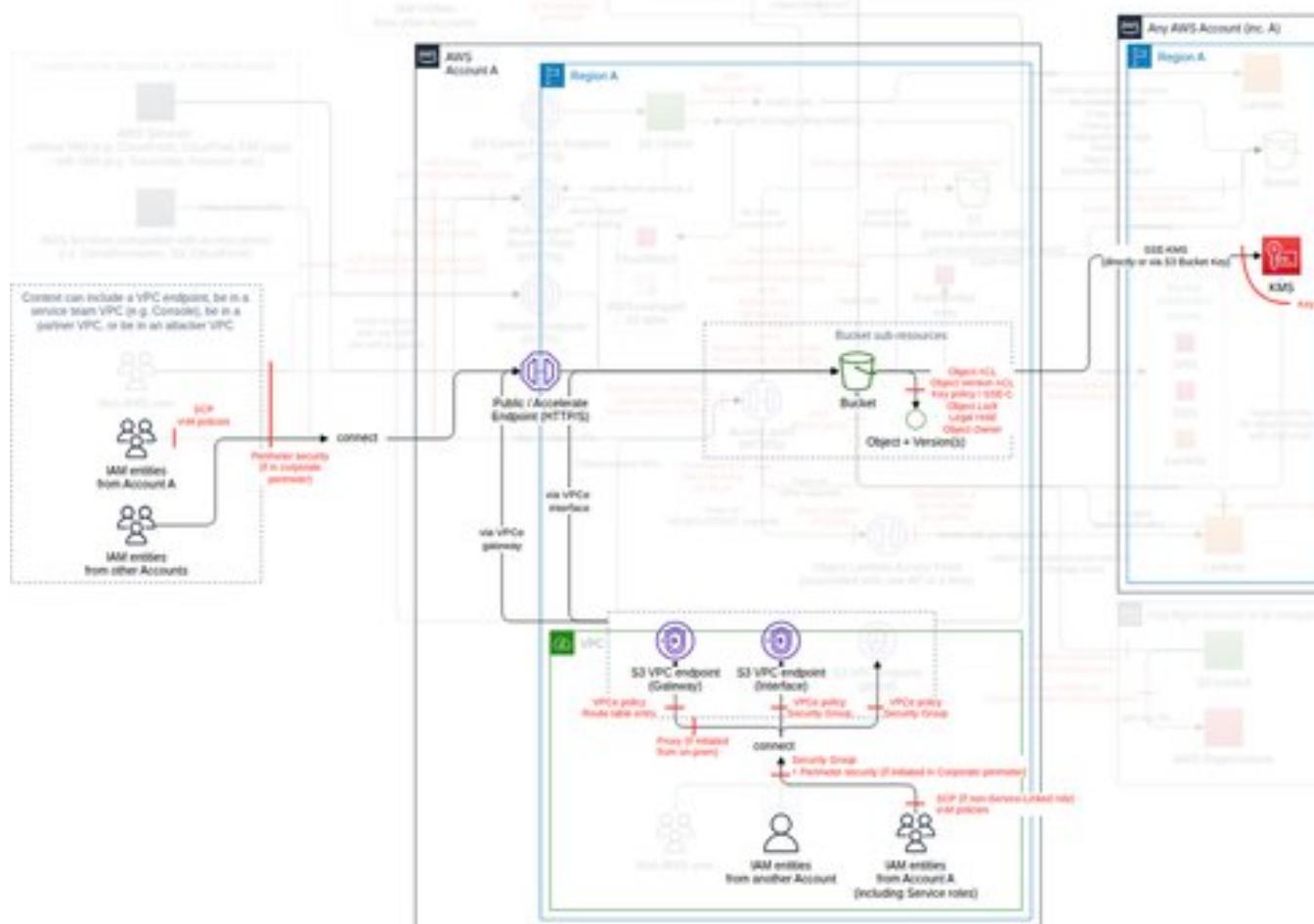


### ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Sets the default encryption configuration for the bucket.	s3:PutEncryptionConfiguration

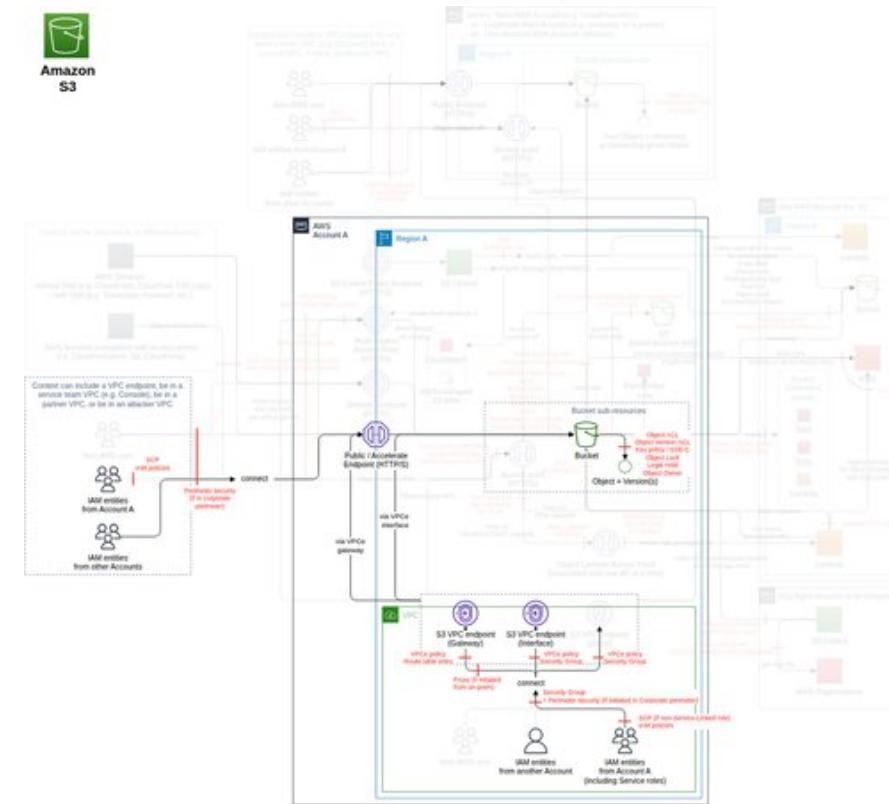
## **Threat List**

Name	CVSS
Disrupting object writes by disabling customer-managed encryption on a bucket using SSE-C	<a href="#">Low (3.5)</a>
Disrupting access by switching the object encryption type or its KMS key	<a href="#">Low (2.9)</a>



## Disrupting object writes by disabling customer-managed encryption on a bucket using SSE-C

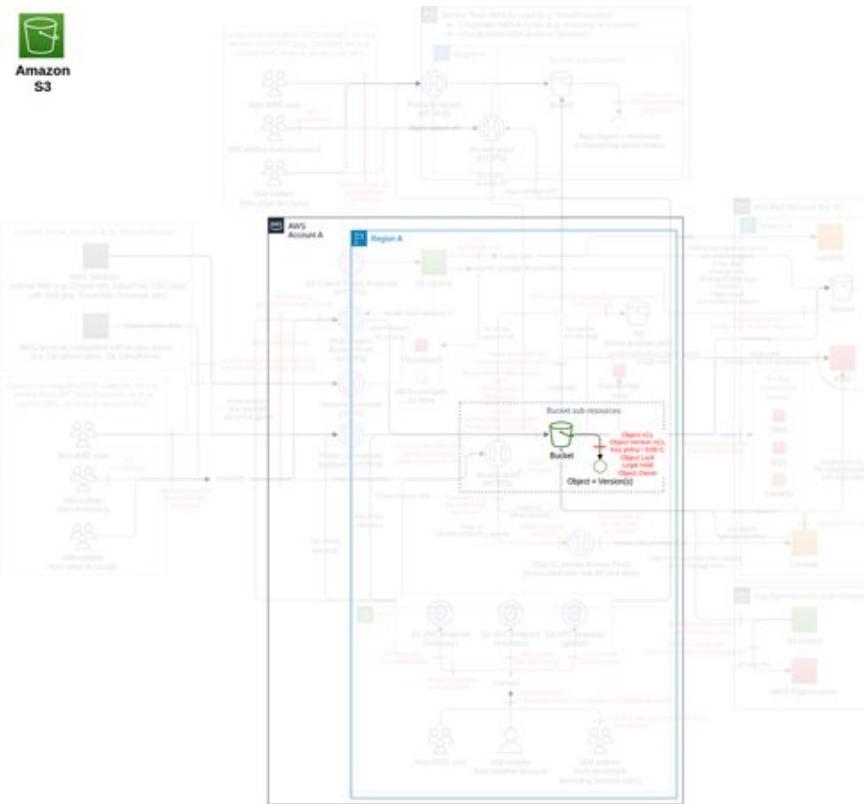
<b>Threat Id</b>	S3.T63
<b>Name</b>	Disrupting object writes by disabling customer-managed encryption on a bucket using SSE-C
<b>Description</b>	Server-side encryption with customer-provided keys [SSE-C] can be blocked on individual general purpose buckets [will be the default from April 2026]. An attacker can change the encryption configuration to disable SSE-C on a bucket using it, resulting in objects failing to be written.
<b>Goal</b>	Disruption of Service
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1531</a>
<b>CVSS</b>	<a href="#">Low (3.5)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutEncryptionConfiguration" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO16 - Enforce encryption at rest</b> C145 - Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C). C167 - Ensure SSE-C is blocked when not required for each bucket [default from April 2026]. C169 - Monitor abnormal increases in the CloudWatch metric for HTTP 4xx client error status code requests (i.e., "4xxErrors").	Very High	2	-	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

## Disrupting access by switching the object encryption type or its KMS key

<b>Threat Id</b>	S3.T65
<b>Name</b>	Disrupting access by switching the object encryption type or its KMS key
<b>Description</b>	An object's encryption type can be changed in some conditions (SSE-S3 to SSE-KMS, or between different KMS keys). The KMS key must be in the same AWS account (via API), or the same AWS Organization (via AWS Support). An attacker can change the encryption type or the KMS key for an object, causing loss of access to the object for applications that do not have permissions to use the new KMS key.
<b>Goal</b>	Disruption of Service
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a>
<b>CVSS</b>	<a href="#">Low (2.9)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:UpdateObjectEncryption" }

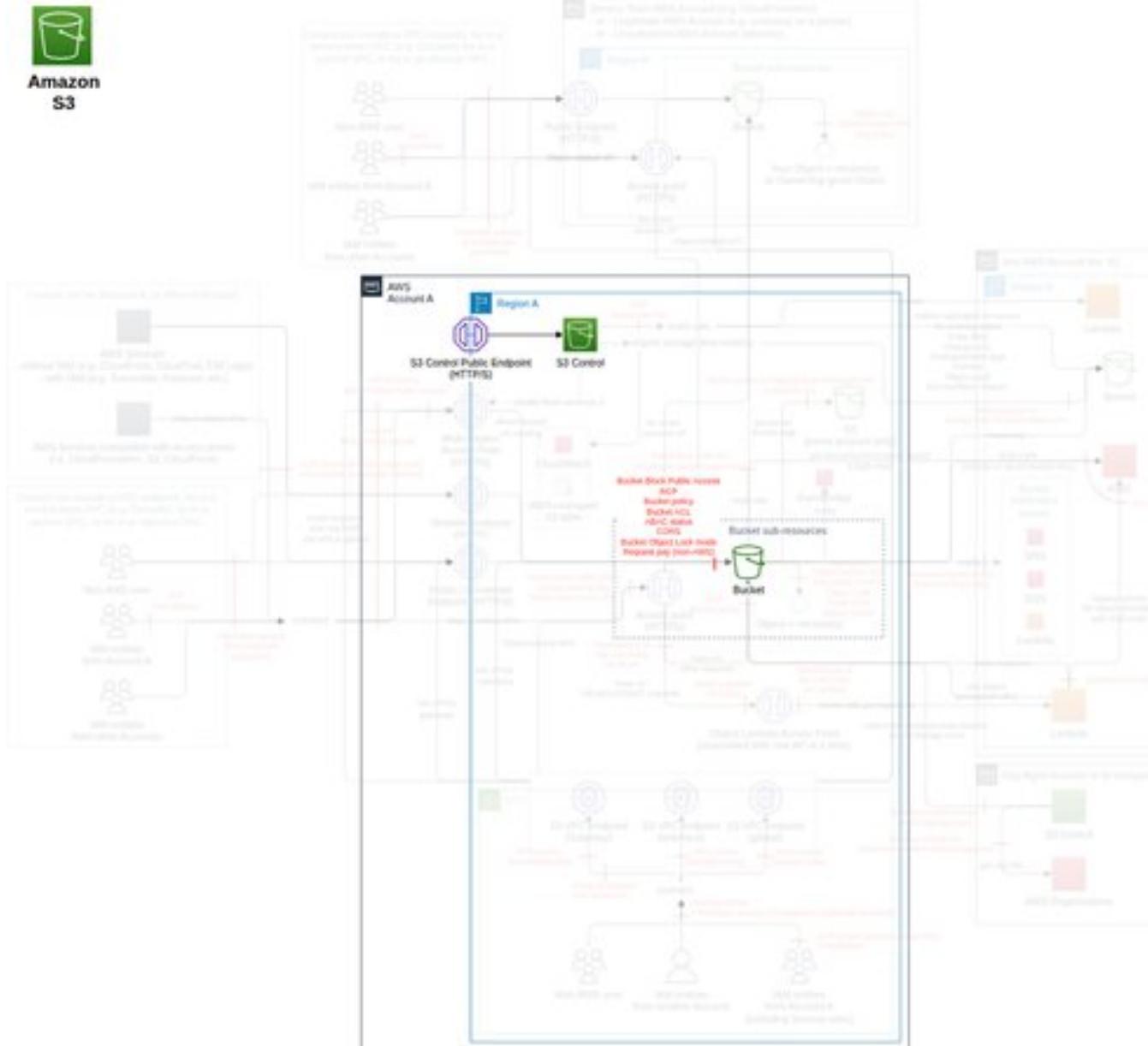


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> <small>C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a>.</small>	Very High	1	-	-
<b>CO16 - Enforce encryption at rest</b> <small>C61 - Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption (<a href="#">ref</a>). C140 - Ensure all objects in S3 buckets are encrypted with an authorized KMS key. C63 - Use KMS ThreatModel to protect the KMS keys used for S3 (e.g., using encryptionContext on the policy of each KMS key).</small>	Very High	3	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> <small>C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.</small>	Medium	2	-	-

# Public Access Block (bucket) (subclass of Bucket, FC24)

S3 Block Public Access (bucket) provides controls at the individual S3 bucket level to ensure objects never have public access.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

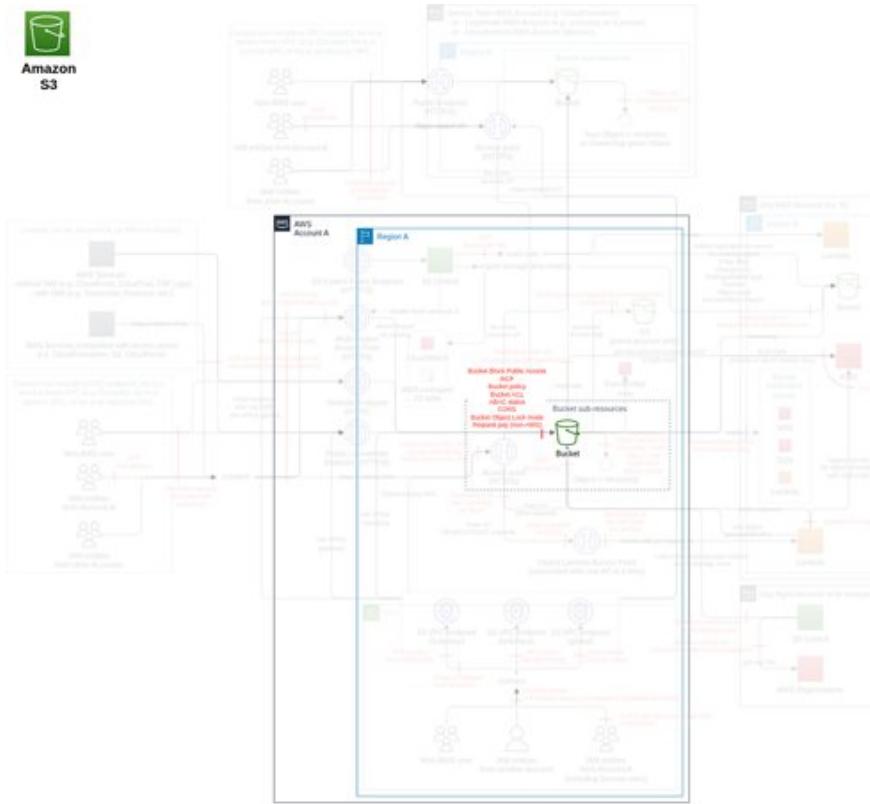
Action	IAM Permission
Creates or modifies the PublicAccessBlock configuration for an Amazon S3 bucket.	s3:PutBucketPublicAccessBlock

## Threat List

Name	CVSS
Reduce bucket security by modifying the bucket's Public Access Block	<a href="#">Medium (4.5)</a>

## Reduce bucket security by modifying the bucket's Public Access Block

<b>Threat Id</b>	S3.T52
<b>Name</b>	Reduce bucket security by modifying the bucket's Public Access Block
<b>Description</b>	Bucket Public Access Block protects individual buckets from leakage (e.g., object ACL set to public). An attacker can remove this protection by modifying the bucket Public Access Block.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (4.5)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketPublicAccessBlock" }

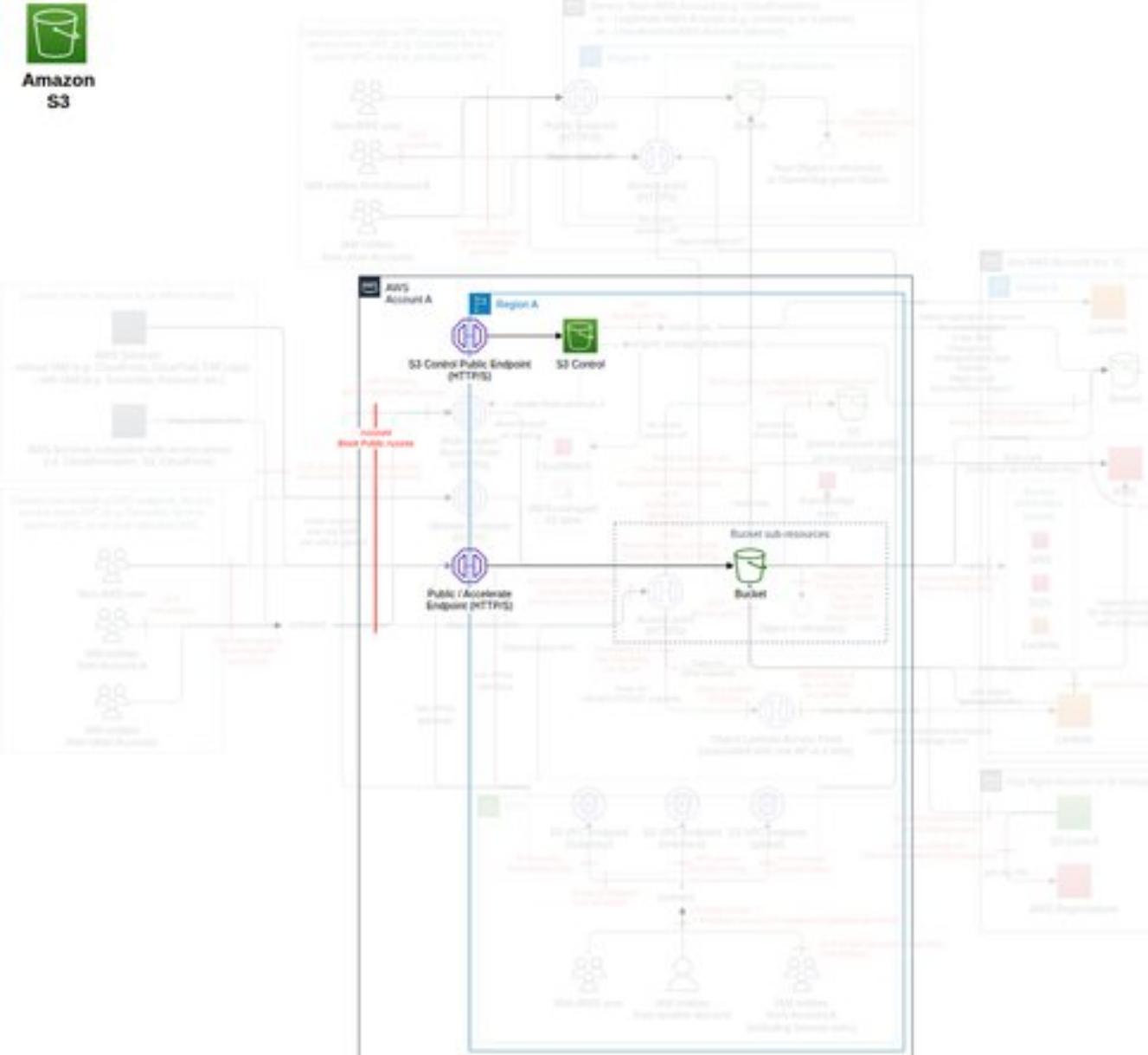


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO37 - Disabling ACLs for all buckets</b> C152 - Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023). C153 - Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3>CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Very High	1	1	-
<b>CO4 - Monitor S3 with Amazon GuardDuty and Macie</b> C10 - Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective).	Medium	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

# Public Access Block (account) (*subclass of Bucket, FC25*)

*S3 Block Public Access (account) provides controls across an entire AWS account to ensure objects never have public access.*

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

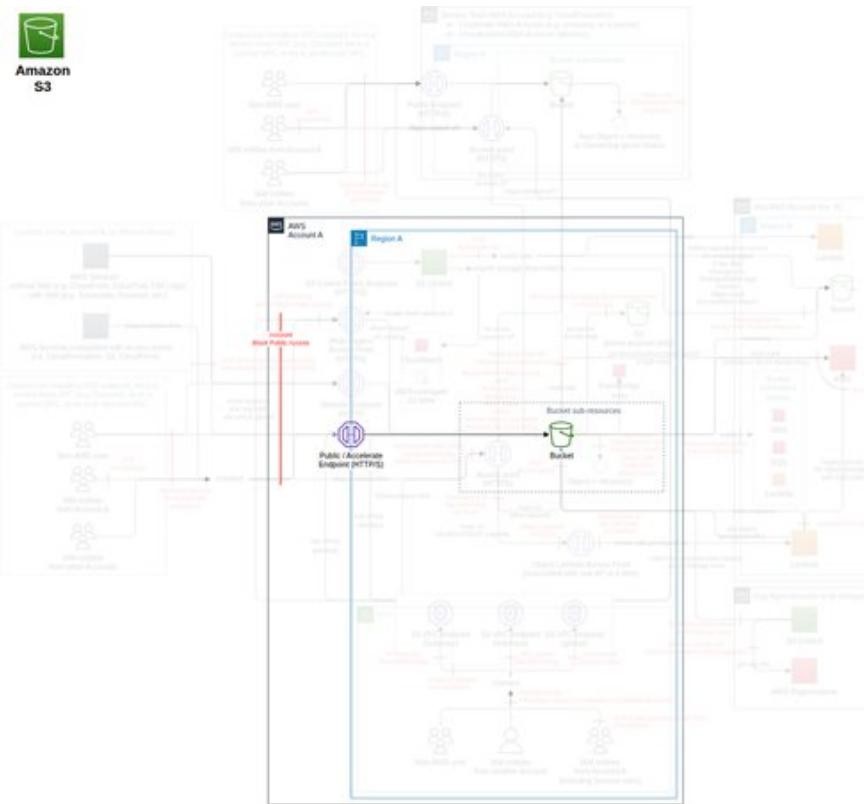
Action	IAM Permission
Creates or modifies the PublicAccessBlock configuration for an AWS account.	s3:PutAccountPublicAccessBlock

## ***Threat List***

Name	CVSS
Reduce bucket security by modifying the account's Public Access Block	<a href="#">Medium (4.5)</a>

## Reduce bucket security by modifying the account's Public Access Block

<b>Threat Id</b>	S3.T53
<b>Name</b>	Reduce bucket security by modifying the account's Public Access Block
<b>Description</b>	Account Public Access Block protects all buckets of an AWS account from leakage (e.g., object ACL set to public). An attacker can remove this protection by modifying the account's Public Access Block.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (4.5)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutAccountPublicAccessBlock" }

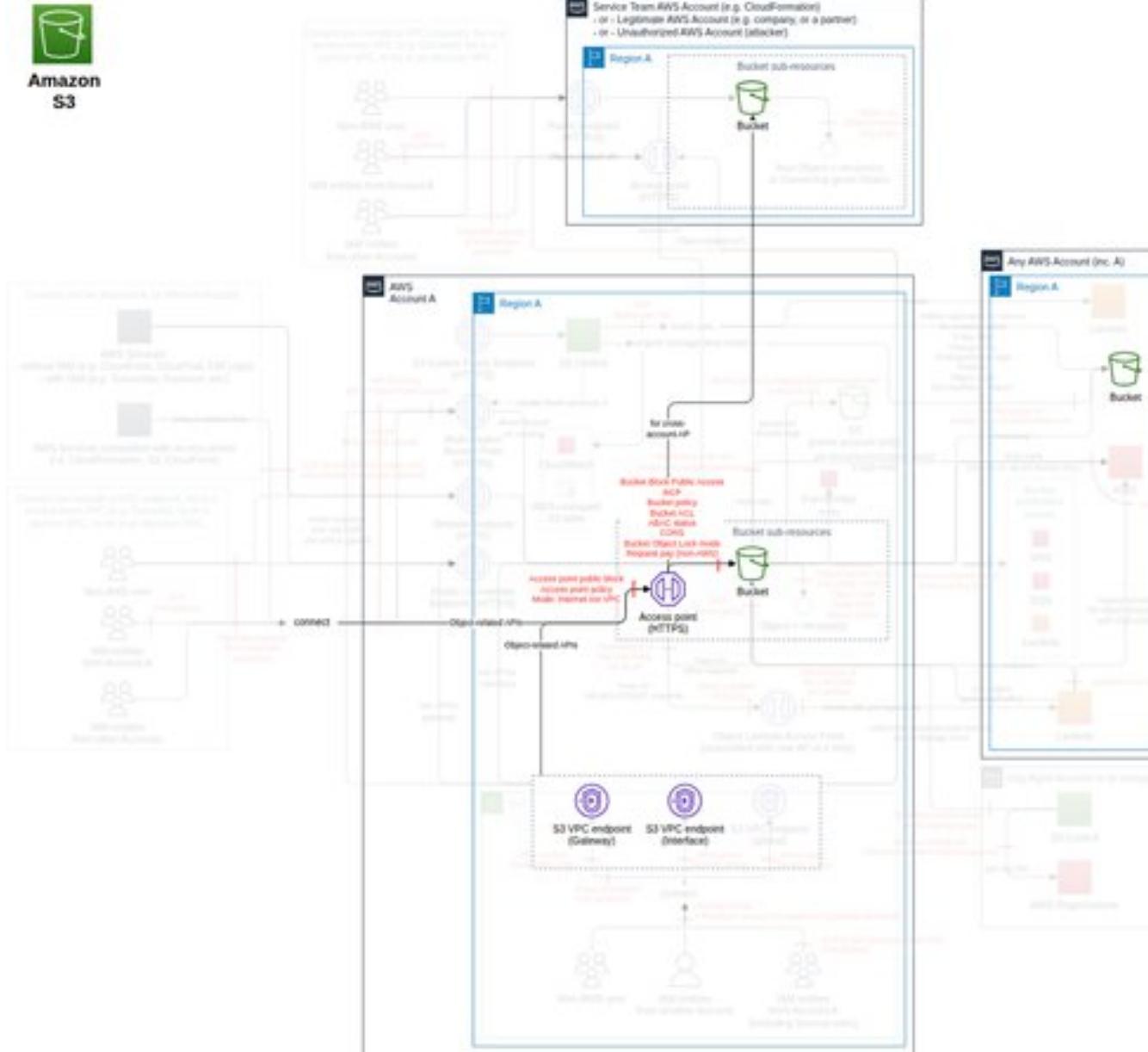


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO37 - Disabling ACLs for all buckets</b> C152 - Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023). C153 - Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3>CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Very High	1	1	-
<b>CO4 - Monitor S3 with Amazon GuardDuty and Macie</b> C10 - Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective).	Medium	1	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

# Access point (subclass of Bucket, FC26)

Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations. Only certain operations and AWS services are compatible ([ref](#)). S3 access points aren't currently compatible with Amazon CloudWatch metrics.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

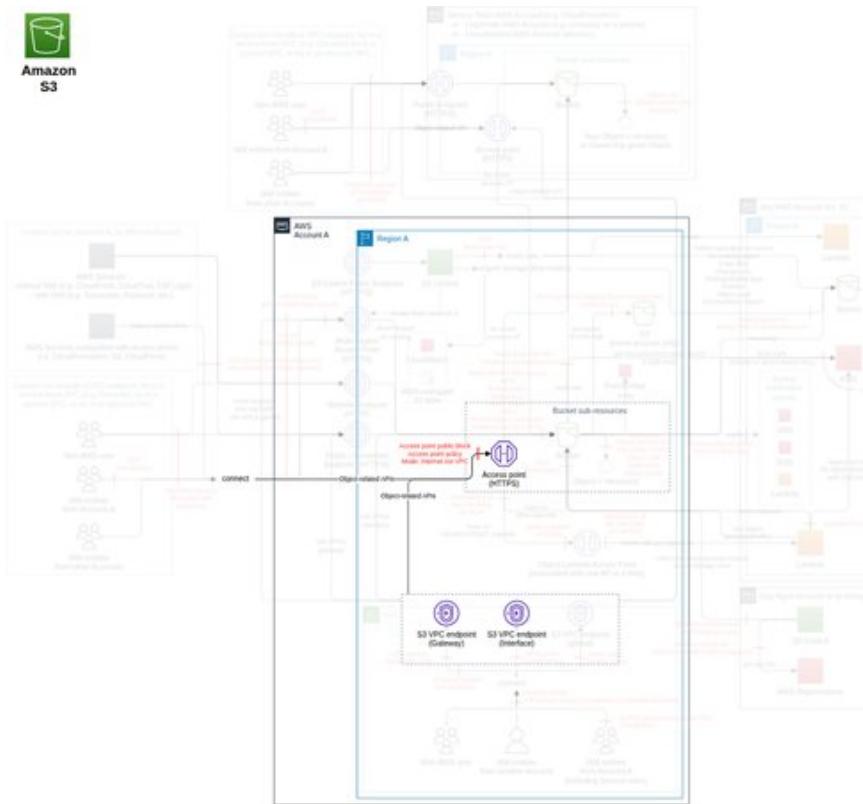
Action	IAM Permission
Creates a new access point.	s3:CreateAccessPoint

## Threat List

Name	CVSS
Grant unauthorized access to a bucket by changing or deleting one of its access points' policies	<a href="#">Medium (6.2)</a>
Unauthorized collection of data by swapping access points	<a href="#">Medium (4.6)</a>
Create an exfiltration vector via cross-account access point	<a href="#">Medium (4.5)</a>

## Grant unauthorized access to a bucket by changing or deleting one of its access points' policies

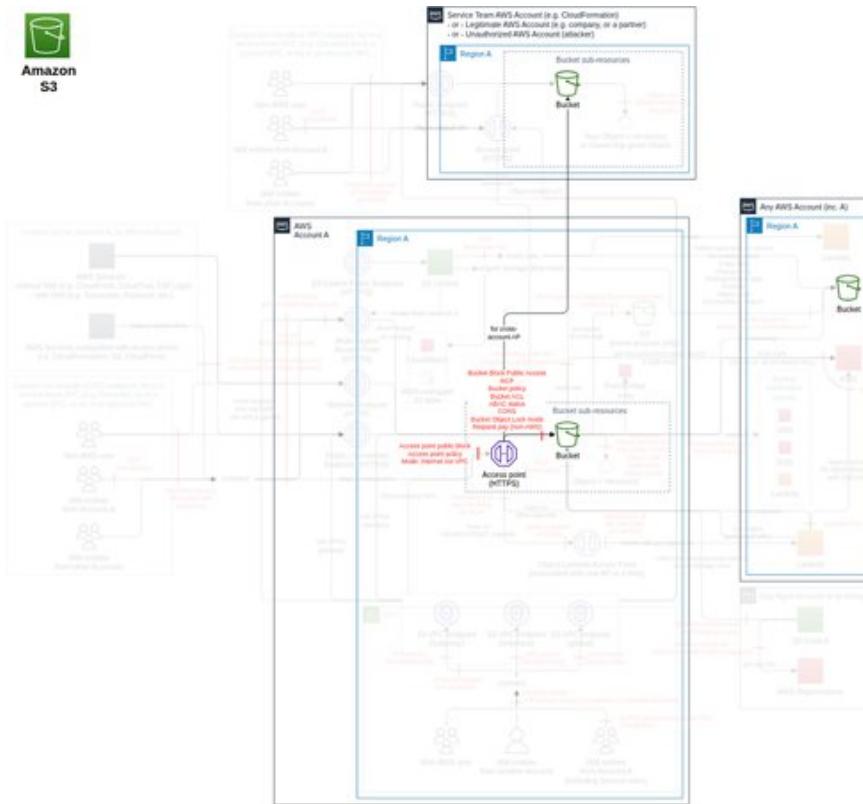
<b>Threat Id</b>	S3.T54
<b>Name</b>	Grant unauthorized access to a bucket by changing or deleting one of its access points' policies
<b>Description</b>	Access point policies can enable access to objects owned by buckets. An attacker (or someone by negligence) can change the access point policy and make the content accessible.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (6.2)</a>
<b>IAM Access</b>	{ "OR": ["s3:PutAccessPointPolicy", "s3>DeleteAccessPointPolicy", "s3:PutAccessPointPublicAccessBlock"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO13 - Block direct public access</b> C53 - Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Very High	1	-	-
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C105 - Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy.	Very High	1	1	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Unauthorized collection of data by swapping access points

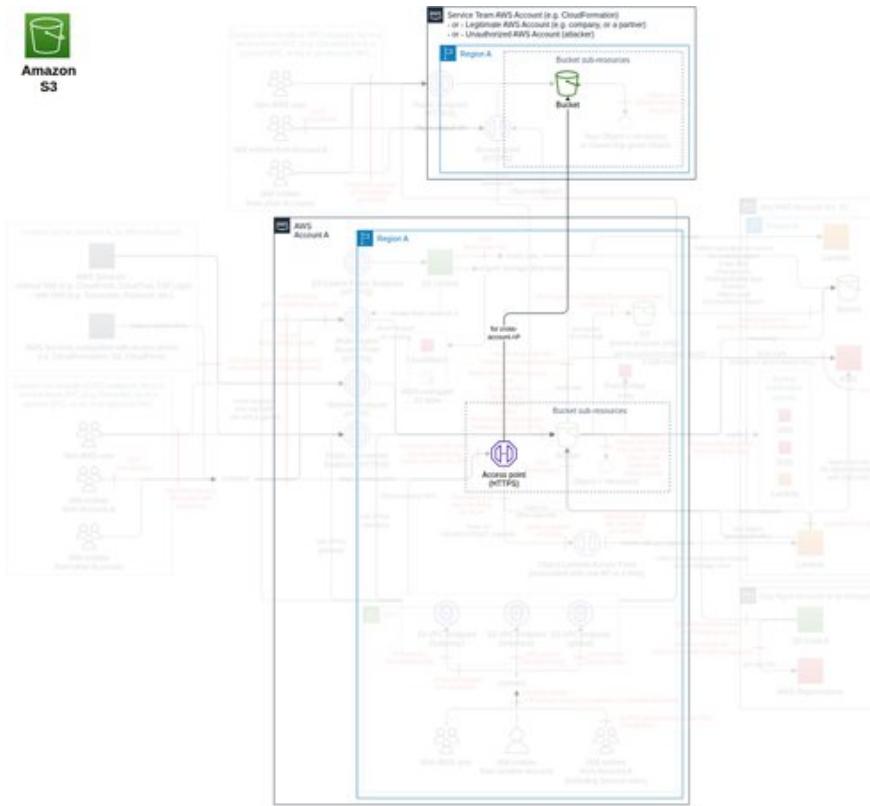
<b>Threat Id</b>	S3.T28
<b>Name</b>	Unauthorized collection of data by swapping access points
<b>Description</b>	Access points can be deleted and recreated with the same name, and therefore the same ARN. An attacker can delete an access point and recreate the same one on a bucket they control to collect/modify data, or make it accessible over the Internet.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1056</a>
<b>CVSS</b>	<a href="#">Medium (4.6)</a>
<b>IAM Access</b>	{ "AND": ["s3>CreateAccessPoint", "s3>DeleteAccessPoint"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C106 - In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn". C107 - Block the creation of non-VPC S3 access point "s3>CreateAccessPoint" (e.g., using IAM policies and SCPs with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}). C108 - Block all traffic from Internet-configured S3 access points (e.g., in their bucket policy, or centrally in an RCP applied to the OU or AWS account, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Very High	1	3	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

## Create an exfiltration vector via cross-account access point

<b>Threat Id</b>	S3.T60
<b>Name</b>	Create an exfiltration vector via cross-account access point
<b>Description</b>	Access points from a given AWS account can be connected to a cross-account bucket. An attacker can create an access point connected to a bucket they control to exfiltrate data.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010, T1537</a>
<b>CVSS</b>	<a href="#">Medium (4.5)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:CreateAccessPoint" }

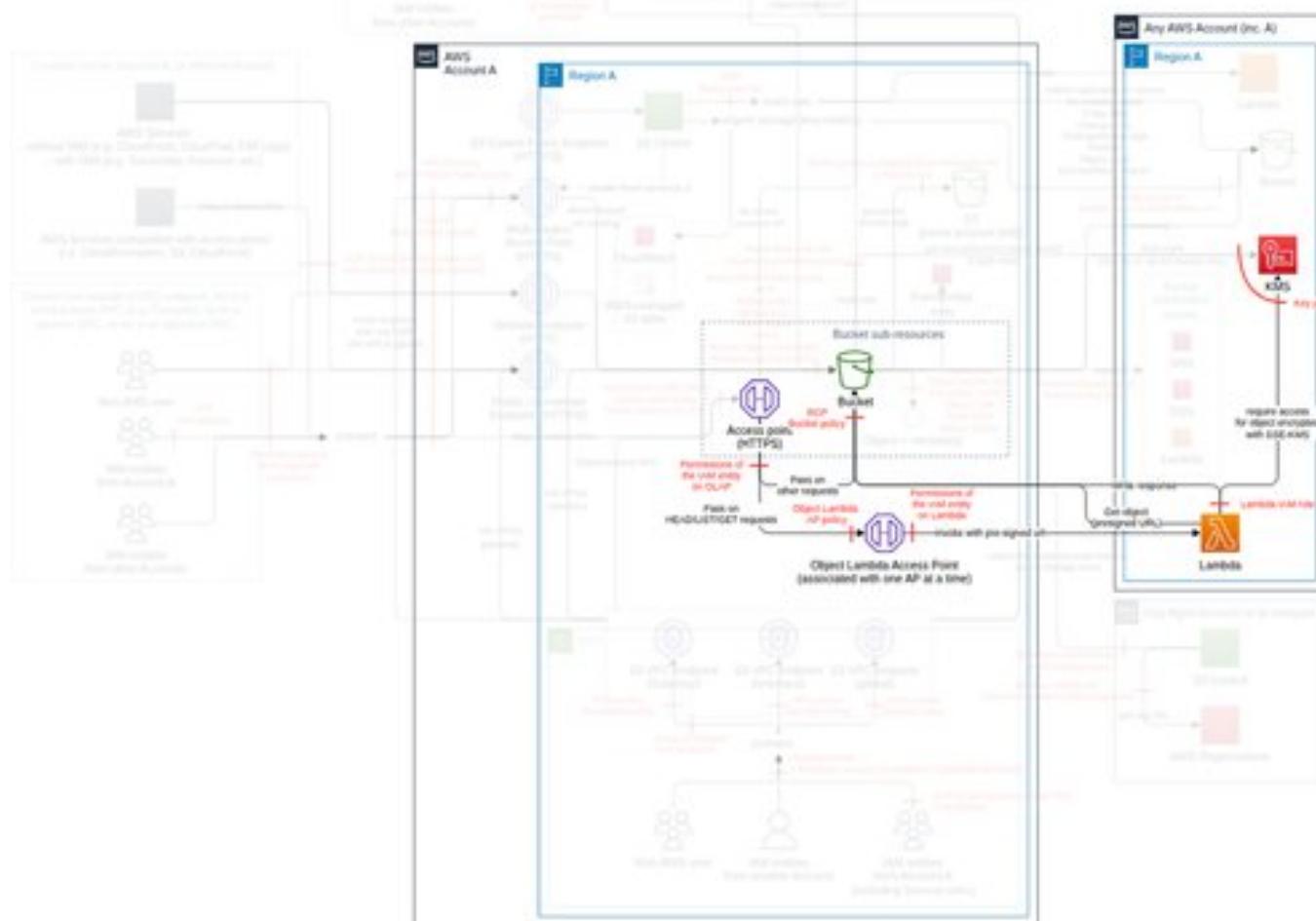
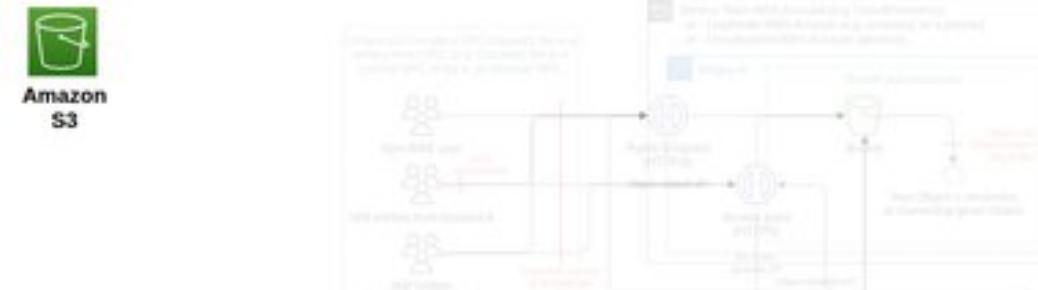


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C106 - In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn". C107 - Block the creation of non-VPC S3 access point "s3:CreateAccessPoint" (e.g., using IAM policies and SCPs with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Very High	1	2	-
<b>CO9 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account).	Very High	1	1	-
<b>CO40 - Restrict access points to authorized AWS accounts</b> C158 - Maintain a list of authorized S3 buckets and their AWS accounts for cross-account access points. C159 - Ensure only authorized S3 buckets and their AWS accounts for cross-account access points are configured. C160 - Monitor CreateAccessPoint to detect unauthorized buckets or AWS accounts (i.e., using CloudTrail event CreateAccessPoint and its fields "requestParameters.CreateAccessPointRequest.Bucket" and "requestParameters.CreateAccessPointRequest.BucketAccountId").	High	2	-	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

# S3 Object Lambda (subclass of Access point, FC32)

S3 Object Lambda enables users to apply their custom code to process the output of a standard S3 request by automatically invoking a Lambda function.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

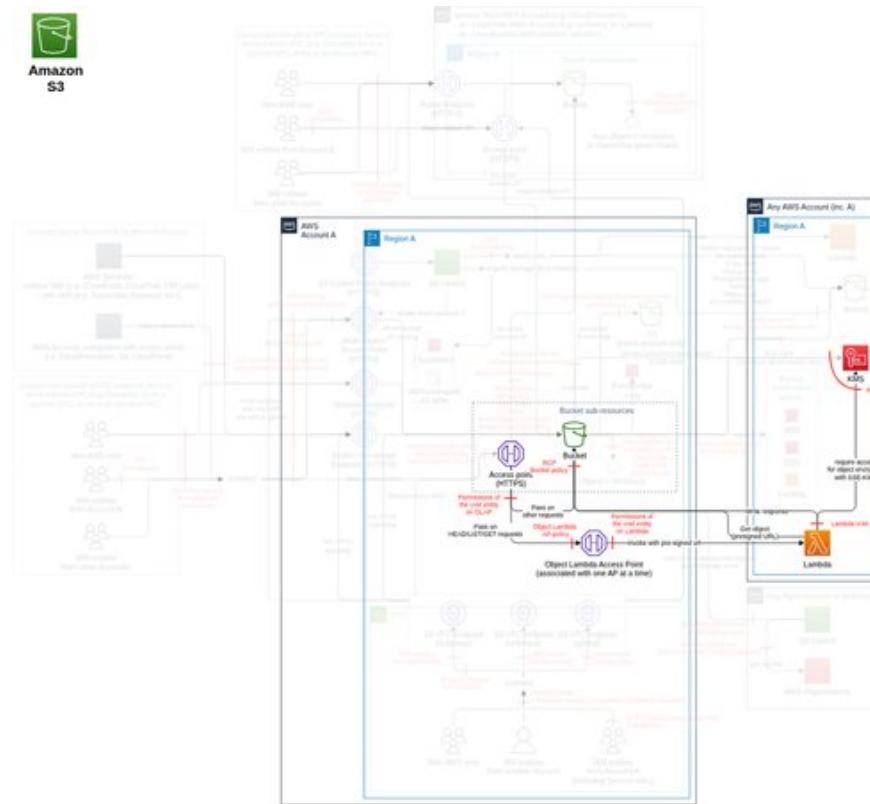
Action	IAM Permission
Creates an Object Lambda Access Point.	s3:CreateAccessPointForObjectLambda
Grants permission to retrieve objects from Amazon S3.	s3-object-lambda:GetObject
Grants permission to add an object to a bucket.	s3-object-lambda:PutObject

## Threat List

Name	CVSS
Hijack a connection with an Object Lambda	<a href="#">Medium (5.7)</a>

## Hijack a connection with an Object Lambda

<b>Threat Id</b>	S3.T46
<b>Name</b>	Hijack a connection with an Object Lambda
<b>Description</b>	Object Lambda is invoked between the access point and the object. An attacker can configure a Lambda to modify, snoop, or exfiltrate data.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1020</a>
<b>CVSS</b>	<a href="#">Medium (5.7)</a>
<b>IAM Access</b>	{ "OR": ["s3>CreateAccessPointForObjectLambda", "s3:PutAccessPointConfigurationForObjectLambda"] }

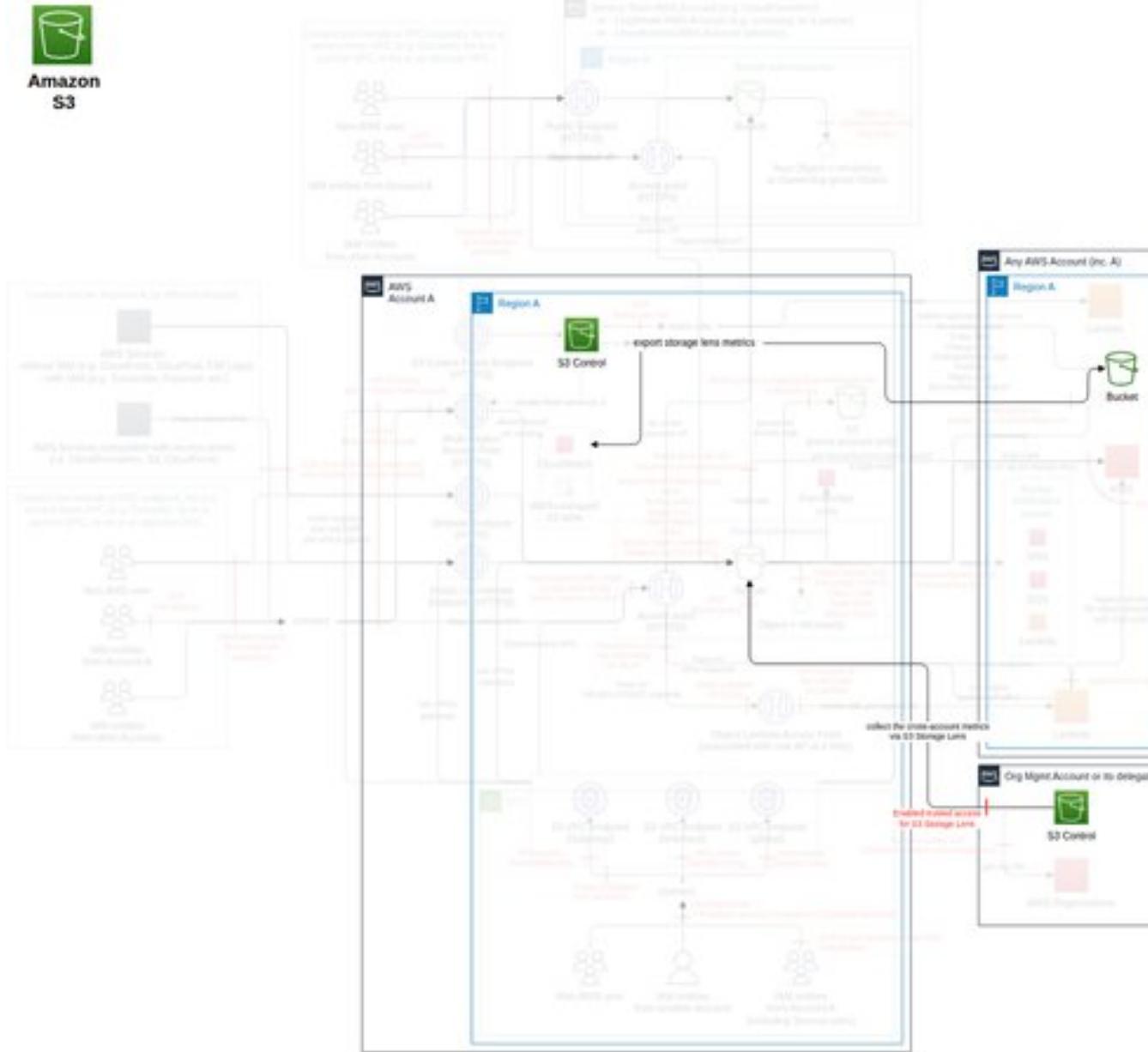


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO34 - Enforce only authorized Object Lambda Access Point and associated access</b> C125 - Maintain a list of authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload. C126 - Ensure only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload are created. C128 - Ensure Lambda functions configured on Object Lambda Access Point are secured using Lambda ThreatModel. C129 - Maintain a list of cross-account access on each Object Lambda Access Point. C130 - Ensure only authorized cross-account IAM entities are allowed in the Object Lambda Access Point policy. C132 - Ensure CloudWatch is enabled for all Object Lambda Access Points.	Very High	6	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

