CIS Oracle Cloud Infrastructure Foundations Benchmark

v2.0.0 - 12-29-2023

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document, CIS Oracle Cloud Infrastructure Foundations Benchmark, provides prescriptive guidance for establishing a secure baseline configuration for the Oracle Cloud Infrastructure environment. The scope of this benchmark is to establish a base level of security for anyone utilizing the included Oracle Cloud Infrastructure services. The benchmark is, however, not an exhaustive list of all possible security configurations and architecture. You should take the benchmark as a starting point and do the required site-specific tailoring wherever needed and when it is prudent to do so.
The Compliance Checking script available in the CIS OCI Landing Zone Quick Start (https://github.com/oracle-quickstart/oci-cis-landingzone-quickstart) repository checks a tenancy's configuration against the CIS OCI Foundations Benchmark. To learn more, please visit https://github.com/oracle-quickstart/oci-cis-landingzone-quickstart/blob/main/compliance-script.md.
Recommendation compliance can, in many cases, also be audited using REST API. More information about using REST API can be found here: https://docs.oracle.com/en/cloud/saas/enterprise-data-management-cloud/edmra/edmcs_accessing_rest_apis.html
To obtain the latest version of this guide, please visit https://www.cisecurity.org/cis-benchmarks/. If you have questions, comments, or have identified ways to improve this guide, please write us at benchmarkinfo@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions in the Oracle Cloud Infrastructure.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile are intend to:

  - be practical and prudent;
  - provide security focused best practice hardening of a technology; and
  - limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is more critical than manageability and usability
  - acts as defense in depth measure
  - may impact the utility or performance of the technology
  - may include additional licensing, cost, or addition of third party software

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Recommendations

1 Identity and Access Management

This section contains recommendations for configuring identity and access management related options.

1.1 Ensure service level admins are created to manage resources of particular service (Manual)

Profile Applicability:

- Level 1

Description:

To apply least-privilege security principle, one can create service-level administrators in corresponding groups and assigning specific users to each service-level administrative group in a tenancy. This limits administrative access in a tenancy.

It means service-level administrators can only manage resources of a specific service.

Example policies for global/tenant level service-administrators

```
Allow group VolumeAdmins to manage volume-family in tenancy
Allow group ComputeAdmins to manage instance-family in tenancy
Allow group NetworkAdmins to manage virtual-network-family in tenancy
A tenancy with identity domains : An Identity Domain is a container of users,
groups, Apps and other security configurations. A tenancy that has Identity
Domains available comes seeded with a 'Default' identity domain.

If a group belongs to a domain different than the default domain, use a
domain prefix in the policy statements.
Example -
Allow group <identity_domain_name>/<group_name> to <verb> <resource-type> in
compartment <compartment_name>

If you do not include the <identity_domain_name> before the <group_name>,
then the policy statement is evaluated as though the group belongs to the
default identity domain.
```

Organizations have various ways of defining service-administrators. Some may prefer creating service administrators at a tenant level and some per department or per project or even per application environment (dev/test/production etc.). Either approach works so long as the policies are written to limit access given to the service-administrators.

Example policies for compartment level service-administrators

```
Allow group NonProdComputeAdmins to manage instance-family in compartment dev
Allow group ProdComputeAdmins to manage instance-family in compartment
production
Allow group A-Admins to manage instance-family in compartment Project-A
Allow group A-Admins to manage volume-family in compartment Project-A
A tenancy with identity domains : An Identity Domain is a container of users,
groups, Apps and other security configurations. A tenancy that has Identity
Domains available comes seeded with a 'Default' identity domain.

If a group belongs to a domain different than the default domain, use a
domain prefix in the policy statements.
Example -
Allow group <identity_domain_name>/<group_name> to <verb> <resource-type> in
compartment <compartment_name>

If you do not include the <identity_domain_name> before the <group_name>,
then the policy statement is evaluated as though the group belongs to the
default identity domain.
```

Rationale:

Creating service-level administrators helps in tightly controlling access to Oracle Cloud Infrastructure (OCI) services to implement the least-privileged security principle.

Audit:

From CLI:

1. Set up OCI CLI with an IAM administrator user who has read access to IAM resources such as groups and policies.
2. Run OCI CLI command providing the root_compartment_OCID
   Get the list of groups in a tenancy

```
oci iam group list --compartment-id <root_compartment_OCID> | grep name
A tenancy with identity domains : The above CLI commands work with the
default identity domain only.
For IaaS resource management, users and groups created in the default domain
are sufficient.
```

3. Ensure distinct administrative groups are created as per your organization's definition of service-administrators.
4. Verify the appropriate policies are created for the service-administrators groups to have the right access to the corresponding services. Retrieve the policy statements scoped at the tenancy level and/or per compartment.

```
oci iam policy list --compartment-id <root_compartment_OCID> | grep "in
tenancy"

oci iam policy list --compartment-id <root_compartment_OCID> | grep "in
compartment"
```

The --compartment-id parameter can be changed to a child compartment to get policies associated with child compartments.

```
oci iam policy list --compartment-id <child_compartment_OCID> | grep "in
compartment"
```

Verify the results to ensure the right policies are created for service-administrators to have the necessary access.

Remediation:

Refer to the policy syntax document and create new policies if the audit results indicate that the required policies are missing.
This can be done via OCI console or OCI CLI/SDK or API.
Creating a new policy:
From CLI:

```
oci iam policy create [OPTIONS]
```

Creates a new policy in the specified compartment (either the tenancy or another of your compartments). If you're new to policies, see
Getting Started with Policies
You must specify a name for the policy, which must be unique across all policies in your tenancy and cannot be changed.
You must also specify a description for the policy (although it can be an empty string). It does not have to be unique, and you can change it anytime with UpdatePolicy.
You must specify one or more policy statements in the statements array.
For information about writing policies, see How Policies Work and Common Policies.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.8 Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	**4.3 Ensure the Use of Dedicated Administrative Accounts** Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.2 Ensure permissions on all resources are given only to the tenancy administrator group (Automated)

Profile Applicability:

- Level 1

Description:

There is a built-in OCI IAM policy enabling the Administrators group to perform any action within a tenancy. In the OCI IAM console, this policy reads:

```
Allow group Administrators to manage all-resources in tenancy
```

Administrators create more users, groups, and policies to provide appropriate access to other groups.

Administrators should not allow any-other-group full access to the tenancy by writing a policy like this -

```
Allow group any-other-group to manage all-resources in tenancy
```

The access should be narrowed down to ensure the least-privileged principle is applied.

Rationale:

Permission to manage all resources in a tenancy should be limited to a small number of users in the `Administrators` group for break-glass situations and to set up users/groups/policies when a tenancy is created.

No group other than `Administrators` in a tenancy should need access to all resources in a tenancy, as this violates the enforcement of the least privilege principle.

Audit:

From CLI:

1. Run OCI CLI command providing the root compartment OCID to get the list of groups having access to manage all resources in your tenancy.

```
oci iam policy list --compartment-id <root_compartment_OCID> | grep -i "to
manage all-resources in tenancy"
```

2. Verify the results to ensure only the `Administrators` group has access to manage all resources in tenancy.

"Allow group Administrators to manage all-resources in tenancy"

Remediation:

From Console:

1. Login to OCI console.
2. Go to `Identity` -> `Policies`, In the compartment dropdown, choose the root compartment. Open each policy to view the policy statements.
3. Remove any policy statement that allows any group other than `Administrators` or any service access to manage all resources in the tenancy.

From CLI:
The policies can also be updated via OCI CLI, SDK and API, with an example of the CLI commands below:

- Delete a policy via the CLI:
  ```
  oci iam policy delete --policy-id <policy-ocid>
  ```
- Update a policy via the CLI:
  ```
  oci iam policy update --policy-id <policy-ocid> --statements <json-
  array-of-statements>
  ```

Note: You should generally **not** delete the policy that allows the `Administrators` group the ability to manage all resources in the tenancy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.3 Ensure IAM administrators cannot update tenancy Administrators group (Automated)

Profile Applicability:

- Level 1

Description:

Tenancy administrators can create more users, groups, and policies to provide other service administrators access to OCI resources.

For example, an IAM administrator will need to have access to manage resources like compartments, users, groups, dynamic-groups, policies, identity-providers, tenancy tag-namespaces, tag-definitions in the tenancy.

The policy that gives IAM-Administrators or any other group full access to 'groups' resources should not allow access to the tenancy 'Administrators' group.

The policy statements would look like -

```
Allow group IAMAdmins to inspect users in tenancy
Allow group IAMAdmins to use users in tenancy where target.group.name !=
'Administrators'
Allow group IAMAdmins to inspect groups in tenancy
Allow group IAMAdmins to use groups in tenancy where target.group.name !=
'Administrators'
```

Note: You must include separate statements for 'inspect' access, because the target.group.name variable is not used by the ListUsers and ListGroups operations

Rationale:

These policy statements ensure that no other group can manage tenancy administrator users or the membership to the 'Administrators' group thereby gain or remove tenancy administrator access.

Audit:

From CLI:

1. Run the following OCI CLI commands providing the root_compartment_OCID

```
oci iam policy list --compartment-id <root_compartment_OCID> | grep -i " to
use users in tenancy"
oci iam policy list --compartment-id <root_compartment_OCID> | grep -i " to
use groups in tenancy"
```

2. Verify the results to ensure that the policy statements that grant access to use or manage users or groups in the tenancy have a condition that excludes access to `Administrators` group or to users in the Administrators group.

Remediation:

From Console:

1. Login to OCI Console.
2. Select `Identity` from Services Menu.
3. Select `Policies` from Identity Menu.
4. Click on an individual policy under the Name heading.
5. Ensure Policy statements look like this -

```
Allow group IAMAdmins to use users in tenancy where target.group.name !=
'Administrators'
Allow group IAMAdmins to use groups in tenancy where target.group.name !=
'Administrators'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	**5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	**3.3 Protect Dedicated Assessment Accounts** Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●
v7	**4.1 Maintain Inventory of Administrative Accounts** Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.4 Ensure IAM password policy requires minimum length of 14 or greater (Automated)

Profile Applicability:

- Level 1

Description:

Password policies are used to enforce password complexity requirements. IAM password policies can be used to ensure passwords are at least a certain length and are composed of certain characters.

It is recommended the password policy require a minimum password length 14 characters and contain 1 non-alphabetic character (Number or "Special Character").

Rationale:

In keeping with the overall goal of having users create a password that is not overly weak, an eight-character minimum password length is recommended for an MFA account, and 14 characters for a password only account. In addition, maximum password length should be made as long as possible based on system/software capabilities and not restricted by policy.

In general, it is true that longer passwords are better (harder to crack), but it is also true that forced password length requirements can cause user behavior that is predictable and undesirable. For example, requiring users to have a minimum 16-character password may cause them to choose repeating patterns like fourfourfourfour or passwordpassword that meet the requirement but aren't hard to guess. Additionally, length requirements increase the chances that users will adopt other insecure practices, like writing them down, re-using them or storing them unencrypted in their documents.

Password composition requirements are a poor defense against guessing attacks. Forcing users to choose some combination of upper-case, lower-case, numbers, and special characters has a negative impact. It places an extra burden on users and many will use predictable patterns (for example, a capital letter in the first position, followed by lowercase letters, then one or two numbers, and a "special character" at the end). Attackers know this, so dictionary attacks will often contain these common patterns and use the most common substitutions like, $ for s, @ for a, 1 for l, 0 for o.

Passwords that are too complex in nature make it harder for users to remember, leading to bad practices. In addition, composition requirements provide no defense against common attack types such as social engineering or insecure storage of passwords.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login to the OCI Console
2. Go to `Identity` in the Services menu.
3. Select `Authentication Settings` from the Identity menu.
4. Click `Edit` in the middle of the page.
5. Ensure the number `14` is entered into the box below the text: `MINIMUM PASSWORD LENGTH (IN CHARACTERS)`.
6. Ensure that one (1) of the checkboxes is selected for `MUST CONTAIN AT LEAST 1 SPECIAL CHARACTER` OR `MUST CONTAIN AT LEAST 1 NUMERIC CHARACTER`

From CLI:
Run the following command

```
oci iam authentication-policy get --compartment-id --query 'data."password-policy"."minimum-password-length"'
```

Result should return a value of 14 or greater

OCI IAM without Identity Domains - Identity Cloud Service (IDCS)

If you use IDCS to login to OCI, verify the password policy settings in IDCS

1. Login to IDCS Admin Console
2. Expand the Navigation Drawer, click `Settings`, and then click `Password Policy`.
3. Verify the `Password length min size` setting.
4. Under The `password must contain these characters` section, ensure that the number given in `Numeric min` setting is `1`, or the `Special min` setting is `1`.

OCI IAM with Identity Domains

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the `Compartment` your Domain to review is in
3. Click on the Domain to review
4. Click on `Settings`
5. Click on `Password policy`
6. Click each Password policy in the domain
7. Ensure `Password length (minimum)` is greater than or equal to 14
8. Under The `The following criteria apply to passwords` section, ensure that the number given in `Numeric (minimum)` setting is `1`, or the `Special (minimum)` setting is `1`.

The following criteria apply to passwords:
6. Ensure that 1 or more is selected for `Numeric (minimum)` OR `Special (minimum)`

From Cloud Guard:

To Enable Cloud Guard Auditing:

Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in "Ensure Cloud Guard is enabled in the root compartment of the tenancy" Recommendation in the "Logging and Monitoring" section.

From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find Password policy does not meet complexity requirements in the Detector Rules column.
6. Select the vertical ellipsis icon and chose `Edit` on the Password policy does not meet complexity requirements row.
7. In the Edit Detector Rule window, find the Input Setting box and verify/change the Required password length setting to 14.
8. Click the `Save` button.

From CLI:

1. Update the Password policy does not meet complexity requirements Detector Rule in Cloud Guard to generate Problems if IAM password policy isn't configured to enforce a password length of at least 14 characters with the following command:

```
oci cloud-guard detector-recipe-detector-rule update --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id PASSWORD_POLICY_NOT_COMPLEX
--details '{"configurations":[{ "configKey" : "passwordPolicyMinLength",
"name" : "Required password length", "value" : "14", "dataType" : null,
"values" : null }]}'
```

Remediation:

OCI IAM without Identity Domains

From Console:

1. Login to the OCI Console
2. Go to `Identity` in the Services menu.
3. Select `Authentication Settings` from the Identity menu.
4. Click `Edit` in the middle of the page.

5. Type the number `14` into the box below the text: `MINIMUM PASSWORD LENGTH (IN CHARACTERS)`.
6. Select checkbox next to `MUST CONTAIN AT LEAST 1 SPECIAL CHARACTER` **OR** `MUST CONTAIN AT LEAST 1 NUMERIC CHARACTER`

OCI IAM without Identity Domains - Identity Cloud Service (IDCS)

1. Login to IDCS Admin Console
2. Expand the Navigation Drawer, click `Settings`, and then click `Password Policy`.
3. Click on `Change Your Password Policy` button.
4. Update the `Password length min size` setting to 14 or greater
5. Click `Save`.
6. Under The `password must contain these characters` section, update the number given in `Special min` setting to `1`

or
Under The `password must contain these characters` section, update the number given in `Numeric min` setting to `1`

7. Click `Save`

OCI IAM with Identity Domains

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the Compartment the Domain to remediate is in
3. Click on the Domain to remediate
4. Click on Settings
5. Click on Password policy to remediate
6. Click Edit password rules
7. Update the `Password length (minimum)` setting to 14 or greater
8. Under The `Passwords must meet the following character requirements` section, update the number given in `Special (minimum)` setting to `1` or greater

or
Under The `Passwords must meet the following character requirements` section, update the number given in `Numeric (minimum)` setting to `1` or greater
7. Click `Save changes`

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 <u>Establish and Maintain a Secure Configuration Process</u>** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**5.2 <u>Use Unique Passwords</u>** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4 <u>Use Unique Passwords</u>** Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	**5.1 <u>Establish Secure Configurations</u>** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5 Ensure IAM password policy expires passwords within 365 days (Manual)

Profile Applicability:

- Level 1

Description:

IAM password policies can require passwords to be rotated or expired after a given number of days. It is recommended that the password policy expire passwords after 365 and are changed immediately based on events.

Rationale:

Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other.10 In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password for example). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead, immediate password changes should be based on key events including, but not limited to:

1. Indication of compromise
2. Change of user roles
3. When a user leaves the organization.

Not only does changing passwords every few weeks or months frustrate the user, it's been suggested that it does more harm than good, because it could lead to bad practices by the user such as adding a character to the end of their existing password.

In addition, we also recommend a yearly password change. This is primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

Audit:

OCI IAM without Identity Domains - Identity Cloud Service (IDCS)

1. Login to IDCS Admin Console
2. Expand the Navigation Drawer, click `Settings`, and then click `Password Policy`.
3. Ensure that the number of days configured in `Expires after` setting is 365.

OCI IAM with Identity Domains

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the `Compartment` your Domain to review is in
3. Click on the Domain to review
4. Click on `Settings`
5. Click on `Password policy`
6. Click each Password policy in the domain
7. Ensure `Expires after (days)` is less than or equal to 365 days

Remediation:

OCI IAM without Identity Domains - Identity Cloud Service (IDCS)

1. Login to IDCS Admin Console
2. Expand the Navigation Drawer, click `Settings`, and then click `Password Policy`.
3. Click on `Change Your Password Policy` button.
4. Update the number of days configured in `Expires after` setting to 365.

OCI IAM with Identity Domains

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the `Compartment` the Domain to remediate is in
3. Click on the Domain to remediate
4. Click on `Settings`
5. Click on `Password policy` to remediate
6. Click `Edit password rules`
7. Change `Expires after (days)` to 365

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2** <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4** <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	**5.1** <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6 Ensure IAM password policy prevents password reuse (Manual)

Profile Applicability:

- Level 1

Description:

IAM password policies can prevent the reuse of a given password by the same user. It is recommended the password policy prevent the reuse of passwords.

Rationale:

Enforcing password history ensures that passwords are not reused in for a certain period of time by the same user. If a user is not allowed to use last 24 passwords, that window of time is greater. This helps maintain the effectiveness of password security.

Audit:

OCI IAM without Identity Domains - Identity Cloud Service (IDCS)

1. Login to IDCS Admin Console
2. Expand the Navigation Drawer, click `Settings`, and then click `Password Policy`.
3. Ensure that the number of remembered passwords in `Previous passwords remembered` setting is set to 24 or greater.

OCI IAM with Identity Domains

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the `Compartment` your Domain to review is in
3. Click on the Domain to review
4. Click on `Settings`
5. Click on `Password policy`
6. Click each Password policy in the domain
7. Ensure `Previous passwords remembered` is set 24 or greater

Remediation:

OCI IAM without Identity Domains - Identity Cloud Service (IDCS)

1. Login to IDCS Admin Console
2. Expand the Navigation Drawer, click `Settings`, and then click `Password Policy`.
3. Click on "Change Your Password Policy" button.
4. Update the number of remembered passwords in `Previous passwords remembered` setting to 24 or greater.

OCI IAM with Identity Domains

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the Compartment the Domain to remediate is in
3. Click on the Domain to remediate
4. Click on Settings
5. Click on Password policy to remediate
6. Click Edit password rules
7. Update the number of remembered passwords in `Previous passwords remembered` setting to 24 or greater.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4 Use Unique Passwords** Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

1.7 Ensure MFA is enabled for all users with a console password (Automated)

Profile Applicability:

- Level 1

Description:

Multi-factor authentication is a method of authentication that requires the use of more than one factor to verify a user's identity.

With MFA enabled in the IAM service, when a user signs in to Oracle Cloud Infrastructure, they are prompted for their user name and password, which is the first factor (something that they know). The user is then prompted to provide a verification code from a registered MFA device, which is the second factor (something that they have). The two factors work together, requiring an extra layer of security to verify the user's identity and complete the sign-in process.

OCI IAM supports two-factor authentication using a password (first factor) and a device that can generate a time-based one-time password (TOTP) (second factor).

See [OCI documentation](#) for more details.

Rationale:

Multi factor authentication adds an extra layer of security during the login process and makes it harder for unauthorized users to gain access to OCI resources.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login into OCI Console.
2. Select `Identity & Security` from Services menu
3. Select Users from Identity menu.
4. Click on an individual user.
5. Ensure the word Enabled is next to Multi-factor authentication.

From CLI:

1. Set up the OCI CLI with an IAM administrator user who has access to read IAM policies.
2. Run OCI CLI command providing the root compartment OCID