# S3 Storage Lens (*subclass of Bucket, FC31*)

*S3 Storage Lens provides a single view of object storage use and activity across your entire S3 storage.*

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Puts an Amazon S3 Storage Lens configuration.	s3:PutStorageLensConfiguration

## ***Threat List***

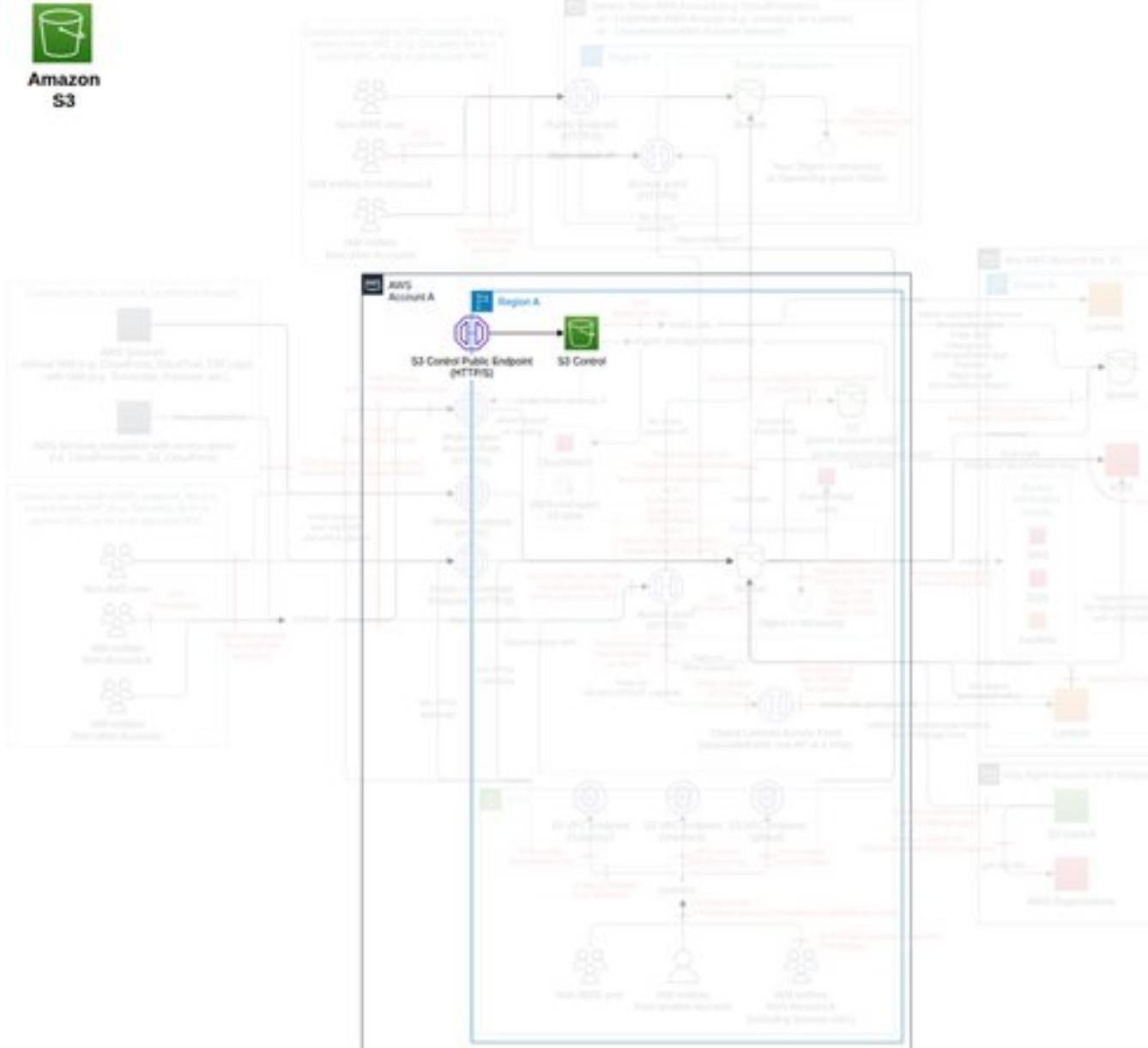
Name	CVSS
None	None

# Tagging (for Storage Lens group only) (subclass of S3)

Storage Lens, FC34)

When you configure your Storage Lens group, you can optionally add AWS resource tags to the group.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

Action	IAM Permission
Add tags to the specified resource.	s3:TagResource

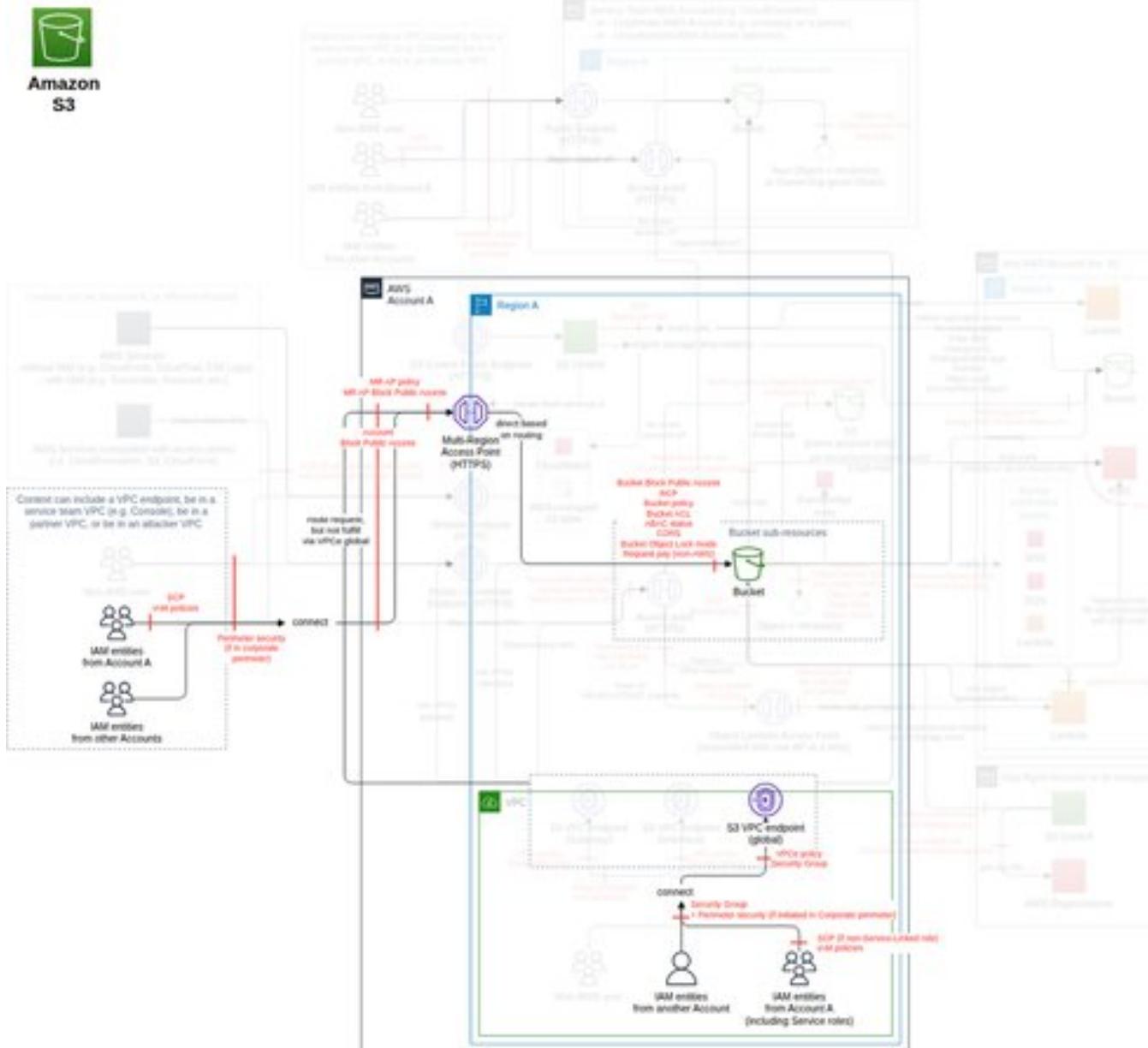
## Threat List

Name	CVSS
None	None

# Multi-Region Access Points (*subclass of Bucket, FC33*)

*S3 Multi-Region Access Points provide a single global endpoint to access a dataset that spans multiple S3 buckets in different AWS Regions or in different AWS accounts.*

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

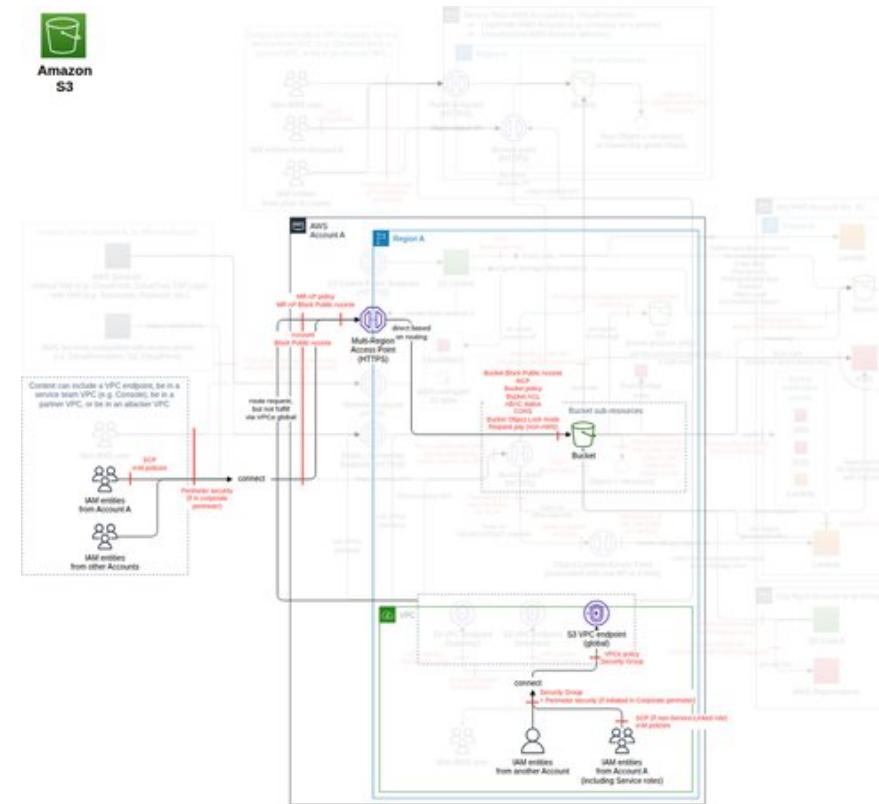
Action	IAM Permission
Creates a Multi-Region Access Point and associates it with the specified buckets.	s3>CreateMultiRegionAccessPoint
Submit a route configuration update for a Multi-Region Access Point.	s3:SubmitMultiRegionAccessPointRoutes

## ***Threat List***

Name	CVSS
Grant unauthorized access to buckets by changing the Multi-Region Access Point policy	<a href="#">Medium (6.2)</a>
Gain unauthorized access to buckets trusting all Multi-Region Access Points	<a href="#">Medium (5.7)</a>

## Grant unauthorized access to buckets by changing the Multi-Region Access Point policy

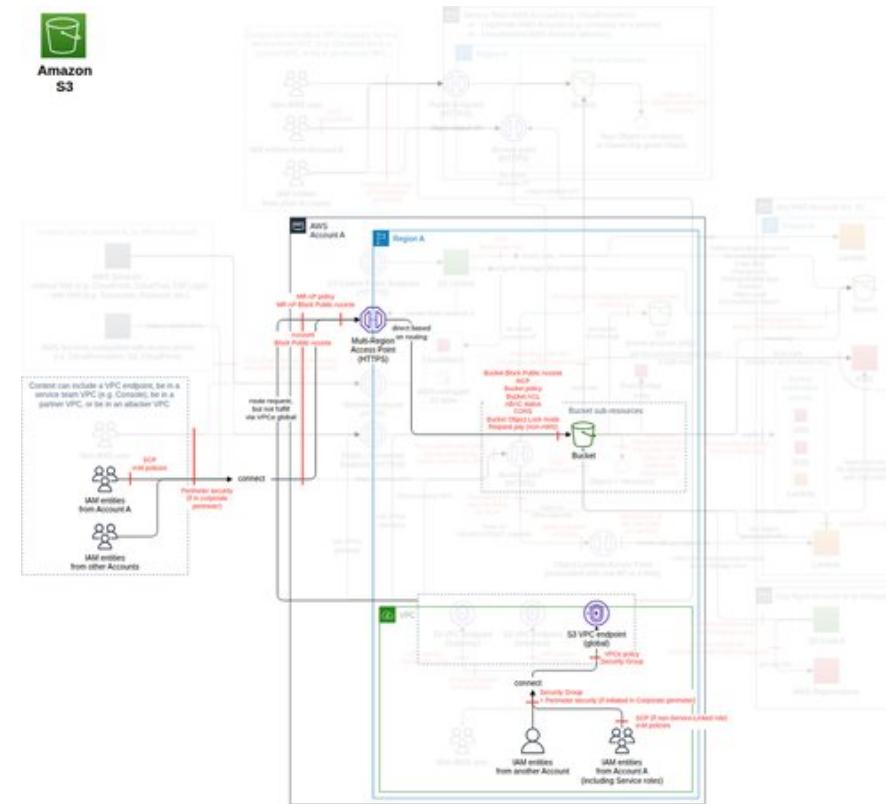
<b>Threat Id</b>	S3.T55
<b>Name</b>	Grant unauthorized access to buckets by changing the Multi-Region Access Point policy
<b>Description</b>	Multi-Region Access Point policy can enable access to objects owned by the bucket. An attacker (or someone by negligence) can change the Multi-Region Access Point policy and make the content accessible.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0005</a> , <a href="#">T1562</a>
<b>CVSS</b>	<a href="#">Medium (6.2)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutMultiRegionAccessPointPolicy" }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO13 - Block direct public access</b> C53 - Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Very High	1	-	-
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C105 - Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy. C106 - In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn".	Very High	1	2	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Gain unauthorized access to buckets trusting all Multi-Region Access Points

<b>Threat Id</b>	S3.T56
<b>Name</b>	Gain unauthorized access to buckets trusting all Multi-Region Access Points
<b>Description</b>	Buckets used by Multi-Region Access Points can be configured to delegate their access to any MRAP using the condition "s3:DataAccessPointAccount". An attacker can create an MRAP, add any misconfigured bucket, and gain access to it.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1530</a>
<b>CVSS</b>	<a href="#">Medium (5.7)</a>
<b>IAM Access</b>	{ "AND": ["s3>CreateMultiRegionAccessPoint", "s3:PutMultiRegionAccessPointPolicy"] }

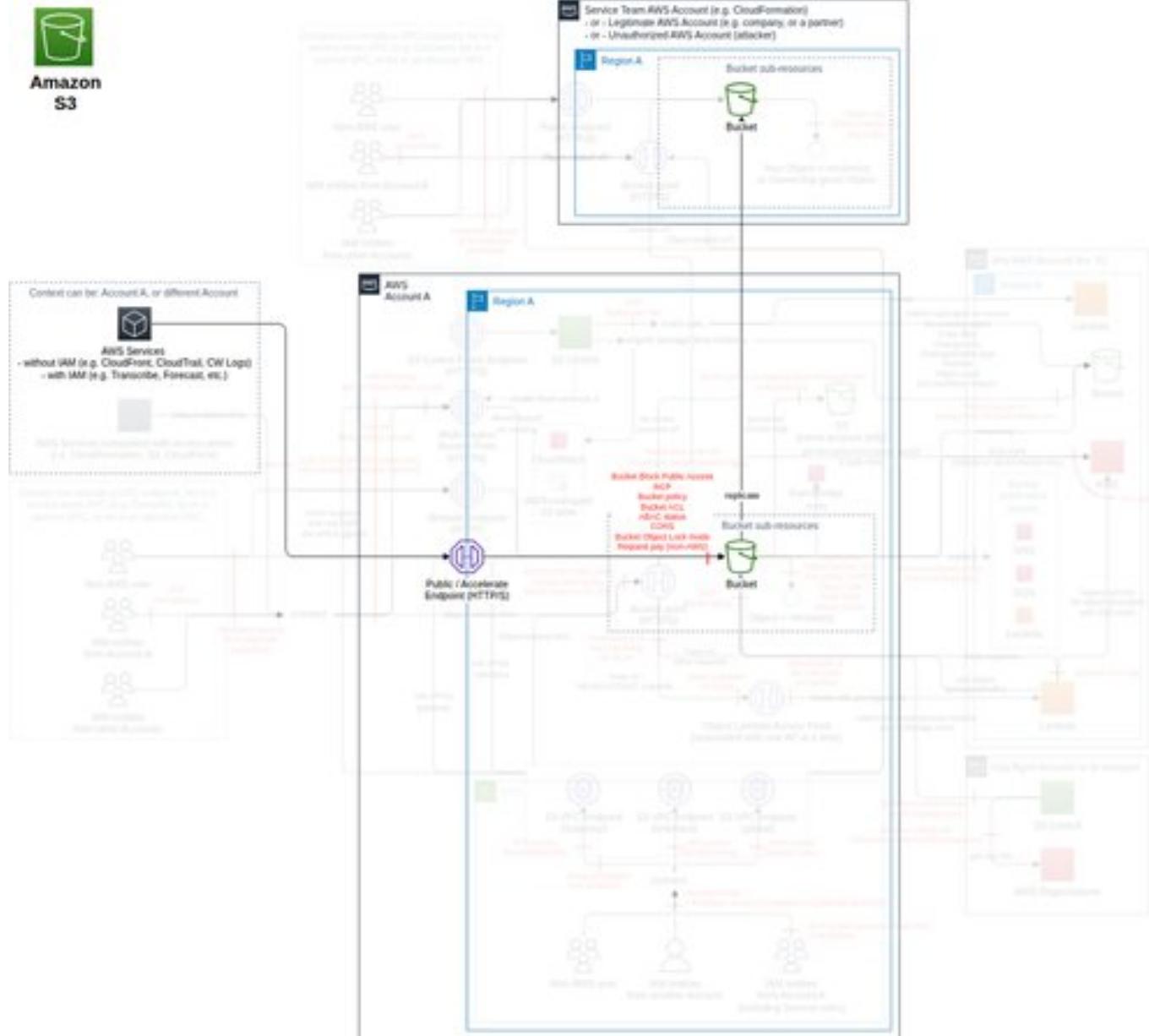


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C106 - In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn".	Very High	1	1	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

## FIS actions (*subclass of Bucket, FC35*)

In AWS Fault Injection Service, the action `aws:s3:bucket-pause-replication` can pause S3 replication from the experiment AWS Region to the destination AWS Region for the targeted buckets. Review FIS ThreatModel for more information.

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Pause S3 replication from target source buckets to destination buckets (used by AWS FIS only).	s3:PauseReplication

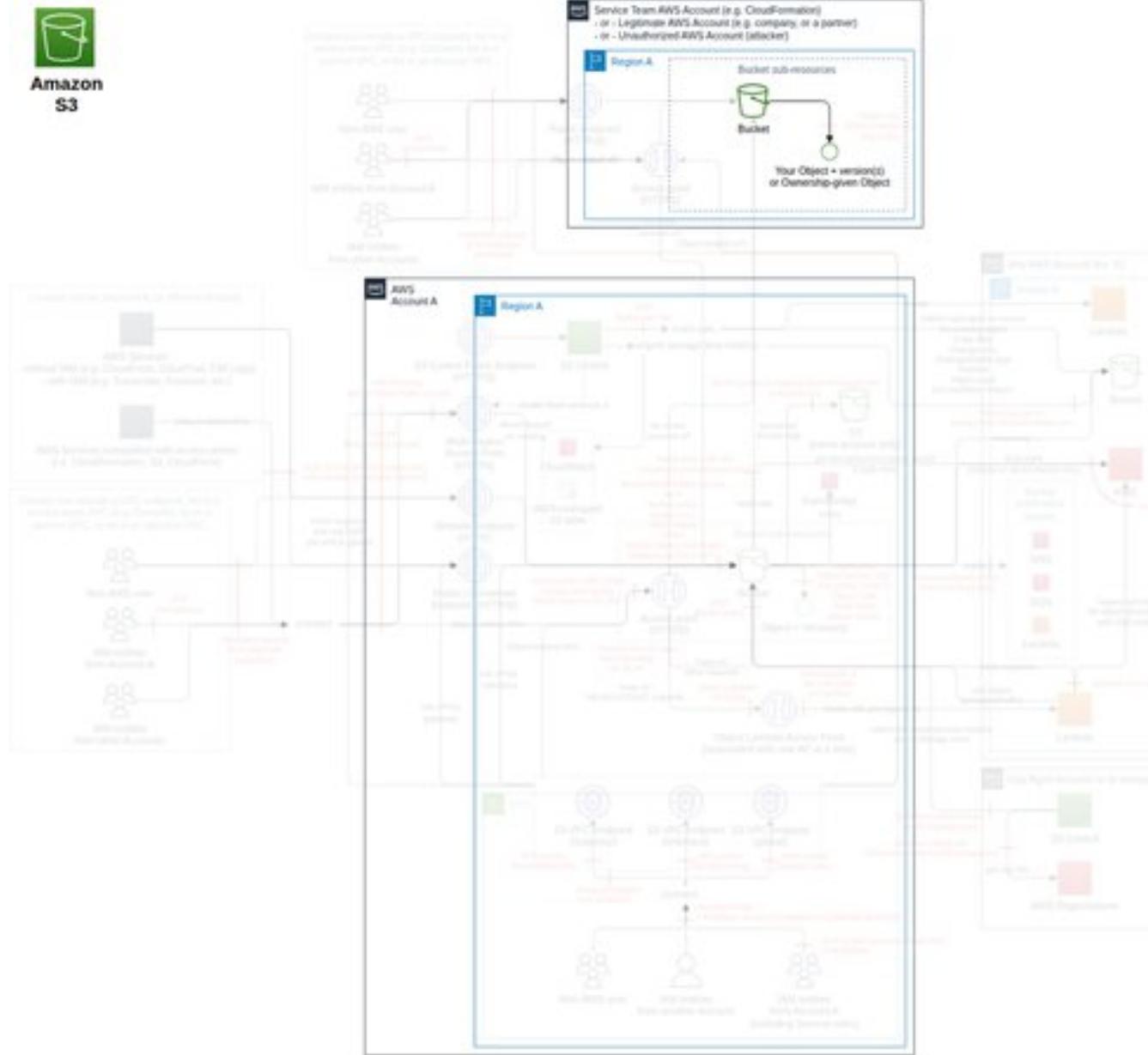
## ***Threat List***

Name	CVSS
None	None

# S3 Object Ownership (subclass of Bucket, used by Object operations, FC30)

Enables bucket owners to automatically assume ownership of objects uploaded to their buckets by other AWS accounts. When an object is put with an ACL of "bucket-owner-full-control", the object will be fully owned by the target bucket owner. If the ACL is added later, ownership is retained by the object owner ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

Action	IAM Permission
Creates or modifies OwnershipControls for an Amazon S3 bucket.	s3:PutBucketOwnershipControls

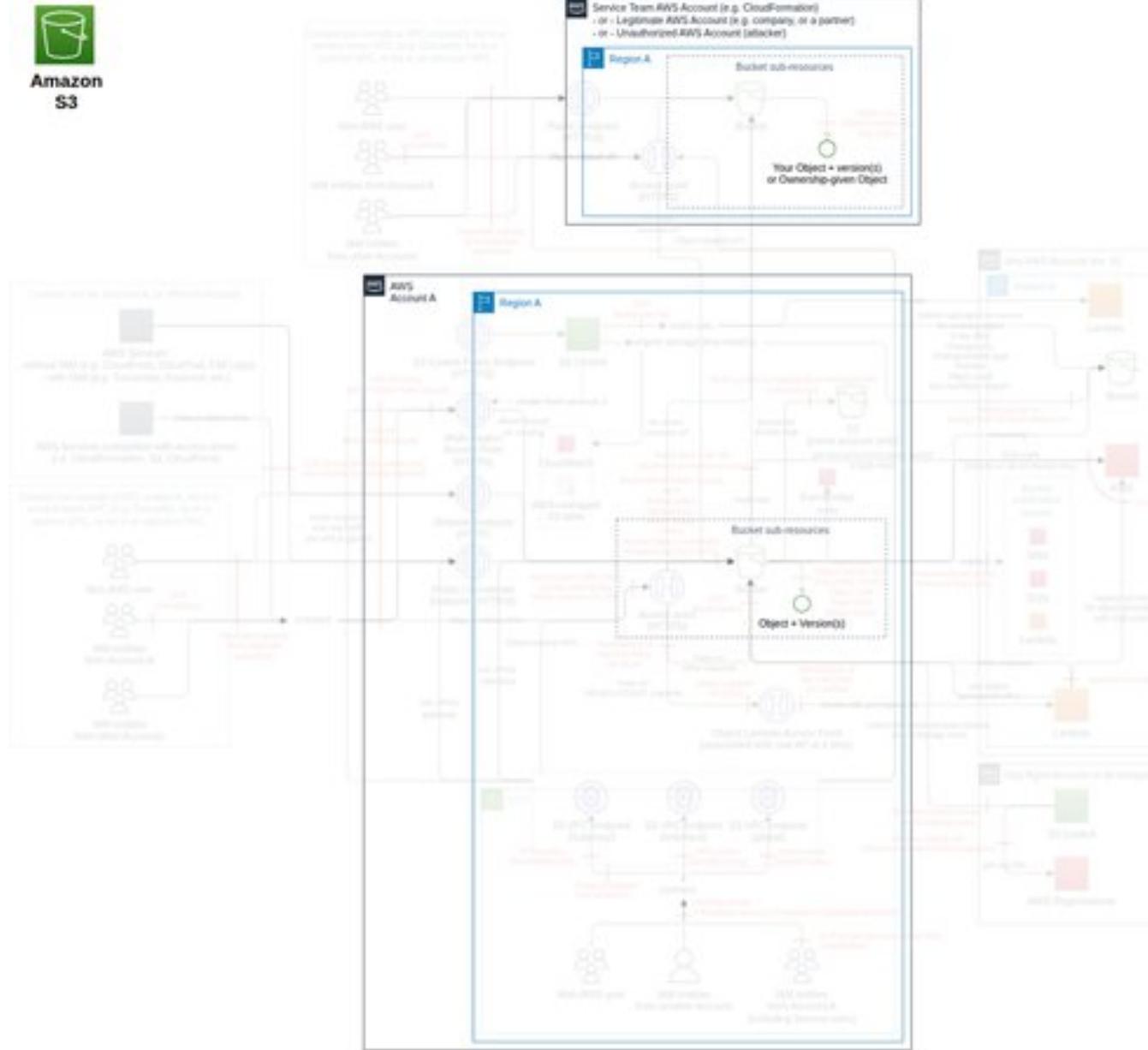
## Threat List

Name	CVSS
None	None

# Object tagging (subclass of Object operations, used by Bucket, FC2)

You can tag objects ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

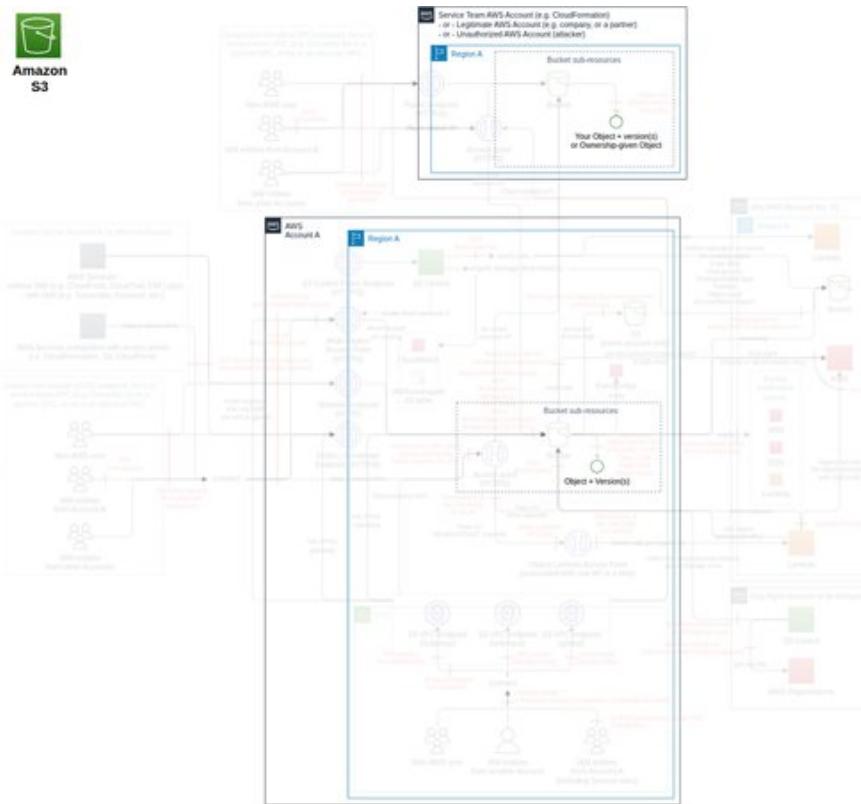
Action	IAM Permission
Adds a set of tags to an existing object.	s3:PutObjectTagging

## Threat List

Name	CVSS
Gain access by modifying or deleting important object tags	<a href="#">Medium (4.4)</a>

## Gain access by modifying or deleting important object tags

<b>Threat Id</b>	S3.T33
<b>Name</b>	Gain access by modifying or deleting important object tags
<b>Description</b>	Tags can be used for various reasons, including security classification or access management (via ABAC). An attacker can change the tagging of an object to another value, enabling them to execute another attack.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0004</a> , <a href="#">T1548</a>
<b>CVSS</b>	<a href="#">Medium (4.4)</a>
<b>IAM Access</b>	{ "OR": ["s3:PutObjectTagging", "s3>DeleteObjectTagging"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b> <small>C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a>.</small>	Very High	1	-	-
<b>CO29 - Limit access from only authorized VPCs</b> <small>C98 - For each S3 bucket, maintain a list of VPCs authorized to access it. C99 - Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).</small>	Very High	1	1	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> <small>C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account. C170 - Integrate and limit the access to general purpose buckets via tags in the IAM Operating Model (including enforcing tagging of buckets and objects at creation using AWS:ResourceTag and s3:BucketTag).</small>	High	3	-	-

# Attribute-based access control (ABAC) for general purpose buckets (subclass of Object tagging/Bucket, FC36)

FC36)

*ABAC for general purpose buckets is an Amazon S3 feature that allows access decisions to be made based on matching attributes such as tags between IAM principals and S3 buckets.*

## ***Data Flow Diagram (DFD)***

## ***Actions and IAM Permissions to deny the feature***

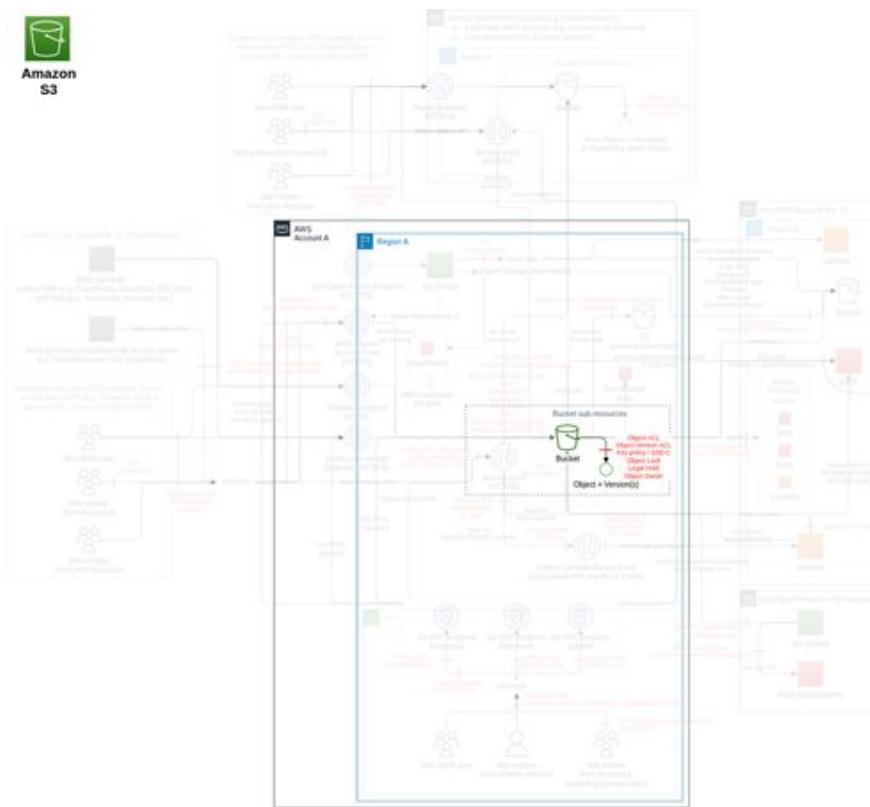
Action	IAM Permission
Set ABAC configuration for a general purpose bucket.	s3:PutBucketAbac

## **Threat List**

Name	CVSS
Privilege escalation by enabling ABAC on general purpose buckets	<a href="#">Medium (5.9)</a>

## Privilege escalation by enabling ABAC on general purpose buckets

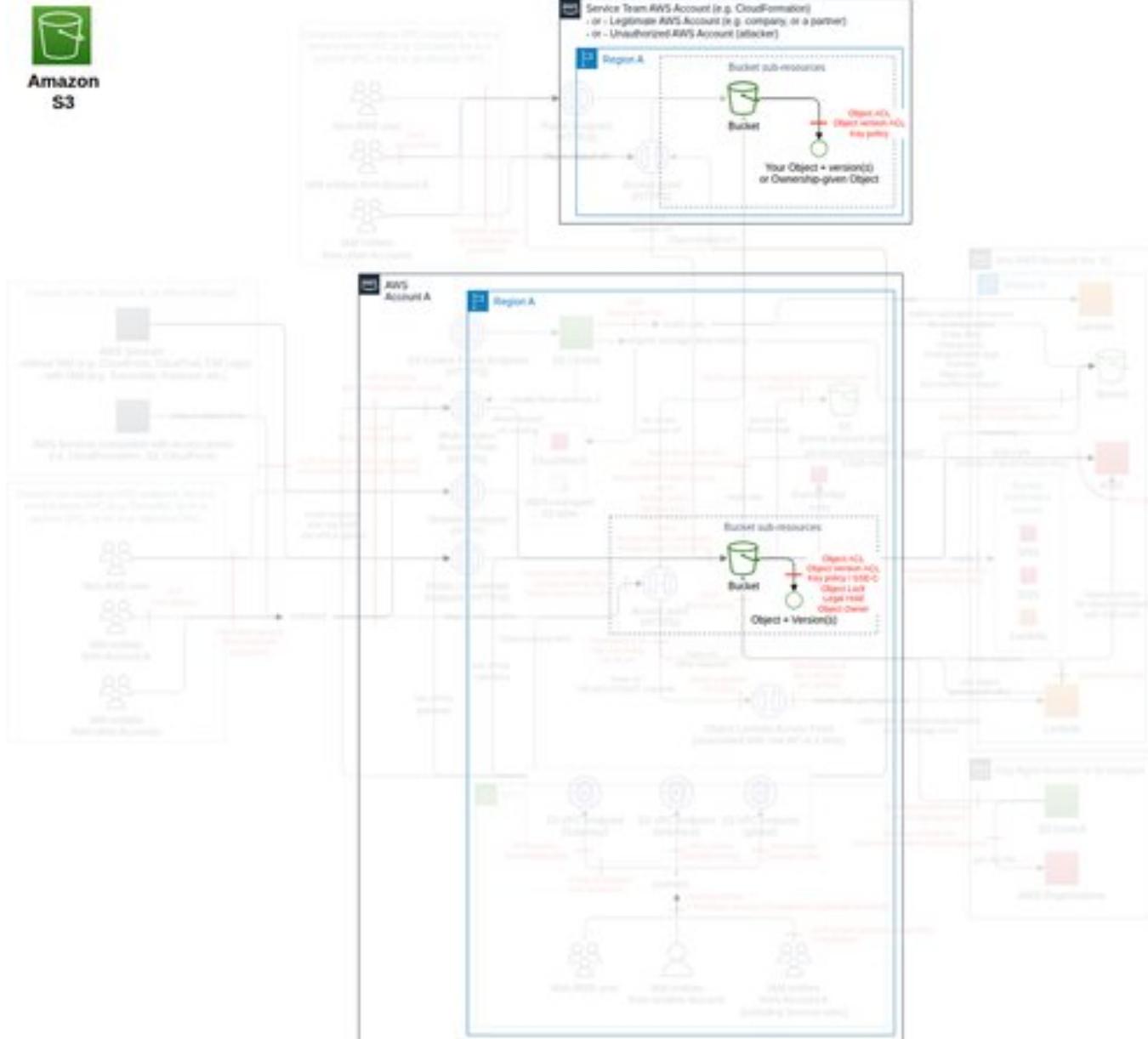
<b>Threat Id</b>	S3.T64
<b>Name</b>	Privilege escalation by enabling ABAC on general purpose buckets
<b>Description</b>	ABAC allows access to be managed by tags on general purpose buckets (disabled by default). An attacker can enable ABAC on a general purpose bucket that was previously not managed through it, allowing for some policy combinations to escalate privileges on the bucket and its objects.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0004</a>
<b>CVSS</b>	<a href="#">Medium (5.9)</a>
<b>IAM Access</b>	{ "AND": ["s3:PutBucketAbac", { "OPTIONAL": "s3:GetBucketAbac" }] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO15 - Identify and ensure the protection of all internal buckets hosting your objects</b>  C58 - Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> . C171 - Ensure only the authorized ABAC configuration for each general purpose bucket is configured.	Very High	2	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

**Object versioning** (*subclass of Object operations, used by Bucket, FC3*)  
 You can version your objects ([ref](#)).

### Data Flow Diagram (DFD)



### Actions and IAM Permissions to deny the feature

Action	IAM Permission
Retrieves an object version from Amazon S3.	s3:GetObjectVersion

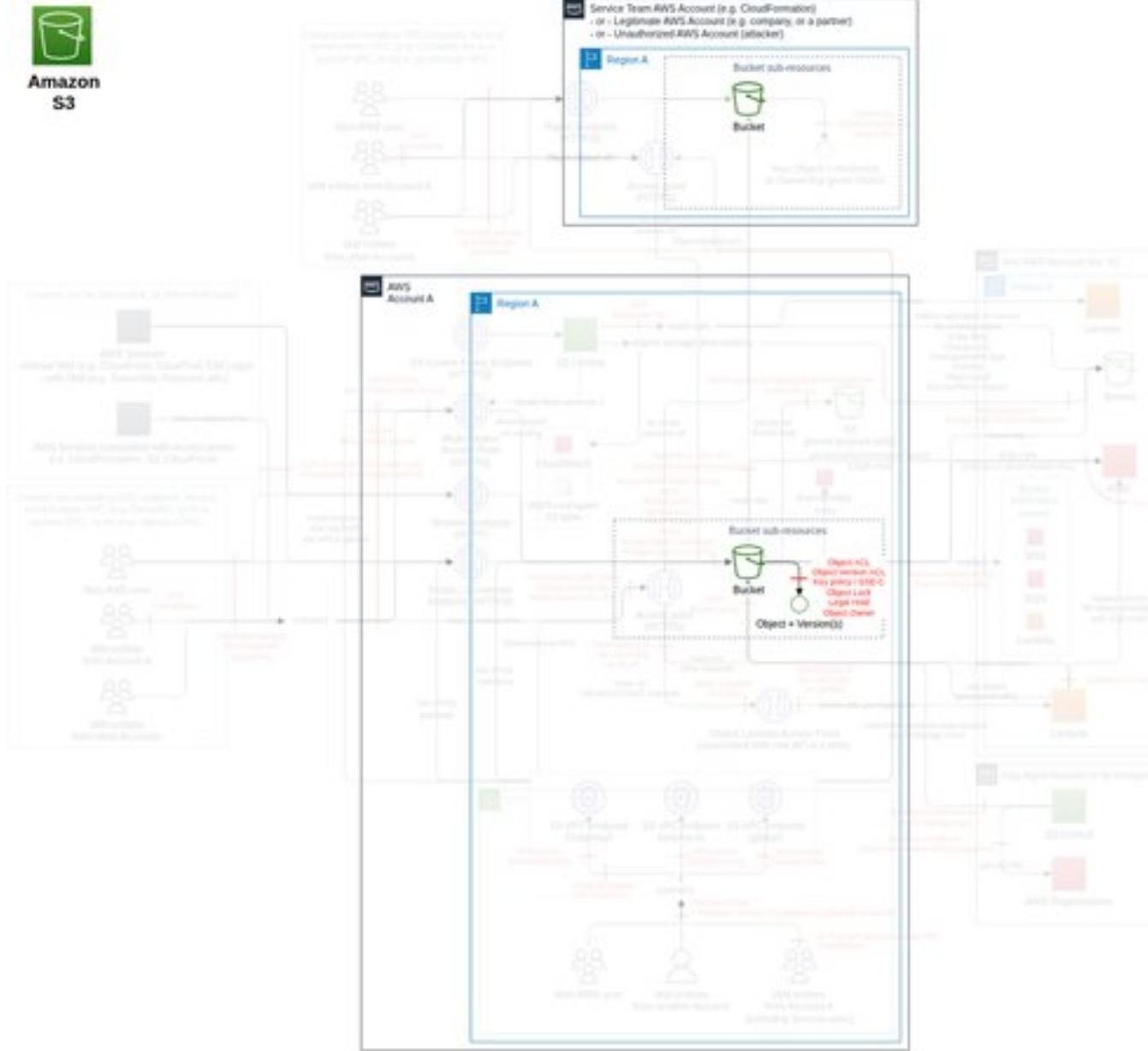
### Threat List

Name	CVSS
None	None

# Bucket versioning (subclass of Object versioning/Bucket, FC6)

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from unintended user actions and application failures ([ref](#)).

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

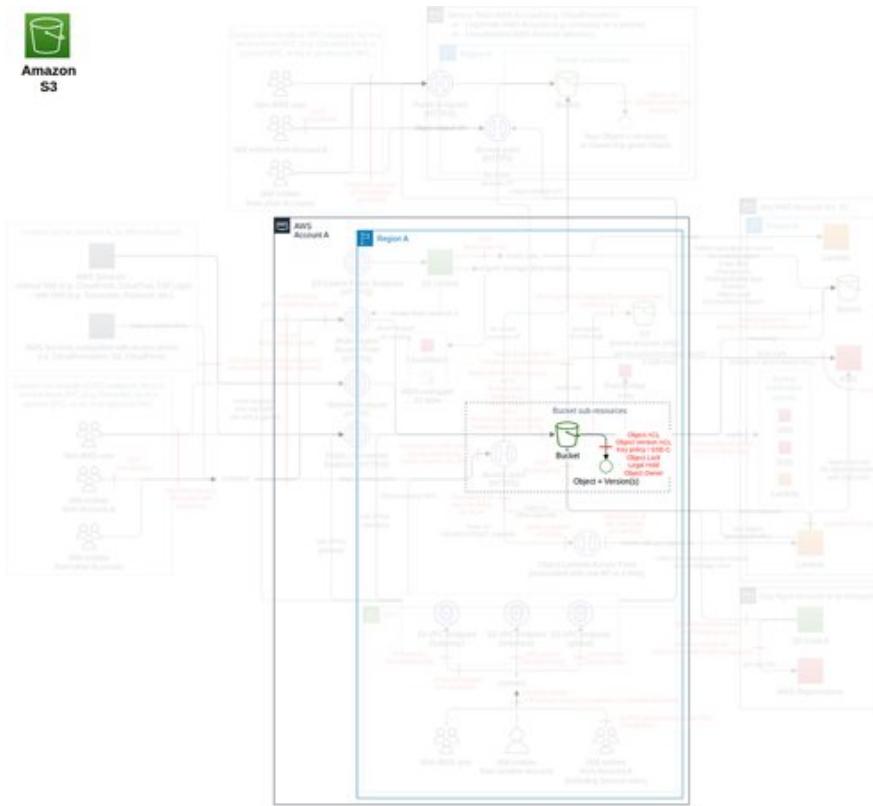
Action	IAM Permission
Sets the versioning state of an existing bucket.	s3:PutBucketVersioning

## Threat List

Name	CVSS
Affect data protection by removing versioning	<a href="#">Low (2.4)</a>

## Affect data protection by removing versioning

<b>Threat Id</b>	S3.T48
<b>Name</b>	Affect data protection by removing versioning
<b>Description</b>	Versioning can be used as the first level of integrity protection. An attacker can suspend versioning to affect the data protection of a bucket.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1490</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutBucketVersioning" }

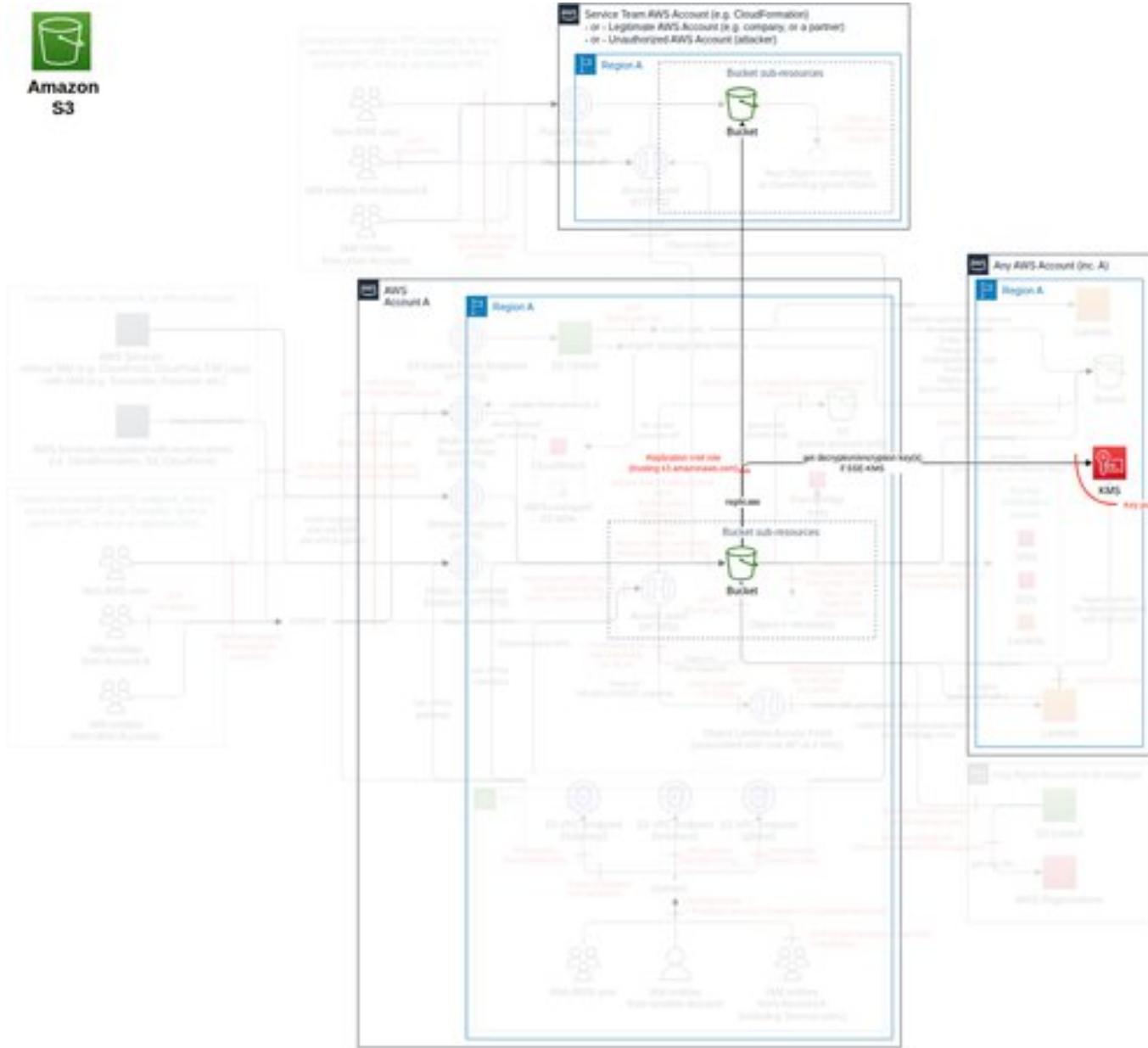


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

# Replication (*subclass of Bucket versioning, FC15*)

Replication enables automatic and asynchronous copying of objects from one bucket to another. It can be cross-region or within the same region. Buckets configured for replication can be in the same AWS account or in different accounts. It is usually used for backing up S3 data, data centralization, or for multi-region applications.