```
oci iam  user list --query 'data[].["id","name","is-mfa-activated", "can-use-
console-password"]' --output table
```

3. Verify that the values in Column3 are not `false`

From Cloud Guard:

To Enable Cloud Guard Auditing:

Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.

From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console
2. Click `Cloud Guard` from the "Services" submenu
3. Click `Detector Recipes` in the Cloud Guard menu
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column
5. Find User does not have MFA enabled in the Detector Rules column
6. Verify that the User does not have MFA enabled Detector Rule is Enabled

From CLI:

1. Verify that the User does not have MFA enabled Detector Rule in Cloud Guard is enabled to generate Problems if multifactor authentication is not required each time a user logs into Oracle Cloud Infrastructure with the following command:

```
oci cloud-guard detector-recipe-detector-rule get --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id NO_MFA_ENABLED_FOR_USER
```

OCI IAM with Identity Domains

From Console:

1. Go to Identity Domains: https://cloud.oracle.com/identity/domains/
2. Select the `Compartment` your Domain to review is in
3. Click on the Domain to review
4. Click on `Security`
5. Click `Sign-on policies`
6. Select the sign-on policy to review
7. Under the sign-on rules header, click the three dots on the rule with the highest priority.
8. Select `Edit sign-on rule`
9. Verify that `allow access` is selected and `prompt for an additional factor` is enabled

- This requires users to enable MFA when they next login next however, to determine users have enabled MFA use the below CLI.

From the CLI:

- This CLI command checks which users have enabled MFA for their accounts

1. Execute the below:

```
tenancy_ocid=`oci iam compartment list --raw-output --query
"data[?contains(\"compartment-id\",'.tenancy.')].\"compartment-id\" | [0]"`
for id_domain_url in `oci iam domain list --compartment-id $tenancy_ocid --
all | jq -r '.data[] | .url'`
do
   oci identity-domains users list --endpoint $id_domain_url 2>/dev/null |
jq -r '.data.resources[] | select(."urn-ietf-params-scim-schemas-oracle-idcs-
extension-mfa-user"."mfa-status"!="ENROLLED")' 2>/dev/null | jq -r '.ocid'

done
for region in `oci iam region-subscription list | jq -r '.data[] | ."region-
name"'`;
   do
      for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE --all 2>/dev/null | jq -r '.data[] | .id'`
        do
           for id_domain_url in `oci iam domain list --compartment-id
$compid --region $region --all 2>/dev/null | jq -r '.data[] | .url'`
           do
              oci identity-domains users list --endpoint $id_domain_url
2>/dev/null | jq -r '.data.resources[] | select(."urn-ietf-params-scim-
schemas-oracle-idcs-extension-mfa-user"."mfa-status"!="ENROLLED")'
2>/dev/null | jq -r '.ocid'
           done
        done
   done
```

2. Ensure no results are returned

Remediation:

OCI IAM without Identity Domains

Each user must enable MFA for themselves using a device they will have access to every time they sign in. An administrator cannot enable MFA for another user but can enforce MFA by identifying the list of non-complaint users, notifying them or disabling access by resetting the password for non-complaint accounts.
Disabling access from Console:

1. Go to https://cloud.oracle.com/identity/.
2. Select Users from Identity menu.
3. Click on each non-complaint user.

4. Click on `Create/Reset Password`.

From CLI:
```
oci iam user ui-password create-or-reset --user-id <OCID of the non-compliant
user>
```

OCI IAM with Identity Domains

Each user must enable MFA for themselves using a device they will have access to every time they sign in. An administrator cannot enable MFA for another user but can enforce MFA by identifying the list of non-complaint users, notifying them or disabling access by resetting the password for non-complaint accounts.

Disabling access from Console:

1. Go to https://cloud.oracle.com/identity/.
2. Select `Domains` from Identity menu.
3. Select the domain
4. Click `Security`
5. Click `Sign-on polices` then the "`Default Sign-on Policy`"
6. Under the sign-on rules header, click the three dots on the rule with the highest priority.
7. Select `Edit sign-on rule`
8. Make a change to ensure that `allow access` is selected and `prompt for an additional factor` is enabled

References:

1. https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/usingmfa.htm
2. https://docs.oracle.com/en-us/iaas/Content/Security/Reference/iam_security_topic-IAM_MFA.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.3 Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	**6.5 Require MFA for Administrative Access** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

1.8 Ensure user API keys rotate within 90 days (Automated)

Profile Applicability:

- Level 1

Description:

API keys are used by administrators, developers, services and scripts for accessing OCI APIs directly or via SDKs/OCI CLI to search, create, update or delete OCI resources.

The API key is an RSA key pair. The private key is used for signing the API requests and the public key is associated with a local or synchronized user's profile.

Rationale:

It is important to secure and rotate an API key every 90 days or less as it provides the same level of access that a user it is associated with has.

In addition to a security engineering best practice, this is also a compliance requirement. For example, PCI-DSS Section 3.6.4 states, "Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined crypto period(s)."

Audit:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `API Keys` in the lower left-hand corner of the page.
6. Ensure the date of the API key under the Created column of the API Key is no more than 90 days old.

From CLI:
```
oci iam user api-key list --user-id <user_ocid> --query data[*].[\"time-created\",\"fingerprint\"]
```

Cloud Guard
To Enable Cloud Guard Auditing:
Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.
From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find API key is too old in the Detector Rules column.
6. Select the vertical ellipsis icon and choose Edit on the API key is too old row.
7. In the Edit Detector Rule window find the Input Setting box and verify/change the Days setting to 90.
8. Click the Save button.

From CLI:

1. Update the API key is too old Detector Rule in Cloud Guard to generate Problems if the IAM password policy isn't configured to expire API keys after 90 days.

```
oci cloud-guard detector-recipe-detector-rule update --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id API_KEY_TOO_OLD --details
'{"configurations":[{ "configKey" : "apiKeyTooOldConfig", "name" : "Days",
"value" : "90", "dataType" : null, "values" : null }]}'
```

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Domains` from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the Name heading.
6. Click on `API Keys` in the lower left-hand corner of the page.
7. Ensure the date of the API key under the `Created` column of the API Key is no more than 90 days old.

Remediation:

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Domains` from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the Name heading.
6. Click on `API Keys` in the lower left-hand corner of the page.
7. Delete any API Keys that are older than 90 days under the `Created` column of the API Key table.

From CLI:

```
oci iam user api-key delete --user-id _<user_ocid>_ --fingerprint
<fingerprint_of_the_key_to_be_deleted>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**4.4 Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.9 Ensure user customer secret keys rotate every 90 days (Automated)

Profile Applicability:

- Level 1

Description:

Object Storage provides an API to enable interoperability with Amazon S3. To use this Amazon S3 Compatibility API, you need to generate the signing key required to authenticate with Amazon S3.

This special signing key is an Access Key/Secret Key pair. Oracle generates the Customer Secret key to pair with the Access Key.

Rationale:

It is important to rotate customer secret keys at least every 90 days, as they provide the same level of object storage access that the user they are associated with has.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `Customer Secret Keys` in the lower left-hand corner of the page.
6. Ensure the date of the Customer Secret Key under the `Created` column of the Customer Secret Key is no more than 90 days old.

From CLI:

1. Execute the following:

```
oci iam customer-secret-key list --user-id <user-ocid> --output table --query
"data [*].{description:description, Created:\"time-created\",id:id}"
```

2. Ensure the date in the column name Created is no more than 90 days.

OCI IAM with Identity Domains

** From Console: **

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Click on `Customer Secret Keys` in the lower left-hand corner of the page.
7. Ensure the date of the Customer Secret Key under the `Created` column of the Customer Secret Key is no more than 90 days old.

Remediation:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `Customer Secret Keys` in the lower left-hand corner of the page.
6. Delete any Access Keys with a date older than 90 days under the `Created` column of the Customer Secret Keys.

From CLI:

1. Execute the following:

```
oci iam customer-secret-key delete --user-id <user_OCID> --customer-secret-key-id <id from above>
```

2. You will then be prompted with the below:

```
Are you sure you want to delete this resource? [y/N]
```

3. Type 'y' and press 'Enter'

OCI IAM with Identity Domains

** From Console: **

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Click on `Customer Secret Keys` in the lower left-hand corner of the page.
7. Delete any Access Keys with a date older than 90 days under the `Created` column of the Customer Secret Keys.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4 Use Unique Passwords** Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.10 Ensure user auth tokens rotate within 90 days or less (Automated)

Profile Applicability:

- Level 1

Description:

Auth tokens are authentication tokens generated by Oracle. You use auth tokens to authenticate with APIs that do not support the Oracle Cloud Infrastructure signature-based authentication. If the service requires an auth token, the service-specific documentation instructs you to generate one and how to use it.

Rationale:

It is important to secure and rotate an auth token every 90 days or less as it provides the same level of access to APIs that do not support the OCI signature-based authentication as the user associated to it.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `Auth Tokens` in the lower left-hand corner of the page.
6. Ensure the date of the Auth Token under the `Created` column of the Auth Token is no more than 90 days old.

From CLI:

1. Execute the following:

```
oci iam auth-token list --user-id <user-ocid> --output table --query "data
[*].{description:description, Created:\"time-created\",id:id}"
```

2. Ensure the date in the column name Created is no more than 90 days.

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Click on `Auth Tokens` in the lower left-hand corner of the page.
7. Ensure the date of the Auth Token under the `Created` column of the Customer Secret Key is no more than 90 days old.

Remediation:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `Auth Tokens` in the lower left-hand corner of the page.
6. Delete any auth token with a date of 90 days or older under the `Created` column of the Auth Tokens.

From CLI:

1. Execute the following:

```
oci iam auth-token delete --user-id <user_OCID> --auth-token-id <id from above>
```

2. You will then be prompted with the below:

```
Are you sure you want to delete this resource? [y/N]
```

3. Type 'y' and press 'Enter'

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Click on `Auth Tokens` in the lower left-hand corner of the page.
7. Delete any auth token with a date older than 90 days under the `Created` column of the Customer Secret Keys.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.11 Ensure user IAM Database Passwords rotate within 90 days (Manual)

Profile Applicability:

- Level 1

Description:

Users can create and manage their database password in their IAM user profile and use that password to authenticate to databases in their tenancy. An IAM database password is a different password than an OCI Console password. Setting an IAM database password allows an authorized IAM user to sign in to one or more Autonomous Databases in their tenancy.

An IAM database password is a different password than an OCI Console password. Setting an IAM database password allows an authorized IAM user to sign in to one or more Autonomous Databases in their tenancy.

Rationale:

It is important to secure and rotate an IAM Database password 90 days or less as it provides the same access the user would have a using a local database user.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `Database Passwords` in the lower left-hand corner of the page.
6. Ensure the date of the Database Passwords under the `Created` column of the Database Passwords is no more than 90 days old.

From CLI:

1. Execute the following:

```
oci iam user list-db-credentials --user-id <user-ocid> --output table --query
"data [*].{description:description, Created:\"time-created\",id:id}"
```

2. Ensure the date in the column name Created is no more than 90 days.

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Click on `Database Passwords` in the lower left-hand corner of the page.
7. Ensure the date of the Database Passwords under the `Created` column of the Database Password is no more than 90 days old.

Remediation:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity` from the Services menu.
3. Select `Users` from the Identity menu.
4. Click on an individual user under the Name heading.
5. Click on `IAM Database Passwords` in the lower left-hand corner of the page.
6. Delete any Database Passwords with a date older than 90 days under the `Created` column of the IAM Database Passwords.

From CLI:

1. Execute the following:

```
oci iam <db-credentials> delete --user-id <user_OCID> --customer-secret-key-
id <id from above>
```

2. You will then be prompted with the below:

```
Are you sure you want to delete this resource? [y/N]
```

3. Type 'y' and press 'Enter'

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.

4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Click on `IAM Database Passwords` in the lower left-hand corner of the page.
7. Delete any Database Passwords with a date older than 90 days under the `Created` column of the Database Passwords.

References:

1. https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/usercredentials.htm#usercredentials_iam_db_pwd

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

1.12 Ensure API keys are not created for tenancy administrator users (Automated)

Profile Applicability:

- Level 1

Description:

Tenancy administrator users have full access to the organization's OCI tenancy. API keys associated with user accounts are used for invoking the OCI APIs via custom programs or clients like CLI/SDKs. The clients are typically used for performing day-to-day operations and should never require full tenancy access. Service-level administrative users with API keys should be used instead.

Rationale:

For performing day-to-day operations tenancy administrator access is not needed. Service-level administrative users with API keys should be used to apply privileged security principle.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login to OCI Console.
2. Verify user profile of each user who is member of the `Administrators` group directly or via federation group mapping.
3. Go to `Identity`-> `Users` and click on each local or synchronized `Administrators` member profile
4. Click on API Keys to verify if a user has an API key associated.

From CLI:

1. Locate the ID of the `Administrators` group:

```
oci iam group list --query "data[?name == 'Administrators'].[{id:"id"}]"
```

2. Locate the users in the group:

```
oci iam group list-users --group-id <group_id> --query "data[].["email",
"id"]"
```

3. For each user ID, check if the user has any API keys:

```
oci iam user api-key list --user-id <user_id>
```

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Domains` from the Identity menu.
4. Click on the 'Default' Domain in the (root).
5. Click on 'Groups'.
6. Select the 'Administrators' group by clicking on the Name
7. Click on each local or synchronized `Administrators` member profile
8. Click on API Keys to verify if a user has an API key associated.

Remediation:

From Console:

1. Login to OCI console.
2. Select `Identity` from Services menu.
3. Select `Users` from Identity menu, or select `Domains`, select a domain, and select `Users`.
4. Select the username of a tenancy administrator user with an API key.
5. Select `API Keys` from the menu in the lower left-hand corner.
6. Delete any associated keys from the `API Keys` table.
7. Repeat steps 3-6 for all tenancy administrator users with an API key.

From CLI:

1. For each tenancy administrator user with an API key, execute the following command to retrieve API key details:

```
oci iam user api-key list --user-id <user_id>
```

2. For each API key, execute the following command to delete the key:

```
oci iam user api-key delete --user-id <user_id> --fingerprint
<api_key_fingerprint>
```

3. The following message will be displayed:

```
Are you sure you want to delete this resource? [y/N]:
```

4. Type 'y' and press 'Enter'.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u>** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	**4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u>** Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.13 Ensure all OCI IAM user accounts have a valid and current email address (Manual)

Profile Applicability:

- Level 1

Description:

All OCI IAM local user accounts have an email address field associated with the account. It is recommended to specify an email address that is valid and current.

If you have an email address in your user profile, you can use the Forgot Password link on the sign on page to have a temporary password sent to you.

Rationale:

Having a valid and current email address associated with an OCI IAM local user account allows you to tie the account to identity in your organization. It also allows that user to reset their password if it is forgotten or lost.

Audit:

OCI IAM without Identity Domains

From Console:

1. Login into OCI Console.
2. Select `Identity & Security` from Services menu
3. Select `Users` from the Identity menu.
4. Click on an individual user.
5. Check if they are local OCI IAM local user account, the word `No` is next to Federated.
6. Ensure a valid and current email address is next to email.