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

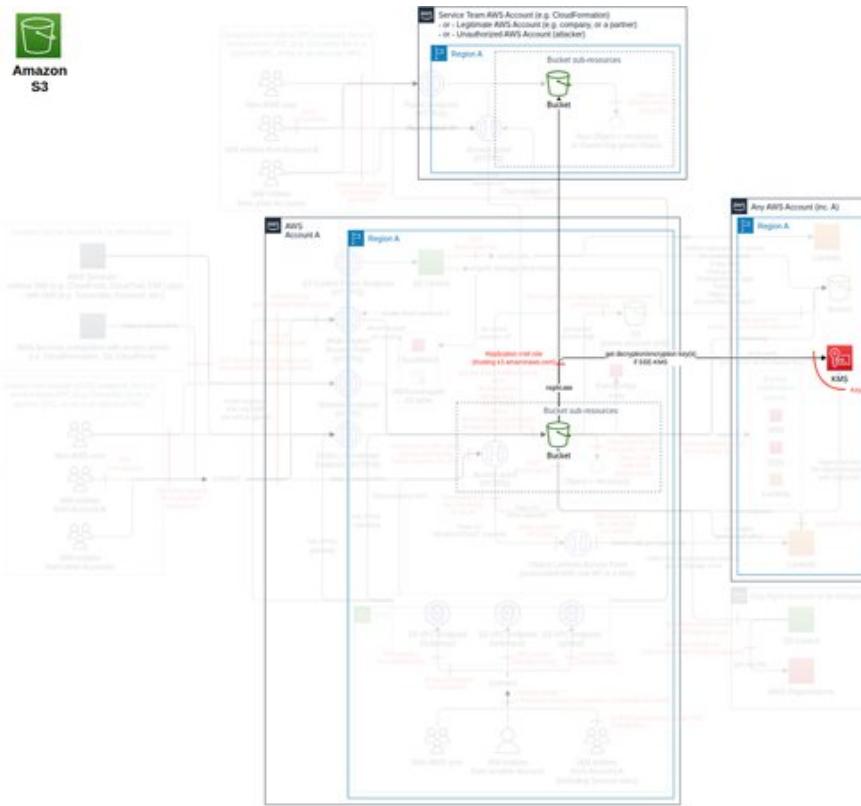
Action	IAM Permission
Creates a new replication configuration (or replaces an existing one, if present).	s3:PutReplicationConfiguration

## **Threat List**

Name	CVSS
Unauthorized access to data or loss of control of SSE-C encrypted data via bucket replication	<a href="#">Medium (4.5)</a>
Affect data protection by removing replication	<a href="#">Low (2.4)</a>

## Unauthorized access to data or loss of control of SSE-C encrypted data via bucket replication

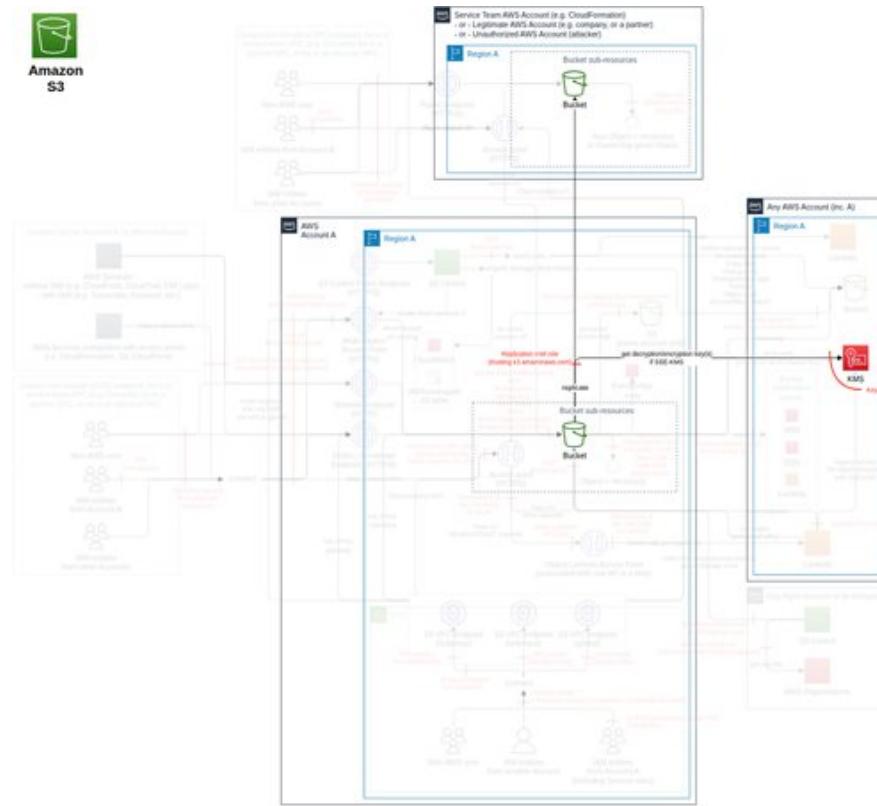
<b>Threat Id</b>	S3.T2
<b>Name</b>	Unauthorized access to data or loss of control of SSE-C encrypted data via bucket replication
<b>Description</b>	Replication allows you to replicate objects and their metadata and change ownership. The configuration only focuses on new objects (old objects replication requires S3 Batch Replication). An attacker can configure replication on a versioned bucket to replicate objects (or their metadata or tagging) in a bucket they control to exfiltrate data. As objects encrypted via SSE-C are also replicated without additional configuration or access requirements, an attacker can then decrypt them in their own bucket if they have the SSE-C key.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1048</a>
<b>CVSS</b>	<a href="#">Medium (4.5)</a>
<b>IAM Access</b>	{ "AND": ["s3:PutReplicationConfiguration", "iam:PassRole"] }



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>C09 - Block requests with KMS keys from unauthorized AWS accounts</b> C31 - Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account. C32 - Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account). C33 - Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Very High	1	1	1
<b>C025 - Restrict bucket replication</b> C86 - Maintain a list of authorized buckets to have replication enabled, their target bucket, and replication type (i.e., encryption type, ownership, RTC, etc.) ( <a href="#">ref</a> ). C134 - Ensure only authorized buckets have replication enabled and are configured correctly. C89 - Maintain a list of IAM roles used for replication, ideally dedicated (e.g., using change management process on infrastructure-as-code). C138 - Ensure only authorized IAM roles are attached for each replication, ideally dedicated. C90 - Limit S3 access to the source and destination buckets and the replication rights of each authorized IAM role configured for replication. C91 - Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole"). C116 - Monitor abnormal behavior on replication CloudWatch metrics (i.e., "BytesPendingReplication", "OperationsPendingReplication", and "OperationsFailedReplication").	High	6	-	1
<b>C04 - Monitor S3 with Amazon GuardDuty and Macie</b> C118 - Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	High	1	-	-
<b>C08 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Affect data protection by removing replication

<b>Threat Id</b>	S3.T49
<b>Name</b>	Affect data protection by removing replication
<b>Description</b>	Replication can be used as a level of integrity protection and backup. An attacker can remove replication to affect data protection.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1490</a>
<b>CVSS</b>	<a href="#">Low (2.4)</a>
<b>IAM Access</b>	{ "UNIQUE": "s3:PutReplicationConfiguration" }



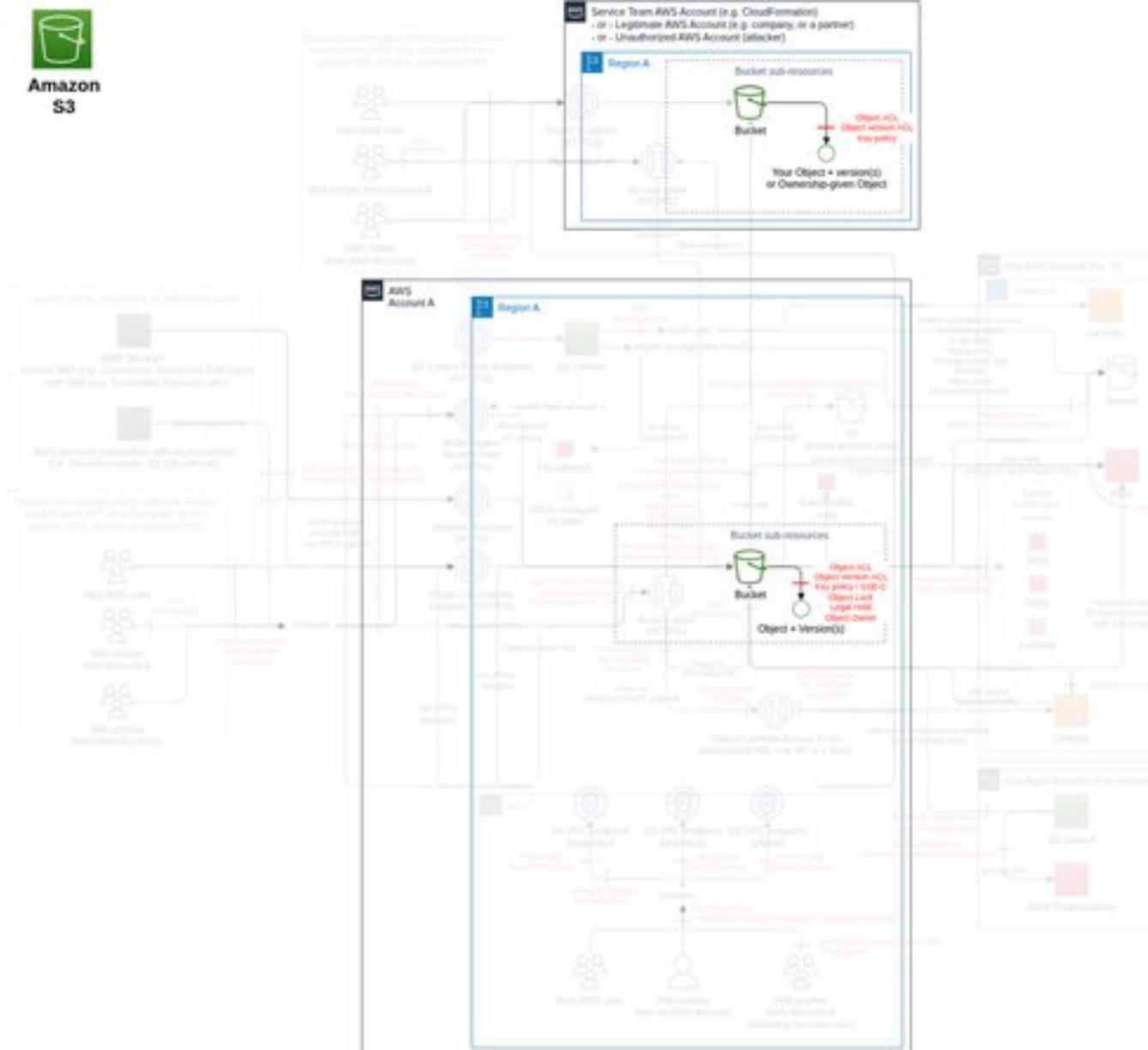
Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO25 - Restrict bucket replication</b> C116 - Monitor abnormal behavior on replication CloudWatch metrics (i.e., "BytesPendingReplication", "OperationsPendingReplication", and "OperationsFailedReplication").	Medium	-	-	1
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b> C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Medium	1	-	-

# ACL on versioned objects (subclass of Object versioning/Bucket)

ACL, FC9)

Amazon S3 Access Control Lists (ACLs) enable you to manage access to object versions ([ref](#))

## **Data Flow Diagram (DFD)**



### ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Sets the Access Control List (ACL) permissions for an object version. You must have WRITE_ACP permission to set the ACL of an object version.	s3:PutObjectVersionAcl

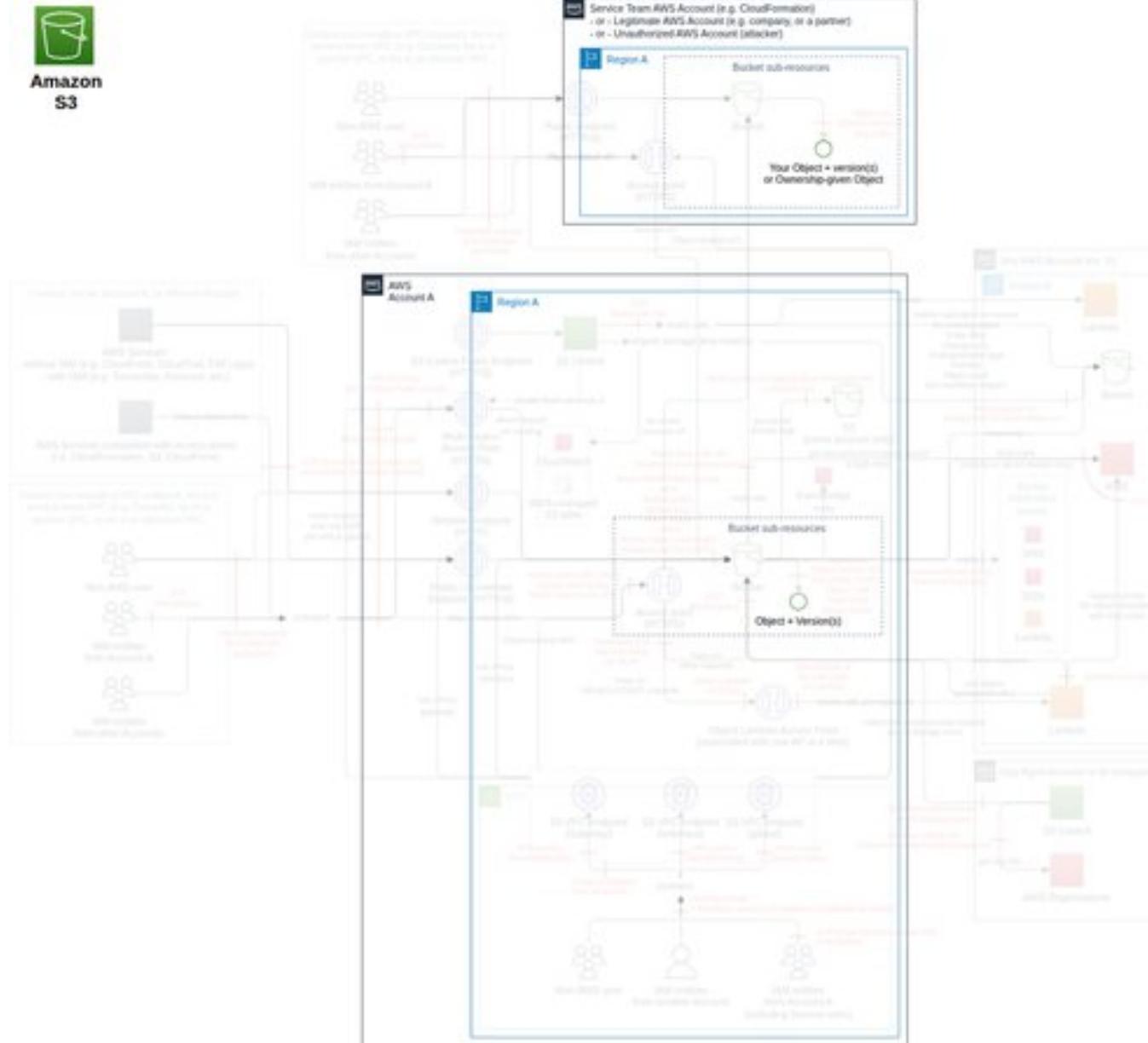
## **Threat List**

Name	CVSS
None	None

# Tag on versioned objects

(subclass of Object tagging/Object versioning, used by Bucket, FC4)  
You can tag each version of an object ([ref](#)).

## ***Data Flow Diagram (DFD)***



### ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Adds a set of tags to an existing object version.	s3:PutObjectVersionTagging

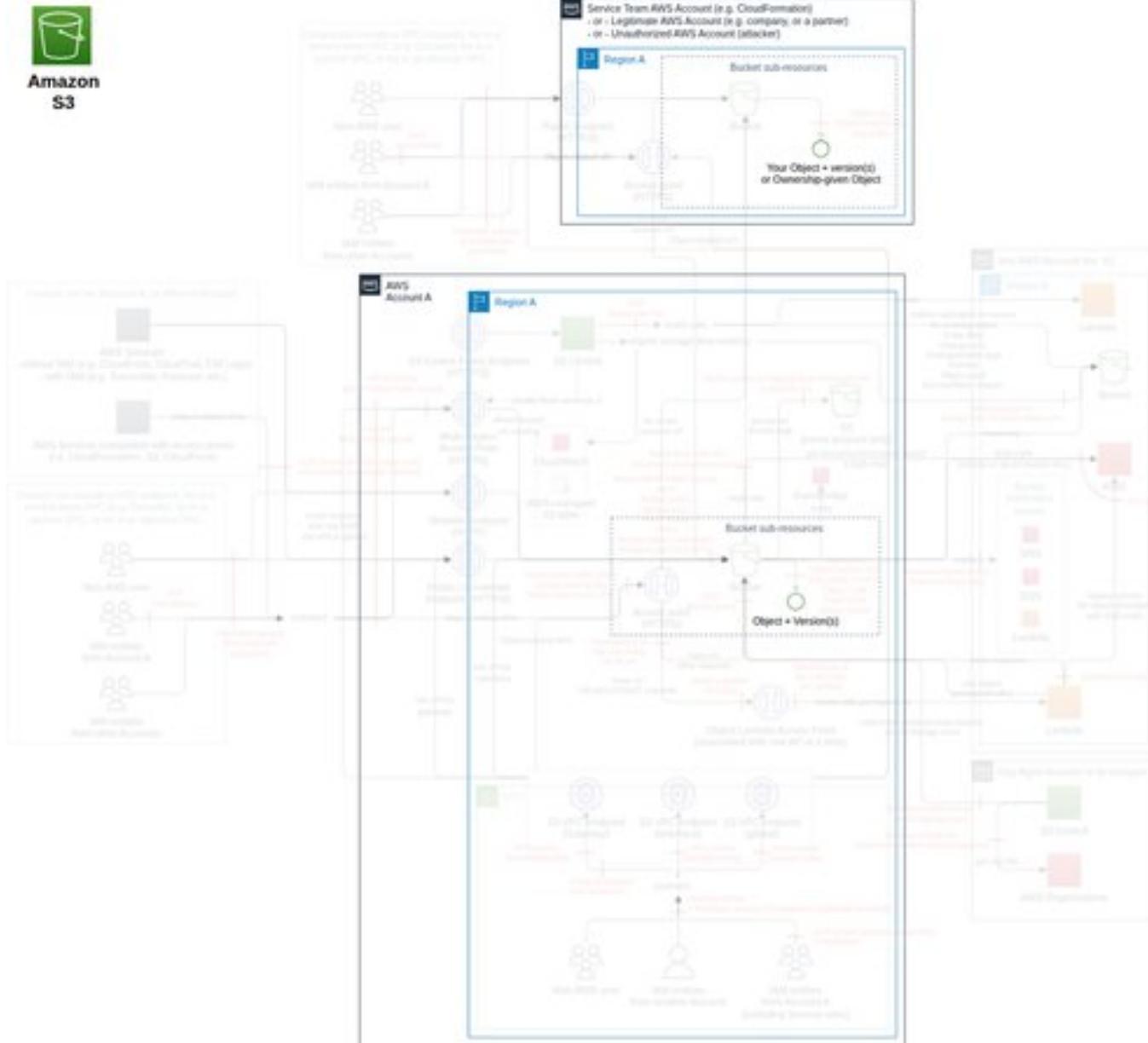
## ***Threat List***

Name	CVSS
None	None

## Torrent (*subclass of Object operations, used by Bucket, FC21*)

**[NOT RECOMMENDED]** You can use the BitTorrent protocol to retrieve objects ([ref](#)). It is only available in the AWS Regions launched before May 30, 2016. The seed rate is 100 KB. After April 29, 2022, BitTorrent clients will no longer connect to Amazon S3.

# **Data Flow Diagram (DFD)**



## ***Actions and IAM Permissions to deny the feature***

Action	IAM Permission
Returns torrent files from an object.	s3:GetObjectTorrent

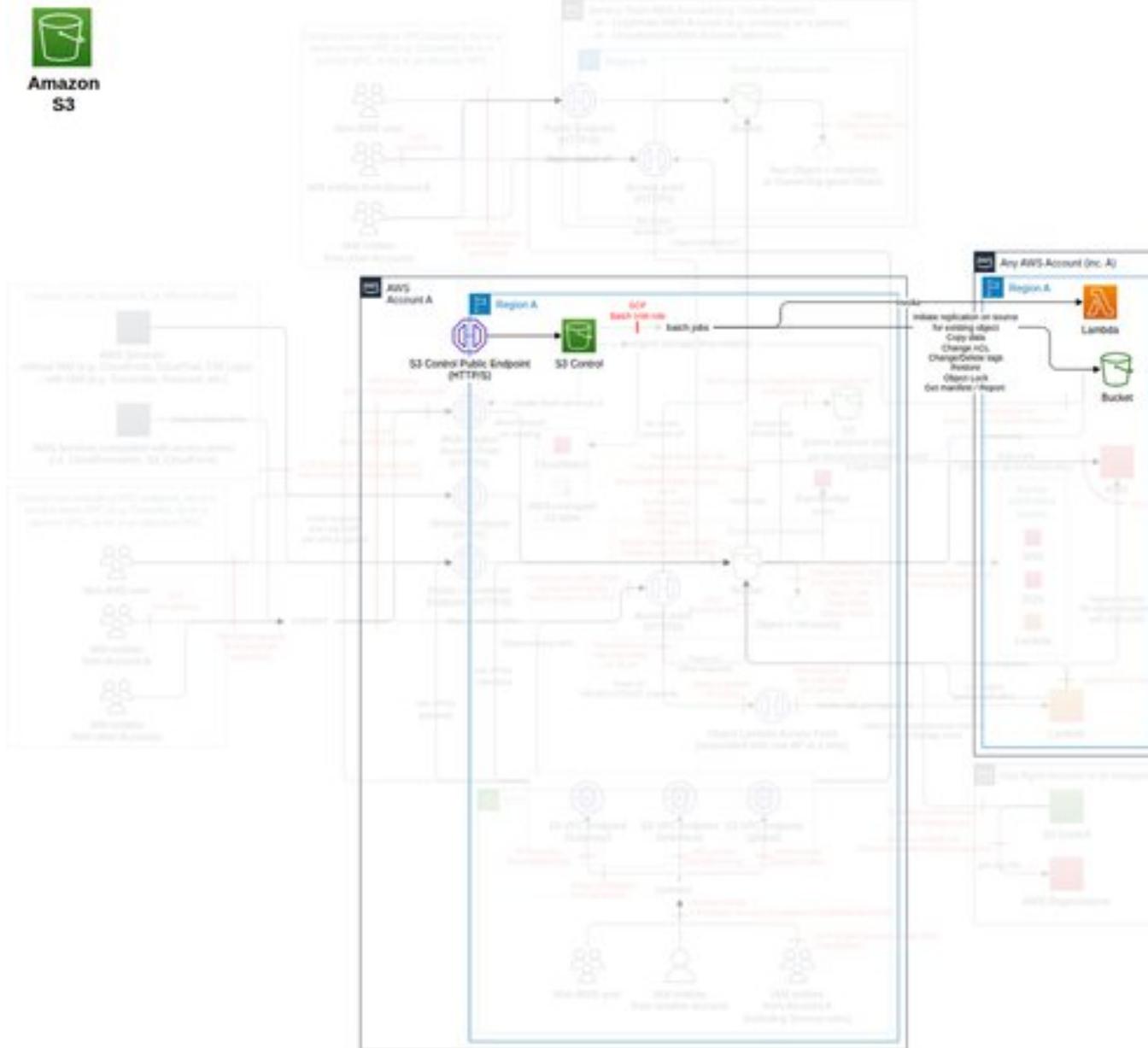
## ***Threat List***

Name	CVSS
None	None

# Batch (subclass of Object operations, used by Bucket, FC27)

S3 Batch Operations performs large-scale Batch Operations on Amazon S3 objects.

## Data Flow Diagram (DFD)



## Actions and IAM Permissions to deny the feature

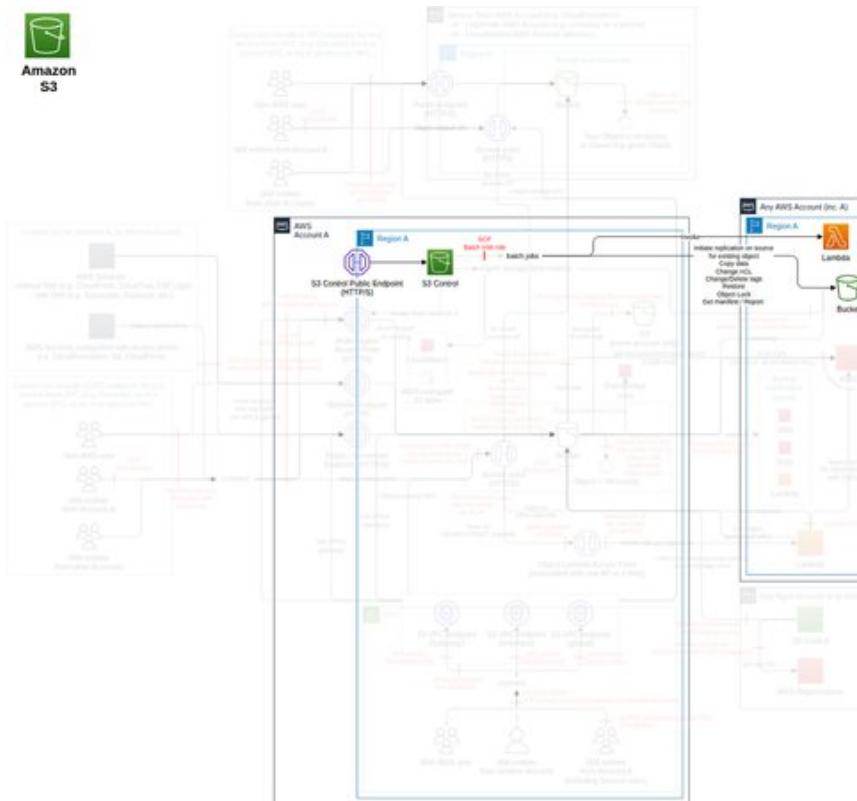
Action	IAM Permission
Creates a new Amazon S3 Batch Operations job.	s3:CreateJob

## Threat List

Name	CVSS
Exfiltrate, modify, or delete objects using Batch	<a href="#">Medium (6.2)</a>

## Exfiltrate, modify, or delete objects using Batch

<b>Threat Id</b>	S3.T44
<b>Name</b>	Exfiltrate, modify, or delete objects using Batch
<b>Description</b>	S3 Batch Operations require an IAM role (with a proper trust policy), and can run operations including replicating existing objects, copying, or replacing/deleting object tags. An attacker can use Batch to copy or modify objects to exfiltrate or change the access management of an object (if relying on a tag).
<b>Goal</b>	Data manipulation
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0040</a> , <a href="#">T1565</a>
<b>CVSS</b>	<a href="#">Medium (6.2)</a>
<b>IAM Access</b>	{ "AND": ["s3:CreateJob", "iam:PassRole"] }

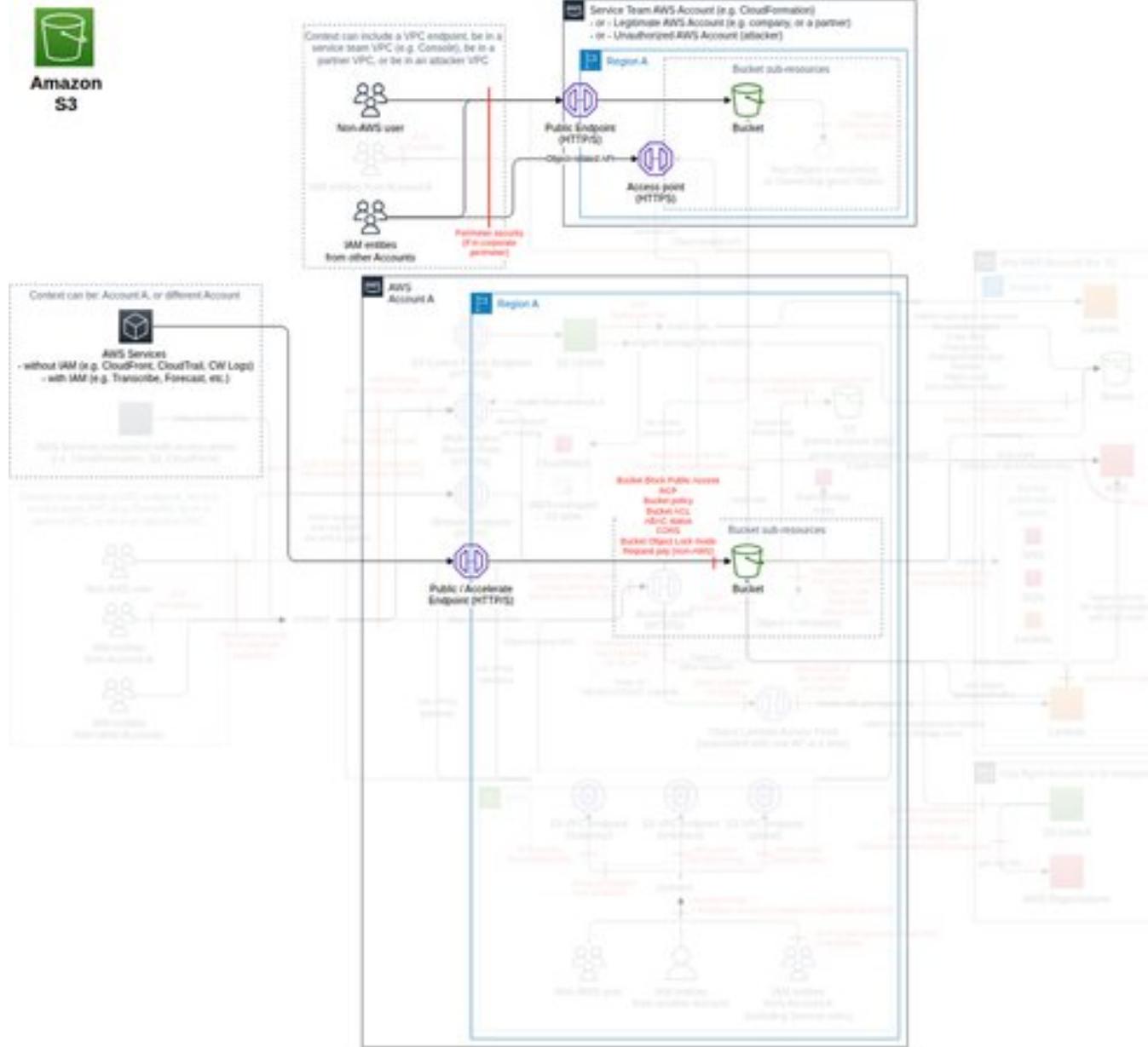


Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO33 - Restrict Batch access using dedicated IAM roles</b>  C120 - Maintain a list of IAM roles used for Batch jobs, ideally dedicated (e.g., using change management process on infrastructure-as-code). C139 - Ensure only an authorized IAM role is attached to each Batch job. C121 - Limit access to only the required resources/permissions (e.g., source/destination buckets, Lambda functions) for each authorized IAM role configured for Batch jobs. C122 - Limit access to authorized IAM roles used for Batch jobs, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Very High	4	-	-
<b>CO8 - Limit the IAM entities allowed to use the IAM actions required to execute attacks</b>  C26 - Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions. C27 - In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Medium	2	-	-

## Other uses (*class, FC28*)

*Others can use their S3 service to impact you in some way.*

## **Data Flow Diagram (DFD)**



## ***Actions and IAM Permissions to deny the feature***

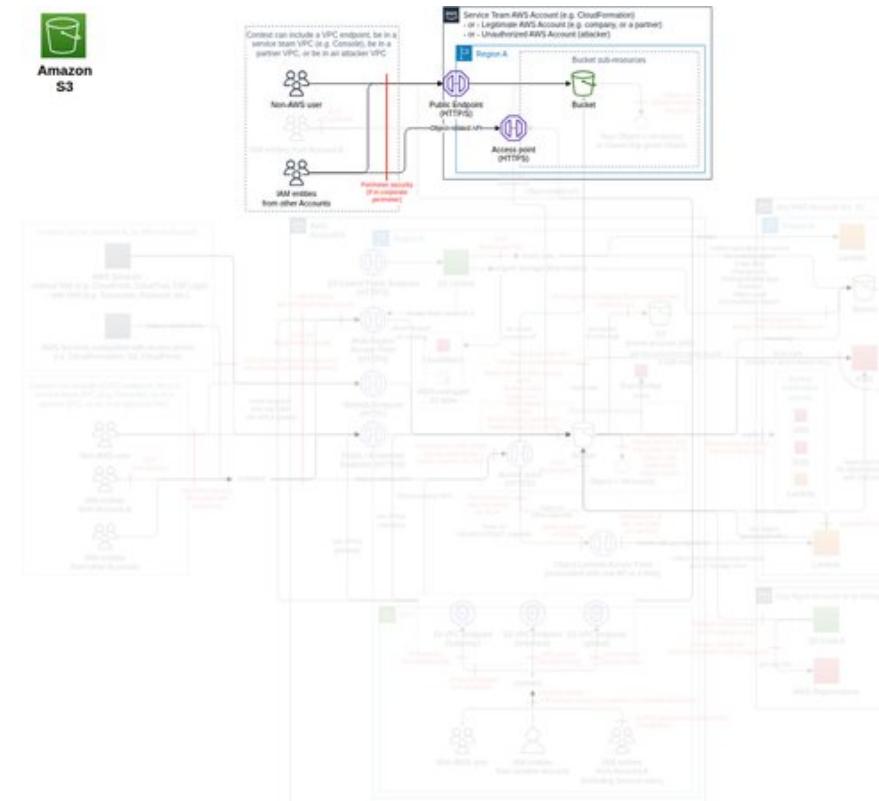
Action	IAM Permission
None	None

## **Threat List**

Name	CVSS
Exfiltrate data by using the public endpoint to upload data to an attacker's bucket, using external credentials	<a href="#">Medium (6.2)</a>
Recon on the AWS Region of a bucket	<a href="#">Medium (4.3)</a>
Phishing using trademarks	<a href="#">Low (3.1)</a>
Uncontrolled change in IAM-managed policies	<a href="#">Low (3.0)</a>
Recon of AWS root account emails using the email ACL grantee feature	<a href="#">Low (2.0)</a>
Recon on valid AWS accounts or IAM principals	<a href="#">Low (2.0)</a>

## Exfiltrate data by using the public endpoint to upload data to an attacker's bucket, using external credentials

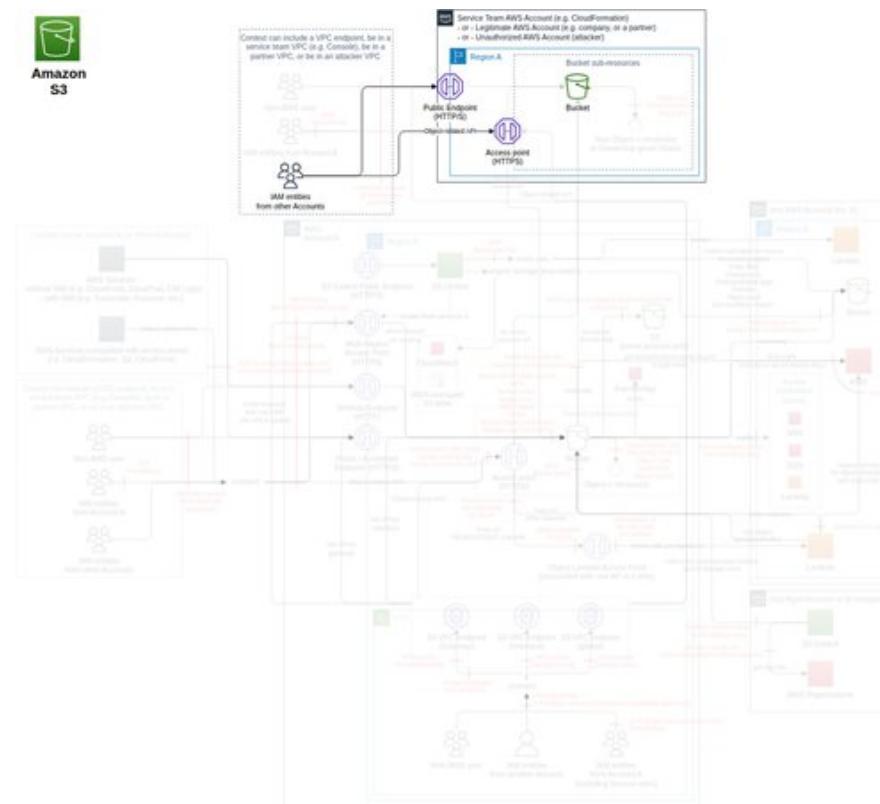
<b>Threat Id</b>	S3.T10
<b>Name</b>	Exfiltrate data by using the public endpoint to upload data to an attacker's bucket, using external credentials
<b>Description</b>	AWS authenticates per AWS account. An attacker can use their own credentials to exfiltrate data to external S3 buckets through the S3 public endpoint. It can be a non-authenticated user as well.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0010</a> , <a href="#">T1537</a>
<b>CVSS</b>	<a href="#">Medium (6.2)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO2 - Block S3 endpoints in your corporate perimeter security</b> C8 - Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Very High	1	-	-
<b>CO32 - Restrict access point access to VPCs when in use</b> C104 - Maintain a list of authorized access between VPCs, S3 access points, and S3. C105 - Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy. C108 - Block all traffic from Internet-configured S3 access points (e.g., in their bucket policy, or centrally in an RCP applied to the OU or AWS account, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Very High	1	2	-

## Recon on the AWS Region of a bucket

<b>Threat Id</b>	S3.T32
<b>Name</b>	Recon on the AWS Region of a bucket
<b>Description</b>	Error messages can give some information about specific buckets. An attacker who knows the bucket name can find its AWS Region. To find the AWS Region, use "aws s3 presign bucket-name/whatever", go to the presign link, and the error message will give you the region, if not in the right region.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0043</a> , <a href="#">T1590</a>
<b>CVSS</b>	<a href="#">Medium (4.3)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
None				

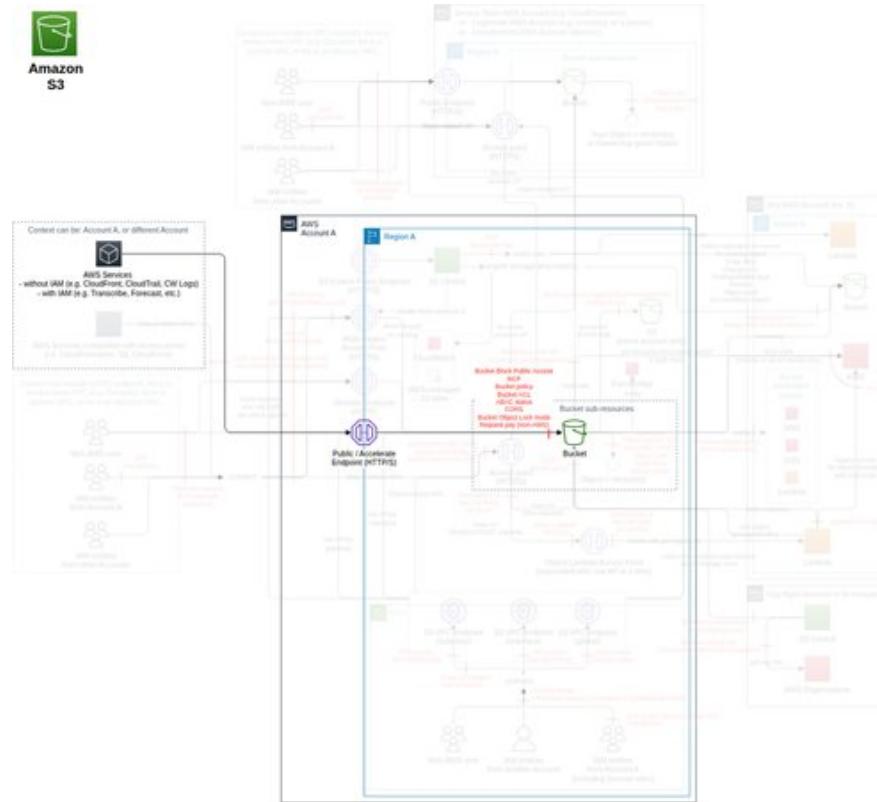
## Phishing using trademarks

<b>Threat Id</b>	S3.T23
<b>Name</b>	Phishing using trademarks
<b>Description</b>	S3 provides URLs to buckets using the bucket name (i.e., "mybucket.s3.amazonaws.com"). An attacker can create a bucket with the name of your trademark to phish users.
<b>Goal</b>	Data theft
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0009</a> , <a href="#">T1056</a>
<b>CVSS</b>	<a href="#">Low (3.1)</a>
<b>IAM Access</b>	{}

Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO31 - Protect and/or claim your domains and trademarks/copyrights</b> C103 - Protect and/or claim your domains and trademarks/copyrights (by creating your trademark buckets and using the <a href="#">copyright infringement process</a> from AWS).	High	1	-	-

## Uncontrolled change in IAM-managed policies

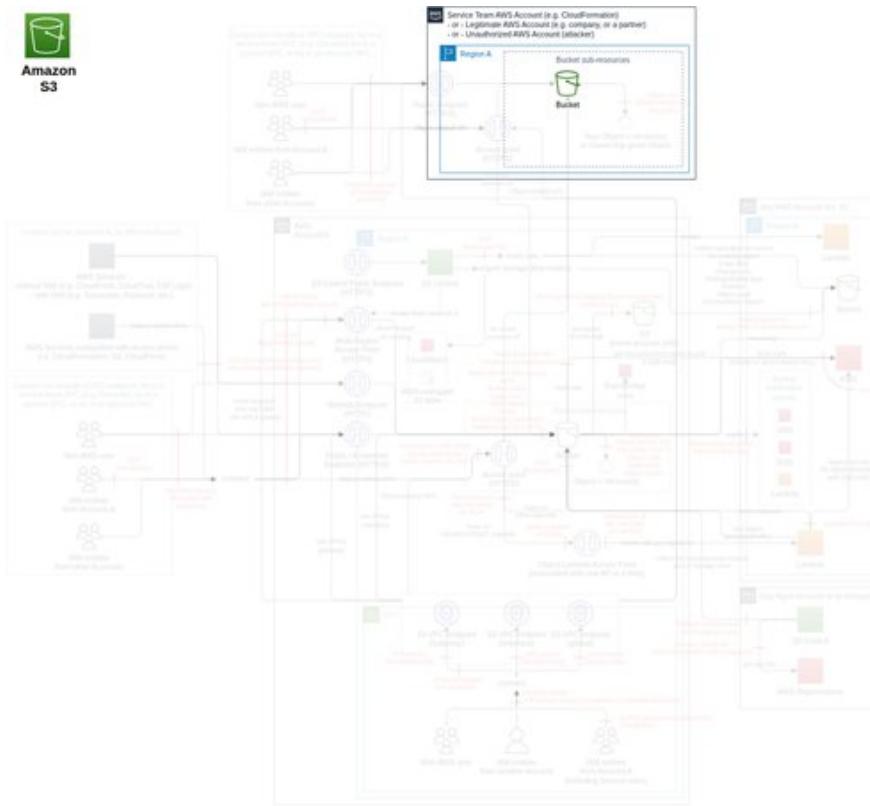
<b>Threat Id</b>	S3.T57
<b>Name</b>	Uncontrolled change in IAM-managed policies
<b>Description</b>	AWS managed policies can be attached to your IAM entities, but their permissions are managed by AWS. An attacker (including an AWS insider via a <a href="#">service-linked role</a> ) can use an overprivileged managed policy to execute an attack.
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0003</a> , <a href="#">T1098</a>
<b>CVSS</b>	<a href="#">Low (3.0)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO38 - Ensure all requests are blocked from unauthorized service roles</b> C155 - Ensure all requests are blocked from AWS service roles that do not require access (e.g., by denying all requests with the principal "arn:aws:iam::*:*/AWSServiceRoleFor*" on S3 bucket policies).	Very High	1	-	-

## Recon of AWS root account emails using the email ACL grantee feature

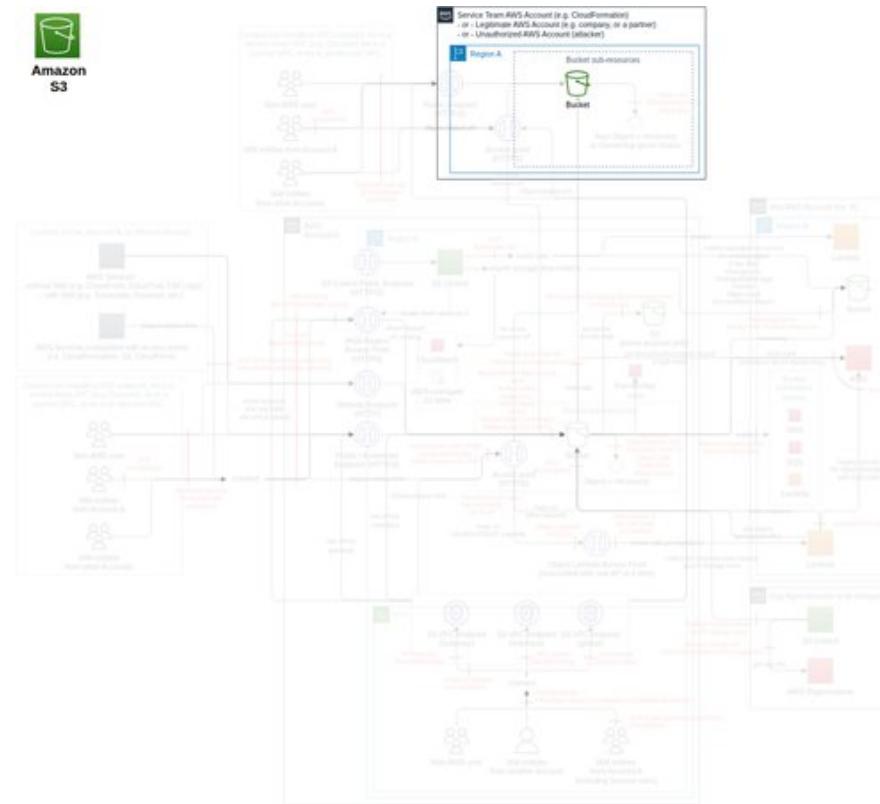
<b>Threat Id</b>	S3.T19
<b>Name</b>	Recon of AWS root account emails using the email ACL grantee feature
<b>Description</b>	S3 allows you to add root account emails to an ACL ( <a href="#">ref</a> , note that it will be discontinued on Oct 1st, 2025), and also resolve the given canonical ID into an AWS account ID (via a bucket policy, which automatically resolves a canonical ID into an ARN). An attacker can use trial-and-error to discover existing AWS root account emails and related AWS account IDs (even if you do not use the region where the feature is available), and use this information to launch another attack (e.g., phishing).
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0043</a> , <a href="#">T1589</a>
<b>CVSS</b>	<a href="#">Low (2.0)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO36 - Use an unguessable naming convention</b> C29 - Use an unguessable naming convention for the email addresses of your AWS accounts (e.g., add a + sign and a random string to redirect the email to the same mailbox).	High	1	-	-

## Recon on valid AWS accounts or IAM principals

<b>Threat Id</b>	S3.T24
<b>Name</b>	Recon on valid AWS accounts or IAM principals
<b>Description</b>	AWS provides error messages in AWS IAM or S3 bucket policy operations that can be used for basic recon. An attacker can discover whether an AWS account with a specific AWS account ID or IAM principal exists by modifying the policy of their own IAM resource or S3 bucket to grant some rights to that target AWS account or IAM principal ( <a href="#">ref</a> , <a href="#">ref2</a> ).
<b>Goal</b>	Launch another attack
<b>MITRE ATT&amp;CK®</b>	<a href="#">TA0043</a> , <a href="#">T1589</a>
<b>CVSS</b>	<a href="#">Low (2.0)</a>
<b>IAM Access</b>	{}



Control Objectives	Priority	# of associated Controls		
		Directive	Preventative	Detective
<b>CO36 - Use an unguessable naming convention</b> C30 - Use an unguessable naming convention for your IAM users and IAM roles (e.g., add a random string).	High	1	-	-