From CLI:

1. Execute the following:

```
oci iam user list --output table --query "data [?\"external-
identifier\"==null].{Name:name,Email:email,OCID:id}"
```

2. Ensure that the column named Email has a valid and current email address.

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on an individual user under the `Username` heading.
6. Ensure a valid and current email address is next to Email and Recovery email.

Remediation:

OCI IAM without Identity Domains

From Console:

1. Login into OCI Console.
2. Select Identity from Services menu
3. Select Users from Identity menu.
4. Click on each non-complaint user.
5. Click on `Edit User`.
6. Enter a valid and current email address in the EMAIL text box.
7. Click `Save Changes`

From CLI:

1. Execute the following for each non-compliant user:

```
oci iam user update --user-id <user-ocid> --email '<email address>'
```

OCI IAM with Identity Domains

From Console:

1. Login to OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select Domains from the Identity menu.
4. For each domain listed, click on the name and select `Users`.
5. Click on each non-complaint user.
6. Click on `Edit User`.
7. Enter a valid and current email address in the Email and Recovery Email text boxes.
8. Click `Save Changes`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.1 <u>Establish and Maintain an Inventory of Accounts</u>** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	**16.6 <u>Maintain an Inventory of Accounts</u>** Maintain an inventory of all accounts organized by authentication system.		●	●

1.14 Ensure Instance Principal authentication is used for OCI instances, OCI Cloud Databases and OCI Functions to access OCI resources. (Manual)

Profile Applicability:

- Level 1

Description:

OCI instances, OCI database and OCI functions can access other OCI resources either via an OCI API key associated to a user or via Instance Principal. Instance Principal authentication can be achieved by inclusion in a Dynamic Group that has an IAM policy granting it the required access or using an OCI IAM policy that has `request.principal` added to the `where` clause. Access to OCI Resources refers to making API calls to another OCI resource like Object Storage, OCI Vaults, etc.

Rationale:

Instance Principal reduces the risks related to hard-coded credentials. Hard-coded API keys can be shared and require rotation, which can open them up to being compromised. Compromised credentials could allow access to OCI services outside of the expected radius.

Impact:

For an OCI instance that contains embedded credential audit the scripts and environment variables to ensure that none of them contain OCI API Keys or credentials.

Audit:

OCI IAM without Identity Domains

From Console (Dynamic Groups):

1. Go to https://cloud.oracle.com/identity/dynamicgroups
2. Click on a Dynamic Group.
3. Check if the Matching Rules includes the instances accessing your OCI resources.

From Console (request.principal):

1. Go to https://cloud.oracle.com/identity/policies
2. Select a Compartment
3. Click on an individual policy under the Name heading.
4. Ensure Policy statements look like this :

```
allow any-user to <verb> <resource> in compartment <compartment-name> where
ALL {request.principal.type='<resource_type>',
request.principal.id='<resource_ocid>'}
```

or

```
allow any-user to <verb> <resource> in compartment <compartment-name> where
ALL {request.principal.type='<resource_type>',
request.principal.compartment.id='<compartment_OCID>'}
```

From CLI (Dynamic Groups):

1. Execute the following:

```
oci iam dynamic-group list --output table --query
"data[*].{Name:name,\"Matching-Rule\":\"matching-rule\"}"
```

1. Ensure that the column named Matching-Rule has a matching rule that includes the instances accessing your OCI resources.

From CLI (request.principal):

1. Execute the following for each compartment_OCID:

```
oci iam policy list --compartment-id <compartment_OCID> | grep
request.principal
```

1. Ensure that the condition includes the instances accessing your OCI resources

OCI IAM with Identity Domains

From Console (Dynamic Groups):

1. Go to https://cloud.oracle.com/identity/domains/
2. Select a Compartment
3. Click on a Domain
4. Click on `Dynamic groups`
5. Click on the Dynamic Group
6. Check if the Matching Rules includes the instances accessing your OCI resources.

From Console (request.principal):

1. Go to https://cloud.oracle.com/identity/policies
2. Select a Compartment
3. Click on an individual policy under the Name heading.
4. Ensure Policy statements look like this :

```
allow any-user to <verb> <resource> in compartment <compartment-name> where
ALL {request.principal.type='<resource_type>',
request.principal.id='<resource_ocid>'}
```

or

```
allow any-user to <verb> <resource> in compartment <compartment-name> where
ALL {request.principal.type='<resource_type>',
request.principal.compartment.id='<compartment_OCID>'}
```

From CLI (request.principal):

1. Execute the following for each compartment_OCID:

```
oci iam policy list --compartment-id <compartment_OCID> | grep
request.principal
```

1. Ensure that the condition includes the instances accessing your OCI resources

Remediation:

OCI IAM without Identity Domains

From Console:

1. Go to https://cloud.oracle.com/identity/dynamicgroups
2. Select Dynamic Groups from Identity menu.
3. Click Create Dynamic Group.
4. Enter a Name
5. Enter a Description
6. Enter Matching Rules to that includes the instances accessing your OCI resources.
7. Click Create.

OCI IAM with Identity Domains

From Console (Dynamic Groups):

1. Go to https://cloud.oracle.com/identity/domains/
2. Select a Compartment
3. Click on the Domain
4. Click on `Dynamic groups`
5. Click Create Dynamic Group.
6. Enter a Name
7. Enter a Description
8. Enter Matching Rules to that includes the instances accessing your OCI resources.
9. Click Create.

References:

1. https://docs.oracle.com/en-
   us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.8 Define and Maintain Role-Based Access Control** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

1.15 Ensure storage service-level admins cannot delete resources they manage. (Manual)

Profile Applicability:

- Level 2

Description:

To apply the separation of duties security principle, one can restrict service-level administrators from being able to delete resources they are managing. It means service-level administrators can only manage resources of a specific service but not delete resources for that specific service.

Example policies for global/tenant level for block volume service-administrators:

```
Allow group VolumeUsers to manage volumes in tenancy where
request.permission!='VOLUME_DELETE'
Allow group VolumeUsers to manage volume-backups in tenancy where
request.permission!='VOLUME_BACKUP_DELETE'
```

Example policies for global/tenant level for file storage system service-administrators:

```
Allow group FileUsers to manage file-systems in tenancy where
request.permission!='FILE_SYSTEM_DELETE'
Allow group FileUsers to manage mount-targets in tenancy where
request.permission!='MOUNT_TARGET_DELETE'
Allow group FileUsers to manage export-sets in tenancy where
request.permission!='EXPORT_SET_DELETE'
```

Example policies for global/tenant level for object storage system service-administrators:

```
Allow group BucketUsers to manage objects in tenancy where
request.permission!='OBJECT_DELETE'
Allow group BucketUsers to manage buckets in tenancy where
request.permission!='BUCKET_DELETE'
```

Rationale:

Creating service-level administrators without the ability to delete the resource they are managing helps in tightly controlling access to Oracle Cloud Infrastructure (OCI) services by implementing the separation of duties security principle.

Audit:

From Console:

1. Login to OCI console.
2. Go to Identity -> Policies, In the compartment dropdown, choose the compartment.
3. Open each policy to view the policy statements.

4. Verify the policies to ensure that the policy statements that grant access to storage service-level administrators have a condition that excludes access to delete the service they are the administrator for.

From CLI:

1. Execute the following command:

```
for compid in `oci iam compartment list --compartment-id-in-subtree TRUE
2>/dev/null | jq -r '.data[] | .id'`
        do
            for policy in `oci iam policy list --compartment-id $compid
2>/dev/null | jq -r '.data[] | .id'`
                do
                output=`oci iam policy list --compartment-id $compid
2>/dev/null | jq -r '.data[] | .id, .name, .statements'`
                if [ ! -z "$output" ]; then echo $output; fi
                done
        done
```

2. Verify the policies to ensure that the policy statements that grant access to storage service-level administrators have a condition that excludes access to delete the service they are the administrator for.

Remediation:

From Console:

1. Login to OCI console.
2. Go to Identity -> Policies, In the compartment dropdown, choose the compartment. Open each policy to view the policy statements.
3. Add the appropriate `where` condition to any policy statement that allows the storage service-level to manage the storage service.

References:

1. https://docs.oracle.com/en/solutions/oci-best-practices/protect-data-rest1.html#GUID-939A5EA1-3057-48E0-9E02-ADAFCB82BA3E
2. https://docs.oracle.com/en-us/iaas/Content/Identity/policyreference/policyreference.htm
3. https://docs.oracle.com/en-us/iaas/Content/Block/home.htm
4. https://docs.oracle.com/en-us/iaas/Content/File/home.htm
5. https://docs.oracle.com/en-us/iaas/Content/Object/home.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2 Networking

This section contains recommendations for configuring network security related options.

2.1 Ensure no security lists allow ingress from 0.0.0.0/0 to port 22 (Automated)

Profile Applicability:

- Level 1

Description:

Security lists provide stateful and stateless filtering of ingress and egress network traffic to OCI resources on a subnet level. It is recommended that no security list allows unrestricted ingress access to port 22.

Rationale:

Removing unfettered connectivity to remote console services, such as Secure Shell (SSH), reduces a server's exposure to risk.

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to ports 22 and/or 3389 through another network security group or security list.

Audit:

From Console:

1. Login to the OCI Console.
2. Click the search bar at the top of the screen.
3. Type `Advanced Resource Query` and hit `enter`.
4. Click the `Advanced Resource Query` button in the upper right corner of the screen.
5. Enter the following query in the query box:

```
query SecurityList resources where
(IngressSecurityRules.source = '0.0.0.0/0' &&
IngressSecurityRules.protocol = 6 &&
IngressSecurityRules.tcpOptions.destinationPortRange.max >= 22 &&
IngressSecurityRules.tcpOptions.destinationPortRange.min =<= 22)
```

6. Ensure the query returns no results.

From CLI:

1. Execute the following command:

```
oci search resource structured-search --query-text "query SecurityList
resources where
(IngressSecurityRules.source = '0.0.0.0/0' &&
IngressSecurityRules.protocol = 6 &&
IngressSecurityRules.tcpOptions.destinationPortRange.max >= 22 &&
IngressSecurityRules.tcpOptions.destinationPortRange.min <= 22)
"
```

2. Ensure the query returns no results.

Cloud Guard
Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more
information about enabling Cloud Guard, please look at the instructions included in
Recommendation 3.15.
From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe
   Name column.
5. Find VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0)
   in the Detector Rules column.
6. Select the vertical ellipsis icon and chose Edit on the VCN Security list allows
   traffic to non-public port from all sources (0.0.0.0/0) row.
7. In the Edit Detector Rule window find the Input Setting box and verify/add to the
   Restricted Protocol: Ports List setting to TCP:[22], UDP:[22].
8. Click the `Save` button.

From CLI:

1. Update the VCN Security list allows traffic to non-public port from all sources
   (0.0.0.0/0) Detector Rule in Cloud Guard to generate Problems if a VCN security
   list allows public access via port 22 with the following command:

```
oci cloud-guard detector-recipe-detector-rule update --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id SECURITY_LISTS_OPEN_SOURCE -
-details '{"configurations":[{ "configKey" : "securityListsOpenSourceConfig",
"name" : "Restricted Protocol:Ports List", "value" : "TCP:[22], UDP:[22]",
"dataType" : null, "values" : null }]}'
```

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each security list in the returned results, click the security list name

3. Either edit the `ingress rule` to be more restrictive, delete the `ingress rule` or click on the `VCN` and terminate the `security list` as appropriate.

From CLI:

1. Follow the audit procedure.
2. For each of the `security lists` identified, execute the following command:

```
oci network security-list get --security-list-id <security list id>
```

3. Then either:

- Update the `security list` by copying the `ingress-security-rules` element from the JSON returned by the above command, edit it appropriately and use it in the following command:

```
oci network security-list update --security-list-id <security-list-id> --
ingress-security-rules '<ingress security rules JSON>'
```

or

- Delete the security list with the following command:

```
oci network security-list delete --security-list-id <security list id>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	12.3 <u>Securely Manage Network Infrastructure</u> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2 Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389 (Automated)

Profile Applicability:

- Level 1

Description:

Security lists provide stateful and stateless filtering of ingress and egress network traffic to OCI resources on a subnet level. It is recommended that no security group allows unrestricted ingress access to port 3389.

Rationale:

Removing unfettered connectivity to remote console services, such as Remote Desktop Protocol (RDP), reduces a server's exposure to risk.

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to ports 22 and/or 3389 through another network security group or security list.

Audit:

From Console:

1. Login into the OCI Console
2. Click in the search bar at the top of the screen.
3. Type `Advanced Resource Query` and hit `enter`.
4. Click the `Advanced Resource Query` button in the upper right corner of the screen.
5. Enter the following query in the query box:

```
query SecurityList resources where
(IngressSecurityRules.source = '0.0.0.0/0' &&
IngressSecurityRules.protocol = 6 &&
IngressSecurityRules.tcpOptions.destinationPortRange.max >= 3389 &&
IngressSecurityRules.tcpOptions.destinationPortRange.min <= 3389)
```

6. Ensure query returns no results.

From CLI:

1. Execute the following command:

```
oci search resource structured-search --query-text "query SecurityList
resources where
(IngressSecurityRules.source = '0.0.0.0/0' &&
IngressSecurityRules.protocol = 6 &&
IngressSecurityRules.tcpOptions.destinationPortRange.max >= 3389 &&
IngressSecurityRules.tcpOptions.destinationPortRange.min <= 3389)
"
```

2. Ensure query returns no results.

Cloud Guard
To Enable Cloud Guard Auditing:
Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.
From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console .
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0) in the Detector Rules column.
6. Select the vertical ellipsis icon and choose Edit on the VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0) row.
7. In the Edit Detector Rule window find the Input Setting box and verify/add to the Restricted Protocol: Ports List setting to TCP:[3389], UDP:[3389].
8. Click the `Save` button.

From CLI:

1. Update the VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0) Detector Rule in Cloud Guard to generate Problems if a VCN security list allows public access via port 3389 with the following command:

```
oci cloud-guard detector-recipe-detector-rule update --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id SECURITY_LISTS_OPEN_SOURCE -
-details '{"configurations":[{ "configKey" : "securityListsOpenSourceConfig",
"name" : "Restricted Protocol:Ports List", "value" : "TCP:[3389],
UDP:[3389]", "dataType" : null, "values" : null }]}'
```

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each security list in the returned results, click the security list name

3. Either edit the `ingress rule` to be more restrictive, delete the `ingress rule` or click on the `VCN` and terminate the `security list` as appropriate.

From CLI:

1. Follow the audit procedure.
2. For each of the `security lists` identified, execute the following command:

```
oci network security-list get --security-list-id <security list id>
```

3. Then either:

- Update the `security list` by copying the `ingress-security-rules` element from the JSON returned by the above command, edit it appropriately, and use it in the following command

```
oci network security-list update --security-list-id <security-list-id> --
ingress-security-rules '<ingress security rules JSON>'
```

or

- Delete the security list with the following command:

```
oci network security-list delete --security-list-id <security list id>
```

Additional Information:

This recommendation can also be audited programmatically using REST API

https://docs.oracle.com/en-us/iaas/api/#/en/iaas/20160918/SecurityList/ListSecurityLists

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	12.3 <u>Securely Manage Network Infrastructure</u> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.3 Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22 (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups provide stateful filtering of ingress/egress network traffic to OCI resources. It is recommended that no security group allows unrestricted ingress to port 22.

Rationale:

Removing unfettered connectivity to remote console services, such as Secure Shell (SSH), reduces a server's exposure to risk.

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to ports 22 and/or 3389 through another network security group or security list.

Audit:

From Console:

1. Login into the OCI Console.
2. Click the search bar at the top of the screen.
3. Type Advanced Resource Query and hit enter.
4. Click the Advanced Resource Query button in the upper right corner of the screen.
5. Enter the following query in the query box:

```
query networksecuritygroup resources where lifeCycleState = 'AVAILABLE'
```

6. For each of the network security groups in the returned results, click the name and inspect each of the security rules.
7. Ensure that there are no security rules with direction: Ingress, Source: 0.0.0.0/0, and Destination Port Range: 22.

From CLI:
Issue the following command, it should return no values.

```
 for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
      for compid in `oci iam compartment list 2>/dev/null | jq -r '.data[] |
.id'`;
         do
            for nsgid in `oci network nsg list --compartment-id $compid --
region $region --all 2>/dev/null | jq -r '.data[] | .id'`
               do
                  output=`oci network nsg rules list --nsg-id=$nsgid --all
2>/dev/null | jq -r '.data[] | select(.source == "0.0.0.0/0" and .direction
== "INGRESS" and ((."tcp-options"."destination-port-range".max >=  22 and
."tcp-options"."destination-port-range".min <= 22) or ."tcp-
options"."destination-port-range" == null))'`
                  if [ ! -z "$output" ]; then echo "NSGID=", $nsgid,
"Security Rules=", $output; fi
               done
         done
   done
```

Cloud Guard:

To Enable Cloud Guard Auditing:

Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.

From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console .
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find NSG ingress rule contains disallowed IP/port in the Detector Rules column.
6. Select the vertical ellipsis icon and chose Edit on the NSG ingress rule contains disallowed IP/port row.
7. In the Edit Detector Rule window find the Input Setting box and verify/add to the Restricted Protocol: Ports List setting to TCP:[22], UDP:[22].
8. Click the `Save` button.

From CLI:

1. Update the NSG ingress rule contains disallowed IP/port Detector Rule in Cloud Guard to generate Problems if a network security group allows ingress network traffic to port 22 with the following command:

```
oci cloud-guard detector-recipe-detector-rule update --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id
VCN_NSG_INGRESS_RULE_PORTS_CHECK --details '{"configurations":[ {"configKey"
: "nsgIngressRuleDisallowedPortsConfig", "name" : "Default disallowed ports",
"value" : "TCP:[22], UDP:[22]", "dataType" : null, "values" : null }]}'
```

Remediation:

From Console:

1. Login into the OCI Console.
2. Click the search bar at the top of the screen.
3. Type Advanced Resource Query and hit enter.
4. Click the Advanced Resource Query button in the upper right corner of the screen.
5. Enter the following query in the query box:

query networksecuritygroup resources where lifeCycleState = 'AVAILABLE'

6. For each of the network security groups in the returned results, click the name and inspect each of the security rules.
7. Remove all security rules with direction: Ingress, Source: 0.0.0.0/0, and Destination Port Range: 22.

From CLI:
Issue the following command and identify the security rule to remove.

```
 for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
       for compid in `oci iam compartment list 2>/dev/null | jq -r '.data[] |
.id'`;
          do
             for nsgid in `oci network nsg list --compartment-id $compid --
region $region --all 2>/dev/null | jq -r '.data[] | .id'`
                do
                     output=`oci network nsg rules list --nsg-id=$nsgid --all
2>/dev/null | jq -r '.data[] | select(.source == "0.0.0.0/0" and .direction
== "INGRESS" and ((."tcp-options"."destination-port-range".max >=  22 and
."tcp-options"."destination-port-range".min <= 22) or ."tcp-
options"."destination-port-range" == null))'`
                     if [ ! -z "$output" ]; then echo "NSGID=", $nsgid,
"Security Rules=", $output; fi
                 done
          done
   done
```

- Remove the security rules

```
oci network nsg rules remove --nsg-id=<NSGID from audit output>
```

or

- Update the security rules

```
oci network nsg rules update --nsg-id=<NSGID from audit output> --security-
rules='[<updated security-rules JSON (without isValid and TimrCreated
fields)>]'

eg:

 oci network nsg rules update --nsg-
id=ocid1.networksecuritygroup.oc1.iad.xxxxxxxxxxxxxxxxxxxxxx --security-
rules='[{ "description": null, "destination": null, "destination-type": null,
"direction": "INGRESS", "icmp-options": null, "id": "709001", "is-stateless":
null, "protocol": "6", "source": "140.238.154.0/24", "source-type":
"CIDR_BLOCK", "tcp-options": { "destination-port-range": { "max": 22, "min":
22 }, "source-port-range": null }, "udp-options": null }]'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	12.3 <u>Securely Manage Network Infrastructure</u> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.4 Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389 (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups provide stateful filtering of ingress/egress network traffic to OCI resources. It is recommended that no security group allows unrestricted ingress access to port 3389.

Rationale:

Removing unfettered connectivity to remote console services, such as Remote Desktop Protocol (RDP), reduces a server's exposure to risk.

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to ports 22 and/or 3389 through another network security group or security list.

Audit:

From CLI:
Issue the following command, it should not return anything.

```
 for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
      for compid in `oci iam compartment list 2>/dev/null | jq -r '.data[] |
.id'`;
         do
            for nsgid in `oci network nsg list --compartment-id $compid --
region $region --all 2>/dev/null | jq -r '.data[] | .id'`
               do
                  output=`oci network nsg rules list --nsg-id=$nsgid --all
2>/dev/null | jq -r '.data[] | select(.source == "0.0.0.0/0" and .direction
== "INGRESS" and ((."tcp-options"."destination-port-range".max >=  3389 and
."tcp-options"."destination-port-range".min <= 3389) or ."tcp-
options"."destination-port-range" == null))'`
                  if [ ! -z "$output" ]; then echo "NSGID=", $nsgid,
"Security Rules=", $output; fi
               done
         done
   done
```

From Cloud Guard:
To Enable Cloud Guard Auditing:
Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.
From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find NSG ingress rule contains disallowed IP/port in the Detector Rules column.
6. Select the vertical ellipsis icon and chose Edit on the NSG ingress rule contains disallowed IP/port row.
7. In the Edit Detector Rule window find the Input Setting box and verify/add to the Restricted Protocol: Ports List setting to TCP:[3389], UDP:[3389].
8. Click the Save button.

From CLI:

1. Update the NSG ingress rule contains disallowed IP/port Detector Rule in Cloud Guard to generate Problems if a network security group allows ingress network traffic to port 3389 with the following command:

```
oci cloud-guard detector-recipe-detector-rule update --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id
VCN_NSG_INGRESS_RULE_PORTS_CHECK --details '{"configurations":[ {"configKey"
: "nsgIngressRuleDisallowedPortsConfig", "name" : "Default disallowed ports",
"value" : "TCP:[3389], UDP:[3389]", "dataType" : null, "values" : null }]}'
```

Remediation:

From CLI:
Using the details returned from the audit procedure either:

- Remove the security rules

```
oci network nsg rules remove --nsg-id=<NSGID from audit output>
```

or

- Update the security rules

```
oci network nsg rules update --nsg-id=<NSGID from audit output>  --security-
rules=<updated security-rules JSON (without the isValid or TimeCreated
fields)>

eg:

 oci network nsg rules update --nsg-
id=ocid1.networksecuritygroup.oc1.iad.xxxxxxxxxxxxxxxxxxxxxx --security-
rules='[{ "description": null, "destination": null, "destination-type": null,
"direction": "INGRESS", "icmp-options": null, "id": "709001", "is-stateless":
null, "protocol": "6", "source": "140.238.154.0/24", "source-type":
"CIDR_BLOCK", "tcp-options": { "destination-port-range": { "max": 3389,
"min": 3389 }, "source-port-range": null }, "udp-options": null }]'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	**12.3 Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.5 Ensure the default security list of every VCN restricts all traffic except ICMP (Automated)

Profile Applicability:

- Level 1

Description:

A default security list is created when a Virtual Cloud Network (VCN) is created. Security lists provide stateful filtering of ingress and egress network traffic to OCI resources. It is recommended no security list allows unrestricted ingress access to resources such as Secure Shell (SSH) via port 22.

Rationale:

Removing unfettered connectivity to remote console services, such as SSH on port 22, reduces a server's exposure to unauthorized access.

Impact:

For updating an existing environment, care should be taken to ensure that administrators currently relying on an existing ingress from 0.0.0.0/0 have access to port 22 through another security group.

Audit:

From Console:

1. Login into the OCI Console
2. Click on `Networking -> Virtual Cloud Networks` from the services menu
3. For each VCN listed `Click on Security Lists`
4. Click on `Default Security List for <VCN Name>`
5. Verify that there is no Ingress rule with 'Source 0.0.0.0/0, IP Protocol 6 (TCP) and Destination Port Range 22'

Remediation:

From Console:

1. Login into the OCI Console
2. Click on `Networking -> Virtual Cloud Networks` from the services menu
3. For each VCN listed `Click on Security Lists`
4. Click on `Default Security List for <VCN Name>`
5. Identify the Ingress Rule with 'Source 0.0.0.0/0, IP Protocol 6 (TCP) and Destination Port Range 22'
6. Either Edit the Security rule to restrict the source and/or port range or delete the rule.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 <u>Securely Manage Network Infrastructure</u> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.6 Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources. (Manual)

Profile Applicability:

- Level 1

Description:

Oracle Integration (OIC) is a complete, secure, but lightweight integration solution that enables you to connect your applications in the cloud. It simplifies connectivity between your applications and connects both your applications that live in the cloud and your applications that still live on premises. Oracle Integration provides secure, enterprise-grade connectivity regardless of the applications you are connecting or where they reside. OIC instances are created within an Oracle managed secure private network with each having a public endpoint. The capability to configure ingress filtering of network traffic to protect your OIC instances from unauthorized network access is included. It is recommended that network access to your OIC instances be restricted to your approved corporate IP Addresses or Virtual Cloud Networks (VCN)s.

Rationale:

Restricting connectivity to OIC Instances reduces an OIC instance's exposure to risk.

Impact:

When updating ingress filters for an existing environment, care should be taken to ensure that IP addresses and VCNs currently used by administrators, users, and services to access your OIC instances are included in the updated filters.

Audit:

From Console:

1. Login into the OCI Console
2. Click in the search bar, top of the screen.
3. Type Advanced Resource Query and hit enter.
4. Click the Advanced Resource Query button in the upper right of the screen.
5. Enter the following query in the query box:

```
query integrationinstance resources
```

6. For each OIC Instance returned click on the link under `Display name`
7. Click on `Network Access`
   8 .Ensure `Restrict Network Access` is selected and the IP Address/CIDR Block as well as Virtual Cloud Networks are correct
8. Repeat for other subscribed regions

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
       for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
         do
            output=`oci integration integration-instance list --compartment-
id $compid --region $region --all 2>/dev/null | jq -r '.data[] |
select(."network-endpoint-details"."network-endpoint-type" == null)'`
            if [ ! -z "$output" ]; then echo $output; fi
         done
   done
```

2. Ensure `allowlisted-http-ips` and `allowed-http-vcns` are correct

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each OIC instance in the returned results, click the OIC Instance name
3. Click `Network Access`
4. Either edit the `Network Access` to be more restrictive

From CLI

1. Follow the audit procedure.
2. Get the json input format using the below command:

```
oci integration integration-instance change-network-endpoint --generate-
param-json-input
```

3.For each of the OIC Instances identified get its details.
4.Update the `Network Access`, copy the `network-endpoint-details` element from the JSON returned by the above get call, edit it appropriately and use it in the following command

```
Oci integration integration-instance change-network-endpoint --id <oic-
instance-id> --from-json '<network endpoints JSON>'
```

References:

1. https://docs.oracle.com/en/cloud/paas/integration-cloud/integrations-user/get-started-integration-cloud-service.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	**12.3 Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.7 Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network. (Manual)

Profile Applicability:

- Level 1

Description:

Oracle Analytics Cloud (OAC) is a scalable and secure public cloud service that provides a full set of capabilities to explore and perform collaborative analytics for you, your workgroup, and your enterprise. OAC instances provide ingress filtering of network traffic or can be deployed with in an existing Virtual Cloud Network VCN. It is recommended that all new OAC instances be deployed within a VCN and that the Access Control Rules are restricted to your corporate IP Addresses or VCNs for existing OAC instances.

Rationale:

Restricting connectivity to Oracle Analytics Cloud instances reduces an OAC instance's exposure to risk.

Impact:

When updating ingress filters for an existing environment, care should be taken to ensure that IP addresses and VCNs currently used by administrators, users, and services to access your OAC instances are included in the updated filters. Also, these changes will temporarily bring the OAC instance offline.

Audit:

From Console:
1 Login into the OCI Console
2. Click in the search bar, top of the screen.
3. Type Advanced Resource Query and hit enter.
4. Click the Advanced Resource Query button in the upper right of the screen.
5. Enter the following query in the query box:

```
query analyticsinstance resources
```

6. For each OAC Instance returned click on the link under `Display name`.
7. Ensure `Access Control Rules` IP Address/CIDR Block as well as Virtual Cloud Networks are correct.
8. Repeat for other subscribed regions.

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
      for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
         do
            output=`oci analytics analytics-instance list --compartment-id
$compid --region $region --all 2>/dev/null | jq -r '.data[] |
select(."network-endpoint-details"."network-endpoint-type"  == "PUBLIC")'`
            if [ ! -z "$output" ]; then echo $output; fi
         done
   done
```

2. Ensure `network-endpoint-type` are correct.

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each OAC instance in the returned results, click the OAC Instance name
3. Click `Edit` next to `Access Control Rules`
4. Click `+Another Rule` and add rules as required

From CLI:

1. Follow the audit procedure.
2. Get the json input format by executing the below command:

```
oci analytics analytics-instance change-network-endpoint --generate-full-
command-json-input
```

3. For each of the OAC Instances identified get its details.
4. Update the `Access Control Rules`, copy the `network-endpoint-details` element
   from the JSON returned by the above get call, edit it appropriately and use it in
   the following command:

```
oci integration analytics-instance change-network-endpoint --from-json
'<network endpoints JSON>'
```

Additional Information:

https://docs.oracle.com/en/cloud/paas/analytics-cloud/acoci/manage-service-access-and-security.html#GUID-3DB25824-4417-4981-9EEC-29C0C6FD3883

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 Implement and Manage a Firewall on Servers** Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	**12.3 Securely Manage Network Infrastructure** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.8 Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network (Manual)

Profile Applicability:

- Level 1

Description:

Oracle Autonomous Database Shared (ADB-S) automates database tuning, security, backups, updates, and other routine management tasks traditionally performed by DBAs. ADB-S provide ingress filtering of network traffic or can be deployed within an existing Virtual Cloud Network (VCN). It is recommended that all new ADB-S databases be deployed within a VCN and that the Access Control Rules are restricted to your corporate IP Addresses or VCNs for existing ADB-S databases.

Rationale:

Restricting connectivity to ADB-S Databases reduces an ADB-S database's exposure to risk.

Impact:

When updating ingress filters for an existing environment, care should be taken to ensure that IP addresses and VCNs currently used by administrators, users, and services to access your ADB-S instances are included in the updated filters.

Audit:

From Console:

1. Login into the OCI Console
2. Click in the search bar, top of the screen.
3. Type Advanced Resource Query and hit enter.
4. Click the `Advanced Resource Query` button in the upper right of the screen.
5. Enter the following query in the query box:

```
query autonomousdatabase resources
```

6. For each ABD-S database returned click on the link under `Display name`
7. Click `Edit` next to `Access Control List`
8. Ensure `Access Control Rules' IP Address/CIDR Block as well as VCNs are correct
9. Repeat for other subscribed regions

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
    do
        for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
        do
            for adbid in `oci db autonomous-database list --compartment-id
$compid --region $region --all 2>/dev/null | jq -r '.data[] | select(."nsg-
ids"  == null).id'`
                do
                output=`oci db autonomous-database get --autonomous-database-
id $adbid --region $region --query=data.{"WhiteListIPs:\"whitelisted-
ips\","id:id""} --output table 2>/dev/null`
                if [ ! -z "$output" ]; then echo $output; fi
                done
        done
    done
```

2. Ensure `WhiteListIPs` are correct.

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each ADB-S database in the returned results, click the ADB-S database name
3. Click `Edit` next to `Access Control Rules`
4. Click `+Another Rule` and add rules as required
5. Click `Save Changes`

From CLI:

1. Follow the audit procedure.
2. Get the json input format by executing the following command:

```
oci db autonomous-database update --generate-full-command-json-input
```

3. For each of the ADB-S Database identified get its details.
4. Update the `whitelistIps`, copy the `WhiteListIPs` element from the JSON returned by the above get call, edit it appropriately and use it in the following command:

```
oci db autonomous-database update --autonomous-database-id <ABD-S OCID> --
from-json '<network endpoints JSON>'
```

References:

1. https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/network-access-options.html#GUID-29D62917-0F18-4F3E-8081-B3BD5C0C79F5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4** <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	**12.3** <u>Securely Manage Network Infrastructure</u> Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	**9.2** <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3 Compute

This section contains recommendations for configuring compute related options

3.1 Ensure Compute Instance Legacy Metadata service endpoint is disabled (Automated)

Profile Applicability:

- Level 2

Description:

Compute Instances that utilize Legacy MetaData service endpoints (IMDSv1) are susceptible to potential SSRF attacks. To bolster security measures, it is strongly advised to reconfigure Compute Instances to adopt Instance Metadata Service v2, aligning with the industry's best security practices.

Rationale:

Enabling Instance Metadata Service v2 enhances security and grants precise control over metadata access. Transitioning from IMDSv1 reduces the risk of SSRF attacks, bolstering system protection.

IMDv1 poses security risks due to its inferior security measures and limited auditing capabilities. Transitioning to IMDv2 ensures a more secure environment with robust security features and improved monitoring capabilities.

Impact:

If you disable IMDSv1 on an instance that does not support IMDSv2, you might not be able to connect to the instance when you launch it.

IMDSv2 is supported on the following platform images:

- Oracle Autonomous Linux 8.x images
- Oracle Autonomous Linux 7.x images released in June 2020 or later
- Oracle Linux 8.x, Oracle Linux 7.x, and Oracle Linux 6.x images released in July 2020 or later

Other platform images, most custom images, and most Marketplace images do not support IMDSv2. Custom Linux images might support IMDSv2 if cloud-init is updated to version 20.3 or later and Oracle Cloud Agent is updated to version 0.0.19 or later. Custom Windows images might support IMDSv2 if Oracle Cloud Agent is updated to version 1.0.0.0 or later; cloudbase-init does not support IMDSv2.

Audit:

From Console:

1. Login to the OCI Console
2. Select compute instance in your compartment.
3. Click on each instance name.

4. In the `Instance Details` section, next to `Instance metadata service` make sure `Version 2 only` is selected.

From CLI:

1. Run command:

```
for region in `oci iam region-subscription list | jq -r '.data[] | ."region-
name"'`;
   do
      for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
        do
           output=`oci compute instance list --compartment-id $compid --
region $region --all 2>/dev/null | jq -r '.data[] | select(."instance-
options"."are-legacy-imds-endpoints-disabled" == false )'`
           if [ ! -z "$output" ]; then echo $output; fi
        done
   done
```

2. No results should be returned

Remediation:

From Console:

1. Login to the OCI Console
2. Click on the search box at the top of the console and search for compute instance name.
3. Click on the instance name, In the `Instance Details` section, next to Instance Metadata Service, click `Edit`.
4. For the `Instance metadata service`, select the `Version 2 only` option.
5. Click `Save Changes`.

Note : Disabling IMDSv1 on an incompatible instance may result in connectivity issues upon launch.
To re-enable IMDSv1, follow these steps:

1. On the Instance Details page in the Console, click `Edit` next to Instance Metadata Service.
2. Choose the `Version 1 and version 2` option, and save your changes.