# Control Implementation

## Enforce encryption in transit [s3.c01]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C1, depends on S3.C119, assured by S3.C2] Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g., by denying all unencrypted requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), using an SCP on your AWS Organization root node).	Make an unencrypted S3 API call; it should be denied.	Low	S3.FC1 S3.FC5	S3.T12 (Very High) S3.T34 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C2] Verify the control blocking unencrypted requests and unauthorized TLS versions from IAM entities you control (e.g., an SCP on your AWS Organization's root node) is properly implemented.	Remove the control blocking unencrypted requests and unauthorized TLS version(s) (e.g., the SCP on your root node); it should be detected.	High	S3.FC1 S3.FC5	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C3, depends on S3.C119, assured by S3.C5] Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), on the VPC endpoint policy).	Make an unencrypted AWS API call from one of your VPCs with a VPC endpoint; it should be denied.	Low	S3.FC1 S3.FC5	S3.T12 (Medium) S3.T34 (Medium)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C4] Monitor and investigate all requests made with HTTP (e.g., via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite).	Make an unencrypted AWS API call from one of your VPCs with VPC endpoint; it should be detected.	Low	S3.FC1 S3.FC5	S3.T12 (Low) S3.T34 (Low)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C5] Verify a statement exists on all your VPC endpoint policies denying all requests with the condition "aws:SecureTransport" = False or using "s3:TlsVersion" != authorized TLS version(s).	Create/remove the statement on a VPC endpoint policy denying 1) all unencrypted requests or 2) unauthorized TLS version(s); it should be detected.	High	S3.FC1 S3.FC5	-	Medium
Preventative (coso) Protect (NIST CSF)	[S3.C6, depends on S3.C119, assured by S3.C7] Block all unencrypted requests to the buckets you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), on their bucket policy or centrally in an RCP applied to the OU or AWS account).	Make an unencrypted AWS API call to a bucket you control; it should be denied.	Low	S3.FC5	S3.T34 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C7] Verify all S3 bucket policies block unencrypted traffic (e.g., using the AWS Config rule: <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a> ) and unauthorized versions of TLS.	Remove the statement on a bucket policy 1) denying all unencrypted requests and 2) denying unauthorized TLS versions; it should be detected.	Medium	S3.FC5	-	High
Directive (coso) Identify (NIST CSF)	[S3.C119] Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org) (e.g., considering <a href="#">quantum-resistant encryption</a> ).	Request the list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org), its review mechanism, and associated records.	Low	S3.FC1 S3.FC5	S3.T12 (Very Low) S3.T34 (Very Low)	High

## Block S3 endpoints in your corporate perimeter security [s3.co2]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C8] Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Request the evidence of the implementation of blocking S3 endpoints in your corporate perimeter security (e.g., firewalls) and tests of its effectiveness.	Low	S3.FC1 S3.FC5 S3.FC28	S3.T7 (High) S3.T10 (High) S3.T12 (Low) S3.T18 (Medium) S3.T34 (Very High)	High

## Enable S3 data events in AWS CloudTrail [s3.co3]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Detect (NIST CSF)	[S3.C9, depends on S3.C58] Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Request the CloudTrail ThreatModel and the evidence of its application for enabling and protecting S3 data events.	Very Low	S3.FC1 S3.FC5 S3.FC8	S3.T1 (Low) S3.T4 (Low) S3.T5 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T12 (Low) S3.T16 (Low) S3.T21 (Low) S3.T31 (Low) S3.T34 (Low) S3.T35 (Low) S3.T36 (Low) S3.T39 (Low)	Medium

## Monitor S3 with Amazon GuardDuty and Macie [s3.co4]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Detect (NIST CSF)	[S3.C10] Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective).	Request the GuardDuty ThreatModel and the evidence of its application for enabling, monitoring, investigating, and protecting S3 use.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	S3.T3 (Low) S3.T4 (Low) S3.T16 (Medium) S3.T52 (Medium) S3.T53 (Medium)	Medium
Directive (coso) Detect (NIST CSF)	[S3.C118] Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	Request the Macie ThreatModel and the evidence of its application for enabling and protecting S3 policy findings.	Very Low	S3.FC5 S3.FC8 S3.FC10 S3.FC15	S3.T2 (Medium) S3.T4 (Medium) S3.T22 (Medium) S3.T36 (Medium) S3.T37 (Medium) S3.T38 (Medium)	Medium

## Identify and ensure the protection of all external buckets hosting your objects [s3.co5]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C11] Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel).	Request the list of all external buckets authorized to host your objects, their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), their data classification, and the mechanism used to ensure the security of those buckets.	Medium	S3.FC1 S3.FC5 S3.FC16	S3.T1 (Very Low) S3.T3 (High) S3.T5 (Very Low) S3.T6 (Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Low) S3.T14 (Very Low) S3.T15 (Very Low) S3.T21 (Very Low) S3.T31 (High) S3.T43 (Very High)	Very High
Preventative (coso) Protect (NIST CSF)	[S3.C12, depends on S3.C11] Allow only authorized ACLs on objects for buckets you don't control (e.g., using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> ).	Put an object with an unauthorized ACL; it should be denied.	Medium	S3.FC1	S3.T5 (Medium) S3.T6 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C13, depends on S3.C11] Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	Make a call to an unauthorized bucket; it should be detected.	Low	S3.FC1 S3.FC5	S3.T1 (Low) S3.T7 (Low) S3.T11 (Low) S3.T21 (Low) S3.T31 (Medium)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C14, depends on S3.C11] Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g., using Macie).	Request 1) the mechanism ensuring all data is scanned for proper data classification before upload to an external bucket, 2) its records of execution for all object upload flows, and 3) the plan to move any older object upload flows.	High	S3.FC1 S3.FC5 S3.FC16	S3.T5 (High) S3.T14 (High) S3.T15 (Medium)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C15] Request access via an S3 access point on a bucket you don't own, if compatible with your interaction with the bucket (e.g., not through an unsupported AWS service).	Request the documented reasons why the access point was not implemented in the use case.	Low	S3.FC1	S3.T8 (Medium) S3.T9 (Medium) S3.T31 (Very High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C114, depends on S3.C11] For all external buckets with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, block the PutObject with any ACL (e.g., using IAM or SCP and a deny on the condition "StringLike": {"s3:x-amz-acl": "*"}). It should be called via PutObjectAcl.	Put an object in an external bucket with the bucket-owner-full-control ACL requirement but without the S3 Object Ownership handover requirement; it should be denied.	High	S3.FC1	S3.T43 (Very High)	High
Detective (coso) Detect (NIST CSF)	[S3.C115, depends on S3.C11] For all external buckets with bucket-owner-full-control ACL requirements but without S3 Object Ownership handover, monitor that the PutObject operation does not include the ACL header.	Make a request to an external bucket with a bucket-owner-full-control ACL requirement but without an S3 Object Ownership handover requirement; it should be detected.	Low	S3.FC1	S3.T43 (Low)	Medium

## Model the threats on all AWS services accessing S3 [s3.co6]

Type	Control	Testing	Effort	Feature	Threat(s)	CVSS-weighted
------	---------	---------	--------	---------	-----------	---------------

				Class(es)	and Impact	Priority
Directive (coso) Protect (NIST CSF)	[S3.C16] Analyze and protect all AWS services accessing S3 (e.g., via ThreatModel). Enforce use in VPC only, whenever possible.	Request the ThreatModels for all AWS services using S3.	High	S3.FC1 S3.FC5	S3.T21 (Very High) S3.T30 (Very High)	Medium

## Limit and monitor access via S3 VPC endpoints [s3.c07]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C17] For each VPC, maintain a list of AWS Organizations, OUs, and/or AWS accounts where IAM entities are authorized to access S3.	For each VPC, request the list of AWS Organizations, OU, and/or AWS account(s), where IAM entities are authorized to access S3, its review process, and its review records.	Medium	S3.FC1 S3.FC5	S3.T9 (Very Low) S3.T11 (Very Low) S3.T62 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C18, depends on S3.C17] For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g., <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ).	Request how the VPC ThreatModel for S3 is being applied.	High	S3.FC1 S3.FC5	S3.T9 (Medium) S3.T11 (Medium) S3.T62 (Medium)	Low
Preventative (coso) Protect (NIST CSF)	[S3.C19, depends on S3.C17, assured by S3.C20] Block any IAM entity not belonging to an authorized AWS Organization, OU, and/or AWS account from calling S3 from your VPCs by adding a deny statement in the S3 VPC endpoint policy for each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org IDs, as those are globally unique.	For each VPC, make an API call with an IAM entity that is not part of its authorized AWS Organizations paths; it should be denied.	Low	S3.FC1 S3.FC5	S3.T9 (Very High) S3.T11 (Very High) S3.T62 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C20] Verify all S3 VPC endpoints are blocking any IAM entity not belonging to authorized AWS Organizations, OUs, and/or AWS accounts.	Remove the policy statement blocking any IAM entity not belonging to authorized AWS Organizations, OUs, and/or AWS accounts from the VPC endpoint; it should be detected.	High	S3.FC1 S3.FC5	-	High
Directive (coso) Detect (NIST CSF)	[S3.C21] Enable <a href="#">VPC DNS query logging</a> in all VPCs.	Request the mechanism to enable VPC DNS query logging in all VPCs.	Medium	S3.FC1 S3.FC5	S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low)	Low
Directive (coso) Identify (NIST CSF)	[S3.C22] Maintain a list of authorized S3 and S3 access points (and their respective AWS accounts) to be accessed for each VPC.	Request the list of authorized S3 buckets and S3 access points to be accessed for each VPC, its review process, and its review records.	Medium	S3.FC1 S3.FC5	S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low)	Medium
Preventative (coso) Protect (NIST CSF)	[S3.C23, depends on S3.C22, assured by S3.C24] Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g., using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use a specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points).	Make a request to an unauthorized bucket from one of your VPCs; it should be denied.	Medium	S3.FC1 S3.FC5	S3.T8 (High) S3.T9 (High) S3.T11 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C24] Verify all VPCs are limited to accessing only authorized S3 bucket(s).	Remove the control limiting access to only authorized S3 bucket(s); it should be detected.	High	S3.FC1 S3.FC5	-	Medium
Detective (coso) Detect (NIST CSF)	[S3.C25, depends on S3.C21,S3.C22] Monitor VPC DNS query logs to ensure only authorized S3 buckets and S3 access points are being queried in each VPC (e.g., using VPC DNS query logging) and protect them using Route 53 ThreatModel.	Make a DNS query to an unauthorized 1) S3 bucket and 2) S3 access points; it should be detected.	Low	S3.FC1 S3.FC5	S3.T8 (Low) S3.T9 (Low) S3.T11 (Low)	Low

Directive (coso) Protect (NIST CSF)	[S3.C124] Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoint controls.	Request 1) the mechanism ensuring all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls, 2) its records of execution for all new VPC endpoints, and 3) the plan to move any older VPC endpoints.	Low	S3.FC1	S3.T8 (Very High) S3.T9 (Very High)	High
--	--	---	-----	--------	--	------

## Limit the IAM entities allowed to use the IAM actions required to execute attacks [s3.c08]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C26] Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Request the list of authorized IAM principals with the permissions required to execute the threat actions, its review process, and its review records.	High	S3.FC1 S3.FC2 S3.FC5 S3.FC6 S3.FC8 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC17 S3.FC19 S3.FC20 S3.FC23 S3.FC24 S3.FC25 S3.FC26 S3.FC27 S3.FC32 S3.FC33 S3.FC36	S3.T1 (High) S3.T2 (High) S3.T5 (Low) S3.T6 (Medium) S3.T7 (High) S3.T8 (High) S3.T11 (High) S3.T14 (Very High) S3.T16 (High) S3.T17 (Very High) S3.T18 (High) S3.T21 (Medium) S3.T25 (High) S3.T26 (High) S3.T28 (High) S3.T30 (High) S3.T33 (Very High) S3.T35 (Very High) S3.T36 (Medium) S3.T37 (Very High) S3.T38 (Very High) S3.T39 (High) S3.T41 (High) S3.T42 (High) S3.T44 (High) S3.T46 (High) S3.T47 (High) S3.T48 (High) S3.T49 (High) S3.T50 (High) S3.T51 (High) S3.T52 (High) S3.T53 (High) S3.T54 (High) S3.T55 (High) S3.T56 (High) S3.T58 (High) S3.T59 (High) S3.T60 (High) S3.T61 (High) S3.T62 (High) S3.T63 (High) S3.T64 (High)	High

					S3.T65 (High)	
Directive (coso) Protect (NIST CSF)	[S3.C27, assured by S3.C28] In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Request all S3 bucket/access point/Object Lambda Access Point policy statements with "allow"; no principal from the same account should be authorized.	Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC19 S3.FC20 S3.FC23 S3.FC26 S3.FC27 S3.FC32 S3.FC33	S3.T1 (Low) S3.T2 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T11 (Low) S3.T14 (Medium) S3.T16 (Low) S3.T17 (Medium) S3.T18 (Low) S3.T21 (Low) S3.T25 (Low) S3.T26 (Medium) S3.T30 (Low) S3.T33 (Medium) S3.T35 (Medium) S3.T36 (Low) S3.T37 (Medium) S3.T38 (Medium) S3.T39 (Low) S3.T41 (Low) S3.T42 (Low) S3.T44 (Low) S3.T46 (Medium) S3.T54 (Medium) S3.T55 (Medium) S3.T58 (Medium) S3.T59 (Medium) S3.T65 (Low)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C28] Verify all S3 bucket/access point/Object Lambda Access Point policies do not allow an IAM principal of the same AWS account (e.g., using the Config rule S3_BUCKET_POLICY_GRANTEE_CHECK for bucket policy).	Add an allow statement for an IAM principal of the same account in 1) a bucket policy, 2) an access point policy, and 3) an Object Lambda Access Point; it should be detected.	Medium	S3.FC1 S3.FC2 S3.FC5 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC19 S3.FC20 S3.FC23 S3.FC26 S3.FC27 S3.FC32 S3.FC33	-	Medium
Directive (coso) Identify (NIST CSF)	[S3.C149] For each bucket, maintain a list of authorized IAM principals allowed to access via the bucket policy.	Request the list of authorized IAM principals allowed to access via bucket policy, its review process, and its review records.	Medium	S3.FC10	S3.T37 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C150, depends on S3.C149, assured by S3.C151] Ensure only authorized IAM principals allowed to access via bucket policy are configured (e.g., using IAM Access Analyzer for reconciliation).	Request 1) the mechanism ensuring only authorized IAM principals are allowed to access buckets via bucket policy, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC10	S3.T37 (Very High)	High
Assurance (coso)	[S3.C151]	Allow an unauthorized IAM principal on a bucket policy; it	Medium	S3.FC10	-	High

Detect (NIST CSF)	Verify only authorized IAM principals allowed to access via bucket policy are used (e.g., using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ).	should be detected.				
Directive (coso) Protect (NIST CSF)	[S3.C170, depends on S3.C58] Integrate and limit the access to general purpose buckets via tags in the IAM Operating Model (including enforcing tagging of buckets and objects at creation using AWS:ResourceTag and s3:BucketTag).	Request the IAM tag Operating Model for the general purpose buckets.	High	S3.FC2	S3.T33 (Very High)	Medium

## Block requests with KMS keys from unauthorized AWS accounts [s3.c09]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C31] Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account.	Request the list of AWS accounts authorized to provide KMS keys for S3 for each AWS account, its review process, and its review records.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC15 S3.FC26	S3.T1 (Very Low) S3.T2 (Very Low) S3.T4 (Very Low) S3.T5 (Very Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low) S3.T16 (Very Low) S3.T21 (Very Low) S3.T27 (Very Low) S3.T28 (Very Low) S3.T30 (Very Low) S3.T31 (Very Low) S3.T60 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C32, depends on S3.C31] Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account).	Make a request encrypted with a KMS key from an unauthorized AWS account; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC15 S3.FC26	S3.T1 (High) S3.T2 (Medium) S3.T4 (High) S3.T5 (High) S3.T7 (High) S3.T8 (High) S3.T9 (High) S3.T11 (Medium) S3.T16 (High) S3.T21 (Medium) S3.T27 (Low) S3.T28 (High) S3.T30 (High) S3.T31 (High) S3.T60 (High)	High
Detective (coso) Detect (NIST CSF)	[S3.C33, depends on S3.C31] Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Encrypt an object using an unauthorized key; it should be detected.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC15 S3.FC26	S3.T1 (Low) S3.T2 (Low) S3.T4 (Low) S3.T5 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low)	Low

					S3.T16 (Low) S3.T21 (Low) S3.T27 (Very Low) S3.T28 (Low) S3.T30 (Low) S3.T31 (Low)	
--	--	--	--	--	---	--

## Block changes to make an object public via object ACL [s3.co10]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C34, assured by S3.C36] Deny requests to change object ACL to public (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy with a deny statement on PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups "http://acs.amazonaws.com/groups/global/AllUsers" and "http://acs.amazonaws.com/groups/global/AuthenticatedUsers").	Make a call to create a public ObjectACL; it should be denied.	Medium	S3.FC1 S3.FC5	S3.T6 (Very High) S3.T36 (Very High)	High
Detective (coso) Detect (NIST CSF)	[S3.C35] Monitor ObjectACL changes (or tentative changes) to public using CloudTrail S3 data events.	Make a call to create a public ObjectACL; it should be detected.	Low	S3.FC1 S3.FC5	S3.T6 (Low) S3.T36 (Low)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C36] Verify the control blocking change ObjectACL to public (e.g., an SCP and VPC endpoint policy) is properly implemented.	Remove the control blocking changes of ObjectACL to public; it should be detected.	High	S3.FC1 S3.FC5	-	High
Detective (coso) Detect (NIST CSF)	[S3.C37] Monitor and investigate anonymous requests to objects (e.g., using CloudTrail S3 data events with userIdentity.accountId=ANONYMOUS_PRINCIPAL).	Make an anonymous call; it should be detected.	Low	S3.FC5	S3.T36 (Low)	Low

## Prevent deletion of buckets [s3.co11]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C38, assured by S3.C39] Block the action "s3:DeleteBucket" (e.g., via SCP or in an RCP applied to the OU or AWS account; exemption can be managed by authorizing a SuperAdmin to delete buckets with a certain tag, and with bucket owners able to tag buckets).	Do a DeleteBucket; it should be denied.	Low	S3.FC5	S3.T1 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C39] Verify the control blocking the action "s3:DeleteBucket" is properly implemented.	Remove the control blocking the action "s3:DeleteBucket"; it should be detected.	High	S3.FC5	-	High
Detective (coso) Detect (NIST CSF)	[S3.C40] Scan your CNAME records (e.g., in Amazon Route 53) and CloudFront origin for deleted buckets.	Create a CNAME record and CloudFront origin with an invalid bucket; it should be detected.	High	S3.FC5	S3.T1 (Very Low)	Very Low

## Enforce secure SDLC processes [s3.co12]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[S3.C41] Parameterize the S3 bucket name or S3 access point in your code (no hardcoding).	Request the process ensuring S3 bucket names or S3 access points are not hard-coded.	Medium	S3.FC5	S3.T1 (Low)	Low
Directive (COSO) Protect (NIST CSF)	[S3.C42] When connecting to S3 endpoints, use the virtual-hosted model ("my-bucket-name.s3.amazonaws.com" or "my-bucket-name.my-s3-regional-endpoint.amazonaws.com") instead of the path-style model ("s3.amazonaws.com/my-bucket-name" or "my-s3-regional-endpoint.amazonaws.com/my-bucket-name") (see <a href="#">ref</a> ). All the latest SDKs make use of domain style by default.	Request the mechanism ensuring the use of domain style instead of path style.	Very Low	S3.FC1	S3.T35 (High)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C43] Monitor that all S3 connections are made with the virtual-hosted model (e.g., via CloudTrail S3 requestParameters.Host).	Make a path-style request to S3; it should be detected.	Medium	S3.FC1	S3.T35 (Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[S3.C44] Ensure the integrity of stored objects ( <a href="#">ref</a> ), using "x-amz-checksum" from the <a href="#">object metadata</a> instead of ETag (e.g., using the compute checksum functionality in S3 Batch Operations). If ETag is used, make sure to properly account for its different definitions ( <a href="#">ref</a> ).	Request 1) the mechanism ensuring the integrity of stored objects using checksums instead of ETag, and otherwise ensuring ETag's different definitions are properly accounted for, and 2) plan to move any older system using ETag to use the checksum metadata.	Low	S3.FC1 S3.FC5	S3.T17 (Medium) S3.T27 (High)	Medium
Directive (COSO) Protect (NIST CSF)	[S3.C45] Do not include sensitive data in bucket names, access point names, object names, object metadata, and tags.	Request the process ensuring no sensitive data is included in bucket names, object names, object metadata, and tags.	Low	S3.FC12 S3.FC20	S3.T41 (Low) S3.T42 (Medium)	Very Low
Directive (COSO) Protect (NIST CSF)	[S3.C46] Ensure all S3 buckets interacted with are in the correct AWS account (e.g., using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner).	Request the process ensuring that all S3 buckets interacted with are in the correct AWS account.	Medium	S3.FC1 S3.FC5	S3.T1 (Medium) S3.T3 (Medium)	Medium
Directive (COSO) Protect (NIST CSF)	[S3.C113, depends on S3.C11] When transmitting an object to an external bucket with bucket-owner-full-control ACL requirements but without S3 Object Ownership handover, use 2 separate APIs (PutObject and PutObjectAcl) instead of the built-in object ACL operation in PutObject.	Request the process for ensuring that PutObject requests on an external bucket with a bucket-owner-full-control ACL requirement, but without S3 Object Ownership handover, use 2 separate APIs.	Medium	S3.FC1	S3.T43 (High)	High

## Block direct public access [s3.co13]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[S3.C47, assured by S3.C48] Front buckets that are required to be public, using authenticated CDN (e.g., CloudFront) or API Gateway, protected with WAF (e.g., for <a href="#">hotlinking</a> ).	Request the process ensuring that buckets required to be public are fronted by an authenticated CDN or API Gateway, and are protected with a WAF.	Medium	S3.FC5 S3.FC16	S3.T13 (Very High) S3.T14 (Medium) S3.T22 (Very High)	High
Assurance (COSO) Detect (NIST CSF)	[S3.C48] Verify no bucket is available publicly for write or read (e.g., using the AWS Config rules: <a href="#">S3_BUCKET_PUBLIC_READ_PROHIBITED</a> and <a href="#">S3_BUCKET_PUBLIC_WRITE_PROHIBITED</a> ).	Create a public S3 bucket; it should be detected.	Very Low	S3.FC5 S3.FC16	-	High

Directive (coso) Protect (NIST CSF)	[S3.C49, assured by S3.C50] Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Request 1) the mechanism ensuring account-level S3 Block Public Access is enabled on all AWS accounts, 2) its records of execution for all new AWS accounts, and 3) the plan to move any older AWS accounts.	Very Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C50] Verify account-level S3 Block Public Access is enabled on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g., using the AWS Config rule: <a href="#">S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS</a> ).	Remove the account-level S3 Block Public Access of an AWS account; it should be detected.	Very Low	S3.FC5 S3.FC8 S3.FC10	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C51, assured by S3.C52] Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023).	Request 1) the mechanism ensuring S3 Block Public Access is enabled on each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C52] Verify S3 Block Public Access is enabled on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g., using the AWS Config rule: <a href="#">S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED</a> ).	Remove the S3 Block Public Access from an S3 bucket; it should be detected.	Very Low	S3.FC5 S3.FC8 S3.FC10	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C53, assured by S3.C54] Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Request 1) the mechanism ensuring S3 Block Public Access is enabled on each S3 access point, 2) its records of execution for all new S3 access points, and 3) the plan to move any older S3 access points.	Low	S3.FC5 S3.FC10 S3.FC26 S3.FC33	S3.T14 (High) S3.T36 (Medium) S3.T37 (Medium) S3.T38 (Medium) S3.T54 (High) S3.T55 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C54] Verify S3 Block Public Access is enabled on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Remove S3 Block Public Access of 1) an access point, and 2) a Multi-Region Access Point; it should be detected.	Medium	S3.FC5 S3.FC10 S3.FC26 S3.FC33	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C173] Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Request the mechanism enforcing block of public access to each bucket at the organization root, OU, or account-level via S3 policies, its records of execution for all new AWS accounts, and the plan to move any older AWS accounts.	Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High

## Block bucket ACL [s3.co14]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C55, assured by S3.C57] Deny requests to add an ACL on a bucket (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy, with a deny statement on "s3:PutBucketAcl").	Make a call to add an ACL on a bucket; it should be denied.	Medium	S3.FC8 S3.FC19	S3.T4 (Very High) S3.T58 (Very High)	High
Detective (coso) Detect (NIST CSF)	[S3.C56] Monitor changes to bucket ACLs to ensure they stay private (e.g., using the CloudTrail event PutBucketAcl and its field requestParameters.x-amz-acl, which should either be	Make a call to have a bucket ACL other than private; it should be detected.	Medium	S3.FC8 S3.FC19	S3.T4 (Low) S3.T58 (Low)	Low

	"private" or not exist).					
Assurance (COSO) Detect (NIST CSF)	[S3.C57] Verify the control blocking bucket ACL changes is properly implemented.	Remove the control blocking bucket ACL changes; it should be detected.	High	S3.FC8 S3.FC19	-	High

## Identify and ensure the protection of all internal buckets hosting your objects [s3.co15]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[S3.C58] Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Request the list of all buckets you control and their related requirements, and the mechanism and records to ensure the accuracy of that metadata.	High	S3.FC1 S3.FC2 S3.FC5 S3.FC8 S3.FC10 S3.FC13 S3.FC16 S3.FC17 S3.FC19 S3.FC23 S3.FC36	S3.T1 (Very Low) S3.T3 (Very Low) S3.T4 (Very Low) S3.T5 (Very Low) S3.T6 (Very Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (High) S3.T12 (Very Low) S3.T13 (Very Low) S3.T14 (Very Low) S3.T15 (Very Low) S3.T16 (Very Low) S3.T17 (Very High) S3.T20 (Very Low) S3.T21 (Very Low) S3.T25 (Low) S3.T30 (Very Low) S3.T31 (Very Low) S3.T33 (Very Low) S3.T34 (Very Low) S3.T35 (Very Low) S3.T36 (Very Low) S3.T37 (Very Low) S3.T39 (Very Low) S3.T59 (Very Low) S3.T61 (Very Low) S3.T64 (Very Low) S3.T65 (Very Low)	Very High
Detective (COSO) Detect (NIST CSF)	[S3.C59, depends on S3.C58] Use a data discovery tool (e.g., Amazon Macie) to ensure no sensitive data is stored in an unauthorized bucket.	Upload higher classification data in a bucket; it should be detected.	Medium	S3.FC5	S3.T11 (Medium)	Medium
Detective (COSO) Detect (NIST CSF)	[S3.C60] Use a data discovery tool (e.g., Amazon Macie) to ensure the bucket names, object names, tags, and metadata do not contain sensitive data.	Create a bucket name, object name, tags, or metadata of an object with sensitive data; it should be detected.	Very High	S3.FC5	S3.T11 (Very Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[S3.C171, depends on S3.C58, assured by S3.C172] Ensure only the authorized ABAC configuration for each general purpose bucket is configured.	Request 1) the mechanism ensuring only the authorized ABAC configuration for each general purpose bucket is configured, 2) its records of execution for all new general purpose buckets, and 3) the plan to move any older general purpose buckets.	Medium	S3.FC36	S3.T64 (High)	Medium

Assurance (coso) Detect (NIST CSF)	[S3.C172] Verify all general purpose buckets use their authorized ABAC configuration.	1) Enable ABAC on an unauthorized general purpose bucket, or 2) disable ABAC on an authorized general purpose bucket; it should be detected.	Medium	S3.FC36	-	Medium
---------------------------------------	--	--	--------	---------	---	--------

## Enforce encryption at rest [S3.C016]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C61, depends on S3.C58] Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).	Request the list of authorized KMS key(s) for each bucket, its review process, and its review records.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC23	S3.T11 (Very Low) S3.T16 (Very Low) S3.T17 (Very Low) S3.T20 (Very Low) S3.T30 (Very Low) S3.T36 (Very Low) S3.T37 (Very Low) S3.T65 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C140, depends on S3.C61, assured by S3.C62] Ensure all objects in S3 buckets are encrypted with an authorized KMS key.	Request the mechanism (including training or utility) ensuring only authorized KMS keys are used for any objects stored in S3.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC23	S3.T11 (Medium) S3.T16 (Medium) S3.T17 (Medium) S3.T20 (Medium) S3.T30 (Medium) S3.T36 (Medium) S3.T37 (Medium) S3.T65 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C62] Verify all objects in S3 buckets are encrypted with an authorized KMS key (e.g., using S3 Inventory or S3 Batch Operations, see <a href="#">blog</a> , or <a href="#">S3 Storage Lens</a> , UnencryptedObjectCount and SSEKMSEnabledBucketCount).	Upload encrypted data 1) using an unauthorized KMS key, or 2) using SSE-S3; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC23	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C63, depends on S3.C61] Use KMS ThreatModel to protect the KMS keys used for S3 (e.g., using encryptionContext on the policy of each KMS key).	Request the KMS ThreatModel and the evidence of its application to protect S3.	High	S3.FC1 S3.FC5 S3.FC10 S3.FC23	S3.T17 (Medium) S3.T36 (Low) S3.T37 (Low) S3.T65 (Medium)	Low
Directive (coso) Protect (NIST CSF)	[S3.C64, depends on S3.C61, assured by S3.C65] Implement an authorized default encryption key on each bucket; enable S3 Bucket Key if not using DSSE-KMS and if CloudTrail events are not required for KMS encrypt/decrypt (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings).	Request 1) the mechanism implementing an authorized default encryption key on each bucket and enabling S3 Bucket Key, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC1 S3.FC5 S3.FC10	S3.T17 (Medium) S3.T20 (High) S3.T36 (High) S3.T37 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C65] Verify each bucket has an authorized default encryption key and has S3 Bucket Key enabled.	Create/modify a bucket 1) without default encryption, 2) with an incorrect default encryption key, or 3) with S3 Bucket Key disabled; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC10	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C66, depends on S3.C61, assured by S3.C67] Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key).	Make a request encrypted with an unauthorized KMS key; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC10	S3.T11 (High) S3.T16 (High) S3.T17 (High) S3.T20 (Very High) S3.T30 (High) S3.T36 (High) S3.T37 (High)	High
Assurance (coso)	[S3.C67]	Create a bucket not blocking PutObject requests with an	Medium	S3.FC1	-	High

Detect (NIST CSF)	Verify all buckets block PutObject requests with an unauthorized KMS key (e.g., using the Config rule: <a href="#">S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE</a> , note that a new rule needs to be deployed for each configuration, then the resource tracked by name or tag; alternatively, you might use <a href="#">S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</a> to ensure limited coverage).	unauthorized KMS key; it should be detected.		S3.FC5 S3.FC10		
Detective (coso) Detect (NIST CSF)	[S3.C68, depends on S3.C61] Monitor that only authorized KMS keys are used for each bucket (using CloudTrail S3 data events in "requestParameters.bucketName" and "response.x-amz-server-side-encryption-aws-kms-key-id").	Make a request encrypted with an unauthorized KMS key; it should be detected.	Low	S3.FC5	S3.T11 (Very Low) S3.T16 (Low) S3.T30 (Very Low) S3.T36 (Low)	Low
Directive (coso) Identify (NIST CSF)	[S3.C145] Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C).	Request the list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C), its review process, and its review records.	Medium	S3.FC5 S3.FC10 S3.FC23	S3.T11 (Very Low) S3.T16 (Very Low) S3.T20 (Very Low) S3.T30 (Very Low) S3.T36 (Very Low) S3.T37 (Very Low) S3.T63 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C146, depends on S3.C145, assured by S3.C147] For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-algorithm"="AES256" is not present).	Make a request to a bucket (or path) requiring SSE-C without the proper encryption; it should be denied.	Low	S3.FC5 S3.FC10	S3.T11 (High) S3.T16 (High) S3.T20 (Very High) S3.T30 (High) S3.T36 (High) S3.T37 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C147] For buckets (or paths) requiring SSE-C, verify all buckets block PutObject requests with unauthorized encryption.	Create a bucket requiring SSE-C, not blocking PutObject requests with unauthorized encryption; it should be detected.	High	S3.FC5 S3.FC10	-	High
Detective (coso) Detect (NIST CSF)	[S3.C148, depends on S3.C145] For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in requestParameters.bucketName and response.x-amz-server-side-encryption-customer-algorithm).	Make a request to a bucket (or path) requiring SSE-C without the proper encryption; it should be detected.	Low	S3.FC5	S3.T11 (Very Low) S3.T16 (Low) S3.T30 (Very Low) S3.T36 (Low)	Low
Preventative (coso) Protect (NIST CSF)	[S3.C162, depends on S3.C58] Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse").	Make a request not using DSSE-KMS on a required S3 bucket; it should be denied.	Low	S3.FC1 S3.FC5	S3.T5 (Low) S3.T7 (Low) S3.T8 (Low) S3.T11 (Low) S3.T31 (Low)	Low
Detective (coso) Detect (NIST CSF)	[S3.C163, depends on S3.C58] Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Make a request not using DSSE-KMS on a required S3 bucket; it should be detected.	Low	S3.FC1 S3.FC5	S3.T5 (Very Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T11 (Very Low) S3.T31 (Very Low)	Very Low
Directive (coso) Protect (NIST CSF)	[S3.C167, depends on S3.C145, assured by S3.C168] Ensure SSE-C is blocked when not required for each bucket [default from April 2026].	Request 1) the mechanism ensuring SSE-C is blocked when not required for each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC5 S3.FC23	S3.T16 (High) S3.T63 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C168] Verify SS3-C is blocked only when not required for each bucket.	1) Block SSE-C on a bucket requiring SSE-C, or 2) remove the block on SSE-C on a bucket not requiring SSE-C; it should be detected.	Low	S3.FC5 S3.FC23	-	High

Detective (COSO) Detect (NIST CSF)	[S3.C169] Monitor abnormal increases in the CloudWatch metric for HTTP 4xx client error status code requests (i.e., "4xxErrors").	Run HTTP 4xx client error status code requests abnormally; it should be detected.	High	S3.FC23	S3.T63 (Low)	Very Low
---------------------------------------	--	---	------	---------	--------------	----------

## Protect primary data against loss [S3.C017]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[S3.C69, depends on S3.C58, assured by S3.C70] Enable versioning on buckets holding primary data.	Request the mechanism used to ensure versioning on buckets holding primary data, and its records.	Very Low	S3.FC1 S3.FC5	S3.T16 (High) S3.T17 (High)	High
Assurance (COSO) Detect (NIST CSF)	[S3.C70] Verify buckets holding primary data are versioned (e.g., using <a href="#">S3_BUCKET_VERSIONING_ENABLED</a> ).	Remove versioning from a bucket holding primary data; it should be detected.	Low	S3.FC1 S3.FC5	-	High
Directive (COSO) Recover (NIST CSF)	[S3.C71, depends on S3.C58] Back up primary data in a secure location under a different security authority (e.g., in an <a href="#">AWS data bunker account</a> via replication, or using AWS Backup for Amazon S3).	Request the mechanism used to back up primary data in a location that has a different security authority, its records of execution, and its records of restoration testing.	Medium	S3.FC1 S3.FC5 S3.FC13	S3.T16 (High) S3.T17 (High) S3.T25 (High)	Medium

## Encrypt or tokenize critical data [S3.C018]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[S3.C72] Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Request the governance and mechanism(s) used to protect data (e.g., encrypt or tokenize critical data on the client side).	Very High	S3.FC1 S3.FC5 S3.FC10 S3.FC16	S3.T1 (Medium) S3.T3 (Medium) S3.T5 (High) S3.T7 (High) S3.T11 (Very High) S3.T12 (Very High) S3.T13 (Very High) S3.T17 (High) S3.T20 (High) S3.T30 (High) S3.T31 (High)	Medium

## Have a process to apply legal holds [S3.C019]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Protect (NIST CSF)	[S3.C73] Create a process to apply a legal hold to any S3 bucket whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.	Request the process of applying legal hold, and its records.	Medium	S3.FC1 S3.FC5	S3.T16 (Low) S3.T17 (Medium)	Medium

## Protect data integrity using S3 Object Lock [S3.C020]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
------	---------	---------	--------	-------------------	----------------------	------------------------

Preventative (coso) Protect (NIST CSF)	[S3.C74, depends on S3.C58, assured by S3.C75] Implement the authorized default S3 Object Lock on buckets requiring WORM (note: Amazon S3 evaluates and applies bucket policies before applying the bucket default S3 Object Lock settings).	Upload an object without the appropriate S3 Object Lock; it should have the S3 Object Lock applied automatically.	Low	S3.FC1 S3.FC5 S3.FC13 S3.FC17	S3.T16 (High) S3.T17 (High) S3.T25 (High) S3.T61 (Medium)	High
Assurance (coso) Detect (NIST CSF)	[S3.C75] Verify all buckets requiring WORM have the correct default S3 Object Lock configuration.	Create a bucket requiring WORM 1) without S3 Object Lock or 2) with an incorrect default S3 Object Lock; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC13 S3.FC17	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C76, depends on S3.C58, assured by S3.C77] Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on buckets requiring WORM (e.g., using their bucket policy and centrally in an RCP applied to the OU or the AWS account with a deny statement on PutObject and PutObjectRetention if the condition "s3:object-lock-mode" exists and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration).	Make a request with an incorrect S3 Object Lock configuration on a bucket requiring WORM; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC17	S3.T16 (High) S3.T17 (High) S3.T61 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C77] Verify all buckets requiring WORM block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock (e.g., using the Config rule: <a href="#">S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE</a> , note that a new rule needs to be deployed for each configuration, then the resource tracked by name or tag).	Create a bucket requiring WORM that does not block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC17	-	High

## Remove incomplete multipart uploads [s3.co21]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C78, assured by S3.C79] Reduce costs related to incomplete multipart uploads by creating a lifecycle policy to remove them after an agreed length of time (e.g., 7 days) ( <a href="#">blog</a> ).	Create an incomplete upload, and wait for the agreed time; it should be deleted automatically.	Low	S3.FC5	S3.T40 (High)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C79] Verify a lifecycle policy on incomplete multipart uploads is implemented on all buckets (e.g., using AWS Config rule: <a href="#">S3_LIFECYCLE_POLICY_CHECK</a> ).	Create a bucket without a lifecycle policy to remove incomplete multipart uploads; it should be detected.	Medium	S3.FC5	-	Low

## Block deprecated actions [s3.co22]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C80] Block deprecated S3 actions using IAM ThreatModel and the S3 actions list.	Request the controls blocking deprecated S3 actions.	Low	S3.FC1	S3.T35 (Medium)	Very Low

## Enforce SigV4 on all requests [s3.co23]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C81] Block all requests not using SigV4 (e.g., using an SCP, bucket policies, or centrally in an RCP applied to the OU or AWS account on all buckets with deny on "StringNotEquals": {"s3:signatureversion": "AWS4-HMAC-SHA256"}).	Make a non-SigV4 AWS API call; it should be denied.	Low	S3.FC1	S3.T35 (High)	Low
Detective (coso) Detect (NIST CSF)	[S3.C82] Monitor and investigate any requests not using SigV4 (e.g., via CloudTrail S3 when the additionalEventData.SignatureVersion is different from "SigV4").	Make a non-SigV4 AWS API call; it should be detected.	Low	S3.FC1	S3.T35 (Low)	Very Low
Directive (coso) Protect (NIST CSF)	[S3.C83] Use SDK with SigV4 enabled ( <a href="#">ref</a> ).	Request the mechanism ensuring the use of SDK with SigV4 enabled.	Low	S3.FC1	S3.T35 (High)	Low

## Block all requests not using an HTTP authorization header, if not explicitly authorized [s3.co24]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Preventative (coso) Protect (NIST CSF)	[S3.C84] Block all requests not using HTTP authorization header, i.e., presigned via query strings or POST ( <a href="#">ref</a> ) (e.g., using an SCP, bucket policies, or centrally in an RCP applied to the OU or AWS account on all buckets with deny on "StringNotEquals": {"s3:authType": "REST-HEADER"}). Note that it blocks uploads via the console, as well.	Make a request without using the HTTP authorization header; it should be denied.	Low	S3.FC5	S3.T39 (Medium)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C85] Monitor and investigate all requests that do not use the HTTP authorization header (e.g., via CloudTrail S3 events where the additionalEventData.AuthenticationMethod is different from "AuthHeader").	Make 1) a presigned AWS API call and 2) a POST request without the HTTP authorization header; it should be detected.	Low	S3.FC5	S3.T39 (Very Low)	Low

## Restrict bucket replication [s3.co25]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C86] Maintain a list of authorized buckets to have replication enabled, their target bucket, and replication type (i.e., encryption type, ownership, RTC, etc.) ( <a href="#">ref</a> ).	Request the list of authorized buckets to have replication enabled, their target bucket and replication rights, its review process, and its review records.	Medium	S3.FC15	S3.T2 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C134, depends on S3.C86, assured by S3.C87,S3.C88,S3.C117] Ensure only authorized buckets have replication enabled and are configured correctly.	Request 1) the mechanism ensuring only authorized buckets have replication enabled with their correct configuration, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC15	S3.T2 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C87] Verify only authorized buckets have replication enabled with their correct configuration (e.g., using <a href="#">S3 Storage Lens</a>	Configure replication on a non-authorized bucket; it should be detected.	Medium	S3.FC15	-	Medium

	CrossAccountReplicationRuleCount).						
Assurance (COSO) Detect (NIST CSF)	[S3.C88] Verify authorized buckets have the correct replication configuration.	Modify the configuration of an authorized replication; it should be detected.	High	S3.FC15	-	Medium	
Directive (COSO) Identify (NIST CSF)	[S3.C89] Maintain a list of IAM roles used for replication, ideally dedicated (e.g., using change management process on infrastructure-as-code).	Request the list of all IAM roles configured for replication.	Medium	S3.FC15	S3.T2 (Very Low)	Medium	
Directive (COSO) Protect (NIST CSF)	[S3.C138, depends on S3.C89, assured by S3.C92] Ensure only authorized IAM roles are attached for each replication, ideally dedicated.	Request the mechanism ensuring authorized IAM roles are attached for each replication, and the evidence of its execution for all replication configurations.	Medium	S3.FC15	S3.T2 (High)	Medium	
Directive (COSO) Protect (NIST CSF)	[S3.C90, depends on S3.C89] Limit S3 access to the source and destination buckets and the replication rights of each authorized IAM role configured for replication.	Request the S3 access for each replication role, and how they align with the replication requirements.	Medium	S3.FC15	S3.T2 (Medium)	Medium	
Directive (COSO) Protect (NIST CSF)	[S3.C91, depends on S3.C89] Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Request the IAM ThreatModel and the evidence of its application to the IAM roles used for replication.	High	S3.FC15	S3.T2 (High)	Medium	
Assurance (COSO) Detect (NIST CSF)	[S3.C92] Verify only the authorized IAM role is configured for each replication.	Create/modify a replication with an unauthorized IAM role; it should be detected.	High	S3.FC15	-	Medium	
Detective (COSO) Detect (NIST CSF)	[S3.C116] Monitor abnormal behavior on replication CloudWatch metrics (i.e., "BytesPendingReplication", "OperationsPendingReplication", and "OperationsFailedReplication").	Create an abnormal replication, or block a replication; it should be detected.	Low	S3.FC15	S3.T2 (Low) S3.T49 (Medium)	Low	
Assurance (COSO) Detect (NIST CSF)	[S3.C117] Verify all replicated buckets have metrics enabled on each replication rule (included by default in S3 RTC).	Modify the replication metric of an authorized replication; it should be detected.	Medium	S3.FC15	-	Medium	

## Scan objects used for input/output of a workflow for malware [s3.co26]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Detective (COSO) Detect (NIST CSF)	[S3.C93, depends on S3.C58] If the bucket is used as an input or the output of a process, scan the objects for malware (e.g., using <a href="#">GuardDuty Malware Protection for S3</a> , <a href="#">BucketAV</a> , <a href="#">Cloud Storage Security</a> , <a href="#">Trend Micro Cloud One</a> , or your own scanning solution).	Inject a malware test file; it should be detected.	Medium	S3.FC5 S3.FC16	S3.T14 (Medium) S3.T15 (Low)	Medium

## Control event receivers [s3.co27]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[S3.C94] Maintain a list of authorized notification receivers (e.g., SNS topic, Lambda) for each bucket. You might use a simpler approach by using authorized account IDs to ensure all your receivers are in authorized AWS accounts.	Request the list of authorized notification receivers for each bucket, its review process, and its review records.	Low	S3.FC20	S3.T41 (Very Low)	Low

Directive (COSO) Protect (NIST CSF)	[S3.C135, depends on S3.C94, assured by S3.C95] Ensure only authorized notification receivers for each bucket are configured.	Request 1) the mechanism ensuring only authorized notification receivers for each bucket are configured, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC20	S3.T41 (High)	Low
Assurance (COSO) Detect (NIST CSF)	[S3.C95] Verify only authorized notification receiver(s) are configured for buckets.	Create an unauthorized receiver; it should be detected.	High	S3.FC20	-	Low

## Control the data collected and the storage location of the inventory [s3.co28]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[S3.C96] Maintain a list of authorized S3 buckets to receive the S3 Inventory of each bucket.	Request the list of authorized bucket(s) to receive S3 Inventory of each bucket, its review process, and its review records.	Low	S3.FC12	S3.T42 (Very Low)	Very Low
Directive (COSO) Protect (NIST CSF)	[S3.C136, depends on S3.C96, assured by S3.C97] Ensure only authorized S3 buckets are configured to receive S3 Inventory for each bucket.	Request 1) the mechanism ensuring only authorized S3 buckets are configured to receive S3 Inventory for each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC12	S3.T42 (Medium)	Very Low
Assurance (COSO) Detect (NIST CSF)	[S3.C97] Verify only authorized buckets are configured to receive inventory.	Create an unauthorized bucket to receive inventory; it should be detected.	High	S3.FC12	-	Very Low
Directive (COSO) Identify (NIST CSF)	[S3.C164, depends on S3.C26] Maintain the list of authorized optional fields allowed to be accessed by each authorized IAM principal.	Request the list of authorized optional fields allowed to be accessed by each authorized IAM principal, its review process, and its review records.	High	S3.FC12	S3.T42 (Very Low)	Very Low
Preventative (COSO) Protect (NIST CSF)	[S3.C165, depends on S3.C164] Prevent the creation of inventories without authorized optional fields (e.g., by using an SCP and/or an IAM policy on "s3:PutInventoryConfiguration" with an allow statement on "s3:InventoryAccessibleOptionalFields" = authorized optional fields only).	Create an inventory with an unauthorized optional field; it should be denied.	Low	S3.FC12	S3.T42 (Medium)	Very Low

## Limit access from only authorized VPCs [s3.co29]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (COSO) Identify (NIST CSF)	[S3.C98] For each S3 bucket, maintain a list of VPCs authorized to access it.	For each S3 bucket, request the list of authorized VPCs to access it, its review process, and its review records.	Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10	S3.T11 (Very Low) S3.T14 (Very Low) S3.T17 (Very Low) S3.T30 (Very Low) S3.T33 (Very Low) S3.T36 (Very Low) S3.T38 (Very Low) S3.T39 (Very Low)	Very High
Preventative (COSO) Protect (NIST CSF)	[S3.C99, depends on S3.C98, assured by S3.C100] Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpc" is met, or if the bucket policy size is	Make a request to the bucket outside an authorized VPC; it should be denied.	Very Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10	S3.T11 (Medium) S3.T14 (Medium) S3.T17 (Medium) S3.T30 (High)	Very High

	beyond the limit, use this condition on the access point).				S3.T33 (High) S3.T36 (High) S3.T38 (High) S3.T39 (High)	
Assurance (coso) Detect (NIST CSF)	[S3.C100] Verify all buckets include a control to limit access to only authorized VPCs (e.g., using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ).	Remove the control limiting access to only authorized VPC(s); it should be detected.	Medium	S3.FC1 S3.FC2 S3.FC5 S3.FC10	-	Very High

## Control CloudFront access [s3.co30]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C101] Maintain a list of authorized CloudFront distributions (via Origin Access Control) and associated bucket, access point, and/or Object Lambda Access Point.	Request the list of all authorized CloudFront distributions and associated S3 buckets, access points, and/or Object Lambda Access Points.	Low	S3.FC10	S3.T20 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C137, depends on S3.C101, assured by S3.C102] Ensure only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa (e.g., using their bucket policy, centrally in an RCP applied to the OU or AWS account, with a deny statement, access point policy, resource policy for an Object Lambda Access Point, limiting the access to only the authorized distribution(s) in the SourceArn).	Request 1) the mechanism ensuring only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa, 2) its records of execution for all new CloudFront distributions, and 3) the plan to move any older CloudFront distributions.	Medium	S3.FC10	S3.T20 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C102] Verify all associations of CloudFront distributions with buckets, access points, and/or Object Lambda Access Points are authorized (e.g., using the Macie finding: "Policy:IAMUser/S3BucketSharedWithCloudFront").	Create a non-authorized distribution or association; it should be detected.	High	S3.FC10	-	Medium

## Protect and/or claim your domains and trademarks/copyrights [s3.co31]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C103] Protect and/or claim your domains and trademarks/copyrights (by creating your trademark buckets and using the <a href="#">copyright infringement process</a> from AWS).	Request the process by protecting and/or claiming your domains and trademarks/copyrights.	Medium	S3.FC28	S3.T23 (High)	Low

## Restrict access point access to VPCs when in use [s3.co32]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C104] Maintain a list of authorized access between VPCs, S3 access points, and S3.	Request the list of authorized access between VPC, S3 access points, and S3.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC26	S3.T7 (Very Low) S3.T9 (Very Low) S3.T10 (Very Low) S3.T11 (Very Low)	High

				S3.FC28 S3.FC33	S3.T28 (Very Low) S3.T37 (Very Low) S3.T54 (Very Low) S3.T55 (Very Low) S3.T56 (Very Low) S3.T60 (Very Low)	
Preventative (coso) Protect (NIST CSF)	[S3.C105, depends on S3.C104, assured by S3.C109] Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy.	Make a request on an unauthorized access point or bucket; it should be denied.	Medium	S3.FC1 S3.FC5 S3.FC26 S3.FC28 S3.FC33	S3.T7 (Medium) S3.T9 (Very High) S3.T10 (Very High) S3.T11 (Medium) S3.T54 (Medium) S3.T55 (Medium)	High
Preventative (coso) Protect (NIST CSF)	[S3.C106, depends on S3.C104, assured by S3.C110] In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn".	Query the bucket outside the S3 access point; it should be denied.	Medium	S3.FC1 S3.FC10 S3.FC26 S3.FC33	S3.T7 (Medium) S3.T28 (High) S3.T37 (High) S3.T55 (Medium) S3.T56 (Very High) S3.T60 (High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C107] Block the creation of non-VPC S3 access point "s3>CreateAccessPoint" (e.g., using IAM policies and SCPs with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Make a request to create an internet-based access point; it should be denied.	Low	S3.FC1 S3.FC26	S3.T7 (Medium) S3.T28 (Very High) S3.T60 (High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C108, assured by S3.C111] Block all traffic from Internet-configured S3 access points (e.g., in their bucket policy, or centrally in an RCP applied to the OU or AWS account, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Create an internet-facing access point and try to access a bucket; it should be denied.	Low	S3.FC1 S3.FC26 S3.FC28	S3.T7 (Medium) S3.T10 (Medium) S3.T28 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C109] Verify only access points are used in the resource-level statements in VPC endpoints.	Create a VPC endpoint giving access to an S3 bucket directly, rather than an access point; it should be detected.	High	S3.FC1 S3.FC5 S3.FC26 S3.FC28 S3.FC33	-	High
Assurance (coso) Detect (NIST CSF)	[S3.C110] Verify S3 bucket policies deny unauthorized S3 access points.	Remove/modify the deny on the bucket policy; it should be detected.	High	S3.FC1 S3.FC10 S3.FC26 S3.FC33	-	High
Assurance (coso) Detect (NIST CSF)	[S3.C111] Verify all S3 access points are VPC-attached.	Create an internet-based access point; it should be detected.	Low	S3.FC1 S3.FC26 S3.FC28	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C112, depends on S3.C104] Block any <a href="#">object-related operations</a> access to S3 buckets not through an access point (i.e., IAM policy, SCP, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on the condition "ArnNotLike": {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"}).	Access any S3 bucket without using an access point; it should be denied.	Low	S3.FC1 S3.FC5	S3.T7 (Medium) S3.T11 (High)	High

## Restrict Batch access using dedicated IAM roles [S3.C033]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C120] Maintain a list of IAM roles used for Batch jobs, ideally dedicated (e.g., using change management process on infrastructure-as-code).	Request the list of all IAM roles configured for Batch jobs.	Medium	S3.FC27	S3.T44 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C139, depends on S3.C120, assured by S3.C123] Ensure only an authorized IAM role is attached to each Batch job.	Request the mechanism ensuring only an authorized IAM role is attached to each Batch job, and the evidence of its execution for all new {resource}.	Medium	S3.FC27	S3.T44 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C121, depends on S3.C120] Limit access to only the required resources/permissions (e.g., source/destination buckets, Lambda functions) for each authorized IAM role configured for Batch jobs.	Request access only to the required resources/permissions for each Batch IAM role, and request information on how they are aligned with the replication requirements.	Medium	S3.FC27	S3.T44 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C122, depends on S3.C120] Limit access to authorized IAM roles used for Batch jobs, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Request the IAM ThreatModel and the evidence of its application to the IAM roles used for Batch jobs.	Medium	S3.FC27	S3.T44 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C123] Verify only the authorized IAM role is configured for each Batch job.	Create/modify a Batch job with an unauthorized IAM role; it should be detected.	High	S3.FC27	-	Medium

## Enforce only authorized Object Lambda Access Point and associated access [S3.C034]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C125] Maintain a list of authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload.	Request the list of authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload, its review process, and its review records.	Low	S3.FC32	S3.T46 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C126, depends on S3.C125, assured by S3.C127] Ensure only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload are created.	Request the mechanism ensuring only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload, and the evidence of its execution.	Medium	S3.FC32	S3.T46 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C127] Verify only the authorized Lambda functions are configured on each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload.	Attach 1) an unauthorized Lambda function to an Object Lambda Access Point, 2) an unauthorized Object Lambda Access Point to an access point, 3) an authorized Lambda function with an unauthorized HEAD/LIST/GET request to an Object Lambda Access Point, and 4) an authorized Lambda function with an unauthorized payload; it should be detected.	Medium	S3.FC32	-	High
Directive (coso) Protect (NIST CSF)	[S3.C128] Ensure Lambda functions configured on Object Lambda Access Point are secured using Lambda ThreatModel.	Request the mechanism ensuring Lambda ThreatModel and its application for Lambda functions associated with Object Lambda Access Points, and its records of execution.	Medium	S3.FC32	S3.T46 (High)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C129] Maintain a list of cross-account access on each Object Lambda Access Point.	Request the list of authorized cross-account access for each Object Lambda Access Point, its review process, and its review records.	Very Low	S3.FC32	S3.T46 (Very Low)	Medium
Directive (coso)	[S3.C130, depends on S3.C129, assured by S3.C131] Ensure only authorized cross-account IAM entities are allowed	Request the mechanism ensuring only cross-account IAM	Low	S3.FC32	S3.T46 (Medium)	Medium

Protect (NIST CSF)	in the Object Lambda Access Point policy.	entities are allowed in the Object Lambda Access Point policy, and the evidence of its execution.				
Assurance (coso) Detect (NIST CSF)	[S3.C131] Verify only the authorized cross-account IAM entities are allowed in the Object Lambda Access Point policy.	Add an unauthorized cross-account IAM entity on an Object Lambda Access Point policy; it should be detected.	High	S3.FC32	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C132, assured by S3.C133] Ensure CloudWatch is enabled for all Object Lambda Access Points.	Request the mechanism ensuring CloudWatch is enabled for all Object Lambda Access Points, and its records of execution.	Low	S3.FC32	S3.T46 (Low)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C133] Verify CloudWatch is enabled for all Object Lambda Access Points.	Create an Object Lambda Access Point without CloudWatch enabled; it should be detected.	Low	S3.FC32	-	Low

## Deploy only authorized S3 websites and place them behind a CDN [s3.co35]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C141] Maintain a list of authorized buckets to be configured as an S3 website endpoint.	Request the list of authorized buckets to be configured as a website endpoint, its review process, and its review records.	Low	S3.FC16	S3.T13 (Very Low) S3.T29 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C142, depends on S3.C141, assured by S3.C143] Ensure only authorized buckets are configured as an S3 website endpoint.	Request 1) the mechanism ensuring only authorized buckets are configured as S3 website endpoints, 2) its records of execution for all new website-enabled buckets, and 3) the plan to move any older website-enabled buckets.	Medium	S3.FC16	S3.T13 (Medium) S3.T29 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C143] Verify only authorized buckets are configured as S3 website endpoints.	Enable static website hosting on an unauthorized bucket; it should be detected.	Medium	S3.FC16	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C144, depends on S3.C141] Ensure S3 website endpoints are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g., CloudFront).	Request the mechanism ensuring S3 website endpoints are protected with HTTP headers.	Medium	S3.FC16	S3.T13 (High) S3.T29 (Very High)	High

## Use an unguessable naming convention [s3.co36]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C29] Use an unguessable naming convention for the email addresses of your AWS accounts (e.g., add a + sign and a random string to redirect the email to the same mailbox).	Review the naming convention for root account email and its implementation.	Medium	S3.FC28	S3.T19 (High)	Low
Directive (coso) Protect (NIST CSF)	[S3.C30] Use an unguessable naming convention for your IAM users and IAM roles (e.g., add a random string).	Review the naming convention for IAM users/roles and their implementation.	Medium	S3.FC28	S3.T24 (High)	Low

## Disabling ACLs for all buckets [s3.co37]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C152, assured by S3.C154] Ensure bucket ACLs and object ACLs are disabled on each	Request 1) the mechanism ensuring bucket ACL and object ACL are disabled on each bucket, 2) its records of execution	Medium	S3.FC1 S3.FC5	S3.T4 (Very High) S3.T6 (Very High)	Very High

	bucket (enabled by default for all new buckets after April 2023).	for all new buckets, and 3) the plan to move any older buckets.		S3.FC8 S3.FC24 S3.FC25	S3.T36 (Very High) S3.T43 (Very High) S3.T52 (Very High) S3.T53 (Very High)	
Preventative (coso) Protect (NIST CSF)	[S3.C153] Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Create a bucket with ACL enabled; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	S3.T4 (High) S3.T6 (High) S3.T36 (High) S3.T43 (High) S3.T52 (High) S3.T53 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C154] Verify bucket ACL and object ACL are disabled on each bucket (e.g., using the AWS Config rule <a href="#">S3_BUCKET_ACL_PROHIBITED</a> for bucket ACL, <a href="#">S3 Storage Lens</a> ObjectOwnershipBucketOwnerEnforcedBucketCount, or S3 Inventory, which includes object ACL metadata).	Create/modify a bucket to enable ACL; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	-	Very High

## Ensure all requests are blocked from unauthorized service roles [s3.co38]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C155, assured by S3.C156] Ensure all requests are blocked from AWS service roles that do not require access (e.g., by denying all requests with the principal "arn:aws:iam::*:*/AWSServiceRoleFor*" on S3 bucket policies).	Request 1) the mechanism ensuring only authorized AWS service roles can access each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC28	S3.T57 (Very High)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C156] Verify all requests from unauthorized service roles are blocked.	Remove the statement on a bucket policy denying all unauthorized service roles; it should be detected.	Medium	S3.FC28	-	Low

## Enforce S3 server access logging on buckets [s3.co39]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Detect (NIST CSF)	[S3.C166, depends on S3.C58] Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Request 1) the mechanism ensuring server access logging is enabled in relevant buckets, 2) its records of execution for all new relevant buckets, and 3) the plan to move any older relevant buckets.	Low	S3.FC1 S3.FC5 S3.FC8	S3.T1 (Low) S3.T4 (Low) S3.T5 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T12 (Low) S3.T16 (Low) S3.T21 (Low) S3.T31 (Low) S3.T34 (Low) S3.T35 (Low) S3.T36 (Low)	Medium

					S3.T39 (Low)	
Detective (coso) Detect (NIST CSF)	[S3.C157, depends on S3.C58] Monitor PutBucketLogging to detect bucket server access logging changes, including deactivation and bucket changes (i.e., using the CloudTrail event "PutBucketLogging" and the "requestParameters.BucketLoggingStatus" field to examine the lack of the "LoggingEnabled" key or an unauthorized bucket in "requestParameters.BucketLoggingStatus.LoggingEnabled.TargetBucket").	Make a call to 1) disable bucket logging, or 2) change to an unauthorized bucket; it should be detected.	Low	S3.FC19	S3.T59 (Medium)	Very Low

## Restrict access points to authorized AWS accounts [s3.co40]

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C158] Maintain a list of authorized S3 buckets and their AWS accounts for cross-account access points.	Request the list of authorized S3 buckets and their AWS account for cross-account access points, its review process, and its review records.	Low	S3.FC26	S3.T60 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C159, depends on S3.C158, assured by S3.C161] Ensure only authorized S3 buckets and their AWS accounts for cross-account access points are configured.	Request 1) the mechanism ensuring only authorized S3 buckets and their AWS account for cross-account access points are configured, 2) its records of execution for all new S3 buckets and their AWS accounts for cross-account access points, and 3) the plan to move any older S3 buckets and their AWS accounts for cross-account access points.	Medium	S3.FC26	S3.T60 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C160, depends on S3.C158] Monitor CreateAccessPoint to detect unauthorized buckets or AWS accounts (i.e., using CloudTrail event CreateAccessPoint and its fields "requestParameters.CreateAccessPointRequest.Bucket" and "requestParameters.CreateAccessPointRequest.BucketAccountId").	Call the API to create a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	S3.T60 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C161] Verify only authorized S3 buckets and their AWS accounts for cross-account access points are used.	Deploy a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	-	Medium

# Compliance Mapping

## PCI DSS v4

PCI DSS v4	Control Objectives	Controls				
		Very High	High	Medium	Low	Very Low
1.1	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C8 S3.C120 S3.C122 S3.C139	S3.C16 S3.C121 S3.C123	-	-
1.2.1	[S3.CO27] Control event receivers [S3.CO34] Enforce only authorized Object Lambda Access Point and associated access [S3.CO38] Ensure all requests are blocked from unauthorized service roles	-	S3.C125 S3.C126 S3.C127	S3.C128 S3.C129 S3.C130 S3.C131	S3.C94 S3.C95 S3.C135 S3.C132 S3.C133 S3.C155 S3.C156	-
1.2.2	[S3.CO1] Enforce encryption in transit [S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO30] Control CloudFront access [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C8 S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C3 S3.C5 S3.C22 S3.C23 S3.C24 S3.C101 S3.C102 S3.C137	S3.C4 S3.C18 S3.C21 S3.C25	-
1.2.3	[S3.CO2] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
1.2.4 1.2.5	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO24] Block all requests not using an HTTP authorization header, if not explicitly authorized [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C8 S3.C120 S3.C122	S3.C16 S3.C84 S3.C121 S3.C123 S3.C139	S3.C85	-
1.2.6	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO24] Block all requests not using an HTTP authorization header, if not explicitly authorized	-	S3.C8	S3.C84	S3.C85	-

	[S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C06] Model the threats on all AWS services accessing S3 [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles	-	S3.C8 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C16 S3.C121 S3.C123 S3.C139 S3.C128 S3.C129 S3.C130 S3.C155 S3.C156	S3.C94 S3.C95 S3.C135 S3.C132 S3.C133 S3.C155 S3.C156	-
1.2.7	[S3.C02] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
1.2.8	[S3.C02] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
1.2.10	[S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles	-	S3.C8 S3.C17 S3.C19 S3.C24 S3.C20 S3.C27 S3.C124 S3.C28 S3.C26 S3.C170 S3.C149 S3.C121 S3.C150 S3.C151 S3.C123 S3.C139 S3.C128 S3.C122 S3.C125 S3.C126 S3.C127	S3.C22 S3.C23 S3.C24 S3.C25 S3.C18 S3.C21	-	-
1.3	[S3.C02] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
1.3.1 1.3.2	[S3.C01] Enforce encryption in transit [S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C029] Limit access from only authorized VPCs [S3.C030] Control CloudFront access [S3.C032] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C8 S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C3 S3.C5 S3.C22 S3.C23 S3.C24 S3.C18 S3.C21 S3.C25	S3.C4	-
1.3.3	[S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C024] Block all requests not using an HTTP authorization header, if not explicitly authorized	-	S3.C8	S3.C84	S3.C85	-
1.4	[S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C024] Block all requests not using an HTTP authorization header, if not explicitly authorized	S3.C98 S3.C99 S3.C100	S3.C8 S3.C17 S3.C19	S3.C22 S3.C23 S3.C21 S3.C24	S3.C18 S3.C21	-

	[S3.CO29] Limit access from only authorized VPCs [S3.CO30] Control CloudFront access [S3.CO32] Restrict access point access to VPCs when in use		S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C84 S3.C101 S3.C102 S3.C137	S3.C85	
1.4.1	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO24] Block all requests not using an HTTP authorization header, if not explicitly authorized	-	S3.C8	S3.C84	S3.C85	-
1.4.2	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C22 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118	S3.C18 S3.C21 S3.C25	-
1.4.3	[S3.CO13] Block direct public access [S3.CO30] Control CloudFront access	S3.C49 S3.C50 S3.C51 S3.C52 S3.C53 S3.C54 S3.C173	S3.C47 S3.C48	S3.C101 S3.C102 S3.C137	-	-
1.4.4	[S3.CO2] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
1.4.5	[S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C120 S3.C122	S3.C16 S3.C121 S3.C123 S3.C139	-	-
1.5	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO24] Block all requests not using an HTTP authorization header, if not explicitly authorized [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C8 S3.C120 S3.C122	S3.C16 S3.C84 S3.C121 S3.C123 S3.C139	S3.C85	-
1.5.1	[S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C120 S3.C122	S3.C16 S3.C121 S3.C123 S3.C139	-	-

2.2.1	[S3.C05] Identify and ensure the protection of all external buckets hosting your objects	S3.C11	S3.C15 S3.C114	S3.C12 S3.C13 S3.C14 S3.C115	-	-
2.2.2	[S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C05] Identify and ensure the protection of all external buckets hosting your objects [S3.C06] Model the threats on all AWS services accessing S3 [S3.C024] Block all requests not using an HTTP authorization header, if not explicitly authorized	S3.C11	S3.C8 S3.C15 S3.C114	S3.C12 S3.C13 S3.C14 S3.C115 S3.C16 S3.C84	S3.C85	-
2.2.4	[S3.C05] Identify and ensure the protection of all external buckets hosting your objects	S3.C11	S3.C15 S3.C114	S3.C12 S3.C13 S3.C14 S3.C115	-	-
2.2.5	[S3.C01] Enforce encryption in transit [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C029] Limit access from only authorized VPCs [S3.C030] Control CloudFront access [S3.C032] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C3 S3.C5 S3.C22 S3.C23 S3.C24 S3.C4 S3.C18 S3.C21 S3.C25	-	-
2.3	[S3.C01] Enforce encryption in transit	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119	S3.C3 S3.C5	S3.C4	-
2.3.1	[S3.C01] Enforce encryption in transit [S3.C09] Block requests with KMS keys from unauthorized AWS accounts [S3.C016] Enforce encryption at rest [S3.C018] Encrypt or tokenize critical data	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C31 S3.C32 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67	S3.C3 S3.C5 S3.C62 S3.C140 S3.C72	S3.C4 S3.C33 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169

				S3.C145 S3.C146 S3.C147 S3.C167 S3.C168			
2.3.2	[S3.CO19] Have a process to apply legal holds [S3.CO20] Protect data integrity using S3 Object Lock	-	S3.C74 S3.C75 S3.C76 S3.C77	S3.C73	-	-	
3.2.1	[S3.CO16] Enforce encryption at rest [S3.CO18] Encrypt or tokenize critical data	-	S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C62 S3.C140 S3.C72	S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169	
3.3.2	[S3.CO5] Identify and ensure the protection of all external buckets hosting your objects [S3.CO15] Identify and ensure the protection of all internal buckets hosting your objects [S3.CO16] Enforce encryption at rest [S3.CO18] Encrypt or tokenize critical data	S3.C11 S3.C58	S3.C15 S3.C114 S3.C61 S3.C64 S3.C14 S3.C65 S3.C66 S3.C67 S3.C171 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C12 S3.C13 S3.C14 S3.C115 S3.C68 S3.C59 S3.C172 S3.C171 S3.C172 S3.C148 S3.C162	S3.C63 S3.C68 S3.C148 S3.C162	S3.C60 S3.C163 S3.C169	
3.5.1	[S3.CO9] Block requests with KMS keys from unauthorized AWS accounts [S3.CO16] Enforce encryption at rest [S3.CO18] Encrypt or tokenize critical data	-	S3.C31 S3.C32 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C62 S3.C140 S3.C72	S3.C33 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169	
3.5.1.1	[S3.CO16] Enforce encryption at rest [S3.CO18] Encrypt or tokenize critical data	-	S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145	S3.C62 S3.C140 S3.C72	S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169	

				S3.C146 S3.C147 S3.C167 S3.C168			
3.5.1.2 3.5.1.3	[S3.C09] Block requests with KMS keys from unauthorized AWS accounts [S3.C016] Enforce encryption at rest [S3.C018] Encrypt or tokenize critical data	-	S3.C31 S3.C32 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C62 S3.C140 S3.C72	S3.C33 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169	
3.6.1 3.6.1.1 3.6.1.2 3.6.1.3 3.6.1.4 3.7.1 3.7.2 3.7.3 3.7.4	[S3.C01] Enforce encryption in transit [S3.C09] Block requests with KMS keys from unauthorized AWS accounts [S3.C016] Enforce encryption at rest [S3.C018] Encrypt or tokenize critical data	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C31 S3.C32 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C3 S3.C5 S3.C62 S3.C140 S3.C72	S3.C4 S3.C33 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169	
3.7.5	[S3.C09] Block requests with KMS keys from unauthorized AWS accounts [S3.C016] Enforce encryption at rest [S3.C018] Encrypt or tokenize critical data	-	S3.C31 S3.C32 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C62 S3.C140 S3.C72	S3.C33 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169	
3.7.6 3.7.7 3.7.9	[S3.C01] Enforce encryption in transit	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119	S3.C3 S3.C5	S3.C4	-	

4.1 4.2.1	[S3.C09] Block requests with KMS keys from unauthorized AWS accounts [S3.C016] Enforce encryption at rest [S3.C018] Encrypt or tokenize critical data	-	S3.C31 S3.C32 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C62 S3.C140 S3.C72	S3.C33 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169
4.2.1.1	[S3.C01] Enforce encryption in transit	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119	S3.C3 S3.C5	S3.C4	-
4.2.1.2 4.2.2	[S3.C026] Scan objects used for input/output of a workflow for malware	-	-	S3.C93	-	-
5.1.2 5.2.1 5.2.2 5.2.3 5.2.3.1 5.3.1 5.3.2 5.3.2.1 5.3.3 5.3.4 5.3.5	[S3.C031] Protect and/or claim your domains and trademarks/copyrights	-	-	-	S3.C103	-
5.4.1	[S3.C012] Enforce secure SDLC processes	-	S3.C113	S3.C44 S3.C46	S3.C41 S3.C42	S3.C43 S3.C45
6.2 6.2.1 6.2.2 6.2.3 6.2.3.1 6.2.4 6.3.1	[S3.C025] Restrict bucket replication	-	S3.C86 S3.C87 S3.C88 S3.C89 S3.C90 S3.C91 S3.C92 S3.C117 S3.C134 S3.C138	S3.C116	-	
6.3.2	[S3.C012] Enforce secure SDLC processes	-	S3.C113	S3.C44 S3.C46	S3.C41 S3.C42	S3.C43 S3.C45
6.4.1 6.4.2	[S3.C027] Control event receivers [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles	-	S3.C125 S3.C126 S3.C127	S3.C128 S3.C129 S3.C130	S3.C94 S3.C95	-

				S3.C131	S3.C132 S3.C133 S3.C155 S3.C156	
6.5 6.5.1	[S3.CO5] Identify and ensure the protection of all external buckets hosting your objects [S3.CO7] Control event receivers [S3.CO34] Enforce only authorized Object Lambda Access Point and associated access [S3.CO38] Ensure all requests are blocked from unauthorized service roles	S3.C11	S3.C15 S3.C114 S3.C125 S3.C126 S3.C127	S3.C12 S3.C13 S3.C14 S3.C115 S3.C128 S3.C129 S3.C130 S3.C131	S3.C94 S3.C95 S3.C135 S3.C132 S3.C133 S3.C155 S3.C156	-
6.5.2	[S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO12] Enforce secure SDLC processes [S3.CO27] Control event receivers [S3.CO33] Restrict Batch access using dedicated IAM roles [S3.CO34] Enforce only authorized Object Lambda Access Point and associated access [S3.CO38] Ensure all requests are blocked from unauthorized service roles	-	S3.C113 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C16 S3.C44 S3.C46 S3.C121 S3.C123 S3.C125 S3.C126 S3.C127	S3.C41 S3.C42 S3.C94 S3.C95 S3.C135 S3.C132 S3.C133 S3.C155 S3.C156	S3.C43 S3.C45
6.5.6	[S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.CO14] Block bucket ACL [S3.CO33] Restrict Batch access using dedicated IAM roles [S3.CO34] Enforce only authorized Object Lambda Access Point and associated access [S3.CO37] Disabling ACLs for all buckets [S3.CO38] Ensure all requests are blocked from unauthorized service roles [S3.CO40] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C17 S3.C19 S3.C20 S3.C27 S3.C124 S3.C26 S3.C149 S3.C150 S3.C151 S3.C55 S3.C57 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C22 S3.C23 S3.C24 S3.C27 S3.C28 S3.C170 S3.C121 S3.C123 S3.C139 S3.C128 S3.C129 S3.C130 S3.C131 S3.C155 S3.C156	S3.C18 S3.C21 S3.C25 S3.C56 S3.C132 S3.C133 S3.C155 S3.C156	-
7.1 7.2	[S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.CO10] Block changes to make an object public via object ACL [S3.CO14] Block bucket ACL [S3.CO20] Protect data integrity using S3 Object Lock [S3.CO33] Restrict Batch access using dedicated IAM roles [S3.CO34] Enforce only authorized Object Lambda Access Point and associated access [S3.CO37] Disabling ACLs for all buckets [S3.CO38] Ensure all requests are blocked from unauthorized service roles [S3.CO40] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C17 S3.C19 S3.C20 S3.C24 S3.C124 S3.C26 S3.C149 S3.C170 S3.C121 S3.C150 S3.C151 S3.C123 S3.C34 S3.C36 S3.C55	S3.C22 S3.C23 S3.C24 S3.C27 S3.C28 S3.C35 S3.C170 S3.C37 S3.C21 S3.C56 S3.C132 S3.C133 S3.C155 S3.C156	S3.C18 S3.C21 S3.C25 S3.C35 S3.C37 S3.C56 S3.C132 S3.C133 S3.C155 S3.C156	-

			S3.C57 S3.C74 S3.C75 S3.C76 S3.C77 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C130 S3.C131 S3.C158 S3.C159 S3.C160 S3.C161		
7.2.1	[S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C010] Block changes to make an object public via object ACL [S3.C020] Protect data integrity using S3 Object Lock [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles	-	S3.C17 S3.C19 S3.C20 S3.C124 S3.C26 S3.C149 S3.C150 S3.C151 S3.C34 S3.C36 S3.C74 S3.C75 S3.C76 S3.C77 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C22 S3.C23 S3.C24 S3.C150 S3.C27 S3.C151 S3.C28 S3.C170 S3.C121 S3.C123 S3.C139 S3.C133 S3.C128 S3.C129 S3.C120 S3.C130 S3.C122 S3.C125 S3.C126 S3.C131	S3.C18 S3.C21 S3.C25 S3.C35 S3.C37 S3.C132 S3.C133 S3.C155 S3.C156	-
7.2.2	[S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles	-	S3.C17 S3.C19 S3.C20 S3.C124 S3.C26 S3.C149 S3.C170 S3.C27 S3.C150 S3.C121 S3.C123 S3.C139 S3.C155 S3.C122 S3.C128 S3.C125 S3.C129 S3.C120 S3.C130 S3.C122 S3.C125 S3.C126 S3.C131	S3.C22 S3.C23 S3.C24 S3.C170 S3.C28 S3.C150 S3.C25 S3.C121 S3.C132 S3.C133 S3.C155 S3.C156	S3.C18 S3.C21 S3.C25 S3.C132 -	-
7.2.3	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks	-	S3.C26 S3.C149 S3.C150 S3.C151	S3.C27 S3.C28 S3.C170	-	-
7.2.4	[S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C010] Block changes to make an object public via object ACL [S3.C020] Protect data integrity using S3 Object Lock	-	S3.C17 S3.C19 S3.C20 S3.C124	S3.C22 S3.C23 S3.C24 S3.C25 S3.C27	S3.C18 S3.C21 S3.C25 S3.C35	-

	[S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles		S3.C26 S3.C149 S3.C150 S3.C151 S3.C34 S3.C36 S3.C74 S3.C75 S3.C76 S3.C77 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C28 S3.C170 S3.C121 S3.C133 S3.C123 S3.C139 S3.C128 S3.C129 S3.C130 S3.C131	S3.C37 S3.C132 S3.C133 S3.C155 S3.C156	
7.2.5	[S3.C03] Enable S3 data events in AWS CloudTrail [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C010] Block changes to make an object public via object ACL [S3.C017] Protect primary data against loss [S3.C020] Protect data integrity using S3 Object Lock [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles [S3.C039] Enforce S3 server access logging on buckets	-	S3.C17 S3.C19 S3.C20 S3.C124 S3.C26 S3.C149 S3.C150 S3.C151 S3.C34 S3.C36 S3.C74 S3.C75 S3.C76 S3.C77 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C9 S3.C22 S3.C23 S3.C24 S3.C27 S3.C28 S3.C170 S3.C171 S3.C172 S3.C173 S3.C174 S3.C175 S3.C176 S3.C177 S3.C178 S3.C179 S3.C180 S3.C181 S3.C182 S3.C183 S3.C184 S3.C185 S3.C186 S3.C187 S3.C188 S3.C189 S3.C190 S3.C191 S3.C192 S3.C193 S3.C194 S3.C195 S3.C196 S3.C197 S3.C198 S3.C199 S3.C200 S3.C201 S3.C202 S3.C203 S3.C204 S3.C205 S3.C206 S3.C207 S3.C208 S3.C209 S3.C210 S3.C211 S3.C212 S3.C213 S3.C214 S3.C215 S3.C216 S3.C217 S3.C218 S3.C219 S3.C220 S3.C221 S3.C222 S3.C223 S3.C224 S3.C225 S3.C226 S3.C227 S3.C228 S3.C229 S3.C230 S3.C231 S3.C232 S3.C233 S3.C234 S3.C235 S3.C236 S3.C237 S3.C238 S3.C239 S3.C240 S3.C241 S3.C242 S3.C243 S3.C244 S3.C245 S3.C246 S3.C247 S3.C248 S3.C249 S3.C250 S3.C251 S3.C252 S3.C253 S3.C254 S3.C255 S3.C256 S3.C257 S3.C258 S3.C259 S3.C260 S3.C261 S3.C262 S3.C263 S3.C264 S3.C265 S3.C266 S3.C267 S3.C268 S3.C269 S3.C270 S3.C271 S3.C272 S3.C273 S3.C274 S3.C275 S3.C276 S3.C277 S3.C278 S3.C279 S3.C280 S3.C281 S3.C282 S3.C283 S3.C284 S3.C285 S3.C286 S3.C287 S3.C288 S3.C289 S3.C290 S3.C291 S3.C292 S3.C293 S3.C294 S3.C295 S3.C296 S3.C297 S3.C298 S3.C299 S3.C300 S3.C301 S3.C302 S3.C303 S3.C304 S3.C305 S3.C306 S3.C307 S3.C308 S3.C309 S3.C310 S3.C311 S3.C312 S3.C313 S3.C314 S3.C315 S3.C316 S3.C317 S3.C318 S3.C319 S3.C320 S3.C321 S3.C322 S3.C323 S3.C324 S3.C325 S3.C326 S3.C327 S3.C328 S3.C329 S3.C330 S3.C331 S3.C332 S3.C333 S3.C334 S3.C335 S3.C336 S3.C337 S3.C338 S3.C339 S3.C340 S3.C341 S3.C342 S3.C343 S3.C344 S3.C345 S3.C346 S3.C347 S3.C348 S3.C349 S3.C350 S3.C351 S3.C352 S3.C353 S3.C354 S3.C355 S3.C356 S3.C357 S3.C358 S3.C359 S3.C360 S3.C361 S3.C362 S3.C363 S3.C364 S3.C365 S3.C366 S3.C367 S3.C368 S3.C369 S3.C370 S3.C371 S3.C372 S3.C373 S3.C374 S3.C375 S3.C376 S3.C377 S3.C378 S3.C379 S3.C380 S3.C381 S3.C382 S3.C383 S3.C384 S3.C385 S3.C386 S3.C387 S3.C388 S3.C389 S3.C390 S3.C391 S3.C392 S3.C393 S3.C394 S3.C395 S3.C396 S3.C397 S3.C398 S3.C399 S3.C400 S3.C401 S3.C402 S3.C403 S3.C404 S3.C405 S3.C406 S3.C407 S3.C408 S3.C409 S3.C410 S3.C411 S3.C412 S3.C413 S3.C414 S3.C415 S3.C416 S3.C417 S3.C418 S3.C419 S3.C420 S3.C421 S3.C422 S3.C423 S3.C424 S3.C425 S3.C426 S3.C427 S3.C428 S3.C429 S3.C430 S3.C431 S3.C432 S3.C433 S3.C434 S3.C435 S3.C436 S3.C437 S3.C438 S3.C439 S3.C440 S3.C441 S3.C442 S3.C443 S3.C444 S3.C445 S3.C446 S3.C447 S3.C448 S3.C449 S3.C450 S3.C451 S3.C452 S3.C453 S3.C454 S3.C455 S3.C456 S3.C457 S3.C458 S3.C459 S3.C460 S3.C461 S3.C462 S3.C463 S3.C464 S3.C465 S3.C466 S3.C467 S3.C468 S3.C469 S3.C470 S3.C471 S3.C472 S3.C473 S3.C474 S3.C475 S3.C476 S3.C477 S3.C478 S3.C479 S3.C480 S3.C481 S3.C482 S3.C483 S3.C484 S3.C485 S3.C486 S3.C487 S3.C488 S3.C489 S3.C490 S3.C491 S3.C492 S3.C493 S3.C494 S3.C495 S3.C496 S3.C497 S3.C498 S3.C499 S3.C500 S3.C501 S3.C502 S3.C503 S3.C504 S3.C505 S3.C506 S3.C507 S3.C508 S3.C509 S3.C510 S3.C511 S3.C512 S3.C513 S3.C514 S3.C515 S3.C516 S3.C517 S3.C518 S3.C519 S3.C520 S3.C521 S3.C522 S3.C523 S3.C524 S3.C525 S3.C526 S3.C527 S3.C528 S3.C529 S3.C530 S3.C531 S3.C532 S3.C533 S3.C534 S3.C535 S3.C536 S3.C537 S3.C538 S3.C539 S3.C540 S3.C541 S3.C542 S3.C543 S3.C544 S3.C545 S3.C546 S3.C547 S3.C548 S3.C549 S3.C550 S3.C551 S3.C552 S3.C553 S3.C554 S3.C555 S3.C556 S3.C557 S3.C558 S3.C559 S3.C560 S3.C561 S3.C562 S3.C563 S3.C564 S3.C565 S3.C566 S3.C567 S3.C568 S3.C569 S3.C570 S3.C571 S3.C572 S3.C573 S3.C574 S3.C575 S3.C576 S3.C577 S3.C578 S3.C579 S3.C580 S3.C581 S3.C582 S3.C583 S3.C584 S3.C585 S3.C586 S3.C587 S3.C588 S3.C589 S3.C590 S3.C591 S3.C592 S3.C593 S3.C594 S3.C595 S3.C596 S3.C597 S3.C598 S3.C599 S3.C600 S3.C601 S3.C602 S3.C603 S3.C604 S3.C605 S3.C606 S3.C607 S3.C608 S3.C609 S3.C610 S3.C611 S3.C612 S3.C613 S3.C614 S3.C615 S3.C616 S3.C617 S3.C618 S3.C619 S3.C620 S3.C621 S3.C622 S3.C623 S3.C624 S3.C625 S3.C626 S3.C627 S3.C628 S3.C629 S3.C630 S3.C631 S3.C632 S3.C633 S3.C634 S3.C635 S3.C636 S3.C637 S3.C638 S3.C639 S3.C640 S3.C641 S3.C642 S3.C643 S3.C644 S3.C645 S3.C646 S3.C647 S3.C648 S3.C649 S3.C650 S3.C651 S3.C652 S3.C653 S3.C654 S3.C655 S3.C656 S3.C657 S3.C658 S3.C659 S3.C660 S3.C661 S3.C662 S3.C663 S3.C664 S3.C665 S3.C666 S3.C667 S3.C668 S3.C669 S3.C670 S3.C671 S3.C672 S3.C673 S3.C674 S3.C675 S3.C676 S3.C677 S3.C678 S3.C679 S3.C680 S3.C681 S3.C682 S3.C683 S3.C684 S3.C685 S3.C686 S3.C687 S3.C688 S3.C689 S3.C690 S3.C691 S3.C692 S3.C693 S3.C694 S3.C695 S3.C696 S3.C697 S3.C698 S3.C699 S3.C700 S3.C701 S3.C702 S3.C703 S3.C704 S3.C705 S3.C706 S3.C707 S3.C708 S3.C709 S3.C710 S3.C711 S3.C712 S3.C713 S3.C714 S3.C715 S3.C716 S3.C717 S3.C718 S3.C719 S3.C720 S3.C721 S3.C722 S3.C723 S3.C724 S3.C725 S3.C726 S3.C727 S3.C728 S3.C729 S3.C730 S3.C731 S3.C732 S3.C733 S3.C734 S3.C735 S3.C736 S3.C737 S3.C738 S3.C739 S3.C740 S3.C741 S3.C742 S3.C743 S3.C744 S3.C745 S3.C746 S3.C747 S3.C748 S3.C749 S3.C750 S3.C751 S3.C752 S3.C753 S3.C754 S3.C755 S3.C756 S3.C757 S3.C758 S3.C759 S3.C760 S3.C761 S3.C762 S3.C763 S3.C764 S3.C765 S3.C766 S3.C767 S3.C768 S3.C769 S3.C770 S3.C771 S3.C772 S3.C773 S3.C774 S3.C775 S3.C776 S3.C777 S3.C778 S3.C779 S3.C780 S3.C781 S3.C782 S3.C783 S3.C784 S3.C785 S3.C786 S3.C787 S3.C788 S3.C789 S3.C790 S3.C791 S3.C792 S3.C793 S3.C794 S3.C795 S3.C796 S3.C797 S3.C798 S3.C799 S3.C800 S3.C801 S3.C802 S3.C803 S3.C804 S3.C805 S3.C806 S3.C807 S3.C808 S3.C809 S3.C810 S3.C811 S3.C812 S3.C813 S3.C814 S3.C815 S3.C816 S3.C817 S3.C818 S3.C819 S3.C820 S3.C821 S3.C822 S3.C823 S3.C824 S3.C825 S3.C826 S3.C827 S3.C828 S3.C829 S3.C830 S3.C831 S3.C832 S3.C833 S3.C834 S3.C835 S3.C836 S3.C837 S3.C838 S3.C839 S3.C840 S3.C841 S3.C842 S3.C843 S3.C844 S3.C845 S3.C846 S3.C847 S3.C848 S3.C849 S3.C850 S3.C851 S3.C852 S3.C853 S3.C854 S3.C855 S3.C856 S3.C857 S3.C858 S3.C859 S3.C860 S3.C861 S3.C862 S3.C863 S3.C864 S3.C865 S3.C866 S3.C867 S3.C868 S3.C869 S3.C870 S3.C871 S3.C872 S3.C873 S3.C874 S3.C875 S3.C876 S3.C877 S3.C878 S3.C879 S3.C880 S3.C881 S3.C882 S3.C883 S3.C884 S3.C885 S3.C886 S3.C887 S3.C888 S3.C889 S3.C890 S3.C891 S3.C892 S3.C893 S3.C894 S3.C895 S3.C896 S3.C897 S3.C898 S3.C899 S3.C900 S3.C901 S3.C902 S3.C903 S3.C904 S3.C905 S3.C906 S3.C907 S3.C908 S3.C909 S3.C910 S3.C911 S3.C912 S3.C913 S3.C914 S3.C915 S3.C916 S3.C917 S3.C918 S3.C919 S3.C920 S3.C921 S3.C922 S3.C923 S3.C924 S3.C925 S3.C926 S3.C927 S3.C928 S3.C929 S3.C930 S3.C931 S3.C932 S3.C933 S3.C934 S3.C935 S3.C936 S3.C937 S3.C938 S3.C939 S3.C940 S3.C941 S3.C942 S3.C943 S3.C944 S3.C945 S3.C946 S3.C947 S3.C948 S3.C949 S3.C950 S3.C951 S3.C952 S3.C953 S3.C954 S3.C955 S3.C956 S3.C957 S3.C958 S3.C959 S3.C960 S3.C961 S3.C962 S3.C963 S3.C964 S3.C965 S3.C966 S3.C967 S3.C968 S3.C969 S3.C970 S3.C971 S3.C972 S3.C973 S3.C974 S3.C975 S3.C976 S3.C977 S3.C978 S3.C979 S3.C980 S3.C981 S3.C982 S3.C983 S3.C984 S3.C985 S3.C986 S3.C987 S3.C988 S3.C989 S3.C990 S3.C991 S3.C992 S3.C993 S3.C994 S3.C995 S3.C996 S3.C997		

				S3.C160 S3.C161		
7.3 7.3.1 7.3.2 7.3.3	[S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.CO14] Block bucket ACL [S3.CO37] Disabling ACLs for all buckets [S3.CO40] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C26 S3.C149 S3.C150 S3.C151 S3.C55 S3.C57	S3.C27 S3.C28 S3.C170 S3.C158 S3.C159 S3.C160 S3.C161	S3.C56	-
8.1 8.2 8.2.2	[S3.CO40] Restrict access points to authorized AWS accounts	-	-	S3.C158 S3.C159 S3.C160 S3.C161	-	-
8.2.3	[S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks	-	S3.C26 S3.C149 S3.C150 S3.C151	S3.C27 S3.C28 S3.C170	-	-
8.2.4 8.2.6	[S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.CO14] Block bucket ACL [S3.CO37] Disabling ACLs for all buckets [S3.CO40] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C26 S3.C149 S3.C150 S3.C151 S3.C55 S3.C57	S3.C27 S3.C28 S3.C170 S3.C158 S3.C159 S3.C160 S3.C161	S3.C56	-
8.3	[S3.CO1] Enforce encryption in transit [S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO16] Enforce encryption at rest [S3.CO18] Encrypt or tokenize critical data [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168 S3.C120 S3.C122	S3.C3 S3.C5 S3.C16 S3.C62 S3.C140 S3.C72 S3.C121 S3.C123 S3.C139	S3.C4 S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169
8.3.2	[S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.CO14] Block bucket ACL [S3.CO37] Disabling ACLs for all buckets [S3.CO40] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C26 S3.C149 S3.C150 S3.C151 S3.C55 S3.C57	S3.C27 S3.C28 S3.C170 S3.C158 S3.C159 S3.C160 S3.C161	S3.C56	-

8.3.3	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks	-	S3.C26 S3.C149 S3.C150 S3.C151	S3.C27 S3.C28 S3.C170	-	-
8.3.8	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C014] Block bucket ACL [S3.C037] Disabling ACLs for all buckets [S3.C040] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C26 S3.C149 S3.C150 S3.C151 S3.C55 S3.C57	S3.C27 S3.C28 S3.C170 S3.C158 S3.C159 S3.C160 S3.C161	S3.C56	-
8.3.9	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks	-	S3.C26 S3.C149 S3.C150 S3.C151	S3.C27 S3.C28 S3.C170	-	-
8.3.10	[S3.C06] Model the threats on all AWS services accessing S3 [S3.C033] Restrict Batch access using dedicated IAM roles	-	S3.C120 S3.C122	S3.C16 S3.C121 S3.C123 S3.C139	-	-
8.5	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C014] Block bucket ACL [S3.C037] Disabling ACLs for all buckets [S3.C040] Restrict access points to authorized AWS accounts	S3.C152 S3.C153 S3.C154	S3.C26 S3.C149 S3.C150 S3.C151 S3.C55 S3.C57	S3.C27 S3.C28 S3.C170 S3.C158 S3.C159 S3.C160 S3.C161	S3.C56	-
8.5.1	[S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C010] Block changes to make an object public via object ACL [S3.C020] Protect data integrity using S3 Object Lock [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles	-	S3.C17 S3.C19 S3.C20 S3.C124 S3.C26 S3.C149 S3.C150 S3.C151 S3.C34 S3.C170 S3.C36 S3.C121 S3.C74 S3.C123 S3.C75 S3.C139 S3.C76 S3.C128 S3.C77 S3.C120 S3.C122 S3.C125 S3.C126 S3.C127	S3.C22 S3.C23 S3.C24 S3.C27 S3.C28 S3.C25 S3.C35 S3.C37 S3.C18	S3.C18	-
8.6 8.6.1	[S3.C05] Identify and ensure the protection of all external buckets hosting your objects [S3.C015] Identify and ensure the protection of all internal buckets hosting your objects [S3.C016] Enforce encryption at rest	S3.C11 S3.C58	S3.C15 S3.C114 S3.C61	S3.C12 S3.C13 S3.C14	S3.C63 S3.C68 S3.C148	S3.C60 S3.C163 S3.C169

	[S3.CO18] Encrypt or tokenize critical data		S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C115 S3.C59 S3.C171 S3.C172 S3.C62 S3.C140 S3.C72	S3.C162	
9.4 9.4.1	[S3.CO11] Prevent deletion of buckets [S3.CO17] Protect primary data against loss	-	S3.C38 S3.C39 S3.C69 S3.C70	S3.C71	-	S3.C40
9.4.1.1 9.4.1.2	[S3.CO5] Identify and ensure the protection of all external buckets hosting your objects	S3.C11	S3.C15 S3.C114	S3.C12 S3.C13 S3.C14 S3.C115	-	-
9.4.2	[S3.CO19] Have a process to apply legal holds [S3.CO20] Protect data integrity using S3 Object Lock	-	S3.C74 S3.C75 S3.C76 S3.C77	S3.C73	-	-
9.4.6 9.4.7	[S3.CO25] Restrict bucket replication	-	-	S3.C86 S3.C87 S3.C88 S3.C89 S3.C90 S3.C91 S3.C92 S3.C117 S3.C134 S3.C138	S3.C116	-
9.5.1 9.5.1.1	[S3.CO21] Remove incomplete multipart uploads	-	-	-	S3.C78 S3.C79	-
9.5.1.2 9.5.1.2.1	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118 S3.C22 S3.C23 S3.C24	S3.C18 S3.C21 S3.C25	-
10.1	[S3.CO3] Enable S3 data events in AWS CloudTrail	S3.C98	S3.C17	S3.C9	S3.C18	S3.C157

	[S3.C04] Monitor S3 with Amazon GuardDuty and Macie [S3.C06] Model the threats on all AWS services accessing S3 [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C017] Protect primary data against loss [S3.C029] Limit access from only authorized VPCs [S3.C032] Restrict access point access to VPCs when in use [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C039] Enforce S3 server access logging on buckets	S3.C99 S3.C100	S3.C19 S3.C20 S3.C124 S3.C16 S3.C26 S3.C22 S3.C149 S3.C23 S3.C150 S3.C24 S3.C151 S3.C27 S3.C69 S3.C28 S3.C70 S3.C170 S3.C104 S3.C71 S3.C105 S3.C121 S3.C106 S3.C123 S3.C107 S3.C139 S3.C108 S3.C166 S3.C109 S3.C110 S3.C111 S3.C112 S3.C120 S3.C122	S3.C10 S3.C118	S3.C21 S3.C25	
10.2	[S3.C03] Enable S3 data events in AWS CloudTrail [S3.C06] Model the threats on all AWS services accessing S3 [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C017] Protect primary data against loss [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C039] Enforce S3 server access logging on buckets	-	S3.C26 S3.C149 S3.C27 S3.C150 S3.C28 S3.C151 S3.C170 S3.C69 S3.C71 S3.C70 S3.C121 S3.C120 S3.C123 S3.C139 S3.C166	S3.C9 S3.C16	-	S3.C157
10.2.1 10.2.1.1	[S3.C03] Enable S3 data events in AWS CloudTrail [S3.C06] Model the threats on all AWS services accessing S3 [S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C017] Protect primary data against loss [S3.C033] Restrict Batch access using dedicated IAM roles [S3.C034] Enforce only authorized Object Lambda Access Point and associated access [S3.C038] Ensure all requests are blocked from unauthorized service roles [S3.C039] Enforce S3 server access logging on buckets	-	S3.C17 S3.C16 S3.C19 S3.C22 S3.C20 S3.C23 S3.C124 S3.C24 S3.C26 S3.C27 S3.C149 S3.C28 S3.C150 S3.C170 S3.C25 S3.C151 S3.C71 S3.C132 S3.C69 S3.C121 S3.C133 S3.C70 S3.C123 S3.C155 S3.C120 S3.C139 S3.C122 S3.C128 S3.C125 S3.C129 S3.C126 S3.C130 S3.C131 S3.C166	S3.C9 S3.C16	-	S3.C157
10.2.1.2	[S3.C03] Enable S3 data events in AWS CloudTrail [S3.C06] Model the threats on all AWS services accessing S3 [S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.C017] Protect primary data against loss	-	S3.C26 S3.C149 S3.C150 S3.C27 S3.C151	S3.C9 S3.C16	-	S3.C157

	[S3.CO33] Restrict Batch access using dedicated IAM roles [S3.CO39] Enforce S3 server access logging on buckets		S3.C69 S3.C70 S3.C120 S3.C122 S3.C139 S3.C166	S3.C170 S3.C71 S3.C121 S3.C123 S3.C139 S3.C166		
10.2.1.3 10.2.1.4 10.2.1.5 10.2.1.6 10.2.1.7 10.2.2	[S3.CO3] Enable S3 data events in AWS CloudTrail [S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO17] Protect primary data against loss [S3.CO39] Enforce S3 server access logging on buckets	-	S3.C69 S3.C70	S3.C9 S3.C10 S3.C118 S3.C71 S3.C166	-	S3.C157
10.3 10.3.1 10.3.2 10.3.3	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118 S3.C22 S3.C23 S3.C24	S3.C18 S3.C21 S3.C25	-
10.3.4 10.4 10.4.1 10.4.1.1 10.4.2 10.4.2.1 10.4.3	[S3.CO19] Have a process to apply legal holds [S3.CO20] Protect data integrity using S3 Object Lock	-	S3.C74 S3.C75 S3.C76 S3.C77	S3.C73	-	-
10.5.1	[S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO33] Restrict Batch access using dedicated IAM roles	-	S3.C120 S3.C122	S3.C16 S3.C121 S3.C123 S3.C139	-	-
10.6 10.6.1 10.6.2 10.6.3	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use [S3.CO33] Restrict Batch access using dedicated IAM roles	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118 S3.C22 S3.C23 S3.C24	S3.C18 S3.C21 S3.C25	-

			S3.C120 S3.C122			
10.7 10.7.1 10.7.2 10.7.3	[S3.CO1] Enforce encryption in transit [S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO6] Model the threats on all AWS services accessing S3 [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO25] Restrict bucket replication [S3.CO29] Limit access from only authorized VPCs [S3.CO30] Control CloudFront access [S3.CO32] Restrict access point access to VPCs when in use [S3.CO33] Restrict Batch access using dedicated IAM roles	S3.C98 S3.C99 S3.C100	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C121 S3.C122 S3.C123 S3.C124 S3.C125 S3.C126 S3.C127 S3.C128 S3.C129 S3.C130 S3.C131 S3.C132 S3.C133 S3.C134 S3.C135 S3.C136 S3.C137 S3.C138 S3.C139	S3.C3 S3.C5 S3.C10 S3.C118 S3.C16 S3.C22 S3.C23 S3.C24 S3.C86 S3.C87 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112 S3.C120 S3.C121 S3.C123 S3.C139	S3.C4 S3.C18 S3.C21 S3.C25 S3.C116	-
11.2	[S3.CO1] Enforce encryption in transit [S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO30] Control CloudFront access [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C121 S3.C122 S3.C123 S3.C124 S3.C125 S3.C126 S3.C127 S3.C128 S3.C129 S3.C130 S3.C131 S3.C132 S3.C133 S3.C134 S3.C135 S3.C136 S3.C137 S3.C138 S3.C139	S3.C3 S3.C5 S3.C22 S3.C23 S3.C24 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112 S3.C120 S3.C121 S3.C123 S3.C137	S3.C4 S3.C18 S3.C21 S3.C25	-
11.2.1	[S3.CO1] Enforce encryption in transit [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO25] Restrict bucket replication [S3.CO29] Limit access from only authorized VPCs [S3.CO30] Control CloudFront access [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119 S3.C121 S3.C122 S3.C123 S3.C124 S3.C125	S3.C3 S3.C5 S3.C22 S3.C23 S3.C24 S3.C119 S3.C121 S3.C123 S3.C124 S3.C126	S3.C4 S3.C18 S3.C21 S3.C25 S3.C116	-

			S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112 S3.C137		S3.C87 S3.C88 S3.C89 S3.C90 S3.C91 S3.C92 S3.C117 S3.C134 S3.C138 S3.C110 S3.C101 S3.C102 S3.C137		
11.2.2	[S3.CO12] Enforce secure SDLC processes [S3.CO19] Have a process to apply legal holds [S3.CO20] Protect data integrity using S3 Object Lock	-	S3.C113 S3.C74 S3.C75 S3.C76 S3.C77	S3.C44 S3.C46 S3.C73	S3.C41 S3.C42	S3.C43 S3.C45	
11.4.1	[S3.CO12] Enforce secure SDLC processes	-	S3.C113	S3.C44 S3.C46	S3.C41 S3.C42	S3.C43 S3.C45	
11.4.4	[S3.CO2] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-	
11.4.5 11.4.6	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118 S3.C22 S3.C23 S3.C24	S3.C18 S3.C21 S3.C25	-	
11.5	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C8 S3.C17 S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118 S3.C22 S3.C23 S3.C24	S3.C18 S3.C21 S3.C25	-	
11.5.1	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie	S3.C98	S3.C17	S3.C10	S3.C18	-	

	[S3.C07] Limit and monitor access via S3 VPC endpoints [S3.C029] Limit access from only authorized VPCs [S3.C032] Restrict access point access to VPCs when in use	S3.C99 S3.C100	S3.C19 S3.C20 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C118 S3.C22 S3.C23 S3.C24	S3.C21 S3.C25	
11.5.1.1 11.5.2	[S3.C06] Model the threats on all AWS services accessing S3	-	-	S3.C16	-	-
12.3 12.3.1 12.3.2	[S3.C016] Enforce encryption at rest	-	S3.C61 S3.C64 S3.C65 S3.C66 S3.C67 S3.C145 S3.C146 S3.C147 S3.C167 S3.C168	S3.C62 S3.C140	S3.C63 S3.C68 S3.C148 S3.C162	S3.C163 S3.C169
12.3.3	[S3.C019] Have a process to apply legal holds [S3.C035] Deploy only authorized S3 websites and place them behind a CDN	-	S3.C141 S3.C144	S3.C73 S3.C142 S3.C143	-	-
12.4.2	[S3.C012] Enforce secure SDLC processes	-	S3.C113	S3.C44 S3.C46	S3.C41 S3.C42	S3.C43 S3.C45
12.4.2.1	[S3.C019] Have a process to apply legal holds	-	-	S3.C73	-	-
12.5 12.5.1	[S3.C02] Block S3 endpoints in your corporate perimeter security [S3.C019] Have a process to apply legal holds	-	S3.C8	S3.C73	-	-
12.5.2	[S3.C01] Enforce encryption in transit	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119	S3.C3 S3.C5	S3.C4	-
12.10.1 12.10.5	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks	-	S3.C26 S3.C149 S3.C150 S3.C151	S3.C27 S3.C28 S3.C170	-	-
15.1	[S3.C02] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
A1.1.4	[S3.C012] Enforce secure SDLC processes	-	S3.C113	S3.C44 S3.C46	S3.C41 S3.C42	S3.C43 S3.C45

A1.2.3	[S3.CO1] Enforce encryption in transit	-	S3.C1 S3.C2 S3.C6 S3.C7 S3.C119	S3.C3 S3.C5	S3.C4	-
A2.1 A2.1.1 A2.1.2	[S3.CO19] Have a process to apply legal holds	-	-	S3.C73	-	-
A3.1 A3.1.1 A3.2	[S3.CO2] Block S3 endpoints in your corporate perimeter security [S3.CO19] Have a process to apply legal holds	-	S3.C8	S3.C73	-	-
A3.2.1	[S3.CO27] Control event receivers [S3.CO34] Enforce only authorized Object Lambda Access Point and associated access [S3.CO38] Ensure all requests are blocked from unauthorized service roles	-	S3.C125 S3.C126 S3.C127	S3.C128 S3.C129 S3.C130 S3.C131	S3.C94 S3.C95 S3.C135 S3.C132 S3.C133 S3.C155 S3.C156	-
A3.2.2.1	[S3.CO19] Have a process to apply legal holds	-	-	S3.C73	-	-
A3.2.3	[S3.CO2] Block S3 endpoints in your corporate perimeter security	-	S3.C8	-	-	-
A3.2.4	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO8] Limit the IAM entities allowed to use the IAM actions required to execute attacks [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C26 S3.C149 S3.C150 S3.C22 S3.C151 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C10 S3.C118 S3.C150 S3.C22 S3.C151 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109 S3.C110 S3.C111 S3.C112	S3.C18 S3.C21 S3.C25	-
A3.2.6.1	[S3.CO4] Monitor S3 with Amazon GuardDuty and Macie [S3.CO7] Limit and monitor access via S3 VPC endpoints [S3.CO29] Limit access from only authorized VPCs [S3.CO32] Restrict access point access to VPCs when in use	S3.C98 S3.C99 S3.C100	S3.C17 S3.C19 S3.C20 S3.C124 S3.C124 S3.C104 S3.C105 S3.C106 S3.C107 S3.C108 S3.C109	S3.C10 S3.C118 S3.C104 S3.C22 S3.C105 S3.C23 S3.C24	S3.C18 S3.C21 S3.C25	-

			S3.C110 S3.C111 S3.C112			
A3.3.1	[S3.C06] Model the threats on all AWS services accessing S3	-	-	S3.C16	-	-
A3.3.1.2	[S3.C08] Limit the IAM entities allowed to use the IAM actions required to execute attacks	-	S3.C26 S3.C149 S3.C150 S3.C151	S3.C27 S3.C28 S3.C170	-	-

The Control Objectives are mapped to the [Secure Controls Framework](#) (SCF), provided under Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0). Compliance mappings are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.