From CLI:
Run Below Command,
```
oci compute instance update --instance-id [instance-ocid] --instance-options
'{"areLegacyImdsEndpointsDisabled" :"true"}'
```

This will set Instance Metadata Service to use Version 2 Only.

Default Value:

Versions 1 and 2

References:

1. https://docs.oracle.com/en-us/iaas/Content/Compute/Tasks/gettingmetadata.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

3.2 Ensure Secure Boot is enabled on Compute Instance (Automated)

Profile Applicability:

- Level 2

Description:

Shielded Instances with Secure Boot enabled prevents unauthorized boot loaders and operating systems from booting. This prevent rootkits, bootkits, and unauthorized software from running before the operating system loads. Secure Boot verifies the digital signature of the system's boot software to check its authenticity. The digital signature ensures the operating system has not been tampered with and is from a trusted source. When the system boots and attempts to execute the software, it will first check the digital signature to ensure validity. If the digital signature is not valid, the system will not allow the software to run. Secure Boot is a feature of UEFI(Unified Extensible Firmware Interface) that only allows approved operating systems to boot up.

Rationale:

A Threat Actor with access to the operating system may seek to alter boot components to persist malware or rootkits during system initialization. Secure Boot helps ensure that the system only runs authentic software by verifying the digital signature of all boot components.

Impact:

An existing instance cannot be changed to a Shielded instance with Secure boot enabled. Shielded Secure Boot not available on all instance shapes and Operating systems. Additionally the following limitations exist:

Thus to enable you have to terminate the instance and create a new one. Also, Shielded instances do not support live migration. During an infrastructure maintenance event, Oracle Cloud Infrastructure live migrates supported VM instances from the physical VM host that needs maintenance to a healthy VM host with minimal disruption to running instances. If you enable Secure Boot on an instance, the instance cannot be migrated, because the hardware TPM is not migratable. This may result in an outage because the TPM can't be migrate from a unhealthy host to healthy host.

Audit:

From Console:

1. Login to the OCI Console
2. Select compute instance in your compartment.
3. Click on each instance name.
4. In the `Launch Options` section,

5. Check if `Secure Boot` is `Enabled`.

From CLI:

Run command:

```
for region in `oci iam region-subscription list | jq -r '.data[] | ."region-
name"'`;
   do
      for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
        do
           output=`oci compute instance list --compartment-id $compid --
region $region --all 2>/dev/null | jq -r '.data[] | select(."platform-config"
== null or "platform-config"."is-secure-boot-enabled" == false )'`
           if [ ! -z "$output" ]; then echo $output; fi
        done
   done
```

In response, check if `platform-config` are not null and `is-secure-boot-enabled` is set to `true`

Remediation:

Note: Secure Boot facility is available on selected VM images and Shapes in OCI. User have to configure Secured Boot at time of instance creation only.
From Console:

1. Navigate to https://cloud.oracle.com/compute/instances
2. Select the instance from the Audit Procedure
3. Click `Terminate`.
4. Determine whether or not to permanently delete instance's attached boot volume.
5. Click `Terminate instance`.
6. Click on `Create Instance`.
7. Select Image and Shape which supports Shielded Instance configuration. Icon for Shield in front of Image/Shape row indicates support of Shielded Instance.
8. Click on `edit` of Security Blade.
9. Turn On Shielded Instance, then Turn on the Secure Boot Toggle.
10. Fill in the rest of the details as per requirements.
11. Click `Create`.

Default Value:

Secure Boot is not Enabled

References:

1. https://docs.oracle.com/en-us/iaas/Content/Compute/References/shielded-instances.htm
2. https://uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

3.3 Ensure In-transit Encryption is enabled on Compute Instance (Automated)

Profile Applicability:

- Level 1

Description:

The Block Volume service provides the option to enable in-transit encryption for paravirtualized volume attachments on virtual machine (VM) instances.

Rationale:

All the data moving between the instance and the block volume is transferred over an internal and highly secure network. If you have specific compliance requirements related to the encryption of the data while it is moving between the instance and the block volume, you should enable the in-transit encryption option.

Impact:

In-transit encryption for boot and block volumes is only available for virtual machine (VM) instances launched from platform images, along with bare metal instances that use the following shapes: BM.Standard.E3.128, BM.Standard.E4.128, BM.DenseIO.E4.128. It is not supported on other bare metal instances.

Audit:

From Console:

1. Go to https://cloud.oracle.com/compute/instances
2. Select compute instance in your compartment.
3. Click on each instance name.
4. Click on `Boot volume` on the bottom left.
5. Under the `In-transit encryption` column make sure it is `Enabled`

From CLI:

1. Execute the following:

```
for region in `oci iam region-subscription list | jq -r '.data[] | ."region-
name"'`;
   do
      for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
         do
            output=`oci compute instance list --compartment-id $compid --
region $region --all 2>/dev/null | jq -r '.data[] | select(."launch-
options"."is-pv-encryption-in-transit-enabled" == false )'`
            if [ ! -z "$output" ]; then echo $output; fi
         done
   done
```

2. Ensure no results are returned

Remediation:

From Console:

1. Navigate to https://cloud.oracle.com/compute/instances
2. Select the instance from the Audit Procedure
3. Click `Terminate`.
4. Determine whether or not to permanently delete instance's attached boot volume.
5. Click `Terminate instance`.
6. Click on `Create Instance`.
7. Fill in the details as per requirements.
8. In the `Boot volume` section ensure `Use in-transit encryption` is checked.
9. Fill in the rest of the details as per requirements.
10. Click `Create`.

Default Value:

Enabled

References:

1. https://docs.oracle.com/en-
   us/iaas/Content/Block/Concepts/overview.htm#BlockVolumeEncryption__intransi
   t

4 Logging and Monitoring

This section contains recommendations for configuring logging and monitoring related options.

4.1 Ensure default tags are used on resources (Automated)

Profile Applicability:

- Level 1

Description:

Using default tags is a way to ensure all resources that support tags are tagged during creation. Tags can be based on static or computed values. It is recommended to set up default tags early after root compartment creation to ensure all created resources will get tagged. Tags are scoped to Compartments and are inherited by Child Compartments. The recommendation is to create default tags like "CreatedBy" at the Root Compartment level to ensure all resources get tagged. When using Tags it is important to ensure that Tag Namespaces are protected by IAM Policies otherwise this will allow users to change tags or tag values. Depending on the age of the OCI Tenancy there may already be Tag defaults setup at the Root Level and no need for further action to implement this action.

Rationale:

In the case of an incident having default tags like "CreatedBy" applied will provide info on who created the resource without having to search the Audit logs.

Impact:

There is no performance impact when enabling the above described features.

Audit:

From Console:

1. Login to OCI Console.
2. From the navigation menu, select `Identity & Security`.
3. Under `Identity`, select `Compartments`.
4. Click the name of the root compartment.
5. Under `Resources`, select `Tag Defaults`.
6. In the `Tag Defaults` table, verify that there is a Tag with a value of `${iam.principal.name}` and a Tag Key Status of `Active`.

Note:
The name of the tag may be different then "CreatedBy" if the Tenancy Administrator has decided to use another tag.
From CLI:

1. List the active tag defaults defined at the Root compartment level by using the Tenancy OCID as compartment id.

Note: The Tenancy OCID can be found in the `~/.oci/config` file used by the OCI Command Line Tool

```
oci iam tag-default list --compartment-id=<tenancy_ocid> --query="data
[?\"lifecycle-state\"=='ACTIVE']".{"name:\"tag-definition-
name\","value:value""} --output table
```

2. Verify in the table returned that there is at least one row that contains the value of `${iam.principal.name}`.

Remediation:

From Console:

1. Login to OCI Console.
2. From the navigation menu, select `Governance & Administration`.
3. Under `Tenancy Management`, select `Tag Namespaces`.
4. Under `Compartment`, select the root compartment.
5. If no tag namespace exists, click `Create Tag Namespace`, enter a name and description and click `Create Tag Namespace`.
6. Click the name of a tag namespace.
7. Click `Create Tag Key Definition`.
8. Enter a tag key (e.g. CreatedBy) and description, and click `Create Tag Key Definition`.
9. From the navigation menu, select `Identity & Security`.
10. Under `Identity`, select `Compartments`.
11. Click the name of the root compartment.
12. Under `Resources`, select `Tag Defaults`.
13. Click `Create Tag Default`.
14. Select a tag namespace, tag key, and enter `${iam.principal.name}` as the tag value.
15. Click `Create`.

From CLI:

1. Create a Tag Namespace in the Root Compartment

```
oci iam tag-namespace create --compartment-id=<tenancy_ocid> --name=<name> --
description=<description> --query data.{"\"Tag Namespace OCID\":id"} --output
table
```

2. Note the Tag Namespace OCID and use it when creating the Tag Key Definition

```
oci iam tag create --tag-namespace-id=<tag_namespace_ocid> --
name=<tag_key_name> --description=<description> --query data.{"\"Tag Key
Definition OCID\":id"} --output table
```

3. Note the Tag Key Definition OCID and use it when creating the Tag Default in the Root compartment

```
oci iam tag-default create --compartment-id=<tenancy_ocid> --tag-definition-
id=<tag_key_definition_id> --value="\${iam.principal.name}"
```

Default Value:

New OCI Tenancies will have Tag Defaults setup for CreatedBy and CreatedOn as default. If this is the case then there is no remediate action required in the Tenancy in order to meet this specific control.

Additional Information:

- There is no requirement to use the "Oracle-Tags" namespace to implement this control. A Tag Namespace Administrator can create any namespace and use it for this control.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**1.1 Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	●	●	●
v7	**1.4 Maintain Detailed Asset Inventory** Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	●	●	●

4.2 Create at least one notification topic and subscription to receive monitoring alerts (Automated)

Profile Applicability:

- Level 1

Description:

Notifications provide a multi-channel messaging service that allow users and applications to be notified of events of interest occurring within OCI. Messages can be sent via eMail, HTTPs, PagerDuty, Slack or the OCI Function service. Some channels, such as eMail require confirmation of the subscription before it becomes active.

Rationale:

Creating one or more notification topics allow administrators to be notified of relevant changes made to OCI infrastructure.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Notifications Service page: https://console.us-ashburn-1.oraclecloud.com/notification/topics
2. Select the `Compartment` that hosts the notifications
3. Find and click the `Topic` relevant to your monitoring alerts.
4. Ensure a valid active subscription is shown.

From CLI:

1. List the topics in the `Compartment` that hosts the notifications

```
oci ons topic list --compartment-id <compartment OCID> --all
```

2. Note the `OCID` of the monitoring topic(s) using the `topic-id` field of the returned JSON and use it to list the subscriptions

```
oci ons subscription list --compartment-id <compartment OCID> --topic-id
<topic OCID> --all
```

3. Ensure at least one active subscription is returned

Remediation:

From Console:

1. Go to the Notifications Service page: https://console.us-ashburn-1.oraclecloud.com/notification/topics
2. Select the `Compartment` that hosts the notifications
3. Click `Create Topic`
4. Set the `name` to something relevant
5. Set the `description` to describe the purpose of the topic
6. Click `Create`
7. Click the newly created topic
8. Click `Create Subscription`
9. Choose the correct `protocol`
10. Complete the correct parameter, for instance `email` address
11. Click `Create`

From CLI:

1. Create a topic in a compartment

```
oci ons topic create --name <topic name> --description <topic description> --
compartment-id <compartment OCID>
```

2. Note the `OCID` of the `topic` using the `topic-id` field of the returned JSON and use it to create a new subscription

```
oci ons subscription create --compartment-id <compartment OCID> --topic-id
<topic OCID> --protocol <protocol> --subscription-endpoint <subscription
endpoint>
```

3. The returned JSON includes the id of the `subscription`.

Additional Information:

- The console URL shown is for the Ashburn region. Your tenancy might have a different home region and thus console URL.
- The same Notification topic can be reused by many Events. A single topic can have multiple subscriptions allowing the same topic to be published to multiple locations.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> 　　Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.11 <u>Conduct Audit Log Reviews</u> 　　Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 <u>Activate audit logging</u> 　　Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.7 <u>Regularly Review Logs</u> 　　On a regular basis, review logs to identify anomalies or abnormal events.		●	●

4.3 Ensure a notification is configured for Identity Provider changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when Identity Providers are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments. It is recommended to create the Event rule at the root compartment level.

Rationale:

OCI Identity Providers allow management of User ID / passwords in external systems and use of those credentials to access OCI resources. Identity Providers allow users to single sign-on to OCI console and have other OCI credentials like API Keys. Monitoring and alerting on changes to Identity Providers will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page:
   https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `Identity Provider` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Identity` and Event Types: `Identity Provider – Create`, `Identity Provider - Delete` and `Identity Provider – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.identitycontrolplane.createidentityprovider
com.oraclecloud.identitycontrolplane.deleteidentityprovider
com.oraclecloud.identitycontrolplane.updateidentityprovider
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Identity` in the Service Name Drop-down and selecting `Identity Provider – Create`, `Identity Provider - Delete` and `Identity Provider – Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.identitycontrolplane.createidentityprovide
r\",\" com.oraclecloud.identitycontrolplane.deleteidentityprovider\",\"
com.oraclecloud.identitycontrolplane.updateidentityprovider\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u>** Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.4 Ensure a notification is configured for IdP group mapping changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when Identity Provider Group Mappings are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments. It is recommended to create the Event rule at the root compartment level.

Rationale:

IAM Policies govern access to all resources within an OCI Tenancy. IAM Policies use OCI Groups for assigning the privileges. Identity Provider Groups could be mapped to OCI Groups to assign privileges to federated users in OCI. Monitoring and alerting on changes to Identity Provider Group mappings will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page:
   https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `Idp Group Mapping` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Identity` and Event Types: `Idp Group Mapping – Create`, `Idp Group Mapping – Delete` and `Idp Group Mapping – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<displa-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.identitycontrolplane.createidpgroupmapping
com.oraclecloud.identitycontrolplane.deleteidpgroupmapping
com.oraclecloud.identitycontrolplane.updateidpgroupmapping
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Identity` in the Service Name Drop-down and selecting `Idp Group Mapping – Create`, `Idp Group Mapping – Delete` and `Idp Group Mapping – Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.identitycontrolplane.createidpgroupmapping
\",\"com.oraclecloud.identitycontrolplane.deleteidpgroupmapping\",\"com.oracl
ecloud.identitycontrolplane.updateidpgroupmapping\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	**4.2 Change Default Passwords** Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	🟢	🟠	🔵
v7	**11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes** Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		🟠	🔵

4.5 Ensure a notification is configured for IAM group changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when IAM Groups are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

IAM Groups control access to all resources within an OCI Tenancy. Monitoring and alerting on changes to IAM Groups will help in identifying changes to satisfy least privilege principle.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles IAM `Group` Changes
4. Click the `Edit Rule` button and verify that the `Rule Conditions` section contains a condition for the Service `Identity` and Event Types: `Group – Create`, `Group – Delete` and `Group – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on `Display Name` and `Compartment OCID`

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.identitycontrolplane.creategroup
com.oraclecloud.identitycontrolplane.deletegroup
com.oraclecloud.identitycontrolplane.updategroup
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is ONS and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Identity` in the Service Name Drop-down and selecting `Group - Create`, `Group - Delete` and `Group - Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.identitycontrolplane.creategroup\",\"com.o
raclecloud.identitycontrolplane.deletegroup\",\"com.oraclecloud.identitycontr
olplane.updategroup\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.6 Ensure a notification is configured for IAM policy changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when IAM Policies are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

IAM Policies govern access to all resources within an OCI Tenancy. Monitoring and alerting on changes to IAM policies will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `IAM Policy` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Identity` and Event Types: `Policy – Create`, `Policy - Delete` and `Policy – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.identitycontrolplane.createpolicy
com.oraclecloud.identitycontrolplane.deletepolicy
com.oraclecloud.identitycontrolplane.updatepolicy
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Identity` in the Service Name Drop-down and selecting `Policy – Change Compartment`, `Policy – Create`, `Policy - Delete` and `Policy – Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.identitycontrolplane.createpolicy\",\"com.
oraclecloud.identitycontrolplane.deletepolicy\",\"com.oraclecloud.identitycon
trolplane.updatepolicy\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.7 Ensure a notification is configured for user changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when IAM Users are created, updated, deleted, capabilities updated, or state updated. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

Users use or manage Oracle Cloud Infrastructure resources. Monitoring and alerting on changes to Users will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Using the search box to navigate to `events`
2. Navigate to the `rules` page
3. Select the `Compartment` that hosts the rules
4. Find and click the `Rule` that handles `IAM User` Changes
5. Click the `Edit Rule` button and verify that the `Rule Conditions` section contains a condition for the Service `Identity` and Event Types:
   ```
   User – Create,
   User – Delete,
   User – Update,
   User Capabilities – Update,
   User State – Update
   ```
6. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on `Display Name` and `Compartment OCID`

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.identitycontrolplane.createuser
com.oraclecloud.identitycontrolplane.deleteuser
com.oraclecloud.identitycontrolplane.updateuser
com.oraclecloud.identitycontrolplane.updateusercapabilities
com.oraclecloud.identitycontrolplane.updateuserstate
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is ONS and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Using the search box to navigate to `events`
2. Navigate to the `rules` page
3. Select the `compartment` that should host the rule
4. Click `Create Rule`
5. Provide a `Display Name` and `Description`
6. Create a Rule Condition by selecting `Identity` in the Service Name Drop-down and selecting:
   ```
   User – Create,
   User – Delete,
   User – Update,
   User Capabilities – Update,
   User State – Update
   ```
7. In the `Actions` section select `Notifications` as Action Type
8. Select the `Compartment` that hosts the Topic to be used.
9. Select the `Topic` to be used
10. Optionally add Tags to the Rule
11. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.identitycontrolplane.createuser\",\"com.or
aclecloud.identitycontrolplane.deleteuser\",\"com.oraclecloud.identitycontrol
plane.updateuser\",\"com.oraclecloud.identitycontrolplane.updateusercapabilit
ies\",\"com.oraclecloud.identitycontrolplane.updateuserstate\"],\"data\":{}}"
,
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.8 Ensure a notification is configured for VCN changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when Virtual Cloud Networks are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