You can change the displayed Compliance mappings by contacting [chatbot@trustoncloud.com](mailto:chatbot@trustoncloud.com).

# Appendices

## Appendix 1 - Prioritized list for control implementation

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C11] Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel).	Request the list of all external buckets authorized to host your objects, their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), their data classification, and the mechanism used to ensure the security of those buckets.	Medium	S3.FC1 S3.FC5 S3.FC16	S3.T1 (Very Low) S3.T3 (High) S3.T5 (Very Low) S3.T6 (Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Low) S3.T14 (Very Low) S3.T15 (Very Low) S3.T21 (Very Low) S3.T31 (High) S3.T43 (Very High)	Very High
Directive (coso) Protect (NIST CSF)	[S3.C49, assured by S3.C50] Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Request 1) the mechanism ensuring account-level S3 Block Public Access is enabled on all AWS accounts, 2) its records of execution for all new AWS accounts, and 3) the plan to move any older AWS accounts.	Very Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C50] Verify account-level S3 Block Public Access is enabled on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g., using the AWS Config rule: <a href="#">S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS</a> ).	Remove the account-level S3 Block Public Access of an AWS account; it should be detected.	Very Low	S3.FC5 S3.FC8 S3.FC10	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C51, assured by S3.C52] Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023).	Request 1) the mechanism ensuring S3 Block Public Access is enabled on each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C52] Verify S3 Block Public Access is enabled on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g., using the AWS Config rule: <a href="#">S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED</a> ).	Remove the S3 Block Public Access from an S3 bucket; it should be detected.	Very Low	S3.FC5 S3.FC8 S3.FC10	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C53, assured by S3.C54] Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Request 1) the mechanism ensuring S3 Block Public Access is enabled on each S3 access point, 2) its records of execution for all new S3 access points, and 3) the plan to move any older S3 access points.	Low	S3.FC5 S3.FC10 S3.FC26 S3.FC33	S3.T14 (High) S3.T36 (Medium) S3.T37 (Medium) S3.T38 (Medium) S3.T54 (High) S3.T55 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C54] Verify S3 Block Public Access is enabled on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and	Remove S3 Block Public Access of 1) an access point, and 2) a Multi-Region Access Point; it should be detected.	Medium	S3.FC5 S3.FC10 S3.FC26	-	Very High

	RestrictPublicBuckets set to true.			S3.FC33		
Directive (coso) Protect (NIST CSF)	[S3.C173] Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Request the mechanism enforcing block of public access to each bucket at the organization root, OU, or account-level via S3 policies, its records of execution for all new AWS accounts, and the plan to move any older AWS accounts.	Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Directive (coso) Protect (NIST CSF)	[S3.C58] Track all buckets you control, define their data classification and their access control (e.g., ABAC or not), identify whether the hosted data is primary (i.e., the source of truth, for example, logs, backups, forensic data, raw data, etc.) or an input/output of a process (e.g., file-processing, software package), their WORM requirements (e.g., SEC 17a-4, CTCC), whether they are production or non-production (preferably done at account-level), their storage class, their logging requirements (e.g., server access log, CloudTrail S3 data events), and their dual-layer server-side encryption requirement (e.g., for NSA CNSSP 15, or DAR CP). You may use tags, Infra-as-code, AWS Glue Data Catalog, or external management tools like <a href="#">FINRA herd</a> .	Request the list of all buckets you control and their related requirements, and the mechanism and records to ensure the accuracy of that metadata.	High	S3.FC1 S3.FC2 S3.FC5 S3.FC8 S3.FC10 S3.FC13 S3.FC16 S3.FC17 S3.FC19 S3.FC23 S3.FC36	S3.T1 (Very Low) S3.T3 (Very Low) S3.T4 (Very Low) S3.T5 (Very Low) S3.T6 (Very Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (High) S3.T12 (Very Low) S3.T13 (Very Low) S3.T14 (Very Low) S3.T15 (Very Low) S3.T16 (Very Low) S3.T17 (Very High) S3.T20 (Very Low) S3.T21 (Very Low) S3.T25 (Low) S3.T30 (Very Low) S3.T31 (Very Low) S3.T33 (Very Low) S3.T34 (Very Low) S3.T35 (Very Low) S3.T36 (Very Low) S3.T37 (Very Low) S3.T39 (Very Low) S3.T59 (Very Low) S3.T61 (Very Low) S3.T64 (Very Low) S3.T65 (Very Low)	Very High
Directive (coso) Identify (NIST CSF)	[S3.C98] For each S3 bucket, maintain a list of VPCs authorized to access it.	For each S3 bucket, request the list of authorized VPCs to access it, its review process, and its review records.	Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10	S3.T11 (Very Low) S3.T14 (Very Low) S3.T17 (Very Low) S3.T30 (Very Low) S3.T33 (Very Low) S3.T36 (Very Low) S3.T38 (Very Low) S3.T39 (Very Low)	Very High
Preventative (coso) Protect (NIST CSF)	[S3.C99, depends on S3.C98, assured by S3.C100] Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Make a request to the bucket outside an authorized VPC; it should be denied.	Very Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10	S3.T11 (Medium) S3.T14 (Medium) S3.T17 (Medium) S3.T30 (High) S3.T33 (High) S3.T36 (High) S3.T38 (High) S3.T39 (High)	Very High

Assurance (coso) Detect (NIST CSF)	[S3.C100] Verify all buckets include a control to limit access to only authorized VPCs (e.g., using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ).	Remove the control limiting access to only authorized VPC(s); it should be detected.	Medium	S3.FC1 S3.FC2 S3.FC5 S3.FC10	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C152, assured by S3.C154] Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023).	Request 1) the mechanism ensuring bucket ACL and object ACL are disabled on each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	S3.T4 (Very High) S3.T6 (Very High) S3.T36 (Very High) S3.T43 (Very High) S3.T52 (Very High) S3.T53 (Very High)	Very High
Preventative (coso) Protect (NIST CSF)	[S3.C153] Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Create a bucket with ACL enabled; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	S3.T4 (High) S3.T6 (High) S3.T36 (High) S3.T43 (High) S3.T52 (High) S3.T53 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C154] Verify bucket ACL and object ACL are disabled on each bucket (e.g., using the AWS Config rule <a href="#">S3_BUCKET_ACL_PROHIBITED</a> for bucket ACL, <a href="#">S3 Storage Lens</a> ObjectOwnershipBucketOwnerEnforcedBucketCount, or S3 Inventory, which includes object ACL metadata).	Create/modify a bucket to enable ACL; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	-	Very High
Preventative (coso) Protect (NIST CSF)	[S3.C1, depends on S3.C119, assured by S3.C2] Block all unencrypted requests and unauthorized TLS version(s) from IAM entities you control (e.g., by denying all unencrypted requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), using an SCP on your AWS Organization root node).	Make an unencrypted S3 API call; it should be denied.	Low	S3.FC1 S3.FC5	S3.T12 (Very High) S3.T34 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C2] Verify the control blocking unencrypted requests and unauthorized TLS versions from IAM entities you control (e.g., an SCP on your AWS Organization's root node) is properly implemented.	Remove the control blocking unencrypted requests and unauthorized TLS version(s) (e.g., the SCP on your root node); it should be detected.	High	S3.FC1 S3.FC5	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C6, depends on S3.C119, assured by S3.C7] Block all unencrypted requests to the buckets you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), on their bucket policy or centrally in an RCP applied to the OU or AWS account).	Make an unencrypted AWS API call to a bucket you control; it should be denied.	Low	S3.FC5	S3.T34 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C7] Verify all S3 bucket policies block unencrypted traffic (e.g., using the AWS Config rule: <a href="#">S3_BUCKET_SSL_REQUESTS_ONLY</a> ) and unauthorized versions of TLS.	Remove the statement on a bucket policy 1) denying all unencrypted requests and 2) denying unauthorized TLS versions; it should be detected.	Medium	S3.FC5	-	High
Directive (coso) Identify (NIST CSF)	[S3.C119] Maintain a list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org) (e.g., considering <a href="#">quantum-resistant encryption</a> ).	Request the list of authorized version(s) of TLS/SSL per bucket (or per account/OU/Org), its review mechanism, and associated records.	Low	S3.FC1 S3.FC5	S3.T12 (Very Low) S3.T34 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C8] Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate	Request the evidence of the implementation of blocking S3 endpoints in your corporate perimeter security (e.g.,	Low	S3.FC1 S3.FC5	S3.T7 (High) S3.T10 (High)	High

	perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	firewalls) and tests of its effectiveness.		S3.FC28	S3.T12 (Low) S3.T18 (Medium) S3.T34 (Very High)	
Directive (coso) Protect (NIST CSF)	[S3.C15] Request access via an S3 access point on a bucket you don't own, if compatible with your interaction with the bucket (e.g., not through an unsupported AWS service).	Request the documented reasons why the access point was not implemented in the use case.	Low	S3.FC1	S3.T8 (Medium) S3.T9 (Medium) S3.T31 (Very High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C114, depends on S3.C11] For all external buckets with bucket-owner-full-control ACL requirement but without S3 Object Ownership handover, block the PutObject with any ACL (e.g., using IAM or SCP and a deny on the condition "StringLike": {"s3:x-amz-acl": "*"}). It should be called via PutObjectAcl.	Put an object in an external bucket with the bucket-owner-full-control ACL requirement but without the S3 Object Ownership handover requirement; it should be denied.	High	S3.FC1	S3.T43 (Very High)	High
Directive (coso) Identify (NIST CSF)	[S3.C17] For each VPC, maintain a list of AWS Organizations, OUs, and/or AWS accounts where IAM entities are authorized to access S3.	For each VPC, request the list of AWS Organizations, OU, and/or AWS account(s), where IAM entities are authorized to access S3, its review process, and its review records.	Medium	S3.FC1 S3.FC5	S3.T9 (Very Low) S3.T11 (Very Low) S3.T62 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C19, depends on S3.C17, assured by S3.C20] Block any IAM entity not belonging to an authorized AWS Organization, OU, and/or AWS account from calling S3 from your VPCs by adding a deny statement in the S3 VPC endpoint policy for each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org IDs, as those are globally unique.	For each VPC, make an API call with an IAM entity that is not part of its authorized AWS Organizations paths; it should be denied.	Low	S3.FC1 S3.FC5	S3.T9 (Very High) S3.T11 (Very High) S3.T62 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C20] Verify all S3 VPC endpoints are blocking any IAM entity not belonging to authorized AWS Organizations, OUs, and/or AWS accounts.	Remove the policy statement blocking any IAM entity not belonging to authorized AWS Organizations, OUs, and/or AWS accounts from the VPC endpoint; it should be detected.	High	S3.FC1 S3.FC5	-	High
Directive (coso) Protect (NIST CSF)	[S3.C124] Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoint controls.	Request 1) the mechanism ensuring all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoint controls, 2) its records of execution for all new VPC endpoints, and 3) the plan to move any older VPC endpoints.	Low	S3.FC1	S3.T8 (Very High) S3.T9 (Very High)	High
Directive (coso) Protect (NIST CSF)	[S3.C26] Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Request the list of authorized IAM principals with the permissions required to execute the threat actions, its review process, and its review records.	High	S3.FC1 S3.FC2 S3.FC5 S3.FC6 S3.FC8 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC17 S3.FC19 S3.FC20 S3.FC23 S3.FC24 S3.FC25 S3.FC26 S3.FC27 S3.FC32	S3.T1 (High) S3.T2 (High) S3.T5 (Low) S3.T6 (Medium) S3.T7 (High) S3.T8 (High) S3.T11 (High) S3.T14 (Very High) S3.T16 (High) S3.T17 (Very High) S3.T18 (High) S3.T21 (Medium) S3.T25 (High) S3.T26 (High) S3.T28 (High) S3.T30 (High) S3.T33 (Very High) S3.T35 (Very High)	High

			S3.FC33 S3.FC36	S3.T36 (Medium) S3.T37 (Very High) S3.T38 (Very High) S3.T39 (High) S3.T41 (High) S3.T42 (High) S3.T44 (High) S3.T46 (High) S3.T47 (High) S3.T48 (High) S3.T49 (High) S3.T50 (High) S3.T51 (High) S3.T52 (High) S3.T53 (High) S3.T54 (High) S3.T55 (High) S3.T56 (High) S3.T58 (High) S3.T59 (High) S3.T60 (High) S3.T61 (High) S3.T62 (High) S3.T63 (High) S3.T64 (High) S3.T65 (High)		
Directive (coso) Identify (NIST CSF)	[S3.C149] For each bucket, maintain a list of authorized IAM principals allowed to access via the bucket policy.	Request the list of authorized IAM principals allowed to access via bucket policy, its review process, and its review records.	Medium	S3.FC10	S3.T37 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C150, depends on S3.C149, assured by S3.C151] Ensure only authorized IAM principals allowed to access via bucket policy are configured (e.g., using IAM Access Analyzer for reconciliation).	Request 1) the mechanism ensuring only authorized IAM principals are allowed to access buckets via bucket policy, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC10	S3.T37 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C151] Verify only authorized IAM principals allowed to access via bucket policy are used (e.g., using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ).	Allow an unauthorized IAM principal on a bucket policy; it should be detected.	Medium	S3.FC10	-	High
Directive (coso) Identify (NIST CSF)	[S3.C31] Maintain a list of AWS accounts authorized to provide KMS keys for S3 for each AWS account.	Request the list of AWS accounts authorized to provide KMS keys for S3 for each AWS account, its review process, and its review records.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC15 S3.FC26	S3.T1 (Very Low) S3.T2 (Very Low) S3.T4 (Very Low) S3.T5 (Very Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low) S3.T16 (Very Low) S3.T21 (Very Low) S3.T27 (Very Low) S3.T28 (Very Low) S3.T30 (Very Low) S3.T31 (Very Low) S3.T60 (Very Low)	High

Preventative (coso) Protect (NIST CSF)	[S3.C32, depends on S3.C31] Block requests with a KMS key from an unauthorized AWS account (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoints with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" is not a KMS key from an authorized AWS account).	Make a request encrypted with a KMS key from an unauthorized AWS account; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC15 S3.FC26	S3.T1 (High) S3.T2 (Medium) S3.T4 (High) S3.T5 (High) S3.T7 (High) S3.T8 (High) S3.T9 (High) S3.T11 (Medium) S3.T16 (High) S3.T21 (Medium) S3.T27 (Low) S3.T28 (High) S3.T30 (High) S3.T31 (High) S3.T60 (High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C34, assured by S3.C36] Deny requests to change object ACL to public (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy with a deny statement on PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups "http://acs.amazonaws.com/groups/global/AllUsers" and "http://acs.amazonaws.com/groups/global/AuthenticatedUsers").	Make a call to create a public ObjectACL; it should be denied.	Medium	S3.FC1 S3.FC5	S3.T6 (Very High) S3.T36 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C36] Verify the control blocking change ObjectACL to public (e.g., an SCP and VPC endpoint policy) is properly implemented.	Remove the control blocking changes of ObjectACL to public; it should be detected.	High	S3.FC1 S3.FC5	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C38, assured by S3.C39] Block the action "s3:DeleteBucket" (e.g., via SCP or in an RCP applied to the OU or AWS account; exemption can be managed by authorizing a SuperAdmin to delete buckets with a certain tag, and with bucket owners able to tag buckets).	Do a DeleteBucket; it should be denied.	Low	S3.FC5	S3.T1 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C39] Verify the control blocking the action "s3:DeleteBucket" is properly implemented.	Remove the control blocking the action "s3:DeleteBucket"; it should be detected.	High	S3.FC5	-	High
Directive (coso) Protect (NIST CSF)	[S3.C113, depends on S3.C11] When transmitting an object to an external bucket with bucket-owner-full-control ACL requirements but without S3 Object Ownership handover, use 2 separate APIs (PutObject and PutObjectAcl) instead of the built-in object ACL operation in PutObject.	Request the process for ensuring that PutObject requests on an external bucket with a bucket-owner-full-control ACL requirement, but without S3 Object Ownership handover, use 2 separate APIs.	Medium	S3.FC1	S3.T43 (High)	High
Directive (coso) Protect (NIST CSF)	[S3.C47, assured by S3.C48] Front buckets that are required to be public, using authenticated CDN (e.g., CloudFront) or API Gateway, protected with WAF (e.g., for <a href="#">hotlinking</a> ).	Request the process ensuring that buckets required to be public are fronted by an authenticated CDN or API Gateway, and are protected with a WAF.	Medium	S3.FC5 S3.FC16	S3.T13 (Very High) S3.T14 (Medium) S3.T22 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C48] Verify no bucket is available publicly for write or read (e.g., using the AWS Config rules: <a href="#">S3_BUCKET_PUBLIC_READ_PROHIBITED</a> and <a href="#">S3_BUCKET_PUBLIC_WRITE_PROHIBITED</a> ).	Create a public S3 bucket; it should be detected.	Very Low	S3.FC5 S3.FC16	-	High
Preventative (coso)	[S3.C55, assured by S3.C57]	Make a call to add an ACL on a bucket; it should be denied.	Medium	S3.FC8	S3.T4 (Very High)	High

Protect (NIST CSF)	Deny requests to add an ACL on a bucket (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy, with a deny statement on "s3:PutBucketAcl").			S3.FC19	S3.T58 (Very High)	
Assurance (coso) Detect (NIST CSF)	[S3.C57] Verify the control blocking bucket ACL changes is properly implemented.	Remove the control blocking bucket ACL changes; it should be detected.	High	S3.FC8 S3.FC19	-	High
Directive (coso) Identify (NIST CSF)	[S3.C61, depends on S3.C58] Maintain a list of authorized KMS keys for each bucket and its default encryption key. You might simplify by using only one key per bucket, ideally dedicated. Note that an S3 server access log bucket does not support KMS encryption ( <a href="#">ref</a> ).	Request the list of authorized KMS key(s) for each bucket, its review process, and its review records.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC23	S3.T11 (Very Low) S3.T16 (Very Low) S3.T17 (Very Low) S3.T20 (Very Low) S3.T30 (Very Low) S3.T36 (Very Low) S3.T37 (Very Low) S3.T65 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C64, depends on S3.C61, assured by S3.C65] Implement an authorized default encryption key on each bucket; enable S3 Bucket Key if not using DSSE-KMS and if CloudTrail events are not required for KMS encrypt/decrypt (note: Amazon S3 evaluates and applies bucket policies before applying bucket default encryption settings).	Request 1) the mechanism implementing an authorized default encryption key on each bucket and enabling S3 Bucket Key, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC1 S3.FC5 S3.FC10	S3.T17 (Medium) S3.T20 (High) S3.T36 (High) S3.T37 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C65] Verify each bucket has an authorized default encryption key and has S3 Bucket Key enabled.	Create/modify a bucket 1) without default encryption, 2) with an incorrect default encryption key, or 3) with S3 Bucket Key disabled; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC10	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C66, depends on S3.C61, assured by S3.C67] Block PutObject requests with unauthorized KMS key on each bucket (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-aws-kms-key-id" exists and is not an authorized KMS key).	Make a request encrypted with an unauthorized KMS key; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC10	S3.T11 (High) S3.T16 (High) S3.T17 (High) S3.T20 (Very High) S3.T30 (High) S3.T36 (High) S3.T37 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C67] Verify all buckets block PutObject requests with an unauthorized KMS key (e.g., using the Config rule: <a href="#">S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE</a> , note that a new rule needs to be deployed for each configuration, then the resource tracked by name or tag; alternatively, you might use <a href="#">S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED</a> to ensure limited coverage).	Create a bucket not blocking PutObject requests with an unauthorized KMS key; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC10	-	High
Directive (coso) Identify (NIST CSF)	[S3.C145] Maintain a list of buckets (or paths) required to be encrypted using server-side encryption with customer-provided keys (SSE-C).	Request the list of buckets (or paths) required to be encrypted with server-side encryption with customer-provided keys (SSE-C), its review process, and its review records.	Medium	S3.FC5 S3.FC10 S3.FC23	S3.T11 (Very Low) S3.T16 (Very Low) S3.T20 (Very Low) S3.T30 (Very Low) S3.T36 (Very Low) S3.T37 (Very Low) S3.T63 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C146, depends on S3.C145, assured by S3.C147] For buckets (or paths) requiring SSE-C, block PutObject requests with unauthorized encryption (e.g., using bucket policies, or centrally in an RCP applied to the OU or AWS account, with a deny statement on PutObject if the condition "s3:x-amz-server-side-encryption-customer-	Make a request to a bucket (or path) requiring SSE-C without the proper encryption; it should be denied.	Low	S3.FC5 S3.FC10	S3.T11 (High) S3.T16 (High) S3.T20 (Very High) S3.T30 (High) S3.T36 (High) S3.T37 (High)	High

	algorithm"="AES256" is not present).					
Assurance (coso) Detect (NIST CSF)	[S3.C147] For buckets (or paths) requiring SSE-C, verify all buckets block PutObject requests with unauthorized encryption.	Create a bucket requiring SSE-C, not blocking PutObject requests with unauthorized encryption; it should be detected.	High	S3.FC5 S3.FC10	-	High
Directive (coso) Protect (NIST CSF)	[S3.C167, depends on S3.C145, assured by S3.C168] Ensure SSE-C is blocked when not required for each bucket [default from April 2026].	Request 1) the mechanism ensuring SSE-C is blocked when not required for each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC5 S3.FC23	S3.T16 (High) S3.T63 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C168] Verify SS3-C is blocked only when not required for each bucket.	1) Block SSE-C on a bucket requiring SSE-C, or 2) remove the block on SSE-C on a bucket not requiring SSE-C; it should be detected.	Low	S3.FC5 S3.FC23	-	High
Directive (coso) Protect (NIST CSF)	[S3.C69, depends on S3.C58, assured by S3.C70] Enable versioning on buckets holding primary data.	Request the mechanism used to ensure versioning on buckets holding primary data, and its records.	Very Low	S3.FC1 S3.FC5	S3.T16 (High) S3.T17 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C70] Verify buckets holding primary data are versioned (e.g., using <a href="#">S3_BUCKET_VERSIONING_ENABLED</a> ).	Remove versioning from a bucket holding primary data; it should be detected.	Low	S3.FC1 S3.FC5	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C74, depends on S3.C58, assured by S3.C75] Implement the authorized default S3 Object Lock on buckets requiring WORM (note: Amazon S3 evaluates and applies bucket policies before applying the bucket default S3 Object Lock settings).	Upload an object without the appropriate S3 Object Lock; it should have the S3 Object Lock applied automatically.	Low	S3.FC1 S3.FC5 S3.FC13 S3.FC17	S3.T16 (High) S3.T17 (High) S3.T25 (High) S3.T61 (Medium)	High
Assurance (coso) Detect (NIST CSF)	[S3.C75] Verify all buckets requiring WORM have the correct default S3 Object Lock configuration.	Create a bucket requiring WORM 1) without S3 Object Lock or 2) with an incorrect default S3 Object Lock; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC13 S3.FC17	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C76, depends on S3.C58, assured by S3.C77] Block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock on buckets requiring WORM (e.g., using their bucket policy and centrally in an RCP applied to the OU or the AWS account with a deny statement on PutObject and PutObjectRetention if the condition "s3:object-lock-mode" exists and "s3:object-lock-remaining-retention-days" is not the defined S3 Object Lock configuration).	Make a request with an incorrect S3 Object Lock configuration on a bucket requiring WORM; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC17	S3.T16 (High) S3.T17 (High) S3.T61 (High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C77] Verify all buckets requiring WORM block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock (e.g., using the Config rule: <a href="#">S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE</a> , note that a new rule needs to be deployed for each configuration, then the resource tracked by name or tag).	Create a bucket requiring WORM that does not block PutObject and PutObjectRetention requests with unauthorized S3 Object Lock; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC17	-	High
Directive (coso) Identify (NIST CSF)	[S3.C104] Maintain a list of authorized access between VPCs, S3 access points, and S3.	Request the list of authorized access between VPC, S3 access points, and S3.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC26 S3.FC28 S3.FC33	S3.T7 (Very Low) S3.T9 (Very Low) S3.T10 (Very Low) S3.T11 (Very Low) S3.T28 (Very Low) S3.T37 (Very Low) S3.T54 (Very Low) S3.T55 (Very Low) S3.T56 (Very Low) S3.T60 (Very Low)	High
Preventative (coso)	[S3.C105, depends on S3.C104, assured by S3.C109]	Make a request on an unauthorized access point or bucket;	Medium	S3.FC1	S3.T7 (Medium)	High

Protect (NIST CSF)	Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy.	it should be denied.		S3.FC5 S3.FC26 S3.FC28 S3.FC33	S3.T9 (Very High) S3.T10 (Very High) S3.T11 (Medium) S3.T54 (Medium) S3.T55 (Medium)	
Preventative (coso) Protect (NIST CSF)	[S3.C106, depends on S3.C104, assured by S3.C110] In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn".	Query the bucket outside the S3 access point; it should be denied.	Medium	S3.FC1 S3.FC10 S3.FC26 S3.FC33	S3.T7 (Medium) S3.T28 (High) S3.T37 (High) S3.T55 (Medium) S3.T56 (Very High) S3.T60 (High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C107] Block the creation of non-VPC S3 access point "s3>CreateAccessPoint" (e.g., using IAM policies and SCPs with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Make a request to create an internet-based access point; it should be denied.	Low	S3.FC1 S3.FC26	S3.T7 (Medium) S3.T28 (Very High) S3.T60 (High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C108, assured by S3.C111] Block all traffic from Internet-configured S3 access points (e.g., in their bucket policy, or centrally in an RCP applied to the OU or AWS account, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Create an internet-facing access point and try to access a bucket; it should be denied.	Low	S3.FC1 S3.FC26 S3.FC28	S3.T7 (Medium) S3.T10 (Medium) S3.T28 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C109] Verify only access points are used in the resource-level statements in VPC endpoints.	Create a VPC endpoint giving access to an S3 bucket directly, rather than an access point; it should be detected.	High	S3.FC1 S3.FC5 S3.FC26 S3.FC28 S3.FC33	-	High
Assurance (coso) Detect (NIST CSF)	[S3.C110] Verify S3 bucket policies deny unauthorized S3 access points.	Remove/modify the deny on the bucket policy; it should be detected.	High	S3.FC1 S3.FC10 S3.FC26 S3.FC33	-	High
Assurance (coso) Detect (NIST CSF)	[S3.C111] Verify all S3 access points are VPC-attached.	Create an internet-based access point; it should be detected.	Low	S3.FC1 S3.FC26 S3.FC28	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C112, depends on S3.C104] Block any <a href="#">object-related operations</a> access to S3 buckets not through an access point (i.e., IAM policy, SCP, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on the condition "ArnNotLike": {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"}).	Access any S3 bucket without using an access point; it should be denied.	Low	S3.FC1 S3.FC5	S3.T7 (Medium) S3.T11 (High)	High
Directive (coso) Identify (NIST CSF)	[S3.C120] Maintain a list of IAM roles used for Batch jobs, ideally dedicated (e.g., using change management process on infrastructure-as-code).	Request the list of all IAM roles configured for Batch jobs.	Medium	S3.FC27	S3.T44 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C122, depends on S3.C120] Limit access to authorized IAM roles used for Batch jobs, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Request the IAM ThreatModel and the evidence of its application to the IAM roles used for Batch jobs.	Medium	S3.FC27	S3.T44 (Very High)	High
Directive (coso)	[S3.C125]	Request the list of authorized Lambda functions for each	Low	S3.FC32	S3.T46 (Very Low)	High

Identify (NIST CSF)	Maintain a list of authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload.	Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload, its review process, and its review records.				
Directive (coso) Protect (NIST CSF)	[S3.C126, depends on S3.C125, assured by S3.C127] Ensure only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload are created.	Request the mechanism ensuring only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload, and the evidence of its execution.	Medium	S3.FC32	S3.T46 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C127] Verify only the authorized Lambda functions are configured on each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload.	Attach 1) an unauthorized Lambda function to an Object Lambda Access Point, 2) an unauthorized Object Lambda Access Point to an access point, 3) an authorized Lambda function with an unauthorized HEAD/LIST/GET request to an Object Lambda Access Point, and 4) an authorized Lambda function with an unauthorized payload; it should be detected.	Medium	S3.FC32	-	High
Directive (coso) Identify (NIST CSF)	[S3.C141] Maintain a list of authorized buckets to be configured as an S3 website endpoint.	Request the list of authorized buckets to be configured as a website endpoint, its review process, and its review records.	Low	S3.FC16	S3.T13 (Very Low) S3.T29 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C144, depends on S3.C141] Ensure S3 website endpoints are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g., CloudFront).	Request the mechanism ensuring S3 website endpoints are protected with HTTP headers.	Medium	S3.FC16	S3.T13 (High) S3.T29 (Very High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C3, depends on S3.C119, assured by S3.C5] Block all unencrypted requests and unauthorized TLS version(s) from VPC endpoints you control (e.g., by denying all requests with the condition "aws:SecureTransport" = False, or by using "s3:TlsVersion" != authorized TLS version(s), on the VPC endpoint policy).	Make an unencrypted AWS API call from one of your VPCs with a VPC endpoint; it should be denied.	Low	S3.FC1 S3.FC5	S3.T12 (Medium) S3.T34 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C5] Verify a statement exists on all your VPC endpoint policies denying all requests with the condition "aws:SecureTransport" = False or using "s3:TlsVersion" != authorized TLS version(s).	Create/remove the statement on a VPC endpoint policy denying 1) all unencrypted requests or 2) unauthorized TLS version(s); it should be detected.	High	S3.FC1 S3.FC5	-	Medium
Directive (coso) Detect (NIST CSF)	[S3.C9, depends on S3.C58] Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Request the CloudTrail ThreatModel and the evidence of its application for enabling and protecting S3 data events.	Very Low	S3.FC1 S3.FC5 S3.FC8	S3.T1 (Low) S3.T4 (Low) S3.T5 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T12 (Low) S3.T16 (Low) S3.T21 (Low) S3.T31 (Low) S3.T34 (Low) S3.T35 (Low) S3.T36 (Low) S3.T39 (Low)	Medium
Directive (coso) Detect (NIST CSF)	[S3.C10] Enable and monitor <a href="#">S3 protection in Amazon GuardDuty</a> in all AWS accounts in all Regions, and protect it using the GuardDuty ThreatModel. Ensure findings are investigated (e.g., using Amazon Detective).	Request the GuardDuty ThreatModel and the evidence of its application for enabling, monitoring, investigating, and protecting S3 use.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC24	S3.T3 (Low) S3.T4 (Low) S3.T16 (Medium) S3.T52 (Medium)	Medium

				S3.FC25	S3.T53 (Medium)	
Directive (coso) Detect (NIST CSF)	[S3.C118] Enable <a href="#">S3 policy findings in Amazon Macie</a> in all AWS accounts in all Regions, and protect them using the Macie ThreatModel.	Request the Macie ThreatModel and the evidence of its application for enabling and protecting S3 policy findings.	Very Low	S3.FC5 S3.FC8 S3.FC10 S3.FC15	S3.T2 (Medium) S3.T4 (Medium) S3.T22 (Medium) S3.T36 (Medium) S3.T37 (Medium) S3.T38 (Medium)	Medium
Preventative (coso) Protect (NIST CSF)	[S3.C12, depends on S3.C11] Allow only authorized ACLs on objects for buckets you don't control (e.g., using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> ).	Put an object with an unauthorized ACL; it should be denied.	Medium	S3.FC1	S3.T5 (Medium) S3.T6 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C13, depends on S3.C11] Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	Make a call to an unauthorized bucket; it should be detected.	Low	S3.FC1 S3.FC5	S3.T1 (Low) S3.T7 (Low) S3.T11 (Low) S3.T21 (Low) S3.T31 (Medium)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C14, depends on S3.C11] Scan all data before uploading to an external bucket to ensure the classification of the data is aligned with the bucket classification (e.g., using Macie).	Request 1) the mechanism ensuring all data is scanned for proper data classification before upload to an external bucket, 2) its records of execution for all object upload flows, and 3) the plan to move any older object upload flows.	High	S3.FC1 S3.FC5 S3.FC16	S3.T5 (High) S3.T14 (High) S3.T15 (Medium)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C115, depends on S3.C11] For all external buckets with bucket-owner-full-control ACL requirements but without S3 Object Ownership handover, monitor that the PutObject operation does not include the ACL header.	Make a request to an external bucket with a bucket-owner-full-control ACL requirement but without an S3 Object Ownership handover requirement; it should be detected.	Low	S3.FC1	S3.T43 (Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C16] Analyze and protect all AWS services accessing S3 (e.g., via ThreatModel). Enforce use in VPC only, whenever possible.	Request the ThreatModels for all AWS services using S3.	High	S3.FC1 S3.FC5	S3.T21 (Very High) S3.T30 (Very High)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C22] Maintain a list of authorized S3 and S3 access points (and their respective AWS accounts) to be accessed for each VPC.	Request the list of authorized S3 buckets and S3 access points to be accessed for each VPC, its review process, and its review records.	Medium	S3.FC1 S3.FC5	S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low)	Medium
Preventative (coso) Protect (NIST CSF)	[S3.C23, depends on S3.C22, assured by S3.C24] Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g., using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use a specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points).	Make a request to an unauthorized bucket from one of your VPCs; it should be denied.	Medium	S3.FC1 S3.FC5	S3.T8 (High) S3.T9 (High) S3.T11 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C24] Verify all VPCs are limited to accessing only authorized S3 bucket(s).	Remove the control limiting access to only authorized S3 bucket(s); it should be detected.	High	S3.FC1 S3.FC5	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C27, assured by S3.C28] In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Request all S3 bucket/access point/Object Lambda Access Point policy statements with "allow"; no principal from the same account should be authorized.	Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC19 S3.FC20	S3.T1 (Low) S3.T2 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T11 (Low) S3.T14 (Medium) S3.T16 (Low) S3.T17 (Medium)	Medium

				S3.FC23 S3.FC26 S3.FC27 S3.FC32 S3.FC33	S3.T18 (Low) S3.T21 (Low) S3.T25 (Low) S3.T26 (Medium) S3.T30 (Low) S3.T33 (Medium) S3.T35 (Medium) S3.T36 (Low) S3.T37 (Medium) S3.T38 (Medium) S3.T39 (Low) S3.T41 (Low) S3.T42 (Low) S3.T44 (Low) S3.T46 (Medium) S3.T54 (Medium) S3.T55 (Medium) S3.T58 (Medium) S3.T59 (Medium) S3.T65 (Low)	
Assurance (coso) Detect (NIST CSF)	[S3.C28] Verify all S3 bucket/access point/Object Lambda Access Point policies do not allow an IAM principal of the same AWS account (e.g., using the Config rule S3_BUCKET_POLICY_GRANTEE_CHECK for bucket policy).	Add an allow statement for an IAM principal of the same account in 1) a bucket policy, 2) an access point policy, and 3) an Object Lambda Access Point; it should be detected.	Medium	S3.FC1 S3.FC2 S3.FC5 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC19 S3.FC20 S3.FC23 S3.FC26 S3.FC27 S3.FC32 S3.FC33	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C170, depends on S3.C58] Integrate and limit the access to general purpose buckets via tags in the IAM Operating Model (including enforcing tagging of buckets and objects at creation using AWS:ResourceTag and s3:BucketTag).	Request the IAM tag Operating Model for the general purpose buckets.	High	S3.FC2	S3.T33 (Very High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C44] Ensure the integrity of stored objects ( <a href="#">ref</a> ), using "x-amz-checksum" from the <a href="#">object metadata</a> instead of ETag (e.g., using the compute checksum functionality in S3 Batch Operations). If ETag is used, make sure to properly account for its different definitions ( <a href="#">ref</a> ).	Request 1) the mechanism ensuring the integrity of stored objects using checksums instead of ETag, and otherwise ensuring ETag's different definitions are properly accounted for, and 2) plan to move any older system using ETag to use the checksum metadata.	Low	S3.FC1 S3.FC5	S3.T17 (Medium) S3.T27 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C46] Ensure all S3 buckets interacted with are in the correct AWS account (e.g., using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner).	Request the process ensuring that all S3 buckets interacted with are in the correct AWS account.	Medium	S3.FC1 S3.FC5	S3.T1 (Medium) S3.T3 (Medium)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C59, depends on S3.C58] Use a data discovery tool (e.g., Amazon Macie) to ensure no sensitive data is stored in an unauthorized bucket.	Upload higher classification data in a bucket; it should be detected.	Medium	S3.FC5	S3.T11 (Medium)	Medium

Directive (coso) Protect (NIST CSF)	[S3.C171, depends on S3.C58, assured by S3.C172] Ensure only the authorized ABAC configuration for each general purpose bucket is configured.	Request 1) the mechanism ensuring only the authorized ABAC configuration for each general purpose bucket is configured, 2) its records of execution for all new general purpose buckets, and 3) the plan to move any older general purpose buckets.	Medium	S3.FC36	S3.T64 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C172] Verify all general purpose buckets use their authorized ABAC configuration.	1) Enable ABAC on an unauthorized general purpose bucket, or 2) disable ABAC on an authorized general purpose bucket; it should be detected.	Medium	S3.FC36	-	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C62] Verify all objects in S3 buckets are encrypted with an authorized KMS key (e.g., using S3 Inventory or S3 Batch Operations, see <a href="#">blog</a> , or <a href="#">S3 Storage Lens</a> , UnencryptedObjectCount and SSEKMSEnabledBucketCount).	Upload encrypted data 1) using an unauthorized KMS key, or 2) using SSE-S3; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC23	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C140, depends on S3.C61, assured by S3.C62] Ensure all objects in S3 buckets are encrypted with an authorized KMS key.	Request the mechanism (including training or utility) ensuring only authorized KMS keys are used for any objects stored in S3.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC23	S3.T11 (Medium) S3.T16 (Medium) S3.T17 (Medium) S3.T20 (Medium) S3.T30 (Medium) S3.T36 (Medium) S3.T37 (Medium) S3.T65 (High)	Medium
Directive (coso) Recover (NIST CSF)	[S3.C71, depends on S3.C58] Back up primary data in a secure location under a different security authority (e.g., in an <a href="#">AWS data bunker account</a> via replication, or using AWS Backup for Amazon S3).	Request the mechanism used to back up primary data in a location that has a different security authority, its records of execution, and its records of restoration testing.	Medium	S3.FC1 S3.FC5 S3.FC13	S3.T16 (High) S3.T17 (High) S3.T25 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C72] Aligned with your data governance, encrypt on the client side - or tokenize - the appropriate data.	Request the governance and mechanism(s) used to protect data (e.g., encrypt or tokenize critical data on the client side).	Very High	S3.FC1 S3.FC5 S3.FC10 S3.FC16	S3.T1 (Medium) S3.T3 (Medium) S3.T5 (High) S3.T7 (High) S3.T11 (Very High) S3.T12 (Very High) S3.T13 (Very High) S3.T17 (High) S3.T20 (High) S3.T30 (High) S3.T31 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C73] Create a process to apply a legal hold to any S3 bucket whenever required. The condition "s3:object-lock-legal-hold" can be used to restrict who can remove such a lock.	Request the process of applying legal hold, and its records.	Medium	S3.FC1 S3.FC5	S3.T16 (Low) S3.T17 (Medium)	Medium
Preventative (coso) Protect (NIST CSF)	[S3.C84] Block all requests not using HTTP authorization header, i.e., presigned via query strings or POST ( <a href="#">ref</a> ) (e.g., using an SCP, bucket policies, or centrally in an RCP applied to the OU or AWS account on all buckets with deny on "StringNotEquals": {"s3:authType": "REST-HEADER"}). Note that it blocks uploads via the console, as well.	Make a request without using the HTTP authorization header; it should be denied.	Low	S3.FC5	S3.T39 (Medium)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C86] Maintain a list of authorized buckets to have replication enabled, their target bucket, and replication type (i.e., encryption type, ownership, RTC, etc.) ( <a href="#">ref</a> ).	Request the list of authorized buckets to have replication enabled, their target bucket and replication rights, its review process, and its review records.	Medium	S3.FC15	S3.T2 (Very Low)	Medium
Assurance (coso)	[S3.C87]	Configure replication on a non-authorized bucket; it should	Medium	S3.FC15	-	Medium

Detect (NIST CSF)	Verify only authorized buckets have replication enabled with their correct configuration (e.g., using <a href="#">S3 Storage Lens</a> CrossAccountReplicationRuleCount).	be detected.				
Assurance (coso) Detect (NIST CSF)	[S3.C88] Verify authorized buckets have the correct replication configuration.	Modify the configuration of an authorized replication; it should be detected.	High	S3.FC15	-	Medium
Directive (coso) Identify (NIST CSF)	[S3.C89] Maintain a list of IAM roles used for replication, ideally dedicated (e.g., using change management process on infrastructure-as-code).	Request the list of all IAM roles configured for replication.	Medium	S3.FC15	S3.T2 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C90, depends on S3.C89] Limit S3 access to the source and destination buckets and the replication rights of each authorized IAM role configured for replication.	Request the S3 access for each replication role, and how they align with the replication requirements.	Medium	S3.FC15	S3.T2 (Medium)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C91, depends on S3.C89] Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Request the IAM ThreatModel and the evidence of its application to the IAM roles used for replication.	High	S3.FC15	S3.T2 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C92] Verify only the authorized IAM role is configured for each replication.	Create/modify a replication with an unauthorized IAM role; it should be detected.	High	S3.FC15	-	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C117] Verify all replicated buckets have metrics enabled on each replication rule (included by default in S3 RTC).	Modify the replication metric of an authorized replication; it should be detected.	Medium	S3.FC15	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C134, depends on S3.C86, assured by S3.C87,S3.C88,S3.C117] Ensure only authorized buckets have replication enabled and are configured correctly.	Request 1) the mechanism ensuring only authorized buckets have replication enabled with their correct configuration, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC15	S3.T2 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C138, depends on S3.C89, assured by S3.C92] Ensure only authorized IAM roles are attached for each replication, ideally dedicated.	Request the mechanism ensuring authorized IAM roles are attached for each replication, and the evidence of its execution for all replication configurations.	Medium	S3.FC15	S3.T2 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C93, depends on S3.C58] If the bucket is used as an input or the output of a process, scan the objects for malware (e.g., using <a href="#">GuardDuty</a> <a href="#">Malware Protection for S3</a> , <a href="#">BucketAV</a> , <a href="#">Cloud Storage Security</a> , <a href="#">Trend Micro Cloud One</a> , or <a href="#">your own scanning solution</a> ).	Inject a malware test file; it should be detected.	Medium	S3.FC5 S3.FC16	S3.T14 (Medium) S3.T15 (Low)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C101] Maintain a list of authorized CloudFront distributions (via Origin Access Control) and associated bucket, access point, and/or Object Lambda Access Point.	Request the list of all authorized CloudFront distributions and associated S3 buckets, access points, and/or Object Lambda Access Points.	Low	S3.FC10	S3.T20 (Very Low)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C102] Verify all associations of CloudFront distributions with buckets, access points, and/or Object Lambda Access Points are authorized (e.g., using the Macie finding: "Policy:IAMUser/S3BucketSharedWithCloudFront").	Create a non-authorized distribution or association; it should be detected.	High	S3.FC10	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C137, depends on S3.C101, assured by S3.C102] Ensure only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa (e.g., using their bucket policy, centrally in an RCP applied to the OU or AWS account, with a deny statement, access point policy, resource policy for an Object Lambda Access Point, limiting	Request 1) the mechanism ensuring only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa, 2) its records of execution for all new CloudFront distributions, and 3) the plan to move any older CloudFront distributions.	Medium	S3.FC10	S3.T20 (High)	Medium

	the access to only the authorized distribution(s) in the SourceArn).					
Directive (coso) Protect (NIST CSF)	[S3.C121, depends on S3.C120] Limit access to only the required resources/permissions (e.g., source/destination buckets, Lambda functions) for each authorized IAM role configured for Batch jobs.	Request access only to the required resources/permissions for each Batch IAM role, and request information on how they are aligned with the replication requirements.	Medium	S3.FC27	S3.T44 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C123] Verify only the authorized IAM role is configured for each Batch job.	Create/modify a Batch job with an unauthorized IAM role; it should be detected.	High	S3.FC27	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C139, depends on S3.C120, assured by S3.C123] Ensure only an authorized IAM role is attached to each Batch job.	Request the mechanism ensuring only an authorized IAM role is attached to each Batch job, and the evidence of its execution for all new {resource}.	Medium	S3.FC27	S3.T44 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C128] Ensure Lambda functions configured on Object Lambda Access Point are secured using Lambda ThreatModel.	Request the mechanism ensuring Lambda ThreatModel and its application for Lambda functions associated with Object Lambda Access Points, and its records of execution.	Medium	S3.FC32	S3.T46 (High)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C129] Maintain a list of cross-account access on each Object Lambda Access Point.	Request the list of authorized cross-account access for each Object Lambda Access Point, its review process, and its review records.	Very Low	S3.FC32	S3.T46 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C130, depends on S3.C129, assured by S3.C131] Ensure only authorized cross-account IAM entities are allowed in the Object Lambda Access Point policy.	Request the mechanism ensuring only cross-account IAM entities are allowed in the Object Lambda Access Point policy, and the evidence of its execution.	Low	S3.FC32	S3.T46 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C131] Verify only the authorized cross-account IAM entities are allowed in the Object Lambda Access Point policy.	Add an unauthorized cross-account IAM entity on an Object Lambda Access Point policy; it should be detected.	High	S3.FC32	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C142, depends on S3.C141, assured by S3.C143] Ensure only authorized buckets are configured as an S3 website endpoint.	Request 1) the mechanism ensuring only authorized buckets are configured as S3 website endpoints, 2) its records of execution for all new website-enabled buckets, and 3) the plan to move any older website-enabled buckets.	Medium	S3.FC16	S3.T13 (Medium) S3.T29 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C143] Verify only authorized buckets are configured as S3 website endpoints.	Enable static website hosting on an unauthorized bucket; it should be detected.	Medium	S3.FC16	-	Medium
Directive (coso) Detect (NIST CSF)	[S3.C166, depends on S3.C58] Enable <a href="#">server access logging</a> in relevant buckets (e.g., production, with sensitive data). Make it available for security analysis.	Request 1) the mechanism ensuring server access logging is enabled in relevant buckets, 2) its records of execution for all new relevant buckets, and 3) the plan to move any older relevant buckets.	Low	S3.FC1 S3.FC5 S3.FC8	S3.T1 (Low) S3.T4 (Low) S3.T5 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T12 (Low) S3.T16 (Low) S3.T21 (Low) S3.T31 (Low) S3.T34 (Low) S3.T35 (Low) S3.T36 (Low) S3.T39 (Low)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C158] Maintain a list of authorized S3 buckets and their AWS accounts for cross-account access points.	Request the list of authorized S3 buckets and their AWS account for cross-account access points, its review process, and its review records.	Low	S3.FC26	S3.T60 (Very Low)	Medium

Directive (COSO) Protect (NIST CSF)	[S3.C159, depends on S3.C158, assured by S3.C161] Ensure only authorized S3 buckets and their AWS accounts for cross-account access points are configured.	Request 1) the mechanism ensuring only authorized S3 buckets and their AWS account for cross-account access points are configured, 2) its records of execution for all new S3 buckets and their AWS accounts for cross-account access points, and 3) the plan to move any older S3 buckets and their AWS accounts for cross-account access points.	Medium	S3.FC26	S3.T60 (High)	Medium
Detective (COSO) Detect (NIST CSF)	[S3.C160, depends on S3.C158] Monitor CreateAccessPoint to detect unauthorized buckets or AWS accounts (i.e., using CloudTrail event CreateAccessPoint and its fields "requestParameters.CreateAccessPointRequest.Bucket" and "requestParameters.CreateAccessPointRequest.BucketAccou ntId").	Call the API to create a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	S3.T60 (Medium)	Medium
Assurance (COSO) Detect (NIST CSF)	[S3.C161] Verify only authorized S3 buckets and their AWS accounts for cross-account access points are used.	Deploy a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	-	Medium
Detective (COSO) Detect (NIST CSF)	[S3.C4] Monitor and investigate all requests made with HTTP (e.g., via CloudTrail S3 data events with the lack of additionalEventData.CipherSuite).	Make an unencrypted AWS API call from one of your VPCs with VPC endpoint; it should be detected.	Low	S3.FC1 S3.FC5	S3.T12 (Low) S3.T34 (Low)	Low
Directive (COSO) Protect (NIST CSF)	[S3.C18, depends on S3.C17] For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g., <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ).	Request how the VPC ThreatModel for S3 is being applied.	High	S3.FC1 S3.FC5	S3.T9 (Medium) S3.T11 (Medium) S3.T62 (Medium)	Low
Directive (COSO) Detect (NIST CSF)	[S3.C21] Enable <a href="#">VPC DNS query logging</a> in all VPCs.	Request the mechanism to enable VPC DNS query logging in all VPCs.	Medium	S3.FC1 S3.FC5	S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C25, depends on S3.C21,S3.C22] Monitor VPC DNS query logs to ensure only authorized S3 buckets and S3 access points are being queried in each VPC (e.g., using VPC DNS query logging) and protect them using Route 53 ThreatModel.	Make a DNS query to an unauthorized 1) S3 bucket and 2) S3 access points; it should be detected.	Low	S3.FC1 S3.FC5	S3.T8 (Low) S3.T9 (Low) S3.T11 (Low)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C33, depends on S3.C31] Monitor that only authorized AWS accounts provide KMS keys for each AWS account (using CloudTrail S3 data events in "response.x-amz-server-side-encryption-aws-kms-key-id").	Encrypt an object using an unauthorized key; it should be detected.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC15 S3.FC26	S3.T1 (Low) S3.T2 (Low) S3.T4 (Low) S3.T5 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T16 (Low) S3.T21 (Low) S3.T27 (Very Low) S3.T28 (Low) S3.T30 (Low) S3.T31 (Low)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C35] Monitor ObjectACL changes (or tentative changes) to public using CloudTrail S3 data events.	Make a call to create a public ObjectACL; it should be detected.	Low	S3.FC1 S3.FC5	S3.T6 (Low) S3.T36 (Low)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C37] Monitor and investigate anonymous requests to objects	Make an anonymous call; it should be detected.	Low	S3.FC5	S3.T36 (Low)	Low

	(e.g., using CloudTrail S3 data events with userIdentity.accountId=ANONYMOUS_PRINCIPAL).					
Directive (coso) Protect (NIST CSF)	[S3.C41] Parameterize the S3 bucket name or S3 access point in your code (no hardcoding).	Request the process ensuring S3 bucket names or S3 access points are not hard-coded.	Medium	S3.FC5	S3.T1 (Low)	Low
Directive (coso) Protect (NIST CSF)	[S3.C42] When connecting to S3 endpoints, use the virtual-hosted model ("my-bucket-name.s3.amazonaws.com" or "my-bucket-name.my-s3-regional-endpoint.amazonaws.com") instead of the path-style model ("s3.amazonaws.com/my-bucket-name" or "my-s3-regional-endpoint.amazonaws.com/my-bucket-name") (see <a href="#">ref</a> ). All the latest SDKs make use of domain style by default.	Request the mechanism ensuring the use of domain style instead of path style.	Very Low	S3.FC1	S3.T35 (High)	Low
Detective (coso) Detect (NIST CSF)	[S3.C56] Monitor changes to bucket ACLs to ensure they stay private (e.g., using the CloudTrail event PutBucketAcl and its field requestParameters.x-amz-acl, which should either be "private" or not exist).	Make a call to have a bucket ACL other than private; it should be detected.	Medium	S3.FC8 S3.FC19	S3.T4 (Low) S3.T58 (Low)	Low
Directive (coso) Protect (NIST CSF)	[S3.C63, depends on S3.C61] Use KMS ThreatModel to protect the KMS keys used for S3 (e.g., using encryptionContext on the policy of each KMS key).	Request the KMS ThreatModel and the evidence of its application to protect S3.	High	S3.FC1 S3.FC5 S3.FC10 S3.FC23	S3.T17 (Medium) S3.T36 (Low) S3.T37 (Low) S3.T65 (Medium)	Low
Detective (coso) Detect (NIST CSF)	[S3.C68, depends on S3.C61] Monitor that only authorized KMS keys are used for each bucket (using CloudTrail S3 data events in "requestParameters.bucketName" and "response.x-amz-server-side-encryption-aws-kms-key-id").	Make a request encrypted with an unauthorized KMS key; it should be detected.	Low	S3.FC5	S3.T11 (Very Low) S3.T16 (Low) S3.T30 (Very Low) S3.T36 (Low)	Low
Detective (coso) Detect (NIST CSF)	[S3.C148, depends on S3.C145] For buckets (or paths) requiring SSE-C, monitor that only authorized encryption is used on each bucket or path (using CloudTrail S3 data events in requestParameters.bucketName and response.x-amz-server-side-encryption-customer-algorithm).	Make a request to a bucket (or path) requiring SSE-C without the proper encryption; it should be detected.	Low	S3.FC5	S3.T11 (Very Low) S3.T16 (Low) S3.T30 (Very Low) S3.T36 (Low)	Low
Preventative (coso) Protect (NIST CSF)	[S3.C162, depends on S3.C58] Block requests not using DSSE-KMS when required (e.g., by using an SCP, IAM policies, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on required bucket names and "s3:x-amz-server-side-encryption" = "aws:kms:dsse").	Make a request not using DSSE-KMS on a required S3 bucket; it should be denied.	Low	S3.FC1 S3.FC5	S3.T5 (Low) S3.T7 (Low) S3.T8 (Low) S3.T11 (Low) S3.T31 (Low)	Low
Preventative (coso) Protect (NIST CSF)	[S3.C78, assured by S3.C79] Reduce costs related to incomplete multipart uploads by creating a lifecycle policy to remove them after an agreed length of time (e.g., 7 days) ( <a href="#">blog</a> ).	Create an incomplete upload, and wait for the agreed time; it should be deleted automatically.	Low	S3.FC5	S3.T40 (High)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C79] Verify a lifecycle policy on incomplete multipart uploads is implemented on all buckets (e.g., using AWS Config rule: <a href="#">S3_LIFECYCLE_POLICY_CHECK</a> ).	Create a bucket without a lifecycle policy to remove incomplete multipart uploads; it should be detected.	Medium	S3.FC5	-	Low
Preventative (coso) Protect (NIST CSF)	[S3.C81] Block all requests not using SigV4 (e.g., using an SCP, bucket policies, or centrally in an RCP applied to the OU or AWS account on all buckets with deny on "StringNotEquals": {"s3:signatureversion": "AWS4-HMAC-SHA256"}).	Make a non-SigV4 AWS API call; it should be denied.	Low	S3.FC1	S3.T35 (High)	Low

Directive (COSO) Protect (NIST CSF)	[S3.C83] Use SDK with SigV4 enabled ( <a href="#">ref</a> ).	Request the mechanism ensuring the use of SDK with SigV4 enabled.	Low	S3.FC1	S3.T35 (High)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C85] Monitor and investigate all requests that do not use the HTTP authorization header (e.g., via CloudTrail S3 events where the additionalEventData.AuthenticationMethod is different from "AuthHeader").	Make 1) a presigned AWS API call and 2) a POST request without the HTTP authorization header; it should be detected.	Low	S3.FC5	S3.T39 (Very Low)	Low
Detective (COSO) Detect (NIST CSF)	[S3.C116] Monitor abnormal behavior on replication CloudWatch metrics (i.e., "BytesPendingReplication", "OperationsPendingReplication", and "OperationsFailedReplication").	Create an abnormal replication, or block a replication; it should be detected.	Low	S3.FC15	S3.T2 (Low) S3.T49 (Medium)	Low
Directive (COSO) Identify (NIST CSF)	[S3.C94] Maintain a list of authorized notification receivers (e.g., SNS topic, Lambda) for each bucket. You might use a simpler approach by using authorized account IDs to ensure all your receivers are in authorized AWS accounts.	Request the list of authorized notification receivers for each bucket, its review process, and its review records.	Low	S3.FC20	S3.T41 (Very Low)	Low
Assurance (COSO) Detect (NIST CSF)	[S3.C95] Verify only authorized notification receiver(s) are configured for buckets.	Create an unauthorized receiver; it should be detected.	High	S3.FC20	-	Low
Directive (COSO) Protect (NIST CSF)	[S3.C135, depends on S3.C94, assured by S3.C95] Ensure only authorized notification receivers for each bucket are configured.	Request 1) the mechanism ensuring only authorized notification receivers for each bucket are configured, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC20	S3.T41 (High)	Low
Directive (COSO) Protect (NIST CSF)	[S3.C103] Protect and/or claim your domains and trademarks/copyrights (by creating your trademark buckets and using the <a href="#">copyright infringement process</a> from AWS).	Request the process by protecting and/or claiming your domains and trademarks/copyrights.	Medium	S3.FC28	S3.T23 (High)	Low
Directive (COSO) Protect (NIST CSF)	[S3.C132, assured by S3.C133] Ensure CloudWatch is enabled for all Object Lambda Access Points.	Request the mechanism ensuring CloudWatch is enabled for all Object Lambda Access Points, and its records of execution.	Low	S3.FC32	S3.T46 (Low)	Low
Assurance (COSO) Detect (NIST CSF)	[S3.C133] Verify CloudWatch is enabled for all Object Lambda Access Points.	Create an Object Lambda Access Point without CloudWatch enabled; it should be detected.	Low	S3.FC32	-	Low
Directive (COSO) Protect (NIST CSF)	[S3.C29] Use an unguessable naming convention for the email addresses of your AWS accounts (e.g., add a + sign and a random string to redirect the email to the same mailbox).	Review the naming convention for root account email and its implementation.	Medium	S3.FC28	S3.T19 (High)	Low
Directive (COSO) Protect (NIST CSF)	[S3.C30] Use an unguessable naming convention for your IAM users and IAM roles (e.g., add a random string).	Review the naming convention for IAM users/roles and their implementation.	Medium	S3.FC28	S3.T24 (High)	Low
Directive (COSO) Protect (NIST CSF)	[S3.C155, assured by S3.C156] Ensure all requests are blocked from AWS service roles that do not require access (e.g., by denying all requests with the principal "arn:aws:iam::*:*/AWSServiceRoleFor*" on S3 bucket policies).	Request 1) the mechanism ensuring only authorized AWS service roles can access each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC28	S3.T57 (Very High)	Low
Assurance (COSO) Detect (NIST CSF)	[S3.C156] Verify all requests from unauthorized service roles are blocked.	Remove the statement on a bucket policy denying all unauthorized service roles; it should be detected.	Medium	S3.FC28	-	Low
Detective (COSO) Detect (NIST CSF)	[S3.C40] Scan your CNAME records (e.g., in Amazon Route 53) and CloudFront origin for deleted buckets.	Create a CNAME record and CloudFront origin with an invalid bucket; it should be detected.	High	S3.FC5	S3.T1 (Very Low)	Very Low

Detective (coso) Detect (NIST CSF)	[S3.C43] Monitor that all S3 connections are made with the virtual-hosted model (e.g., via CloudTrail S3 requestParameters.Host).	Make a path-style request to S3; it should be detected.	Medium	S3.FC1	S3.T35 (Low)	Very Low
Directive (coso) Protect (NIST CSF)	[S3.C45] Do not include sensitive data in bucket names, access point names, object names, object metadata, and tags.	Request the process ensuring no sensitive data is included in bucket names, object names, object metadata, and tags.	Low	S3.FC12 S3.FC20	S3.T41 (Low) S3.T42 (Medium)	Very Low
Detective (coso) Detect (NIST CSF)	[S3.C60] Use a data discovery tool (e.g., Amazon Macie) to ensure the bucket names, object names, tags, and metadata do not contain sensitive data.	Create a bucket name, object name, tags, or metadata of an object with sensitive data; it should be detected.	Very High	S3.FC5	S3.T11 (Very Low)	Very Low
Detective (coso) Detect (NIST CSF)	[S3.C163, depends on S3.C58] Monitor requests not using DSSE-KMS when required (e.g., using CloudTrail log event name(s), CloudTrail S3 data events with field(s) requestParameter.bucketName, and "response.x-amz-server-side-encryption-aws").	Make a request not using DSSE-KMS on a required S3 bucket; it should be detected.	Low	S3.FC1 S3.FC5	S3.T5 (Very Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T11 (Very Low) S3.T31 (Very Low)	Very Low
Detective (coso) Detect (NIST CSF)	[S3.C169] Monitor abnormal increases in the CloudWatch metric for HTTP 4xx client error status code requests (i.e., "4xxErrors").	Run HTTP 4xx client error status code requests abnormally; it should be detected.	High	S3.FC23	S3.T63 (Low)	Very Low
Directive (coso) Protect (NIST CSF)	[S3.C80] Block deprecated S3 actions using IAM ThreatModel and the S3 actions list.	Request the controls blocking deprecated S3 actions.	Low	S3.FC1	S3.T35 (Medium)	Very Low
Detective (coso) Detect (NIST CSF)	[S3.C82] Monitor and investigate any requests not using SigV4 (e.g., via CloudTrail S3 when the additionalEventData.SignatureVersion is different from "SigV4").	Make a non-SigV4 AWS API call; it should be detected.	Low	S3.FC1	S3.T35 (Low)	Very Low
Directive (coso) Identify (NIST CSF)	[S3.C96] Maintain a list of authorized S3 buckets to receive the S3 Inventory of each bucket.	Request the list of authorized bucket(s) to receive S3 Inventory of each bucket, its review process, and its review records.	Low	S3.FC12	S3.T42 (Very Low)	Very Low
Assurance (coso) Detect (NIST CSF)	[S3.C97] Verify only authorized buckets are configured to receive inventory.	Create an unauthorized bucket to receive inventory; it should be detected.	High	S3.FC12	-	Very Low
Directive (coso) Protect (NIST CSF)	[S3.C136, depends on S3.C96, assured by S3.C97] Ensure only authorized S3 buckets are configured to receive S3 Inventory for each bucket.	Request 1) the mechanism ensuring only authorized S3 buckets are configured to receive S3 Inventory for each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC12	S3.T42 (Medium)	Very Low
Directive (coso) Identify (NIST CSF)	[S3.C164, depends on S3.C26] Maintain the list of authorized optional fields allowed to be accessed by each authorized IAM principal.	Request the list of authorized optional fields allowed to be accessed by each authorized IAM principal, its review process, and its review records.	High	S3.FC12	S3.T42 (Very Low)	Very Low
Preventative (coso) Protect (NIST CSF)	[S3.C165, depends on S3.C164] Prevent the creation of inventories without authorized optional fields (e.g., by using an SCP and/or an IAM policy on "s3:PutInventoryConfiguration" with an allow statement on "s3:InventoryAccessibleOptionalFields" = authorized optional fields only).	Create an inventory with an unauthorized optional field; it should be denied.	Low	S3.FC12	S3.T42 (Medium)	Very Low
Detective (coso) Detect (NIST CSF)	[S3.C157, depends on S3.C58] Monitor PutBucketLogging to detect bucket server access logging changes, including deactivation and bucket changes (i.e., using the CloudTrail event "PutBucketLogging" and the "requestParameters.BucketLoggingStatus" field to examine	Make a call to 1) disable bucket logging, or 2) change to an unauthorized bucket; it should be detected.	Low	S3.FC19	S3.T59 (Medium)	Very Low

the lack of the "LoggingEnabled" key or an unauthorized bucket in "requestParameters.BucketLoggingStatus.LoggingEnabled.TargetBucket").					
---	--	--	--	--	--

## Appendix 2 - List of all Actions and their details

<b>Id</b>	<b>Description</b>	<b>Feature Class ID</b>	<b>IAM Permission</b>	<b>Event</b>	<b>API</b>
S3.A1	Aborts a multipart upload.	S3.FC1	s3:AbortMultipartUpload	Data-AWS::S3::Object-AbortMultipartUpload	AbortMultipartUpload
S3.A2	Grants permission to allow circumvention of governance-mode object retention settings (for DeleteObject, DeleteObjects and PutObjectRetention).	S3.FC17	s3:BypassGovernanceRetention	-	-
S3.A3	Completes a multipart upload by assembling previously uploaded parts.	S3.FC1	s3:PutObject	Data-AWS::S3::Object-CompleteMultipartUpload	CompleteMultipartUpload
S3.A4	Creates a copy of an object that is already stored in Amazon S3.	S3.FC1	s3:GetObject s3:PutObject	Data-AWS::S3::Object-CopyObject	CopyObject
S3.A5	Creates a new bucket.	S3.FC5	s3:CreateBucket	CreateBucket	CreateBucket
S3.A6	Initiates a multipart upload and returns an upload ID.	S3.FC1	s3:GetObject s3:PutObject	Data-AWS::S3::Object-CreateMultipartUpload	CreateMultipartUpload
S3.A7	Deletes the bucket. All objects (including all object versions and delete markers) in the bucket must be deleted before the bucket itself can be deleted.	S3.FC5	s3:DeleteBucket	DeleteBucket	DeleteBucket
S3.A8	Deletes an analytics configuration for the bucket.	S3.FC11	s3:PutAnalyticsConfiguration	DeleteBucketAnalyticsConfiguration	DeleteBucketAnalyticsConfiguration
S3.A9	Deletes the CORS configuration information set for the bucket.	S3.FC22	s3:PutBucketCors	DeleteBucketCors	DeleteBucketCors
S3.A10	Removes default encryption from the bucket.	S3.FC23	s3:PutEncryptionConfiguration	DeleteBucketEncryption	DeleteBucketEncryption
S3.A11	Deletes an inventory configuration from the bucket.	S3.FC12	s3:PutInventoryConfiguration	DeleteBucketInventoryConfiguration	DeleteBucketInventoryConfiguration
S3.A12	Deletes the lifecycle configuration from the bucket.	S3.FC13	s3:PutLifecycleConfiguration	DeleteBucketLifecycle	DeleteBucketLifecycle
S3.A13	Deletes a metrics configuration for the Amazon CloudWatch request metrics (specified by the metrics configuration ID) from the bucket. Note that this doesn't include the daily storage metrics.	S3.FC14	s3:PutMetricsConfiguration	DeleteBucketMetricsConfiguration	DeleteBucketMetricsConfiguration
S3.A14	Deletes the policy on a specified bucket.	S3.FC10	s3:DeleteBucketPolicy	DeleteBucketPolicy	DeleteBucketPolicy
S3.A15	Deletes the replication configuration from the bucket.	S3.FC15	s3:PutReplicationConfiguration	DeleteBucketReplication	DeleteBucketReplication
S3.A16	Deletes the tags from the bucket.	S3.FC7	s3:PutBucketTagging	DeleteBucketTagging	DeleteBucketTagging
S3.A17	Removes the website configuration for a bucket.	S3.FC16	s3:DeleteBucketWebsite	DeleteBucketWebsite	DeleteBucketWebsite
S3.A18	Deletes an object permanently (non-versioned bucket) or inserts a delete marker (versioned bucket).	S3.FC1	s3:DeleteObject	Data-AWS::S3::Object-DeleteObject	DeleteObject
S3.A19	Permanently deletes an object or a delete marker from a bucket.	S3.FC3	s3:DeleteObjectVersion	Data-AWS::S3::Object-DeleteObject	DeleteObject(VersionId=)
S3.A20	Deletes multiple objects permanently (non-versioned bucket) or inserts delete markers (versioned bucket).	S3.FC1	s3:DeleteObject	Data-AWS::S3::Object-DeleteObjects	DeleteObjects
S3.A21	Permanently deletes multiple objects or delete markers from a bucket.	S3.FC3	s3:DeleteObjectVersion	Data-AWS::S3::Object-DeleteObjects	DeleteObjects(VersionId=)
S3.A22	Removes the entire tag set from the specified object.	S3.FC2	s3:DeleteObjectTagging	Data-AWS::S3::Object-DeleteObjectTagging	DeleteObjectTagging
S3.A23	Removes the entire tag set from the specified object version.	S3.FC4	s3:DeleteObjectVersionTagging	Data-AWS::S3::Object-DeleteObjectTagging	DeleteObjectTagging(VersionId=)

S3.A24	Removes the PublicAccessBlock configuration for an Amazon S3 bucket.	S3.FC24	s3:PutBucketPublicAccessBlock	DeletePublicAccessBlock	DeletePublicAccessBlock
S3.A25	Returns the Transfer Acceleration state of a bucket, which is either "Enabled" or "Suspended".	S3.FC18	s3:GetAccelerateConfiguration	GetBucketAccelerateConfiguration	GetBucketAccelerateConfiguration
S3.A26	Returns the Access Control List (ACL) of a bucket.	S3.FC8	s3:GetBucketAcl	GetBucketAcl	GetBucketAcl
S3.A27	Returns an analytics configuration from the bucket.	S3.FC11	s3:GetAnalyticsConfiguration	GetBucketAnalyticsConfiguration	GetBucketAnalyticsConfiguration
S3.A28	Returns the CORS configuration information set for the bucket.	S3.FC22	s3:GetBucketCors	GetBucketCors	GetBucketCors
S3.A29	Returns the default encryption configuration for an Amazon S3 bucket.	S3.FC23	s3:GetEncryptionConfiguration	GetBucketEncryption	GetBucketEncryption
S3.A30	Returns an inventory configuration from the bucket.	S3.FC12	s3:GetInventoryConfiguration	GetBucketInventoryConfiguration	GetBucketInventoryConfiguration
S3.A31	(Deprecated) Returns the lifecycle configuration information set on the bucket.	S3.FC13	s3:GetLifecycleConfiguration	GetBucketLifecycle	GetBucketLifecycle
S3.A32	Returns the lifecycle configuration information set on the bucket.	S3.FC13	s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	GetBucketLifecycleConfiguration
S3.A33	Returns a bucket's region.	S3.FC5	s3:GetBucketLocation	GetBucketLocation	GetBucketLocation
S3.A34	Returns the logging status of a bucket and the permissions users have to view and modify that status.	S3.FC19	s3:GetBucketLogging	GetBucketLogging	GetBucketLogging
S3.A35	Gets a metrics configuration from the bucket.	S3.FC14	s3:GetMetricsConfiguration	GetBucketMetricsConfiguration	GetBucketMetricsConfiguration
S3.A36	(Deprecated) Returns the notification configuration of a bucket.	S3.FC20	s3:GetBucketNotification	GetBucketNotification	GetBucketNotification
S3.A37	Returns the notification configuration of a bucket.	S3.FC20	s3:GetBucketNotification	GetBucketNotificationConfiguration	GetBucketNotificationConfiguration
S3.A38	Returns the policy of a specified bucket.	S3.FC10	s3:GetBucketPolicy	GetBucketPolicy	GetBucketPolicy
S3.A39	Retrieves the policy status for an Amazon S3 bucket, indicating whether the bucket is public.	S3.FC10	s3:GetBucketPolicyStatus	GetBucketPolicyStatus	GetBucketPolicyStatus
S3.A40	Returns the replication configuration of a bucket.	S3.FC15	s3:GetReplicationConfiguration	GetBucketReplication	GetBucketReplication
S3.A41	Returns the request payment configuration of a bucket.	S3.FC5	s3:GetBucketRequestPayment	GetBucketRequestPayment	GetBucketRequestPayment
S3.A42	Returns the tag set associated with the bucket.	S3.FC7	s3:GetBucketTagging	GetBucketTagging	GetBucketTagging
S3.A43	Returns the versioning state of a bucket.	S3.FC6	s3:GetBucketVersioning	GetBucketVersioning	GetBucketVersioning
S3.A44	Returns the website configuration for a bucket.	S3.FC16	s3:GetBucketWebsite	GetBucketWebsite	GetBucketWebsite
S3.A45	Retrieves an object from Amazon S3.	S3.FC1	s3:GetObject	Data-AWS::S3::Object-GetObject	GetObject
S3.A46	Retrieves an object version from Amazon S3.	S3.FC3	s3:GetObjectVersion	Data-AWS::S3::Object-GetObject	GetObject(VersionId=)
S3.A47	Returns ACL information about an object.	S3.FC1	s3:GetObjectAcl	Data-AWS::S3::Object-GetObjectAcl	GetObjectAcl
S3.A48	Returns ACL information about an object version, use the versionId subresource.	S3.FC9	s3:GetObjectVersionAcl	Data-AWS::S3::Object-GetObjectAcl	GetObjectAcl(VersionId=)
S3.A49	Gets Object Lock legal hold for a specific object.	S3.FC29	s3:GetObjectLegalHold	Data-AWS::S3::Object-GetObjectLockLegalHold	GetObjectLegalHold
S3.A50	Gets the default S3 Object Lock configuration for a bucket.	S3.FC17	s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	GetObjectLockConfiguration
S3.A51	Retrieves an object's retention settings.	S3.FC17	s3:GetObjectRetention	Data-AWS::S3::Object-GetObjectLockRetention	GetObjectRetention
S3.A52	Returns the tag-set of an object.	S3.FC2	s3:GetObjectTagging	Data-AWS::S3::Object-GetObjectTagging	GetObjectTagging
S3.A53	Returns the tag-set of a specific version of an object.	S3.FC4	s3:GetObjectVersionTagging	Data-AWS::S3::Object-GetObjectTagging	GetObjectTagging(VersionId=)

S3.A54	Returns torrent files from an object.	S3.FC21	s3:GetObjectTorrent	Data-AWS::S3::Object-GetObjectTorrent	GetObjectTorrent
S3.A55	(Deprecated) No documented use of this action.	S3.FC21	s3:GetObjectVersionTorrent	-	-
S3.A56	Grants Amazon S3 the permission to replicate both unencrypted objects and objects encrypted with SSE-S3 or SSE-KMS.	S3.FC15	s3:GetObjectVersionForReplication	-	-
S3.A57	Retrieves the PublicAccessBlock configuration for an Amazon S3 bucket.	S3.FC24	s3:GetBucketPublicAccessBlock	GetPublicAccessBlock	GetPublicAccessBlock
S3.A58	Determines if a bucket exists and you have permission to access it.	S3.FC1	s3:HeadBucket	Data-AWS::S3::Object-HeadBucket	HeadBucket
S3.A59	Retrieves metadata from an object without returning the object itself.	S3.FC1	s3:GetObject	Data-AWS::S3::Object-HeadObject	HeadObject
S3.A60	Retrieves metadata from an object version without returning the object itself.	S3.FC3	s3:GetObjectVersion	Data-AWS::S3::Object-HeadObject	HeadObject(VersionId=)
S3.A61	Lists the analytics configurations for the bucket.	S3.FC11	s3:GetAnalyticsConfiguration	ListBucketAnalyticsConfigurations	ListBucketAnalyticsConfigurations
S3.A62	Returns a list of inventory configurations for the bucket.	S3.FC12	s3:GetInventoryConfiguration	ListBucketInventoryConfigurations	ListBucketInventoryConfigurations
S3.A63	Lists the metrics configurations for the bucket.	S3.FC14	s3:GetMetricsConfiguration	ListBucketMetricsConfigurations	ListBucketMetricsConfigurations
S3.A64	Returns a list of all buckets owned by the authenticated sender of the request.	S3.FC5	s3>ListAllMyBuckets	ListBuckets	ListBuckets
S3.A65	Lists in-progress multipart uploads.	S3.FC1	s3>ListBucketMultipartUploads	ListMultipartUploads	ListMultipartUploads
S3.A66	(Deprecated) Returns some or all (up to 1000) of the objects in a bucket.	S3.FC1	s3>ListBucket	Data-AWS::S3::Object-ListObjects	ListObjects
S3.A67	Returns some or all (up to 1000) of the objects in a bucket.	S3.FC1	s3>ListBucket	Data-AWS::S3::Object-ListObjects	ListObjectsV2
S3.A68	Lists metadata about all of the versions of objects in a bucket.	S3.FC3	s3>ListBucketVersions	Data-AWS::S3::Object-ListObjectVersions	ListObjectVersions
S3.A69	Lists the parts that have been uploaded for a specific multipart upload.	S3.FC1	s3>ListMultipartUploadParts	Data-AWS::S3::Object-ListParts	ListParts
S3.A70	Allows Amazon S3 to change the ownership of a replicated object.	S3.FC15	s3:ObjectOwnerOverrideToBucketOwner	-	-
S3.A71	Sets the Transfer Acceleration state of an existing bucket.	S3.FC18	s3:PutAccelerateConfiguration	PutBucketAccelerateConfiguration	PutBucketAccelerateConfiguration
S3.A72	Sets the permissions on an existing bucket using Access Control Lists (ACL).	S3.FC8	s3:PutBucketAcl	PutBucketAcl	PutBucketAcl
S3.A73	Adds an analytics configuration (identified by the analytics ID) to the bucket.	S3.FC11	s3:PutAnalyticsConfiguration	PutBucketAnalyticsConfiguration	PutBucketAnalyticsConfiguration
S3.A74	Sets the CORS configuration for your bucket.	S3.FC22	s3:PutBucketCors	PutBucketCors	PutBucketCors
S3.A75	Sets the default encryption configuration for the bucket.	S3.FC23	s3:PutEncryptionConfiguration	PutBucketEncryption	PutBucketEncryption
S3.A76	Adds an inventory configuration (identified by the inventory ID) to the bucket.	S3.FC12	s3:PutInventoryConfiguration	PutBucketInventoryConfiguration	PutBucketInventoryConfiguration
S3.A77	(Deprecated) Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration.	S3.FC13	s3:PutLifecycleConfiguration	PutBucketLifecycle	PutBucketLifecycle
S3.A78	Creates a new lifecycle configuration for the bucket or replaces an existing lifecycle configuration.	S3.FC13	s3:PutLifecycleConfiguration	PutBucketLifecycleConfiguration	PutBucketLifecycleConfiguration
S3.A79	Sets the logging parameters for a bucket.	S3.FC19	s3:PutBucketLogging	PutBucketLogging	PutBucketLogging
S3.A80	Sets or updates a metrics configuration for the CloudWatch request metrics (specified by the metrics configuration ID) from the bucket.	S3.FC14	s3:PutMetricsConfiguration	PutBucketMetricsConfiguration	PutBucketMetricsConfiguration
S3.A81	(Deprecated) Enables you to receive notifications when certain events happen in your bucket.	S3.FC20	s3:PutBucketNotification	PutBucketNotification	PutBucketNotification
S3.A82	Enables you to receive notifications when certain events happen in your	S3.FC20	s3:PutBucketNotification	PutBucketNotificationConfiguration	PutBucketNotificationConfiguration

	bucket.			n	n
S3.A83	Adds to or replaces a policy on a bucket.	S3.FC10	s3:PutBucketPolicy	PutBucketPolicy	PutBucketPolicy
S3.A84	Creates a new replication configuration (or replaces an existing one, if present).	S3.FC15	s3:PutReplicationConfiguration	PutBucketReplication	PutBucketReplication
S3.A85	Sets the request payment configuration of a bucket.	S3.FC5	s3:PutBucketRequestPayment	PutBucketRequestPayment	PutBucketRequestPayment
S3.A86	Adds a set of tags to an existing bucket.	S3.FC7	s3:PutBucketTagging	PutBucketTagging	PutBucketTagging
S3.A87	Sets the versioning state of an existing bucket.	S3.FC6	s3:PutBucketVersioning	PutBucketVersioning	PutBucketVersioning
S3.A88	Sets the configuration of the website that is specified in the website subresource.	S3.FC16	s3:PutBucketWebsite	PutBucketWebsite	PutBucketWebsite
S3.A89	Adds an object to a bucket.	S3.FC1	s3:PutObject	Data-AWS::S3::Object-PutObject	PutObject
S3.A90	Sets the Access Control List (ACL) permissions for an object. You must have WRITE_ACP permission to set the ACL of an object.	S3.FC1	s3:PutObjectAcl	Data-AWS::S3::Object-PutObjectAcl	PutObjectAcl
S3.A91	Sets the Access Control List (ACL) permissions for an object version. You must have WRITE_ACP permission to set the ACL of an object version.	S3.FC9	s3:PutObjectVersionAcl	Data-AWS::S3::Object-PutObjectAcl	PutObjectAcl(VersionId=)
S3.A92	Puts Object Lock legal hold on a specific object.	S3.FC29	s3:PutObjectLegalHold	Data-AWS::S3::Object-PutObjectLockLegalHold	PutObjectLegalHold
S3.A93	Allows placing a default S3 Object Lock configuration at bucket creation (AWS Support needs to be contacted for existing buckets). It automatically enables versioning, even without permission.	S3.FC17	s3:PutBucketObjectLockConfiguration	PutObjectLockConfiguration	PutObjectLockConfiguration
S3.A94	Puts object retention on a specific object.	S3.FC17	s3:PutObjectRetention	PutObjectRetention	PutObjectRetention
S3.A95	Adds a set of tags to an existing object.	S3.FC2	s3:PutObjectTagging	Data-AWS::S3::Object-PutObjectTagging	PutObjectTagging
S3.A96	Adds a set of tags to an existing object version.	S3.FC4	s3:PutObjectVersionTagging	Data-AWS::S3::Object-PutObjectTagging	PutObjectTagging(VersionId=)
S3.A97	Creates or modifies the PublicAccessBlock configuration for an Amazon S3 bucket.	S3.FC24	s3:PutBucketPublicAccessBlock	PutPublicAccessBlock	PutPublicAccessBlock
S3.A98	Allows Amazon S3 to replicate delete markers to the destination bucket.	S3.FC15	s3:ReplicateDelete	-	-
S3.A99	Allows Amazon S3 to replicate objects to the destination bucket, including tags.	S3.FC15	s3:ReplicateObject	-	-
S3.A100	Allows Amazon S3 to replicate object tags to the destination bucket.	S3.FC15	s3:ReplicateTags	-	-
S3.A101	Restores a temporary copy of an archived object.	S3.FC1	s3:RestoreObject	Data-AWS::S3::Object-RestoreObject	RestoreObject
S3.A102	Filters the contents of an Amazon S3 object based on a simple structured query language (SQL) statement.	S3.FC1	s3:GetObject	Data-AWS::S3::Object-SelectObjectContent	SelectObjectContent
S3.A103	Uploads a part in a multipart upload.	S3.FC1	s3:PutObject	Data-AWS::S3::Object-UploadPart	UploadPart
S3.A104	Uploads a part by copying data from an existing object as a data source.	S3.FC1	s3:PutObject s3:GetObject	Data-AWS::S3::Object-UploadPartCopy	UploadPartCopy
S3.A105	Creates a new access point.	S3.FC26	s3>CreateAccessPoint	CreateAccessPoint	CreateAccessPoint
S3.A106	Creates a new Amazon S3 Batch Operations job.	S3.FC27	s3:CreateJob	JobCreated	CreateJob
S3.A107	Deletes the specified access point.	S3.FC26	s3:DeleteAccessPoint	DeleteAccessPoint	DeleteAccessPoint
S3.A108	Deletes the policy on a specified access point.	S3.FC26	s3:DeleteAccessPointPolicy	DeleteAccessPointPolicy	DeleteAccessPointPolicy
S3.A109	Removes the PublicAccessBlock configuration for an AWS account.	S3.FC25	s3:PutAccountPublicAccessBlock	DeletePublicAccessBlock	DeletePublicAccessBlock
S3.A110	Retrieves the configuration parameters and status for a Batch Operations	S3.FC27	s3:DescribeJob	DescribeJob	DescribeJob

	job.				
S3.A111	Retrieves access point metadata.	S3.FC26	s3:GetAccessPoint	GetAccessPoint	GetAccessPoint
S3.A112	Returns the policy of a specified access point.	S3.FC26	s3:GetAccessPointPolicy	GetAccessPointPolicy	GetAccessPointPolicy
S3.A113	Retrieves the policy status for a specific access point's policy.	S3.FC26	s3:GetAccessPointPolicyStatus	GetAccessPointPolicyStatus	GetAccessPointPolicyStatus
S3.A114	Retrieves the PublicAccessBlock configuration for an AWS account.	S3.FC25	s3:GetAccountPublicAccessBlock	GetPublicAccessBlock	GetPublicAccessBlock
S3.A115	Returns a list of the access points currently associated with the specified bucket.	S3.FC26	s3>ListAccessPoints	ListAccessPoints	ListAccessPoints
S3.A116	Lists current jobs and jobs that have ended recently.	S3.FC27	s3>ListJobs	ListJobs	ListJobs
S3.A117	Adds to or replaces a data policy on an access point.	S3.FC26	s3:PutAccessPointPolicy	PutAccessPointPolicy	PutAccessPointPolicy
S3.A118	Creates or modifies the PublicAccessBlock configuration for an AWS account.	S3.FC25	s3:PutAccountPublicAccessBlock	PutPublicAccessBlock	PutPublicAccessBlock
S3.A119	Updates an existing job's priority.	S3.FC27	s3:UpdateJobPriority	UpdateJobPriority	UpdateJobPriority
S3.A120	Updates the status for the specified job.	S3.FC27	s3:UpdateJobStatus	JobStatusChanged	UpdateJobStatus
S3.A121	Removes OwnershipControls for an Amazon S3 bucket.	S3.FC30	s3:PutBucketOwnershipControls	DeleteBucketOwnershipControls	DeleteBucketOwnershipControls
S3.A122	Retrieves OwnershipControls for an Amazon S3 bucket.	S3.FC30	s3:GetBucketOwnershipControls	GetBucketOwnershipControls	GetBucketOwnershipControls
S3.A123	Creates or modifies OwnershipControls for an Amazon S3 bucket.	S3.FC30	s3:PutBucketOwnershipControls	PutBucketOwnershipControls	PutBucketOwnershipControls
S3.A124	Deletes the S3 Intelligent-Tiering configuration from the specified bucket.	S3.FC13	s3:DeleteIntelligentTieringConfiguration	DeleteBucketIntelligentTieringConfiguration	DeleteBucketIntelligentTieringConfiguration
S3.A125	Gets the S3 Intelligent-Tiering configuration from the specified bucket.	S3.FC13	s3:GetIntelligentTieringConfiguration	GetBucketIntelligentTieringConfiguration	GetBucketIntelligentTieringConfiguration
S3.A126	Lists the S3 Intelligent-Tiering configuration from the specified bucket.	S3.FC13	s3>ListIntelligentTieringConfigurations	ListBucketIntelligentTieringConfigurations	ListBucketIntelligentTieringConfigurations
S3.A127	Puts a S3 Intelligent-Tiering configuration to the specified bucket.	S3.FC13	s3:PutIntelligentTieringConfiguration	PutBucketIntelligentTieringConfiguration	PutBucketIntelligentTieringConfiguration
S3.A128	Deletes the Amazon S3 Storage Lens configuration.	S3.FC31	s3:DeleteStorageLensConfiguration	DeleteStorageLensConfiguration	DeleteStorageLensConfiguration
S3.A129	Deletes the Amazon S3 Storage Lens configuration tags.	S3.FC31	s3:DeleteStorageLensConfigurationTagging	DeleteStorageLensConfigurationTagging	DeleteStorageLensConfigurationTagging
S3.A130	Gets the Amazon S3 Storage Lens configuration.	S3.FC31	s3:GetStorageLensConfiguration	GetStorageLensConfiguration	GetStorageLensConfiguration
S3.A131	Gets the tags of Amazon S3 Storage Lens configuration.	S3.FC31	s3:GetStorageLensConfigurationTagging	GetStorageLensConfigurationTagging	GetStorageLensConfigurationTagging
S3.A132	Gets a list of Amazon S3 Storage Lens configurations.	S3.FC31	s3>ListStorageLensConfigurations	ListStorageLensConfigurations	ListStorageLensConfigurations
S3.A133	Puts an Amazon S3 Storage Lens configuration.	S3.FC31	s3:PutStorageLensConfiguration	PutStorageLensConfiguration	PutStorageLensConfiguration
S3.A134	Puts or replaces tags on an existing Amazon S3 Storage Lens configuration.	S3.FC31	s3:PutStorageLensConfigurationTagging	PutStorageLensConfigurationTagging	PutStorageLensConfigurationTagging
S3.A135	Creates an Object Lambda Access Point.	S3.FC32	s3>CreateAccessPointForObjectLambda	CreateAccessPointForObjectLambda	CreateAccessPointForObjectLambda
S3.A136	Deletes the specified Object Lambda Access Point.	S3.FC32	s3:DeleteAccessPointForObjectLambda	DeleteAccessPointForObjectLambda	DeleteAccessPointForObjectLambda
S3.A137	Removes the resource policy for an Object Lambda Access Point.	S3.FC32	s3:DeleteAccessPointPolicyForObjectLambda	DeleteAccessPointPolicyForObjectLambda	DeleteAccessPointPolicyForObjectLambda
S3.A138	Returns configuration for an Object Lambda Access Point.	S3.FC32	s3:GetAccessPointConfigurationForObjectLambda	GetAccessPointConfigurationForObjectLambda	GetAccessPointConfigurationForObjectLambda

S3.A139	Returns configuration information about the specified Object Lambda Access Point.	S3.FC32	s3:GetAccessPointForObjectLambda	GetAccessPointForObjectLambda	GetAccessPointForObjectLambda
S3.A140	Returns the resource policy for an Object Lambda Access Point.	S3.FC32	s3:GetAccessPointPolicyForObjectLambda	GetAccessPointPolicyForObjectLambda	GetAccessPointPolicyForObjectLambda
S3.A141	Returns the status of the resource policy associated with an Object Lambda Access Point.	S3.FC32	s3:GetAccessPointPolicyStatusForObjectLambda	GetAccessPointPolicyStatusForObjectLambda	GetAccessPointPolicyStatusForObjectLambda
S3.A142	Returns a list of the access points associated with the Object Lambda Access Point.	S3.FC32	s3>ListAccessPointsForObjectLambda	ListAccessPointsForObjectLambda	ListAccessPointsForObjectLambda
S3.A143	Replaces configuration for an Object Lambda Access Point.	S3.FC32	s3:PutAccessPointConfigurationForObjectLambda	PutAccessPointConfigurationForObjectLambda	PutAccessPointConfigurationForObjectLambda
S3.A144	Creates or replaces resource policy for an Object Lambda Access Point.	S3.FC32	s3:PutAccessPointPolicyForObjectLambda	PutAccessPointPolicyForObjectLambda	PutAccessPointPolicyForObjectLambda
S3.A145	Grants permission to abort a multipart upload.	S3.FC32	s3-object-lambda:AbortMultipartUpload	-	-
S3.A146	Grants permission to remove the null version of an object and insert a delete marker, which becomes the current version of the object.	S3.FC32	s3-object-lambda>DeleteObject	-	-
S3.A147	Grants permission to use the tagging subresource to remove the entire tag set from the specified object.	S3.FC32	s3-object-lambda>DeleteObjectTagging	-	-
S3.A148	Grants permission to retrieve objects from Amazon S3.	S3.FC32	s3-object-lambda:GetObject	-	-
S3.A149	Grants permission to return the Access Control List (ACL) of an object.	S3.FC32	s3-object-lambda:GetObjectAcl	-	-
S3.A150	Grants permission to get an object's current legal hold status.	S3.FC32	s3-object-lambda:GetObjectLegalHold	-	-
S3.A151	Grants permission to retrieve the retention settings for an object.	S3.FC32	s3-object-lambda:GetObjectRetention	-	-
S3.A152	Grants permission to return the tag set of an object.	S3.FC32	s3-object-lambda:GetObjectTagging	-	-
S3.A153	Grants permission to retrieve a specific version of an object.	S3.FC32	s3-object-lambda:GetObjectVersion	-	-
S3.A154	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000).	S3.FC32	s3-object-lambda>ListBucket	-	-
S3.A155	Grants permission to list the parts that have been uploaded for a specific multipart upload.	S3.FC32	s3-object-lambda>ListMultipartUploadParts	-	-
S3.A156	Grants permission to add an object to a bucket.	S3.FC32	s3-object-lambda:PutObject	-	-
S3.A157	Grants permission to set the Access Control List (ACL) permissions for new or existing objects in an S3 bucket.	S3.FC32	s3-object-lambda:PutObjectAcl	-	-
S3.A158	Grants permission to apply a legal hold configuration to the specified object.	S3.FC32	s3-object-lambda:PutObjectLegalHold	-	-
S3.A159	Grants permission to place an object retention configuration on an object.	S3.FC32	s3-object-lambda:PutObjectRetention	-	-
S3.A160	Grants permission to set the supplied tag-set to an object that already exists in a bucket.	S3.FC32	s3-object-lambda:PutObjectTagging	-	-
S3.A161	Grants permission to restore an archived copy of an object back into Amazon S3.	S3.FC32	s3-object-lambda:RestoreObject	-	-
S3.A162	Passes transformed objects to a GetObject operation when using Object Lambda Access Points.	S3.FC32	s3-object-lambda:WriteGetObjectResponse	WriteGetObjectResponse	WriteGetObjectResponse