Virtual Cloud Networks (VCNs) closely resembles a traditional network. Monitoring and alerting on changes to VCNs will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `VCN` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Networking` and Event Types: `VCN – Create`, `VCN - Delete and VCN – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.virtualnetwork.createvcn
com.oraclecloud.virtualnetwork.deletevcn
com.oraclecloud.virtualnetwork.updatevcn
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Networking` in the Service Name Drop-down and selecting `VCN - Create`, `VCN - Delete` and `VCN - Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.virtualnetwork.createvcn\",\"com.oracleclo
ud.virtualnetwork.deletevcn\",\"com.oraclecloud.virtualnetwork.updatevcn\"],\
"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.9 Ensure a notification is configured for changes to route tables (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when route tables are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

Route tables control traffic flowing to or from Virtual Cloud Networks and Subnets. Monitoring and alerting on changes to route tables will help in identifying changes these traffic flows.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `Route Table` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Networking` and Event Types: `Route Table – Change Compartment`, `Route Table – Create`, `Route Table - Delete` and `Route Table - Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.virtualnetwork.changeroutetablecompartment
com.oraclecloud.virtualnetwork.createroutetable
com.oraclecloud.virtualnetwork.deleteroutetable
com.oraclecloud.virtualnetwork.updateroutetable
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Networking` in the Service Name Drop-down and selecting `Route Table – Change Compartment`, `Route Table – Create`, `Route Table - Delete` and `Route Table – Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.virtualnetwork.changeroutetablecompartment
\",\"com.oraclecloud.virtualnetwork.createroutetable\",\"com.oraclecloud.virt
ualnetwork.deleteroutetable\",\"com.oraclecloud.virtualnetwork.updateroutetab
le\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**11.3** <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		🟠	🔵

4.10 Ensure a notification is configured for security list changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when security lists are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

Security Lists control traffic flowing into and out of Subnets within a Virtual Cloud Network. Monitoring and alerting on changes to Security Lists will help in identifying changes to these security controls.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `Security List` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Networking` and Event Types: `Security List – Change Compartment`, `Security List – Create`, `Security List - Delete` and `Security List – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-ocid>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.virtualnetwork.changesecuritylistcompartment
com.oraclecloud.virtualnetwork.createsecuritylist
com.oraclecloud.virtualnetwork.deletesecuritylist
com.oraclecloud.virtualnetwork.updatesecuritylist
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Networking` in the Service Name Drop-down and selecting `Security List – Change Compartment`, `Security List – Create`, `Security List - Delete` and `Security List – Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic-id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic-id>"
        }]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.virtualnetwork.changesecuritylistcompartme
nt\",\"com.oraclecloud.virtualnetwork.createsecuritylist\",\"com.oraclecloud.
virtualnetwork.deletesecuritylist\",\"com.oraclecloud.virtualnetwork.updatese
curitylist\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**11.3** <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.11 Ensure a notification is configured for network security group changes (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when network security groups are created, updated or deleted. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

Network Security Groups control traffic flowing between Virtual Network Cards attached to Compute instances. Monitoring and alerting on changes to Network Security Groups will help in identifying changes these security controls.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `Network Security Group` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Networking` and Event Types: `Network Security Group – Change Compartment`, `Network Security Group – Create`, `Network Security Group - Delete` and `Network Security Group – Update`
5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display name used>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following conditions are present:

```
com.oraclecloud.virtualnetwork.changenetworksecuritygroupcompartment
com.oraclecloud.virtualnetwork.createnetworksecuritygroup
com.oraclecloud.virtualnetwork.deletenetworksecuritygroup
com.oraclecloud.virtualnetwork.updatenetworksecuritygroup
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Networking` in the Service Name Drop-down and selecting `Network Security Group - Change Compartment`, `Network Security Group - Create`, `Network Security Group - Delete` and `Network Security Group - Update`
6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic-name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions": {
        "actions": [
            {
                "actionType": "ONS",
                "isEnabled": true,
                "topicId": "<topic-id>"
            }
        ]
    },
    "condition":
"{\"eventType\":[\"com.oraclecloud.virtualnetwork.changenetworksecuritygroupc
ompartment\",\"com.oraclecloud.virtualnetwork.createnetworksecuritygroup\",\"
com.oraclecloud.virtualnetwork.deletenetworksecuritygroup\",\"com.oraclecloud
.virtualnetwork.updatenetworksecuritygroup\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	4.8 <u>Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

4.12 Ensure a notification is configured for changes to network gateways (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to setup an Event Rule and Notification that gets triggered when Network Gateways are created, updated, deleted, attached, detached, or moved. This recommendation includes Internet Gateways, Dynamic Routing Gateways, Service Gateways, Local Peering Gateways, and NAT Gateways. Event Rules are compartment scoped and will detect events in child compartments, it is recommended to create the Event rule at the root compartment level.

Rationale:

Network Gateways act as routers between VCNs and the Internet, Oracle Services Networks, other VCNS, and on-premise networks. Monitoring and alerting on changes to Network Gateways will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page:
   https://cloud.oracle.com/events/rules
2. Select the `Compartment` that hosts the rules
3. Find and click the `Rule` that handles `Network Gateways` Changes (if any)
4. Click the `Edit Rule` button and verify that the `RuleConditions` section contains a condition for the Service `Networking` and Event Types:

```
DRG – Create
DRG – Delete
DRG – Update
DRG Attachment – Create
DRG Attachment – Delete
DRG Attachment – Update
Internet Gateway – Create
Internet Gateway – Delete
Internet Gateway – Update
Internet Gateway – Change Compartment
Local Peering Gateway – Create
Local Peering Gateway – Delete End
Local Peering Gateway – Update
Local Peering Gateway – Change Compartment
NAT Gateway – Create
NAT Gateway – Delete
NAT Gateway – Update
NAT Gateway – Change Compartment
Service Gateway – Create
Service Gateway – Delete End
Service Gateway – Update
Service Gateway – Attach Service
Service Gateway – Detach Service
Service Gateway – Change Compartment
```

5. Verify that in the `Actions` section the Action Type contains: `Notifications` and that a valid `Topic` is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<display-name>']".{"id:id"} --output table
```

2. List the details of a specific Event Rule based on the OCID of the rule.

```
oci events rule get --rule-id <rule-id>
```

3. In the JSON output locate the Conditions key value pair and verify that the following Conditions are present:

```
com.oraclecloud.virtualnetwork.createdrg
com.oraclecloud.virtualnetwork.deletedrg
com.oraclecloud.virtualnetwork.updatedrg
com.oraclecloud.virtualnetwork.createdrgattachment
com.oraclecloud.virtualnetwork.deletedrgattachment
com.oraclecloud.virtualnetwork.updatedrgattachment
com.oraclecloud.virtualnetwork.changeinternetgatewaycompartment
com.oraclecloud.virtualnetwork.createinternetgateway
com.oraclecloud.virtualnetwork.deleteinternetgateway
com.oraclecloud.virtualnetwork.updateinternetgateway
com.oraclecloud.virtualnetwork.changelocalpeeringgatewaycompartment
com.oraclecloud.virtualnetwork.createlocalpeeringgateway
com.oraclecloud.virtualnetwork.deletelocalpeeringgateway.end
com.oraclecloud.virtualnetwork.updatelocalpeeringgateway
com.oraclecloud.natgateway.changenatgatewaycompartment
com.oraclecloud.natgateway.createnatgateway
com.oraclecloud.natgateway.deletenatgateway
com.oraclecloud.natgateway.updatenatgateway
com.oraclecloud.servicegateway.attachserviceid
com.oraclecloud.servicegateway.changeservicegatewaycompartment
com.oraclecloud.servicegateway.createservicegateway
com.oraclecloud.servicegateway.deleteservicegateway.end
com.oraclecloud.servicegateway.detachserviceid
com.oraclecloud.servicegateway.updateservicegateway
```

4. Verify the value of the `is-enabled` attribute is `true`
5. In the JSON output verify that `actionType` is `ONS` and locate the `topic-id`
6. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id <topic-id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the `Events Service` page: https://cloud.oracle.com/events/rules
2. Select the `compartment` that should host the rule
3. Click `Create Rule`
4. Provide a `Display Name` and `Description`
5. Create a Rule Condition by selecting `Networking` in the Service Name Drop-down and selecting:

```
DRG - Create
DRG - Delete
DRG - Update
DRG Attachment - Create
DRG Attachment - Delete
DRG Attachment - Update
Internet Gateway - Create
Internet Gateway - Delete
Internet Gateway - Update
Internet Gateway - Change Compartment
Local Peering Gateway - Create
Local Peering Gateway - Delete End
Local Peering Gateway - Update
Local Peering Gateway - Change Compartment
NAT Gateway - Create
NAT Gateway - Delete
NAT Gateway - Update
NAT Gateway - Change Compartment
Service Gateway - Create
Service Gateway - Delete End
Service Gateway - Update
Service Gateway - Attach Service
Service Gateway - Detach Service
Service Gateway - Change Compartment
```

6. In the `Actions` section select `Notifications` as Action Type
7. Select the `Compartment` that hosts the Topic to be used.
8. Select the `Topic` to be used
9. Optionally add Tags to the Rule
10. Click `Create Rule`

From CLI:

1. Find the `topic-id` of the topic the Event Rule should use for sending Notifications by using the topic `name` and `Compartment OCID`

```
oci ons topic list --compartment-id <compartment-ocid> --all --query "data
[?name=='<topic_name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

2. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions": {
        "actions": [
            {
                "actionType": "ONS",
                "isEnabled": true,
                "topicId": "<topic-id>"
            }
        ]
    },
    "condition":
"{\"eventType\":\"com.oraclecloud.virtualnetwork.createdrg\",\"com.oraclelou
d.virtualnetwork.deletedrg\",\"com.oraclecloud.virtualnetwork.updatedrg\",\"c
om.oraclecloud.virtualnetwork.createdrgattachment\",\"com.oraclecloud.virtual
network.deletedrgattachment\",\"com.oraclecloud.virtualnetwork.updatedrgattac
hment\",\"com.oraclecloud.virtualnetwork.changeinternetgatewaycompartment\",\
"com.oraclecloud.virtualnetwork.createinternetgateway\",\"com.oraclecloud.vir
tualnetwork.deleteinternetgateway\",\"com.oraclecloud.virtualnetwork.updatein
ternetgateway\",\"com.oraclecloud.virtualnetwork.changelocalpeeringgatewaycom
partment\",\"com.oraclecloud.virtualnetwork.createlocalpeeringgateway\",\"com
.oraclecloud.virtualnetwork.deletelocalpeeringgateway.end\",\"com.oraclecloud
.virtualnetwork.updatelocalpeeringgateway\",\"com.oraclecloud.natgateway.chan
genatgatewaycompartment\",\"com.oraclecloud.natgateway.createnatgateway\",\"c
om.oraclecloud.natgateway.deletenatgateway\",\"com.oraclecloud.natgateway.upd
atenatgateway\",\"com.oraclecloud.servicegateway.attachserviceid\",\"com.orac
lecloud.servicegateway.changeservicegatewaycompartment\",\"com.oraclecloud.se
rvicegateway.createservicegateway\",\"com.oraclecloud.servicegateway.deletese
rvicegateway.end\",\"com.oraclecloud.servicegateway.detachserviceid\",\"com.o
raclecloud.servicegateway.updateservicegateway\"],\"data\":{}}",
    "displayName": "<display-name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "<compartment-ocid>"
}
```

3. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

4. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

Additional Information:

- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.13 Ensure VCN flow logging is enabled for all subnets (Automated)

Profile Applicability:

- Level 2

Description:

VCN flow logs record details about traffic that has been accepted or rejected based on the security list rule.

Rationale:

Enabling VCN flow logs enables you to monitor traffic flowing within your virtual network and can be used to detect anomalous traffic.

Impact:

Enabling VCN flow logs will not affect the performance of your virtual network but it will generate additional use of object storage that should be controlled via object lifecycle management.

By default, VCN flow logs are stored for 30 days in object storage. Users can specify a longer retention period.

Audit:

From Console:

1. Go to the Virtual Cloud Network (VCN) page (https://cloud.oracle.com/networking/vcns)
2. Click on the name of each `VCN`
3. Click on each `subnet` within the `VCN`
4. Under Resources click on `Logs`
5. Verify that there is a log enabled for the `subnet`

From CLI:

1. Find the `OCID` of the specific Subnet based on Display Name and Compartment OCID

```
oci network subnet list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<subnet-display-name>']".{"id:id"} --output table
```

2. Find the `OCID` of the LogGroup used for FlowLogs

```
oci logging log-group list --compartment-id <compartment-ocid> --query "data
[?\"display-name\"=='<log-group-display-name>']"
```

3. List the logs associated with the `OCID` of the subnet.

```
oci logging log list --log-group-id <log-group-ocid> --query "data
[?configuration.source.resource=='<subnet-ocid>']"
```

4. Ensure a `log` is listed for this `subnet`

Remediation:

From Console:
First, if a log group for holding these logs has not already been created, create a log group by the following steps:

1. Go to the Log Groups page (https://cloud.oracle.com/logging/log-groups)
2. Click the `Create Log Groups` button in the middle of the screen.
3. Select the relevant compartment to place these logs.
4. Type a name for the log group in the Name box.
5. Add an optional description in the Description box.
6. Click the `Create` button in the lower left-hand corner.

Second, enable VCN flow logging for your subnet(s) by the following steps:

1. Go to the Logs page (https://cloud.oracle.com/logging/logs)
2. Click the `Enable Service Log` button in the middle of the screen.
3. Select the relevant resource compartment.
4. Select `Virtual Cloud Networks (subnets)` from the Service drop down menu.
5. Select the relevant resource from the resource drop down menu.
6. Select `Flow Logs (all records)` from the Log Category drop down menu.
7. Type a name for your flow logs in the Log Name drop down menu.
8. Click the `Enable Log` button in the lower left-hand corner.

From CLI:

1. Create a log group:

```
oci logging log-group create --compartment-id <compartment-ocid> --display-
name "<display-name>" --description "<description>"
```

The output of the command gives you a work request id. You can query the work request to see the status of the job by issuing the following command:

```
oci logging work-request get --work-request-id <work-request-id>
```

Look for the status filed to be SUCCEEDED.

2. Get the Log group ID, needed for creating the Log:

```
oci logging log-group list --compartment-id <compartment-ocid> --query
'data[?contains("display-name", `'"<display-name>"'`)].id|join(`\n`, @)' --
raw-output
```

3. Create a JSON file called config.json with the following content:

```
{
    "compartment-id":"ocid1.compartment.oc1.......",
    "source": {
        "resource": "ocid1.subnet.oc1.iad.......",
        "service": "flowlogs",
        "source-type": "OCISERVICE",
        "category": "all"
    }
}
```

The compartment-id is the Compartment OCID of where the subnet resource is present.
The resource value is the OCID of subnet for which flowlogs is enabled.

4. Create the Service Log:

```
oci logging log create --log-group-id <log-group-ocid> --display-name
"<display-name>" --log-type SERVICE --is-enabled TRUE --configuration
file://config.json
```

The output of the command gives you a work request id. You can query the work
request to see that status of the job by issuing the following command:

```
 oci logging work-request get --work-request-id <work-request-id>
```

Look for the status filed to be SUCCEEDED.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	🟢	🟠	🔵
v7	12.5 <u>Configure Monitoring Systems to Record Network Packets</u> Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.		🟠	🔵

4.14 Ensure Cloud Guard is enabled in the root compartment of the tenancy (Automated)

Profile Applicability:

- Level 1

Description:

Cloud Guard detects misconfigured resources and insecure activity within a tenancy and provides security administrators with the visibility to resolve these issues. Upon detection, Cloud Guard can suggest, assist, or take corrective actions to mitigate these issues. Cloud Guard should be enabled in the root compartment of your tenancy with the default configuration, activity detectors and responders.

Rationale:

Cloud Guard provides an automated means to monitor a tenancy for resources that are configured in an insecure manner as well as risky network activity from these resources.

Impact:

There is no performance impact when enabling the above described features, but additional IAM policies will be required.

Audit:

From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. View if `Cloud Guard` is enabled

From CLI:

1. Retrieve the `Cloud Guard` status from the console

```
oci cloud-guard configuration get --compartment-id <tenancy-ocid> --query
'data.status'
```

2. Ensure the returned value is "ENABLED"`

Remediation:

From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.

2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Enable Cloud Guard`.
4. Click `Create Policy`.
5. Click `Next`.
6. Under `Reporting Region`, select a region.
7. Under `Compartments To Monitor`, choose `Select Compartment`.
8. Under `Select Compartments`, select the `root` compartment.
9. Under `Configuration Detector Recipe`, select `OCI Configuration Detector Recipe (Oracle Managed)`.
10. Under `Activity Detector Recipe`, select `OCI Activity Detector Recipe (Oracle Managed)`.
11. Click `Enable`.