S3.A163	Grants permission to remove a specific version of an object.	S3.FC32	s3-object-lambda:DeleteObjectVersion	-	-
S3.A164	Grants permission to remove the entire tag set for a specific version of the object.	S3.FC32	s3-object-lambda:DeleteObjectVersionTagging	-	-
S3.A165	Grants permission to return the Access Control List (ACL) of a specific object version.	S3.FC32	s3-object-lambda:GetObjectVersionAcl	-	-
S3.A166	Grants permission to return the tag set for a specific version of the object.	S3.FC32	s3-object-lambda:GetObjectVersionTagging	-	-
S3.A167	Grants permission to list in-progress multipart uploads.	S3.FC32	s3-object-lambda>ListBucketMultipartUploads	-	-
S3.A168	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket.	S3.FC32	s3-object-lambda>ListBucketVersions	-	-
S3.A169	Grants permission to use the ACL subresource to set the Access Control List (ACL) permissions for an object that already exists in a bucket.	S3.FC32	s3-object-lambda:PutObjectVersionAcl	-	-
S3.A170	Grants permission to set the supplied tag-set for a specific version of an object.	S3.FC32	s3-object-lambda:PutObjectVersionTagging	-	-
S3.A171	Returns configuration information about the specified Multi-Region Access Point.	S3.FC33	s3:GetMultiRegionAccessPoint	GetMultiRegionAccessPoint	GetMultiRegionAccessPoint
S3.A172	Indicates whether the specified Multi-Region Access Point has an access control policy that allows public access.	S3.FC33	s3:GetMultiRegionAccessPointPolicyStatus	GetMultiRegionAccessPointPolicyStatus	GetMultiRegionAccessPointPolicyStatus
S3.A173	Creates a Multi-Region Access Point and associates it with the specified buckets.	S3.FC33	s3>CreateMultiRegionAccessPoint	CreateMultiRegionAccessPoint	CreateMultiRegionAccessPoint
S3.A174	Retrieves the status of an asynchronous request to manage a Multi-Region Access Point.	S3.FC33	s3:DescribeMultiRegionAccessPointOperation	DescribeMultiRegionAccessPointOperation	DescribeMultiRegionAccessPointOperation
S3.A175	Deletes a Multi-Region Access Point. This action does not delete the buckets associated with the Multi-Region Access Point, only the Multi-Region Access Point itself.	S3.FC33	s3>DeleteMultiRegionAccessPoint	DeleteMultiRegionAccessPoint	DeleteMultiRegionAccessPoint
S3.A176	Returns a list of the Multi-Region Access Points currently associated with the specified AWS account.	S3.FC33	s3>ListMultiRegionAccessPoints	ListMultiRegionAccessPoints	ListMultiRegionAccessPoints
S3.A177	Returns the access control policy of the specified Multi-Region Access Point.	S3.FC33	s3:GetMultiRegionAccessPointPolicy	GetMultiRegionAccessPointPolicy	GetMultiRegionAccessPointPolicy
S3.A178	Associates an access control policy with the specified Multi-Region Access Point.	S3.FC33	s3:PutMultiRegionAccessPointPolicy	PutMultiRegionAccessPointPolicy	PutMultiRegionAccessPointPolicy
S3.A179	Remove tags from an existing Amazon S3 Batch Operations job.	S3.FC27	s3>DeleteJobTagging	DeleteJobTagging	DeleteJobTagging
S3.A180	Return the tag set of an existing Amazon S3 Batch Operations job.	S3.FC27	s3:GetJobTagging	GetJobTagging	GetJobTagging
S3.A181	Get an Amazon S3 Storage Lens dashboard.	S3.FC31	s3:GetStorageLensDashboard	GetStorageLensDashboardDataInternal	GetStorageLensDashboard
S3.A182	Replace tags on an existing Amazon S3 Batch Operations job.	S3.FC27	s3:PutJobTagging	PutJobTagging	PutJobTagging
S3.A183	Associate Public Access Block configurations with a specified access point, while creating a access point.	S3.FC26	s3:PutAccessPointPublicAccessBlock	PutAccessPointPublicAccessBlock	PutAccessPointPublicAccessBlock
S3.A184	Initiate the replication process by setting replication status of an object to pending.	S3.FC27	s3:InitiateReplication	-	-
S3.A185	Retrieves all the metadata from an object without returning the object itself.	S3.FC1	s3:GetObjectAttributes	Data-AWS::S3::Object-	GetObjectAttributes

	This action is useful if you're interested only in an object's metadata.		s3:GetObject	GetObjectAttributes	
S3.A186	Retrieves all the metadata from a versioned object without returning the object itself. This action is useful if you're interested only in an object's metadata.	S3.FC9	s3:GetObjectVersionAttributes s3:GetObjectVersion	Data-AWS::S3::Object-GetObjectAttributes	GetObjectAttributes(VersionId=)
S3.A187	Return the route configuration for a Multi-Region Access Point.	S3.FC33	s3:GetMultiRegionAccessPointRoutes	GetMultiRegionAccessPointRoutes	GetMultiRegionAccessPointRoutes
S3.A188	Submit a route configuration update for a Multi-Region Access Point.	S3.FC33	s3:SubmitMultiRegionAccessPointRoutes	SubmitMultiRegionAccessPointRoutes	SubmitMultiRegionAccessPointRoutes
S3.A189	Create an Amazon S3 Storage Lens group.	S3.FC31	s3:CreateStorageLensGroup	CreateStorageLensGroup	CreateStorageLensGroup
S3.A190	Delete an existing S3 Storage Lens group.	S3.FC31	s3:DeleteStorageLensGroup	DeleteStorageLensGroup	DeleteStorageLensGroup
S3.A191	Get an Amazon S3 Storage Lens group.	S3.FC31	s3:GetStorageLensGroup	GetStorageLensGroup	GetStorageLensGroup
S3.A192	List S3 Storage Lens groups.	S3.FC31	s3>ListStorageLensGroups	ListStorageLensGroups	ListStorageLensGroups
S3.A193	List the tags attached to the specified resource.	S3.FC34	s3>ListTagsForResource	ListTagsForResource	ListTagsForResource
S3.A194	Add tags to the specified resource.	S3.FC34	s3:TagResource	TagResource	TagResource
S3.A195	Remove tags from the specified resource.	S3.FC34	s3:UntagResource	UntagResource	UntagResource
S3.A196	Update an existing S3 Storage Lens group.	S3.FC31	s3:UpdateStorageLensGroup	UpdateStorageLensGroup	UpdateStorageLensGroup
S3.A197	Pause S3 replication from target source buckets to destination buckets (used by AWS FIS only).	S3.FC35	s3:PauseReplication	-	-
S3.A198	Retrieve ABAC configuration for a general purpose bucket.	S3.FC36	s3:GetBucketAbac	GetBucketAbac	GetBucketAbac
S3.A199	Set ABAC configuration for a general purpose bucket.	S3.FC36	s3:PutBucketAbac	PutBucketAbac	PutBucketAbac
S3.A200	Update the server-side encryption type of an existing object in a general purpose bucket (within same AWS Organizations).	S3.FC23	s3:UpdateObjectEncryption	Data-AWS::S3::Object-UpdateObjectEncryption	UpdateObjectEncryption

## Appendix 3 - AWS Data Perimeter

### Identity perimeter

#### [IP1] Only trusted identities can access my resources

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C152, assured by S3.C154] Ensure bucket ACLs and object ACLs are disabled on each bucket (enabled by default for all new buckets after April 2023).	Request 1) the mechanism ensuring bucket ACL and object ACL are disabled on each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	S3.T4 (Very High) S3.T6 (Very High) S3.T36 (Very High) S3.T43 (Very High) S3.T52 (Very High) S3.T53 (Very High)	Very High
Preventative (coso) Protect (NIST CSF)	[S3.C153] Prevent the creation of buckets with ACL enabled (e.g., by using an SCP and/or an IAM policy on "s3:CreateBucket" with a deny statement on StringNotEquals "s3:x-amz-object-ownership":"BucketOwnerEnforced"). Note that it does not block someone from enabling an ACL afterward via PutBucketOwnershipControls.	Create a bucket with ACL enabled; it should be denied.	Low	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	S3.T4 (High) S3.T6 (High) S3.T36 (High) S3.T43 (High) S3.T52 (High) S3.T53 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C154] Verify bucket ACL and object ACL are disabled on each bucket (e.g., using the AWS Config rule <a href="#">S3_BUCKET_ACL_PROHIBITED</a> for bucket ACL, <a href="#">S3 Storage Lens</a> ObjectOwnershipBucketOwnerEnforcedBucketCount, or S3 Inventory, which includes object ACL metadata).	Create/modify a bucket to enable ACL; it should be detected.	Medium	S3.FC1 S3.FC5 S3.FC8 S3.FC24 S3.FC25	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C26] Limit the access to the IAM actions required to execute the threats using AWS IAM and/or SCP, following the IAM Operating Model and using the IAM ThreatModel. Use the <a href="#">IAM Access Advisor</a> to review the use of non-object-related S3 actions.	Request the list of authorized IAM principals with the permissions required to execute the threat actions, its review process, and its review records.	High	S3.FC1 S3.FC2 S3.FC5 S3.FC6 S3.FC8 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC17 S3.FC19 S3.FC20 S3.FC23 S3.FC24 S3.FC25 S3.FC26 S3.FC27 S3.FC32 S3.FC33 S3.FC36	S3.T1 (High) S3.T2 (High) S3.T5 (Low) S3.T6 (Medium) S3.T7 (High) S3.T8 (High) S3.T11 (High) S3.T14 (Very High) S3.T16 (High) S3.T17 (Very High) S3.T18 (High) S3.T21 (Medium) S3.T25 (High) S3.T26 (High) S3.T28 (High) S3.T30 (High) S3.T33 (Very High) S3.T35 (Very High) S3.T36 (Medium) S3.T37 (Very High) S3.T38 (Very High) S3.T39 (High) S3.T41 (High) S3.T42 (High) S3.T44 (High) S3.T46 (High)	High

					S3.T47 (High) S3.T48 (High) S3.T49 (High) S3.T50 (High) S3.T51 (High) S3.T52 (High) S3.T53 (High) S3.T54 (High) S3.T55 (High) S3.T56 (High) S3.T58 (High) S3.T59 (High) S3.T60 (High) S3.T61 (High) S3.T62 (High) S3.T63 (High) S3.T64 (High) S3.T65 (High)	
Directive (coso) Identify (NIST CSF)	[S3.C149] For each bucket, maintain a list of authorized IAM principals allowed to access via the bucket policy.	Request the list of authorized IAM principals allowed to access via bucket policy, its review process, and its review records.	Medium	S3.FC10	S3.T37 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C150, depends on S3.C149, assured by S3.C151] Ensure only authorized IAM principals allowed to access via bucket policy are configured (e.g., using IAM Access Analyzer for reconciliation).	Request 1) the mechanism ensuring only authorized IAM principals are allowed to access buckets via bucket policy, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC10	S3.T37 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C151] Verify only authorized IAM principals allowed to access via bucket policy are used (e.g., using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ).	Allow an unauthorized IAM principal on a bucket policy; it should be detected.	Medium	S3.FC10	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C34, assured by S3.C36] Deny requests to change object ACL to public (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy with a deny statement on PutObjectAcl for "s3:x-amz-grant-read", "s3:x-amz-grant-read-acp", "s3:x-amz-grant-write-acp", "s3:x-amz-grant-full-control" on the following predefined groups "http://acs.amazonaws.com/groups/global/AllUsers" and "http://acs.amazonaws.com/groups/global/AuthenticatedUsers").	Make a call to create a public ObjectACL; it should be denied.	Medium	S3.FC1 S3.FC5	S3.T6 (Very High) S3.T36 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C36] Verify the control blocking change ObjectACL to public (e.g., an SCP and VPC endpoint policy) is properly implemented.	Remove the control blocking changes of ObjectACL to public; it should be detected.	High	S3.FC1 S3.FC5	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C55, assured by S3.C57] Deny requests to add an ACL on a bucket (e.g., using an SCP, bucket policies, centrally in an RCP applied to the OU or AWS account, or VPC endpoint policy, with a deny statement on "s3:PutBucketAcl").	Make a call to add an ACL on a bucket; it should be denied.	Medium	S3.FC8 S3.FC19	S3.T4 (Very High) S3.T58 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C57] Verify the control blocking bucket ACL changes is properly implemented.	Remove the control blocking bucket ACL changes; it should be detected.	High	S3.FC8 S3.FC19	-	High
Directive (coso) Detect (NIST CSF)	[S3.C9, depends on S3.C58] Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data).	Request the CloudTrail ThreatModel and the evidence of its application for enabling and protecting S3 data events.	Very Low	S3.FC1 S3.FC5	S3.T1 (Low) S3.T4 (Low)	Medium

	Make it available for security analysis, and protect it using CloudTrail ThreatModel.			S3.FC8	S3.T5 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T12 (Low) S3.T16 (Low) S3.T21 (Low) S3.T31 (Low) S3.T34 (Low) S3.T35 (Low) S3.T36 (Low) S3.T39 (Low)	
Directive (coso) Protect (NIST CSF)	[S3.C27, assured by S3.C28] In the S3 bucket/access point/Object Lambda Access Point policy, do not allow IAM principals of the same AWS account. Only AWS IAM policies, and not resource policies such as S3 bucket/access point/Object Lambda Access Point policies, should be used to provide permissions to a principal of the same AWS account.	Request all S3 bucket/access point/Object Lambda Access Point policy statements with "allow"; no principal from the same account should be authorized.	Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC19 S3.FC20 S3.FC23 S3.FC26 S3.FC27 S3.FC32 S3.FC33	S3.T1 (Low) S3.T2 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T11 (Low) S3.T14 (Medium) S3.T16 (Low) S3.T17 (Medium) S3.T18 (Low) S3.T21 (Low) S3.T25 (Low) S3.T26 (Medium) S3.T30 (Low) S3.T33 (Medium) S3.T35 (Medium) S3.T36 (Low) S3.T37 (Medium) S3.T38 (Medium) S3.T39 (Low) S3.T41 (Low) S3.T42 (Low) S3.T44 (Low) S3.T46 (Medium) S3.T54 (Medium) S3.T55 (Medium) S3.T58 (Medium) S3.T59 (Medium) S3.T65 (Low)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C28] Verify all S3 bucket/access point/Object Lambda Access Point policies do not allow an IAM principal of the same AWS account (e.g., using the Config rule S3_BUCKET_POLICY_GRANTEE_CHECK for bucket policy).	Add an allow statement for an IAM principal of the same account in 1) a bucket policy, 2) an access point policy, and 3) an Object Lambda Access Point; it should be detected.	Medium	S3.FC1 S3.FC2 S3.FC5 S3.FC10 S3.FC12 S3.FC13 S3.FC15 S3.FC19 S3.FC20 S3.FC23	-	Medium

				S3.FC26 S3.FC27 S3.FC32 S3.FC33		
Directive (coso) Protect (NIST CSF)	[S3.C170, depends on S3.C58] Integrate and limit the access to general purpose buckets via tags in the IAM Operating Model (including enforcing tagging of buckets and objects at creation using AWS:ResourceTag and s3:BucketTag).	Request the IAM tag Operating Model for the general purpose buckets.	High	S3.FC2	S3.T33 (Very High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C171, depends on S3.C58, assured by S3.C172] Ensure only the authorized ABAC configuration for each general purpose bucket is configured.	Request 1) the mechanism ensuring only the authorized ABAC configuration for each general purpose bucket is configured, 2) its records of execution for all new general purpose buckets, and 3) the plan to move any older general purpose buckets.	Medium	S3.FC36	S3.T64 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C172] Verify all general purpose buckets use their authorized ABAC configuration.	1) Enable ABAC on an unauthorized general purpose bucket, or 2) disable ABAC on an authorized general purpose bucket; it should be detected.	Medium	S3.FC36	-	Medium
Directive (coso) Identify (NIST CSF)	[S3.C129] Maintain a list of cross-account access on each Object Lambda Access Point.	Request the list of authorized cross-account access for each Object Lambda Access Point, its review process, and its review records.	Very Low	S3.FC32	S3.T46 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C130, depends on S3.C129, assured by S3.C131] Ensure only authorized cross-account IAM entities are allowed in the Object Lambda Access Point policy.	Request the mechanism ensuring only cross-account IAM entities are allowed in the Object Lambda Access Point policy, and the evidence of its execution.	Low	S3.FC32	S3.T46 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C131] Verify only the authorized cross-account IAM entities are allowed in the Object Lambda Access Point policy.	Add an unauthorized cross-account IAM entity on an Object Lambda Access Point policy; it should be detected.	High	S3.FC32	-	Medium
Detective (coso) Detect (NIST CSF)	[S3.C35] Monitor ObjectACL changes (or tentative changes) to public using CloudTrail S3 data events.	Make a call to create a public ObjectACL; it should be detected.	Low	S3.FC1 S3.FC5	S3.T6 (Low) S3.T36 (Low)	Low
Detective (coso) Detect (NIST CSF)	[S3.C56] Monitor changes to bucket ACLs to ensure they stay private (e.g., using the CloudTrail event PutBucketAcl and its field requestParameters.x-amz-acl, which should either be "private" or not exist).	Make a call to have a bucket ACL other than private; it should be detected.	Medium	S3.FC8 S3.FC19	S3.T4 (Low) S3.T58 (Low)	Low
Directive (coso) Protect (NIST CSF)	[S3.C155, assured by S3.C156] Ensure all requests are blocked from AWS service roles that do not require access (e.g., by denying all requests with the principal "arn:aws:iam::*:*/AWSServiceRoleFor*" on S3 bucket policies).	Request 1) the mechanism ensuring only authorized AWS service roles can access each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC28	S3.T57 (Very High)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C156] Verify all requests from unauthorized service roles are blocked.	Remove the statement on a bucket policy denying all unauthorized service roles; it should be detected.	Medium	S3.FC28	-	Low

#### [IP2] Only trusted identities are allowed from my network

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C124] Ensure all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoint controls.	Request 1) the mechanism ensuring all S3 VPC endpoints (Interface and Gateway) are covered by the VPC endpoints controls, 2) its records of execution for all new VPC endpoints, and 3) the plan to move any older VPC endpoints.	Low	S3.FC1	S3.T8 (Very High) S3.T9 (Very High)	High



## Resource perimeter

### [RP1] My identities can access only trusted resources

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C11] Track all buckets you don't control that host your objects, define their data classification, identify their respective owners (and AWS account ID), determine their ObjectACL requirements (including S3 Object Ownership), and get assurance of their protection (e.g., through contractual agreement, verified by assurance programs, or using this ThreatModel).	Request the list of all external buckets authorized to host your objects, their respective owners (and AWS account ID), their ObjectACL requirements (including S3 Object Ownership), their data classification, and the mechanism used to ensure the security of those buckets.	Medium	S3.FC1 S3.FC5 S3.FC16	S3.T1 (Very Low) S3.T3 (High) S3.T5 (Very Low) S3.T6 (Low) S3.T7 (Very Low) S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Low) S3.T14 (Very Low) S3.T15 (Very Low) S3.T21 (Very Low) S3.T31 (High) S3.T43 (Very High)	Very High
Directive (coso) Protect (NIST CSF)	[S3.C15] Request access via an S3 access point on a bucket you don't own, if compatible with your interaction with the bucket (e.g., not through an unsupported AWS service).	Request the documented reasons why the access point was not implemented in the use case.	Low	S3.FC1	S3.T8 (Medium) S3.T9 (Medium) S3.T31 (Very High)	High
Directive (coso) Identify (NIST CSF)	[S3.C120] Maintain a list of IAM roles used for Batch jobs, ideally dedicated (e.g., using change management process on infrastructure-as-code).	Request the list of all IAM roles configured for Batch jobs.	Medium	S3.FC27	S3.T44 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C122, depends on S3.C120] Limit access to authorized IAM roles used for Batch jobs, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Request the IAM ThreatModel and the evidence of its application to the IAM roles used for Batch jobs.	Medium	S3.FC27	S3.T44 (Very High)	High
Directive (coso) Detect (NIST CSF)	[S3.C9, depends on S3.C58] Enable <a href="#">CloudTrail S3 data events</a> in relevant AWS accounts, Regions, and buckets (e.g., production, with sensitive data). Make it available for security analysis, and protect it using CloudTrail ThreatModel.	Request the CloudTrail ThreatModel and the evidence of its application for enabling and protecting S3 data events.	Very Low	S3.FC1 S3.FC5 S3.FC8	S3.T1 (Low) S3.T4 (Low) S3.T5 (Low) S3.T6 (Low) S3.T7 (Low) S3.T8 (Low) S3.T9 (Low) S3.T11 (Low) S3.T12 (Low) S3.T16 (Low) S3.T21 (Low) S3.T31 (Low) S3.T34 (Low) S3.T35 (Low) S3.T36 (Low) S3.T39 (Low)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C13, depends on S3.C11] Monitor that only authorized external buckets are used (e.g., via CloudTrail S3 data events in resources[].accountId and resources[].ARN). Both account ID and bucket name must be verified.	Make a call to an unauthorized bucket; it should be detected.	Low	S3.FC1 S3.FC5	S3.T1 (Low) S3.T7 (Low) S3.T11 (Low) S3.T21 (Low) S3.T31 (Medium)	Medium
Directive (coso)	[S3.C46]	Request the process ensuring that all S3 buckets interacted	Medium	S3.FC1	S3.T1 (Medium)	Medium

Protect (NIST CSF)	Ensure all S3 buckets interacted with are in the correct AWS account (e.g., using the condition in all compatible S3 requests: x-amz-expected-bucket-owner and x-amz-source-expected-bucket-owner).	with are in the correct AWS account.		S3.FC5	S3.T3 (Medium)	
Directive (coso) Identify (NIST CSF)	[S3.C86] Maintain a list of authorized buckets to have replication enabled, their target bucket, and replication type (i.e., encryption type, ownership, RTC, etc.) ( <a href="#">ref</a> ).	Request the list of authorized buckets to have replication enabled, their target bucket and replication rights, its review process, and its review records.	Medium	S3.FC15	S3.T2 (Very Low)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C89] Maintain a list of IAM roles used for replication, ideally dedicated (e.g., using change management process on infrastructure-as-code).	Request the list of all IAM roles configured for replication.	Medium	S3.FC15	S3.T2 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C90, depends on S3.C89] Limit S3 access to the source and destination buckets and the replication rights of each authorized IAM role configured for replication.	Request the S3 access for each replication role, and how they align with the replication requirements.	Medium	S3.FC15	S3.T2 (Medium)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C91, depends on S3.C89] Limit access to authorized IAM roles used for replication, using the IAM ThreatModel (e.g., trust policy, and "iam:PassRole").	Request the IAM ThreatModel and the evidence of its application to the IAM roles used for replication.	High	S3.FC15	S3.T2 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C134, depends on S3.C86, assured by S3.C87,S3.C88,S3.C117] Ensure only authorized buckets have replication enabled and are configured correctly.	Request 1) the mechanism ensuring only authorized buckets have replication enabled with their correct configuration, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC15	S3.T2 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C138, depends on S3.C89, assured by S3.C92] Ensure only authorized IAM roles are attached for each replication, ideally dedicated.	Request the mechanism ensuring authorized IAM roles are attached for each replication, and the evidence of its execution for all replication configurations.	Medium	S3.FC15	S3.T2 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C121, depends on S3.C120] Limit access to only the required resources/permissions (e.g., source/destination buckets, Lambda functions) for each authorized IAM role configured for Batch jobs.	Request access only to the required resources/permissions for each Batch IAM role, and request information on how they are aligned with the replication requirements.	Medium	S3.FC27	S3.T44 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C139, depends on S3.C120, assured by S3.C123] Ensure only an authorized IAM role is attached to each Batch job.	Request the mechanism ensuring only an authorized IAM role is attached to each Batch job, and the evidence of its execution for all new {resource}.	Medium	S3.FC27	S3.T44 (High)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C158] Maintain a list of authorized S3 buckets and their AWS accounts for cross-account access points.	Request the list of authorized S3 buckets and their AWS account for cross-account access points, its review process, and its review records.	Low	S3.FC26	S3.T60 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C159, depends on S3.C158, assured by S3.C161] Ensure only authorized S3 buckets and their AWS accounts for cross-account access points are configured.	Request 1) the mechanism ensuring only authorized S3 buckets and their AWS account for cross-account access points are configured, 2) its records of execution for all new S3 buckets and their AWS accounts for cross-account access points, and 3) the plan to move any older S3 buckets and their AWS accounts for cross-account access points.	Medium	S3.FC26	S3.T60 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C160, depends on S3.C158] Monitor CreateAccessPoint to detect unauthorized buckets or AWS accounts (i.e., using CloudTrail event CreateAccessPoint and its fields "requestParameters.CreateAccessPointRequest.Bucket" and "requestParameters.CreateAccessPointRequest.BucketAccount").	Call the API to create a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	S3.T60 (Medium)	Medium
Assurance (coso)	[S3.C161]	Deploy a cross-account access point with an unauthorized 1)	Medium	S3.FC26	-	Medium

Detect (NIST CSF)	Verify only authorized S3 buckets and their AWS accounts for cross-account access points are used.	bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.				
Directive (coso) Identify (NIST CSF)	[S3.C94] Maintain a list of authorized notification receivers (e.g., SNS topic, Lambda) for each bucket. You might use a simpler approach by using authorized account IDs to ensure all your receivers are in authorized AWS accounts.	Request the list of authorized notification receivers for each bucket, its review process, and its review records.	Low	S3.FC20	S3.T41 (Very Low)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C95] Verify only authorized notification receiver(s) are configured for buckets.	Create an unauthorized receiver; it should be detected.	High	S3.FC20	-	Low
Directive (coso) Protect (NIST CSF)	[S3.C135, depends on S3.C94, assured by S3.C95] Ensure only authorized notification receivers for each bucket are configured.	Request 1) the mechanism ensuring only authorized notification receivers for each bucket are configured, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC20	S3.T41 (High)	Low
Directive (coso) Identify (NIST CSF)	[S3.C96] Maintain a list of authorized S3 buckets to receive the S3 Inventory of each bucket.	Request the list of authorized bucket(s) to receive S3 Inventory of each bucket, its review process, and its review records.	Low	S3.FC12	S3.T42 (Very Low)	Very Low
Assurance (coso) Detect (NIST CSF)	[S3.C97] Verify only authorized buckets are configured to receive inventory.	Create an unauthorized bucket to receive inventory; it should be detected.	High	S3.FC12	-	Very Low
Directive (coso) Protect (NIST CSF)	[S3.C136, depends on S3.C96, assured by S3.C97] Ensure only authorized S3 buckets are configured to receive S3 Inventory for each bucket.	Request 1) the mechanism ensuring only authorized S3 buckets are configured to receive S3 Inventory for each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC12	S3.T42 (Medium)	Very Low

#### [RP2] Only trusted resources can be accessed from my network

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Identify (NIST CSF)	[S3.C104] Maintain a list of authorized access between VPCs, S3 access points, and S3.	Request the list of authorized access between VPC, S3 access points, and S3.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC26 S3.FC28 S3.FC33	S3.T7 (Very Low) S3.T9 (Very Low) S3.T10 (Very Low) S3.T11 (Very Low) S3.T28 (Very Low) S3.T37 (Very Low) S3.T54 (Very Low) S3.T55 (Very Low) S3.T56 (Very Low) S3.T60 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C105, depends on S3.C104, assured by S3.C109] Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy.	Make a request on an unauthorized access point or bucket; it should be denied.	Medium	S3.FC1 S3.FC5 S3.FC26 S3.FC28 S3.FC33	S3.T7 (Medium) S3.T9 (Very High) S3.T10 (Very High) S3.T11 (Medium) S3.T54 (Medium) S3.T55 (Medium)	High
Directive (coso) Identify (NIST CSF)	[S3.C125] Maintain a list of authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload.	Request the list of authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload, its review process, and its review records.	Low	S3.FC32	S3.T46 (Very Low)	High

Directive (coso) Protect (NIST CSF)	[S3.C126, depends on S3.C125, assured by S3.C127] Ensure only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload are created.	Request the mechanism ensuring only authorized Lambda functions for each Object Lambda Access Point, its associated access point, its associated HEAD/LIST/GET request(s), and payload, and the evidence of its execution.	Medium	S3.FC32	S3.T46 (Very High)	High
Directive (coso) Identify (NIST CSF)	[S3.C22] Maintain a list of authorized S3 and S3 access points (and their respective AWS accounts) to be accessed for each VPC.	Request the list of authorized S3 buckets and S3 access points to be accessed for each VPC, its review process, and its review records.	Medium	S3.FC1 S3.FC5	S3.T8 (Very Low) S3.T9 (Very Low) S3.T11 (Very Low)	Medium
Preventative (coso) Protect (NIST CSF)	[S3.C23, depends on S3.C22, assured by S3.C24] Limit the access to only authorized S3 bucket(s) or their AWS account(s) from each VPC (e.g., using the condition key "s3:ResourceAccount" on the VPC endpoint policy, alternatively use a specific resource-level statement for each bucket, or if the VPC endpoint policy size is beyond the limit and more granular control on VPC is required, use access points).	Make a request to an unauthorized bucket from one of your VPCs; it should be denied.	Medium	S3.FC1 S3.FC5	S3.T8 (High) S3.T9 (High) S3.T11 (High)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C24] Verify all VPCs are limited to accessing only authorized S3 bucket(s).	Remove the control limiting access to only authorized S3 bucket(s); it should be detected.	High	S3.FC1 S3.FC5	-	Medium
Directive (coso) Identify (NIST CSF)	[S3.C86] Maintain a list of authorized buckets to have replication enabled, their target bucket, and replication type (i.e., encryption type, ownership, RTC, etc.) ( <a href="#">ref</a> ).	Request the list of authorized buckets to have replication enabled, their target bucket and replication rights, its review process, and its review records.	Medium	S3.FC15	S3.T2 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C134, depends on S3.C86, assured by S3.C87,S3.C88,S3.C117] Ensure only authorized buckets have replication enabled and are configured correctly.	Request 1) the mechanism ensuring only authorized buckets have replication enabled with their correct configuration, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC15	S3.T2 (High)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C158] Maintain a list of authorized S3 buckets and their AWS accounts for cross-account access points.	Request the list of authorized S3 buckets and their AWS account for cross-account access points, its review process, and its review records.	Low	S3.FC26	S3.T60 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C159, depends on S3.C158, assured by S3.C161] Ensure only authorized S3 buckets and their AWS accounts for cross-account access points are configured.	Request 1) the mechanism ensuring only authorized S3 buckets and their AWS account for cross-account access points are configured, 2) its records of execution for all new S3 buckets and their AWS accounts for cross-account access points, and 3) the plan to move any older S3 buckets and their AWS accounts for cross-account access points.	Medium	S3.FC26	S3.T60 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C160, depends on S3.C158] Monitor CreateAccessPoint to detect unauthorized buckets or AWS accounts (i.e., using CloudTrail event CreateAccessPoint and its fields "requestParameters.CreateAccessPointRequest.Bucket" and "requestParameters.CreateAccessPointRequest.BucketAccou ntId").	Call the API to create a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	S3.T60 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C161] Verify only authorized S3 buckets and their AWS accounts for cross-account access points are used.	Deploy a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C18, depends on S3.C17] For each VPC with an IAM entity allowed to use S3, secure them with the VPC ThreatModel (e.g., <a href="#">modification of VPC endpoints</a> , <a href="#">VPC endpoint policy</a> , <a href="#">routing table</a> , <a href="#">Security Groups</a> ).	Request how the VPC ThreatModel for S3 is being applied.	High	S3.FC1 S3.FC5	S3.T9 (Medium) S3.T11 (Medium) S3.T62 (Medium)	Low
Directive (coso)	[S3.C21]	Request the mechanism to enable VPC DNS query logging in	Medium	S3.FC1	S3.T8 (Very Low)	Low

Detect (NIST CSF)	Enable <a href="#">VPC DNS query logging</a> in all VPCs.	all VPCs.		S3.FC5	S3.T9 (Very Low) S3.T11 (Very Low)	
Detective (coso) Detect (NIST CSF)	[S3.C25, depends on S3.C21,S3.C22] Monitor VPC DNS query logs to ensure only authorized S3 buckets and S3 access points are being queried in each VPC (e.g., using VPC DNS query logging) and protect them using Route 53 ThreatModel.	Make a DNS query to an unauthorized 1) S3 bucket and 2) S3 access points; it should be detected.	Low	S3.FC1 S3.FC5	S3.T8 (Low) S3.T9 (Low) S3.T11 (Low)	Low
Directive (coso) Identify (NIST CSF)	[S3.C94] Maintain a list of authorized notification receivers (e.g., SNS topic, Lambda) for each bucket. You might use a simpler approach by using authorized account IDs to ensure all your receivers are in authorized AWS accounts.	Request the list of authorized notification receivers for each bucket, its review process, and its review records.	Low	S3.FC20	S3.T41 (Very Low)	Low
Assurance (coso) Detect (NIST CSF)	[S3.C95] Verify only authorized notification receiver(s) are configured for buckets.	Create an unauthorized receiver; it should be detected.	High	S3.FC20	-	Low
Directive (coso) Protect (NIST CSF)	[S3.C135, depends on S3.C94, assured by S3.C95] Ensure only authorized notification receivers for each bucket are configured.	Request 1) the mechanism ensuring only authorized notification receivers for each bucket are configured, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Medium	S3.FC20	S3.T41 (High)	Low

## Network perimeter

### [NP1] My identities can access resources only from expected networks

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C8] Block S3 endpoints ( <a href="#">DNS</a> and <a href="#">IP ranges</a> ) in your corporate perimeter security to the Internet (e.g., firewalls or a cloud interception proxy), including via Internet Gateway, to force the use of VPC endpoints. It will block data-plane transfer. Note: AWS Management Console stays functional as it proxies non-data-plane requests (via "console.aws.amazon.com").	Request the evidence of the implementation of blocking S3 endpoints in your corporate perimeter security (e.g., firewalls) and tests of its effectiveness.	Low	S3.FC1 S3.FC5 S3.FC28	S3.T7 (High) S3.T10 (High) S3.T12 (Low) S3.T18 (Medium) S3.T34 (Very High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C12, depends on S3.C11] Allow only authorized ACLs on objects for buckets you don't control (e.g., using IAM and VPC endpoint policy with the <a href="#">ACL conditions</a> ).	Put an object with an unauthorized ACL; it should be denied.	Medium	S3.FC1	S3.T5 (Medium) S3.T6 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C16] Analyze and protect all AWS services accessing S3 (e.g., via ThreatModel). Enforce use in VPC only, whenever possible.	Request the ThreatModels for all AWS services using S3.	High	S3.FC1 S3.FC5	S3.T21 (Very High) S3.T30 (Very High)	Medium
Directive (coso) Identify (NIST CSF)	[S3.C158] Maintain a list of authorized S3 buckets and their AWS accounts for cross-account access points.	Request the list of authorized S3 buckets and their AWS account for cross-account access points, its review process, and its review records.	Low	S3.FC26	S3.T60 (Very Low)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C159, depends on S3.C158, assured by S3.C161] Ensure only authorized S3 buckets and their AWS accounts for cross-account access points are configured.	Request 1) the mechanism ensuring only authorized S3 buckets and their AWS account for cross-account access points are configured, 2) its records of execution for all new S3 buckets and their AWS accounts for cross-account access points, and 3) the plan to move any older S3 buckets and their AWS accounts for cross-account access points.	Medium	S3.FC26	S3.T60 (High)	Medium
Detective (coso) Detect (NIST CSF)	[S3.C160, depends on S3.C158] Monitor CreateAccessPoint to detect unauthorized buckets or AWS accounts (i.e., using CloudTrail event CreateAccessPoint and its fields "requestParameters.CreateAccessPointRequest.Bucket" and "requestParameters.CreateAccessPointRequest.BucketAccou ntId").	Call the API to create a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	S3.T60 (Medium)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C161] Verify only authorized S3 buckets and their AWS accounts for cross-account access points are used.	Deploy a cross-account access point with an unauthorized 1) bucket or 2) an authorized bucket in an unauthorized AWS account; it should be detected.	Medium	S3.FC26	-	Medium

### [NP2] My resources can be accessed only from expected networks

Type	Control	Testing	Effort	Feature Class(es)	Threat(s) and Impact	CVSS-weighted Priority
Directive (coso) Protect (NIST CSF)	[S3.C49, assured by S3.C50] Enable account-level S3 Block Public Access on all AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Request 1) the mechanism ensuring account-level S3 Block Public Access is enabled on all AWS accounts, 2) its records of execution for all new AWS accounts, and 3) the plan to move any older AWS accounts.	Very Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C50] Verify account-level S3 Block Public Access is enabled on all	Remove the account-level S3 Block Public Access of an AWS account; it should be detected.	Very Low	S3.FC5 S3.FC8	-	Very High

	AWS accounts, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g., using the AWS Config rule: <a href="#">S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS</a> ).			S3.FC10		
Directive (coso) Protect (NIST CSF)	[S3.C51, assured by S3.C52] Enable S3 Block Public Access on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (enabled by default for all new buckets after April 2023).	Request 1) the mechanism ensuring S3 Block Public Access is enabled on each bucket, 2) its records of execution for all new buckets, and 3) the plan to move any older buckets.	Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C52] Verify S3 Block Public Access is enabled on all S3 buckets, with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true (e.g., using the AWS Config rule: <a href="#">S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED</a> ).	Remove the S3 Block Public Access from an S3 bucket; it should be detected.	Very Low	S3.FC5 S3.FC8 S3.FC10	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C53, assured by S3.C54] Enable S3 Block Public Access on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Request 1) the mechanism ensuring S3 Block Public Access is enabled on each S3 access point, 2) its records of execution for all new S3 access points, and 3) the plan to move any older S3 access points.	Low	S3.FC5 S3.FC10 S3.FC26 S3.FC33	S3.T14 (High) S3.T36 (Medium) S3.T37 (Medium) S3.T38 (Medium) S3.T54 (High) S3.T55 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C54] Verify S3 Block Public Access is enabled on all S3 access points (including multi-region), with BlockPublicAcls, IgnorePublicAcls, BlockPublicPolicy, and RestrictPublicBuckets set to true.	Remove S3 Block Public Access of 1) an access point, and 2) a Multi-Region Access Point; it should be detected.	Medium	S3.FC5 S3.FC10 S3.FC26 S3.FC33	-	Very High
Directive (coso) Protect (NIST CSF)	[S3.C173] Block public access to each S3 bucket at the organization root, OU, or account-level by enforcing S3 policies in AWS Organizations.	Request the mechanism enforcing block of public access to each bucket at the organization root, OU, or account-level via S3 policies, its records of execution for all new AWS accounts, and the plan to move any older AWS accounts.	Low	S3.FC5 S3.FC8 S3.FC10	S3.T4 (High) S3.T14 (High) S3.T36 (Very High) S3.T37 (Very High) S3.T38 (Medium)	Very High
Directive (coso) Identify (NIST CSF)	[S3.C98] For each S3 bucket, maintain a list of VPCs authorized to access it.	For each S3 bucket, request the list of authorized VPCs to access it, its review process, and its review records.	Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10	S3.T11 (Very Low) S3.T14 (Very Low) S3.T17 (Very Low) S3.T30 (Very Low) S3.T33 (Very Low) S3.T36 (Very Low) S3.T38 (Very Low) S3.T39 (Very Low)	Very High
Preventative (coso) Protect (NIST CSF)	[S3.C99, depends on S3.C98, assured by S3.C100] Limit access to only authorized VPCs (e.g., using their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement if the condition "aws:SourceVpce" is met, or if the bucket policy size is beyond the limit, use this condition on the access point).	Make a request to the bucket outside an authorized VPC; it should be denied.	Very Low	S3.FC1 S3.FC2 S3.FC5 S3.FC10	S3.T11 (Medium) S3.T14 (Medium) S3.T17 (Medium) S3.T30 (High) S3.T33 (High) S3.T36 (High) S3.T38 (High) S3.T39 (High)	Very High
Assurance (coso) Detect (NIST CSF)	[S3.C100] Verify all buckets include a control to limit access to only authorized VPCs (e.g., using the AWS Config rule <a href="#">S3_BUCKET_POLICY_GRANTEE_CHECK</a> ).	Remove the control limiting access to only authorized VPC(s); it should be detected.	Medium	S3.FC1 S3.FC2 S3.FC5 S3.FC10	-	Very High

Directive (coso) Identify (NIST CSF)	[S3.C17] For each VPC, maintain a list of AWS Organizations, OUs, and/or AWS accounts where IAM entities are authorized to access S3.	For each VPC, request the list of AWS Organizations, OU, and/or AWS account(s), where IAM entities are authorized to access S3, its review process, and its review records.	Medium	S3.FC1 S3.FC5	S3.T9 (Very Low) S3.T11 (Very Low) S3.T62 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C19, depends on S3.C17, assured by S3.C20] Block any IAM entity not belonging to an authorized AWS Organization, OU, and/or AWS account from calling S3 from your VPCs by adding a deny statement in the S3 VPC endpoint policy for each VPC, with the condition using "aws:PrincipalOrgPaths" ( <a href="#">ref</a> ) including the full Org IDs, as those are globally unique.	For each VPC, make an API call with an IAM entity that is not part of its authorized AWS Organizations paths; it should be denied.	Low	S3.FC1 S3.FC5	S3.T9 (Very High) S3.T11 (Very High) S3.T62 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C20] Verify all S3 VPC endpoints are blocking any IAM entity not belonging to authorized AWS Organizations, OUs, and/or AWS accounts.	Remove the policy statement blocking any IAM entity not belonging to authorized AWS Organizations, OUs, and/or AWS accounts from the VPC endpoint; it should be detected.	High	S3.FC1 S3.FC5	-	High
Directive (coso) Protect (NIST CSF)	[S3.C47, assured by S3.C48] Front buckets that are required to be public, using authenticated CDN (e.g., CloudFront) or API Gateway, protected with WAF (e.g., for <a href="#">hotlinking</a> ).	Request the process ensuring that buckets required to be public are fronted by an authenticated CDN or API Gateway, and are protected with a WAF.	Medium	S3.FC5 S3.FC16	S3.T13 (Very High) S3.T14 (Medium) S3.T22 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C48] Verify no bucket is available publicly for write or read (e.g., using the AWS Config rules: <a href="#">S3_BUCKET_PUBLIC_READ_PROHIBITED</a> and <a href="#">S3_BUCKET_PUBLIC_WRITE_PROHIBITED</a> ).	Create a public S3 bucket; it should be detected.	Very Low	S3.FC5 S3.FC16	-	High
Directive (coso) Identify (NIST CSF)	[S3.C104] Maintain a list of authorized access between VPCs, S3 access points, and S3.	Request the list of authorized access between VPC, S3 access points, and S3.	Medium	S3.FC1 S3.FC5 S3.FC10 S3.FC26 S3.FC28 S3.FC33	S3.T7 (Very Low) S3.T9 (Very Low) S3.T10 (Very Low) S3.T11 (Very Low) S3.T28 (Very Low) S3.T37 (Very Low) S3.T54 (Very Low) S3.T55 (Very Low) S3.T56 (Very Low) S3.T60 (Very Low)	High
Preventative (coso) Protect (NIST CSF)	[S3.C105, depends on S3.C104, assured by S3.C109] Limit access via the S3 access point by using a VPC endpoint, bucket policy, or centrally in an RCP applied to the OU or AWS account, with the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn" in an allow statement to reduce the length of the allowlist bucket name in the VPC endpoint/bucket policy.	Make a request on an unauthorized access point or bucket; it should be denied.	Medium	S3.FC1 S3.FC5 S3.FC26 S3.FC28 S3.FC33	S3.T7 (Medium) S3.T9 (Very High) S3.T10 (Very High) S3.T11 (Medium) S3.T54 (Medium) S3.T55 (Medium)	High
Preventative (coso) Protect (NIST CSF)	[S3.C106, depends on S3.C104, assured by S3.C110] In bucket policies, or centrally in an RCP applied to the OU or AWS account, deny all IAM principals not using an authorized S3 access point(s) using the condition "s3:DataAccessPointAccount" or preferably "s3:DataAccessPointArn".	Query the bucket outside the S3 access point; it should be denied.	Medium	S3.FC1 S3.FC10 S3.FC26 S3.FC33	S3.T7 (Medium) S3.T28 (High) S3.T37 (High) S3.T55 (Medium) S3.T56 (Very High) S3.T60 (High)	High
Preventative (coso) Protect (NIST CSF)	[S3.C107] Block the creation of non-VPC S3 access point "s3>CreateAccessPoint" (e.g., using IAM policies and SCPs with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Make a request to create an internet-based access point; it should be denied.	Low	S3.FC1 S3.FC26	S3.T7 (Medium) S3.T28 (Very High) S3.T60 (High)	High

Preventative (coso) Protect (NIST CSF)	[S3.C108, assured by S3.C111] Block all traffic from Internet-configured S3 access points (e.g., in their bucket policy, or centrally in an RCP applied to the OU or AWS account, using a deny statement with the condition "StringNotEquals": {"s3:AccessPointNetworkOrigin": "VPC"}).	Create an internet-facing access point and try to access a bucket; it should be denied.	Low	S3.FC1 S3.FC26 S3.FC28	S3.T7 (Medium) S3.T10 (Medium) S3.T28 (Very High)	High
Assurance (coso) Detect (NIST CSF)	[S3.C109] Verify only access points are used in the resource-level statements in VPC endpoints.	Create a VPC endpoint giving access to an S3 bucket directly, rather than an access point; it should be detected.	High	S3.FC1 S3.FC5 S3.FC26 S3.FC28 S3.FC33	-	High
Assurance (coso) Detect (NIST CSF)	[S3.C110] Verify S3 bucket policies deny unauthorized S3 access points.	Remove/modify the deny on the bucket policy; it should be detected.	High	S3.FC1 S3.FC10 S3.FC26 S3.FC33	-	High
Assurance (coso) Detect (NIST CSF)	[S3.C111] Verify all S3 access points are VPC-attached.	Create an internet-based access point; it should be detected.	Low	S3.FC1 S3.FC26 S3.FC28	-	High
Preventative (coso) Protect (NIST CSF)	[S3.C112, depends on S3.C104] Block any <a href="#">object-related operations</a> access to S3 buckets not through an access point (i.e., IAM policy, SCP, their bucket policy, or centrally in an RCP applied to the OU or AWS account, with a deny statement on the condition "ArnNotLike": {"s3:DataAccessPointArn": "arn:aws:s3:Region:AccountId:accesspoint/*"}).	Access any S3 bucket without using an access point; it should be denied.	Low	S3.FC1 S3.FC5	S3.T7 (Medium) S3.T11 (High)	High
Directive (coso) Identify (NIST CSF)	[S3.C141] Maintain a list of authorized buckets to be configured as an S3 website endpoint.	Request the list of authorized buckets to be configured as a website endpoint, its review process, and its review records.	Low	S3.FC16	S3.T13 (Very Low) S3.T29 (Very Low)	High
Directive (coso) Protect (NIST CSF)	[S3.C144, depends on S3.C141] Ensure S3 website endpoints are protected with HTTP headers ( <a href="#">ref</a> ) using a CDN (e.g., CloudFront).	Request the mechanism ensuring S3 website endpoints are protected with HTTP headers.	Medium	S3.FC16	S3.T13 (High) S3.T29 (Very High)	High
Directive (coso) Identify (NIST CSF)	[S3.C101] Maintain a list of authorized CloudFront distributions (via Origin Access Control) and associated bucket, access point, and/or Object Lambda Access Point.	Request the list of all authorized CloudFront distributions and associated S3 buckets, access points, and/or Object Lambda Access Points.	Low	S3.FC10	S3.T20 (Very Low)	Medium
Assurance (coso) Detect (NIST CSF)	[S3.C102] Verify all associations of CloudFront distributions with buckets, access points, and/or Object Lambda Access Points are authorized (e.g., using the Macie finding: "Policy:IAMUser/S3BucketSharedWithCloudFront").	Create a non-authorized distribution or association; it should be detected.	High	S3.FC10	-	Medium
Directive (coso) Protect (NIST CSF)	[S3.C137, depends on S3.C101, assured by S3.C102] Ensure only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa (e.g., using their bucket policy, centrally in an RCP applied to the OU or AWS account, with a deny statement, access point policy, resource policy for an Object Lambda Access Point, limiting the access to only the authorized distribution(s) in the SourceArn).	Request 1) the mechanism ensuring only authorized CloudFront distributions are associated with their authorized bucket, access point, and/or Object Lambda Access Point; and vice versa, 2) its records of execution for all new CloudFront distributions, and 3) the plan to move any older CloudFront distributions.	Medium	S3.FC10	S3.T20 (High)	Medium
Directive (coso) Protect (NIST CSF)	[S3.C142, depends on S3.C141, assured by S3.C143] Ensure only authorized buckets are configured as an S3 website endpoint.	Request 1) the mechanism ensuring only authorized buckets are configured as S3 website endpoints, 2) its records of execution for all new website-enabled buckets, and 3) the	Medium	S3.FC16	S3.T13 (Medium) S3.T29 (Medium)	Medium

		plan to move any older website-enabled buckets.				
Assurance (COSO) Detect (NIST CSF)	[S3.C143] Verify only authorized buckets are configured as S3 website endpoints.	Enable static website hosting on an unauthorized bucket; it should be detected.	Medium	S3.FC16	-	Medium