From CLI:

1. Create OCI IAM Policy for Cloud Guard

```
oci iam policy create --compartment-id '<tenancy-id>' --name
'CloudGuardPolicies' --description 'Cloud Guard Access Policy' --statements
'[
    "allow service cloudguard to read vaults in tenancy",
    "allow service cloudguard to read keys in tenancy",
    "allow service cloudguard to read compartments in tenancy",
    "allow service cloudguard to read tenancies in tenancy",
    "allow service cloudguard to read audit-events in tenancy",
    "allow service cloudguard to read compute-management-family in tenancy",
    "allow service cloudguard to read instance-family in tenancy",
    "allow service cloudguard to read virtual-network-family in tenancy",
    "allow service cloudguard to read volume-family in tenancy",
    "allow service cloudguard to read database-family in tenancy",
    "allow service cloudguard to read object-family in tenancy",
    "allow service cloudguard to read load-balancers in tenancy",
    "allow service cloudguard to read users in tenancy",
    "allow service cloudguard to read groups in tenancy",
    "allow service cloudguard to read policies in tenancy",
    "allow service cloudguard to read dynamic-groups in tenancy",
    "allow service cloudguard to read authentication-policies in tenancy"
    ]'
```

2. Enable Cloud Guard in root compartment

```
oci cloud-guard configuration update --reporting-region '<region-name>' --
compartment-id '<tenancy-id>' --status 'ENABLED'
```

References:

1. https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	8.11 <u>Conduct Audit Log Reviews</u> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

4.15 Ensure a notification is configured for Oracle Cloud Guard problems detected (Automated)

Profile Applicability:

- Level 1

Description:

Cloud Guard detects misconfigured resources and insecure activity within a tenancy and provides security administrators with the visibility to resolve these issues. Upon detection, Cloud Guard generates a Problem. It is recommended to setup an Event Rule and Notification that gets triggered when Oracle Cloud Guard Problems are created, dismissed or remediated. Event Rules are compartment scoped and will detect events in child compartments. It is recommended to create the Event rule at the root compartment level.

Rationale:

Cloud Guard provides an automated means to monitor a tenancy for resources that are configured in an insecure manner as well as risky network activity from these resources. Monitoring and alerting on Problems detected by Cloud Guard will help in identifying changes to the security posture.

Impact:

There is no performance impact when enabling the above described features but depending on the amount of notifications sent per month there may be a cost associated.

Audit:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the Compartment that hosts the rules
3. Find and click the Rule that handles Cloud Guard Changes (if any)
4. Click the Edit Rule button and verify that the RuleConditions section contains a condition for the Service Cloud Guard and Event Types: Detected – Problem, Remediated – Problem, and Dismissed - Problem
5. Verify that in the Actions section the Action Type contains: Notifications and that a valid Topic is referenced.

From CLI:

1. Find the OCID of the specific Event Rule based on Display Name and Compartment OCID

```
oci events rule list --compartment-id=<compartment OCID> --query "data
[?\"display-name\"=='<display name used>']".{"id:id"} --output table
```

1. List the details of a specific Event Rule based on the OCID of the rule.
2. In the JSON output locate the Conditions key-value pair and verify that the following Conditions are present:

```
"com.oraclecloud.cloudguard.problemdetected","com.oraclecloud.cloudguard.prob
lemdismissed","com.oraclecloud.cloudguard.problemremediated"
```

1. Verify the value of the is-enabled attribute is true
2. In the JSON output verify that actionType is ONS and locate the topic-id
3. Verify the correct topic is used by checking the topic name

```
oci ons topic get --topic-id=<topic id> --query data.{"name:name"} --output
table
```

Remediation:

From Console:

1. Go to the Events Service page: https://cloud.oracle.com/events/rules
2. Select the compartment that should host the rule
3. Click Create Rule
4. Provide a Display Name and Description
5. Create a Rule Condition by selecting Cloud Guard in the Service Name Drop-down and selecting: `Detected - Problem`, `Remediated - Problem`, and `Dismissed - Problem`
6. In the Actions section select Notifications as Action Type
7. Select the Compartment that hosts the Topic to be used.
8. Select the Topic to be used
9. Optionally add Tags to the Rule
10. Click Create Rule

From CLI:

1. Find the topic-id of the topic the Event Rule should use for sending Notifications by using the topic name and Compartment OCID

```
oci ons topic list --compartment-id=<compartment OCID> --all --query "data
[?name=='<topic_name>']".{"name:name,topic_id:\"topic-id\""} --output table
```

1. Create a JSON file to be used when creating the Event Rule. Replace topic id, display name, description and compartment OCID.

```
{
    "actions":
    {
        "actions": [
        {
            "actionType": "ONS",
            "isEnabled": true,
            "topicId": "<topic id>"
        }]
    },
    "condition":
"{\"eventType\":[\" com.oraclecloud.cloudguard.problemdetected\",\"
com.oraclecloud.cloudguard.problemdismissed\",\"
com.oraclecloud.cloudguard.problemremediated\"],\"data\":{}}",
    "displayName": "<display name>",
    "description": "<description>",
    "isEnabled": true,
    "compartmentId": "compartment OCID"
}
```

1. Create the actual event rule

```
oci events rule create --from-json file://event_rule.json
```

1. Note in the JSON returned that it lists the parameters specified in the JSON file provided and that there is an OCID provided for the Event Rule

References:

1. https://docs.oracle.com/en-us/iaas/cloud-guard/using/export-notifs-config.htm

Additional Information:

- Your tenancy might have a different Cloud Reporting region than your home region.
- The same Notification topic can be reused by many Event Rules.
- The generated notification will include an eventID that can be used when querying the Audit Logs in case further investigation is required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		🟠	🔵

4.16 Ensure customer created Customer Managed Key (CMK) is rotated at least annually (Automated)

Profile Applicability:

- Level 1

Description:

Oracle Cloud Infrastructure Vault securely stores master encryption keys that protect your encrypted data. You can use the Vault service to rotate keys to generate new cryptographic material. Periodically rotating keys limits the amount of data encrypted by one key version.

Rationale:

Rotating keys annually limits the data encrypted under one key version. Key rotation thereby reduces the risk in case a key is ever compromised.

Audit:

From Console:

1. Login into OCI Console.
2. Select `Identity & Security` from the Services menu.
3. Select `Vault`.
4. Click on the individual Vault under the Name heading.
5. Ensure the date of each Master Encryption key under the `Created` column of the Master Encryption key is no more than 365 days old, and that the key is in the `ENABLED` state
6. Repeat for all Vaults in all compartments

From CLI:

1. Execute the following for each Vault in each compartment

```
oci kms management key list --compartment-id '<compartment-id>' --endpoint
'<management-endpoint-url>' --all --query "data[*].[\"time-
created\",\"display-name\",\"lifecycle-state\"]"
```

2. Ensure the date of the Master Encryption key is no more than 365 days old and is also in the `ENABLED` state.

Remediation:

From Console:

1. Login into OCI Console.

2. Select `Identity & Security` from the Services menu.
3. Select `Vault`.
4. Click on the individual Vault under the Name heading.
5. Click on the menu next to the time created.
6. Click `Rotate Key`

From CLI:

1. Execute the following:

```
oci kms management key rotate --key-id <key-ocid> --endpoint <management-
endpoint-url>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.17 Ensure write level Object Storage logging is enabled for all buckets (Automated)

Profile Applicability:

- Level 2

Description:

Object Storage write logs will log all write requests made to objects in a bucket.

Rationale:

Enabling an Object Storage write log, the `requestAction` property would contain values of `PUT`, `POST`, or `DELETE`. This will provide you more visibility into changes to objects in your buckets.

Impact:

There is no performance impact when enabling the above described features, but will generate additional use of object storage that should be controlled via object lifecycle management.

By default, Object Storage logs are stored for 30 days in object storage. Users can specify a longer retention period.

Audit:

From Console:

1. Log into the OCI console.
2. Select `Storage` from the Services, and click on `Buckets`.
3. Click on the individual Bucket under the Name heading.
4. Click `Logs` from the Resource menu on the left.
5. Click on the slider under Enable Log in row labeled `Write Access Events`.
6. Select the Compartment.
7. Select the Log Group.
8. Enter a `Log Name`.
9. Select a Log Retention.
10. Click `Enable Log`.

From CLI:

1. Find the bucket `name` of the specific bucket.

```
oci os bucket list --compartment-id <compartment-id>
```

2. Find the `OCID` of the Log Group used for `FlowLogs`.

```
oci logging log-group list --compartment-id <compartment-id> --query "data
[?\"display-name\"=='<log-group-name>']"
```

3. List the logs associated with the bucket `name` for this bucket

```
oci logging log list --log-group-id <log-group-id> --query "data
[?configuration.source.resource=='<bucket-name>']"
```

4. Ensure a `log` is listed for this bucket `name`

Remediation:

From Console:
First, if a log group for holding these logs has not already been created, create a log group by the following steps:

1. Go to the Log Groups page https://cloud.oracle.com/logging/log-groups
2. Click the Create Log Groups button in the middle of the screen.
3. Select the relevant compartment to place these logs.
4. Type a name for the log group in the Name box.
5. Add an optional description in the Description box.
6. Click the Create button in the lower left-hand corner.

Second, enable Object Storage write log logging for your bucket(s) by the following steps:

1. Go to the Logs page https://cloud.oracle.com/logging/logs
2. Click the Enable Service Log button in the middle of the screen.
3. Select the relevant resource compartment.
4. Select Object Storage from the Service drop down menu.
5. Select the relevant bucket from the resource drop down menu.
6. Select 'Write Access Events` from the Log Category drop down menu.
7. Type a name for your Object Storage write log in the Log Name drop down menu.
8. Click the `Enable Log` button in the lower left-hand corner.

From CLI:
First, if a log group for holding these logs has not already been created, create a log group by the following steps:

1. Create a log group:

```
oci logging log-group create --compartment-id <compartment-id> --display-name
"<display-name>" --description "<description>"
```

The output of the command gives you a work request id. You can query the work request to see the status of the job by issuing the following command:

```
oci logging work-request get --work-request-id <work-request-id>
```

Look for status filed to be SUCCEEDED.
Second, enable Object Storage write log logging for your bucket(s) by the following steps:

2. Get the Log group ID needed for creating the Log:

```
oci logging log-group list --compartment-id <compartment-id> --query
'data[?contains("display-name", `'"<display-name>"'`)].id|join(`\n`, @)' --
raw-output
```

3. Create a JSON file called config.json with the following content:

```
{
    "compartment-id":"<compartment-id>",
    "source": {
        "resource": "<bucket-name.",
        "service": "ObjectStorage",
        "source-type": "OCISERVICE",
        "category": "write"
    }
}
```

The compartment-id is the Compartment OCID of where the bucket is exists. The resource value is the bucket name.

4. Create the Service Log:

```
oci logging log create --log-group-id <log-group-id> --display-name
"<display-name>" --log-type SERVICE --is-enabled TRUE --configuration
file://config.json
```

The output of the command gives you a work request id. You can query the work request to see that status of the job by issuing the following command:

```
oci logging work-request get --work-request-id <work-request-id>
```

Look for the status filed to be SUCCEEDED.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5 Storage

This section contains recommendations for configuring object, file and block storage.

5.1 Object Storage

This section contains recommendations for configuring storage related options.

5.1.1 Ensure no Object Storage buckets are publicly visible. (Automated)

Profile Applicability:

- Level 1

Description:

A bucket is a logical container for storing objects. It is associated with a single compartment that has policies that determine what action a user can perform on a bucket and on all the objects in the bucket. By Default a newly created bucket is private. It is recommended that no bucket be publicly accessible.

Rationale:

Removing unfettered reading of objects in a bucket reduces an organization's exposure to data loss.

Impact:

For updating an existing bucket, care should be taken to ensure objects in the bucket can be accessed through either IAM policies or pre-authenticated requests.

Audit:

From Console:

1. Login into the OCI Console
2. Click in the search bar at the top of the screen.
3. Type `Advanced Resource Query` and click `enter`.
4. Click the `Advanced Resource Query` button in the upper right of the screen.
5. Enter the following query in the query box:

```
query
bucket resources
where
        (publicAccessType == 'ObjectRead') || (publicAccessType ==
'ObjectReadWithoutList')
```

6. Ensure query returns no results

From CLI:

1. Execute the following command:

```
oci search resource structured-search --query-text "query
bucket resources
where
(publicAccessType == 'ObjectRead') || (publicAccessType ==
'ObjectReadWithoutList')"
```

2. Ensure query returns no results

Cloud Guard
To Enable Cloud Guard Auditing:
Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.
From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find Bucket is public in the Detector Rules column.
6. Verify that the Bucket is public Detector Rule is Enabled.

From CLI:

1. Verify the Bucket is public Detector Rule in Cloud Guard is enabled to generate Problems if Object Storage Buckets are configured to be accessible over the public Internet with the following command:

```
oci cloud-guard detector-recipe-detector-rule get --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id BUCKET_IS_PUBLIC
```

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each `bucket` in the returned results, click the Bucket `Display Name`
3. Click `Edit Visibility`
4. Select `Private`
5. Click `Save Changes`

From CLI:

1. Follow the audit procedure
2. For each of the `buckets` identified, execute the following command:

```
oci os bucket update --bucket-name <bucket-name> --public-access-type
NoPublicAccess
```

Default Value:

Private

References:

1. https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/managingbuckets.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3** <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6** <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.1.2 Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK). (Automated)

Profile Applicability:

- Level 2

Description:

Oracle Object Storage buckets support encryption with a Customer Managed Key (CMK). By default, Object Storage buckets are encrypted with an Oracle managed key.

Rationale:

Encryption of Object Storage buckets with a Customer Managed Key (CMK) provides an additional level of security on your data by allowing you to manage your own encryption key lifecycle management for the bucket.

Impact:

Encrypting with a Customer Managed Keys requires a Vault and a Customer Master Key. In addition, you must authorize Object Storage service to use keys on your behalf.

Required Policy:

```
Allow service objectstorage-<region_name>,  to use keys in compartment
<compartment-id> where target.key.id = '<key_OCID>'
```

Audit:

From Console:

1. Go to https://cloud.oracle.com/object-storage/buckets

2. Click on an individual bucket under the Name heading.
3. Ensure that the `Encryption Key` is not set to `Oracle managed key`.
4. Repeat for each compartment

From CLI:

1. Execute the following command

```
oci os bucket get --bucket-name <bucket-name>
```

2. Ensure `kms-key-id` is not `null`

Cloud Guard

To Enable Cloud Guard Auditing:

Ensure Cloud Guard is enabled in the root compartment of the tenancy. For more information about enabling Cloud Guard, please look at the instructions included in Recommendation 3.15.

From Console:

1. Type `Cloud Guard` into the Search box at the top of the Console.
2. Click `Cloud Guard` from the "Services" submenu.
3. Click `Detector Recipes` in the Cloud Guard menu.
4. Click `OCI Configuration Detector Recipe (Oracle Managed)` under the Recipe Name column.
5. Find Object Storage bucket is encrypted with Oracle-managed key in the Detector Rules column.
6. Verify that the Object Storage bucket is encrypted with Oracle-managed key Detector Rule is Enabled.

From CLI:

1. Verify the Object Storage bucket is encrypted with Oracle-managed key Detector Rule in Cloud Guard is enabled to generate Problems if Object Storage Buckets are configured without a customer managed key with the following command:

```
oci cloud-guard detector-recipe-detector-rule get --detector-recipe-id
<insert detector recipe ocid> --detector-rule-id
BUCKET_ENCRYPTED_WITH_ORACLE_MANAGED_KEY
```

Remediation:

From Console:

1. Go to https://cloud.oracle.com/object-storage/buckets

2. Click on an individual bucket under the Name heading.
3. Click `Assign` next to `Encryption Key: Oracle managed key`.
4. Select a `Vault`
5. Select a `Master Encryption Key`
6. Click `Assign`

From CLI:

1. Execute the following command

```
oci os bucket update --bucket-name <bucket-name> --kms-key-id <master-
encryption-key-id>
```

Default Value:

`Oracle Managed Key` for Encryption

References:

1. https://docs.oracle.com/en/solutions/oci-best-practices/protect-data-rest1.html#GUID-9C0F713E-4C67-43C6-80CA-525A6AB221F1
2. https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/encryption.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.11** <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		🟠	🔵
v7	**14.8** <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			🔵

5.1.3 Ensure Versioning is Enabled for Object Storage Buckets (Automated)

Profile Applicability:

- Level 2

Description:

A bucket is a logical container for storing objects. Object versioning is enabled at the bucket level and is disabled by default upon creation. Versioning directs Object Storage to automatically create an object version each time a new object is uploaded, an existing object is overwritten, or when an object is deleted. You can enable object versioning at bucket creation time or later.

Rationale:

Versioning object storage buckets provides for additional integrity of your data. Management of data integrity is critical to protecting and accessing protected data. Some customers want to identify object storage buckets without versioning in order to apply their own data lifecycle protection and management policy.

Audit:

From Console:

1. Login to OCI Console.
2. Select `Storage` from the Services menu.
3. Select `Buckets` from under the `Object Storage & Archive Storage` section.
4. Click on an individual bucket under the Name heading.
5. Ensure that the `Object Versioning` is set to Enabled.
6. Repeat for each compartment

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
      for compid in `oci iam compartment list --compartment-id-in-subtree
TRUE 2>/dev/null | jq -r '.data[] | .id'`
       do
          for bkt in `oci os bucket list --compartment-id $compid --region
$region 2>/dev/null | jq -r '.data[] | .name'`
              do
              output=`oci os bucket get --bucket-name $bkt --region $region
2>/dev/null | jq -r '.data | select(."versioning" == "Disabled").name'`
              if [ ! -z "$output" ]; then echo $output; fi
              done
       done
   done
```

2. Ensure no results are returned.

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each bucket in the returned results, click the Bucket Display Name
3. Click `Edit` next to `Object Versioning: Disabled`
4. Click `Enable Versioning`

From CLI:

1. Follow the audit procedure
2. For each of the buckets identified, execute the following command:

```
oci os bucket update --bucket-name <bucket name> --versioning Enabled
```

Default Value:

Object versioning is `Disabled`.

References:

1. https://docs.oracle.com/en-us/iaas/Content/Object/Tasks/usingversioning.htm
2. https://docs.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/Bucket/GetBucket

5.2 Block Volumes

This section contains recommendations for configuring block volume related options.

5.2.1 Ensure Block Volumes are encrypted with Customer Managed Keys (CMK). (Automated)

Profile Applicability:

- Level 2

Description:

Oracle Cloud Infrastructure Block Volume service lets you dynamically provision and manage block storage volumes. By default, the Oracle service manages the keys that encrypt block volumes. Block Volumes can also be encrypted using a customer managed key.

Terminated Block Volumes cannot be recovered and any data on a terminated volume is permanently lost. However, Block Volumes can exist in a terminated state within the OCI Portal and CLI for some time after deleting. As such, any Block Volumes in this state should not be considered when assessing this policy.

Rationale:

Encryption of block volumes provides an additional level of security for your data. Management of encryption keys is critical to protecting and accessing protected data. Customers should identify block volumes encrypted with Oracle service managed keys in order to determine if they want to manage the keys for certain volumes and then apply their own key lifecycle management to the selected block volumes.

Impact:

Encrypting with a Customer Managed Key requires a Vault and a Customer Master Key. In addition, you must authorize the Block Volume service to use the keys you create. Required IAM Policy:

```
Allow service blockstorage to use keys in compartment <compartment-id> where
target.key.id = '<key_OCID>'
```

Audit:

From Console:

1. Login to the OCI Console.
2. Click the search bar at the top of the screen.
3. Type 'Advanced Resource Query' and press return.
4. Click `Advanced resource query`.
5. Enter the following query in the query box:

```
query volume resources
```

6. For each block volume returned, click the link under `Display name`.
7. Ensure the value for `Encryption Key` is not `Oracle-managed key`.
8. Repeat for other subscribed regions.

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
do
  for compid in `oci iam compartment list --compartment-id-in-subtree TRUE
2>/dev/null | jq -r '.data[] | .id'`
  do
    for bvid in `oci bv volume list --compartment-id $compid --region $region
2>/dev/null | jq -r '.data[] | select(."kms-key-id" == null).id'`
    do
      output=`oci bv volume get --volume-id $bvid --region $region --
query=data.{"name:\"display-name\","id:id""} --output table 2>/dev/null`
      if [ ! -z "$output" ]; then echo $output; fi
    done
  done
done
```

2. Ensure the query returns no results.

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each block volume returned, click the link under Display name.
3. If the value for `Encryption Key` is `Oracle-managed key`, click `Assign` next to `Oracle-managed key`.
4. Select a `Vault Compartment` and `Vault`.
5. Select a `Master Encryption Key Compartment` and `Master Encryption key`.
6. Click `Assign`.

From CLI:

1. Follow the audit procedure.
2. For each `boot volume` identified, get the OCID.
3. Execute the following command:

```
oci bv volume-kms-key update –volume-id <volume OCID> --kms-key-id <kms key
OCID>
```

References:

1. https://docs.oracle.com/en/solutions/oci-best-practices/protect-data-rest1.html#GUID-BA1F5A20-8C78-49E3-8183-927F0CC6F6CC
2. https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/overview.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

5.2.2 Ensure boot volumes are encrypted with Customer Managed Key (CMK). (Automated)

Profile Applicability:

- Level 2

Description:

When you launch a virtual machine (VM) or bare metal instance based on a platform image or custom image, a new boot volume for the instance is created in the same compartment. That boot volume is associated with that instance until you terminate the instance. By default, the Oracle service manages the keys that encrypt this boot volume. Boot Volumes can also be encrypted using a customer managed key.

Rationale:

Encryption of boot volumes provides an additional level of security for your data. Management of encryption keys is critical to protecting and accessing protected data. Customers should identify boot volumes encrypted with Oracle service managed keys in order to determine if they want to manage the keys for certain boot volumes and then apply their own key lifecycle management to the selected boot volumes.

Impact:

Encrypting with a Customer Managed Keys requires a Vault and a Customer Master Key. In addition, you must authorize the Boot Volume service to use the keys you create. Required IAM Policy:

```
Allow service Bootstorage to use keys in compartment <compartment-id> where
target.key.id = '<key_OCID>'
```

Audit:

From Console:

1. Login into the OCI Console
2. Click in the search bar, top of the screen.
3. Type Advanced Resource Query and click enter.
4. Click the `Advanced Resource Query` button in the upper right of the screen.
5. Enter the following query in the query box:

```
query bootvolume resources
```

6. For each boot volume returned click on the link under `Display name`
7. Ensure `Encryption Key` does not say `Oracle managed key`
8. Repeat for other subscribed regions

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
      for bvid in `oci search resource structured-search --region $region --
query-text "query bootvolume resources" 2>/dev/null | jq -r '.data.items[] |
.identifier'`
        do
          output=`oci bv boot-volume get --boot-volume-id $bvid  2>/dev/null
| jq -r '.data | select(."kms-key-id" == null).id'`
           if [ ! -z "$output" ]; then echo $output; fi
        done
   done
```

2. Ensure query returns no results.

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each Boot Volume in the returned results, click the Boot Volume name
3. Click `Assign` next to `Encryption Key`
4. Select the `Vault Compartment` and `Vault`
5. Select the `Master Encryption Key Compartment` and `Master Encryption key`
6. Click `Assign`

From CLI:

1. Follow the audit procedure.
2. For each `boot volume` identified get its OCID. Execute the following command:

```
oci bv boot-volume-kms-key update --boot-volume-id <Boot Volume OCID> --kms-
key-id <KMS Key OCID>
```

References:

1. https://docs.oracle.com/en/solutions/oci-best-practices/protect-data-rest1.html#GUID-BA1F5A20-8C78-49E3-8183-927F0CC6F6CC

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.11 Encrypt Sensitive Data at Rest** Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		🟠	🔵
v7	**14.8 Encrypt Sensitive Information at Rest** Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			🔵

5.3 File Storage Service

This section contains recommendations for configuring File Storage Service related options.

5.3.1 Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Oracle Cloud Infrastructure File Storage service (FSS) provides a durable, scalable, secure, enterprise-grade network file system. By default, the Oracle service manages the keys that encrypt FSS file systems. FSS file systems can also be encrypted using a customer managed key.

Rationale:

Encryption of FSS systems provides an additional level of security for your data. Management of encryption keys is critical to protecting and accessing protected data. Customers should identify FSS file systems that are encrypted with Oracle service managed keys in order to determine if they want to manage the keys for certain FSS file systems and then apply their own key lifecycle management to the selected FSS file systems.

Impact:

Encrypting with a Customer Managed Keys requires a Vault and a Customer Master Key. In addition, you must authorize the File Storage service to use the keys you create. Required IAM Policy:

```
Allow service FssOc1Prod to use keys in compartment <compartment-id> where
target.key.id = '<key_OCID>'
```

Audit:

From Console:

1. Login into the OCI Console
2. Click in the search bar, top of the screen.
3. Type Advanced Resource Query and click enter.
4. Click the `Advanced Resource Query` button in the upper right of the screen.
5. Enter the following query in the query box:

```
query filesystem resources
```

6. For each file storage system returned click on the link under `Display name`
7. Ensure `Encryption Key` does not say `Oracle-managed key`
8. Repeat for other subscribed regions

From CLI:

1. Execute the following command:

```
for region in `oci iam region list | jq -r '.data[] | .name'`;
   do
      for fssid in `oci search resource structured-search --region $region -
-query-text "query filesystem resources" 2>/dev/null | jq -r '.data.items[] |
.identifier'`
        do
           output=`oci fs file-system get --file-system-id $fssid --region
$region 2>/dev/null | jq -r '.data | select(."kms-key-id" == "").id'`
            if [ ! -z "$output" ]; then echo $output; fi
        done
   done
```

2. Ensure query returns no results

Remediation:

From Console:

1. Follow the audit procedure above.
2. For each File Storage System in the returned results, click the File System Storage
3. Click `Edit` next to `Encryption Key`
4. Select `Encrypt using customer-managed keys`
5. Select the `Vault Compartment` and `Vault`
6. Select the `Master Encryption Key Compartment` and `Master Encryption key`
7. Click `Save Changes`

From CLI:

1. Follow the audit procedure.
2. For each `File Storage System` identified get its OCID. Execute the following command:

```
oci bv volume-kms-key update –volume-id <volume OCID> --kms-key-id <kms key
OCID>
```

References:

1. https://docs.oracle.com/en/solutions/oci-best-practices/protect-data-rest1.html#GUID-BA1F5A20-8C78-49E3-8183-927F0CC6F6CC
2. https://docs.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.11** <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		🟠	🔵
v7	**14.8** <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			🔵

6 Asset Management

This section contains recommendations for managing the creation of resources within a tenancy.

6.1 Create at least one compartment in your tenancy to store cloud resources (Automated)

Profile Applicability:

- Level 1

Description:

When you sign up for Oracle Cloud Infrastructure, Oracle creates your tenancy, which is the root compartment that holds all your cloud resources. You then create additional compartments within the tenancy (root compartment) and corresponding policies to control access to the resources in each compartment.

Compartments allow you to organize and control access to your cloud resources. A compartment is a collection of related resources (such as instances, databases, virtual cloud networks, block volumes) that can be accessed only by certain groups that have been given permission by an administrator.

Rationale:

Compartments are a logical group that adds an extra layer of isolation, organization and authorization making it harder for unauthorized users to gain access to OCI resources.

Impact:

Once the compartment is created an OCI IAM policy must be created to allow a group to resources in the compartment otherwise only group with tenancy access will have access.

Audit:

From Console:

1. Login into the OCI Console.
2. Click in the search bar, top of the screen.
3. Type `Advanced Resource Query` and hit `enter`.
4. Click the `Advanced Resource Query` button in the upper right of the screen.
5. Enter the following query in the query box:

```
query
  compartment resources
where
(compartmentId='<tenancy-id>' && lifecycleState='ACTIVE')
```

6. Ensure query returns at least one compartment in addition to the `ManagedCompartmentForPaaS` compartment

---

From CLI:

1. Execute the following command

```
oci search resource structured-search --query-text "query
   compartment resources
where
(compartmentId='<tenancy-id>' && lifecycleState='ACTIVE')"
```

2. Ensure `items` are returned.

Remediation:

From Console:

1. Login to OCI Console.
2. Select `Identity` from the Services menu.
3. Select `Compartments` from the Identity menu.
4. Click `Create Compartment`
5. Enter a `Name`
6. Enter a `Description`
7. Select the root compartment as the `Parent Compartment`
8. Click `Create Compartment`

From CLI:

1. Execute the following command

```
oci iam compartment create --compartment-id '<tenancy-id>' --name
'<compartment-name>' --description '<compartment description>'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 <u>Establish and Maintain a Data Management Process</u> Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

6.2 Ensure no resources are created in the root compartment (Automated)

Profile Applicability:

- Level 1

Description:

When you create a cloud resource such as an instance, block volume, or cloud network, you must specify to which compartment you want the resource to belong. Placing resources in the root compartment makes it difficult to organize and isolate those resources.

Rationale:

Placing resources into a compartment will allow you to organize and have more granular access controls to your cloud resources.

Impact:

Placing a resource in a compartment will impact how you write policies to manage access and organize that resource.

Audit:

From Console:

1. Login into the OCI Console.
2. Click in the search bar, top of the screen.
3. Type `Advance Resource Query` and hit `enter`.
4. Click the `Advanced Resource Query` button in the upper right of the screen.
5. Enter the following query into the query box:

```
query
  VCN, instance, volume, filesystem, bucket,
autonomousdatabase, database, dbsystem resources
    where compartmentId = '<tenancy-id>'
```

6. Ensure query returns no results.

From CLI:

1. Execute the following command:

```
oci search resource structured-search --query-text "query
  VCN, instance, volume, filesystem, bucket,
autonomousdatabase, database, dbsystem resources
    where compartmentId = '<tenancy-id>'"
```

2. Ensure query return no results.

Remediation:

From Console:

1. Follow audit procedure above.
2. For each item in the returned results, click the item name.
3. Then select Move Resource or More Actions then Move Resource.
4. Select a compartment that is not the root compartment in CHOOSE NEW COMPARTMENT.
5. Click Move Resource.

From CLI:

1. Follow the audit procedure above.
2. For each bucket item execute the below command:

```
oci os bucket update --bucket-name <bucket-name> --compartment-id <not root
compartment-id>
```

3. For other resources use the change-compartment command for the resource type:

```
oci <service-command> <resource-command> change-compartment --<item-id>
<item-id> --compartment-id <not root compartment-id>
i. Example for an Autonomous Database:
oci db autonomous-database change-compartment --autonomous-database-id
<autonmous-database-id> --compartment-id <not root compartment-id>
```

Additional Information:

https://docs.cloud.oracle.com/en-
us/iaas/Content/GSG/Concepts/settinguptenancy.htm#Understa

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**14.1 Segment the Network Based on Sensitivity** Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Identity and Access Management**		
1.1	Ensure service level admins are created to manage resources of particular service (Manual)	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group (Automated)	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group (Automated)	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater (Automated)	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days (Manual)	☐	☐
1.6	Ensure IAM password policy prevents password reuse (Manual)	☐	☐
1.7	Ensure MFA is enabled for all users with a console password (Automated)	☐	☐
1.8	Ensure user API keys rotate within 90 days (Automated)	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days (Automated)	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less (Automated)	☐	☐
1.11	Ensure user IAM Database Passwords rotate within 90 days (Manual)	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.13	Ensure all OCI IAM user accounts have a valid and current email address (Manual)	☐	☐
1.14	Ensure Instance Principal authentication is used for OCI instances, OCI Cloud Databases and OCI Functions to access OCI resources. (Manual)	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage. (Manual)	☐	☐
2	**Networking**		
2.1	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22 (Automated)	☐	☐
2.2	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389 (Automated)	☐	☐
2.3	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22 (Automated)	☐	☐
2.4	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389 (Automated)	☐	☐
2.5	Ensure the default security list of every VCN restricts all traffic except ICMP (Automated)	☐	☐
2.6	Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources. (Manual)	☐	☐
2.7	Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network. (Manual)	☐	☐
2.8	Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network (Manual)	☐	☐
3	**Compute**		
3.1	Ensure Compute Instance Legacy Metadata service endpoint is disabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.2	Ensure Secure Boot is enabled on Compute Instance (Automated)	☐	☐
3.3	Ensure In-transit Encryption is enabled on Compute Instance (Automated)	☐	☐
4	**Logging and Monitoring**		
4.1	Ensure default tags are used on resources (Automated)	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts (Automated)	☐	☐
4.3	Ensure a notification is configured for Identity Provider changes (Automated)	☐	☐
4.4	Ensure a notification is configured for IdP group mapping changes (Automated)	☐	☐
4.5	Ensure a notification is configured for IAM group changes (Automated)	☐	☐
4.6	Ensure a notification is configured for IAM policy changes (Automated)	☐	☐
4.7	Ensure a notification is configured for user changes (Automated)	☐	☐
4.8	Ensure a notification is configured for VCN changes (Automated)	☐	☐
4.9	Ensure a notification is configured for changes to route tables (Automated)	☐	☐
4.10	Ensure a notification is configured for security list changes (Automated)	☐	☐
4.11	Ensure a notification is configured for network security group changes (Automated)	☐	☐
4.12	Ensure a notification is configured for changes to network gateways (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.13	Ensure VCN flow logging is enabled for all subnets (Automated)	☐	☐
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy (Automated)	☐	☐
4.15	Ensure a notification is configured for Oracle Cloud Guard problems detected (Automated)	☐	☐
4.16	Ensure customer created Customer Managed Key (CMK) is rotated at least annually (Automated)	☐	☐
4.17	Ensure write level Object Storage logging is enabled for all buckets (Automated)	☐	☐
5	**Storage**		
5.1	**Object Storage**		
5.1.1	Ensure no Object Storage buckets are publicly visible. (Automated)	☐	☐
5.1.2	Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK). (Automated)	☐	☐
5.1.3	Ensure Versioning is Enabled for Object Storage Buckets (Automated)	☐	☐
5.2	**Block Volumes**		
5.2.1	Ensure Block Volumes are encrypted with Customer Managed Keys (CMK). (Automated)	☐	☐
5.2.2	Ensure boot volumes are encrypted with Customer Managed Key (CMK). (Automated)	☐	☐
5.3	**File Storage Service**		
5.3.1	Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK) (Automated)	☐	☐
6	**Asset Management**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1	Create at least one compartment in your tenancy to store cloud resources (Automated)	☐	☐
6.2	Ensure no resources are created in the root compartment (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure service level admins are created to manage resources of particular service	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days	☐	☐
1.8	Ensure user API keys rotate within 90 days	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users	☐	☐
1.14	Ensure Instance Principal authentication is used for OCI instances, OCI Cloud Databases and OCI Functions to access OCI resources.	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage.	☐	☐
4.1	Ensure default tags are used on resources	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts	☐	☐
4.4	Ensure a notification is configured for IdP group mapping changes	☐	☐
4.13	Ensure VCN flow logging is enabled for all subnets	☐	☐
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy	☐	☐
4.17	Ensure write level Object Storage logging is enabled for all buckets	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1	Ensure no Object Storage buckets are publicly visible.	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure service level admins are created to manage resources of particular service	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days	☐	☐
1.6	Ensure IAM password policy prevents password reuse	☐	☐
1.7	Ensure MFA is enabled for all users with a console password	☐	☐
1.8	Ensure user API keys rotate within 90 days	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users	☐	☐
1.13	Ensure all OCI IAM user accounts have a valid and current email address	☐	☐
1.14	Ensure Instance Principal authentication is used for OCI instances, OCI Cloud Databases and OCI Functions to access OCI resources.	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage.	☐	☐
2.1	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22	☐	☐
2.2	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.3	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.5	Ensure the default security list of every VCN restricts all traffic except ICMP	☐	☐
2.6	Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources.	☐	☐
2.7	Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network.	☐	☐
2.8	Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network	☐	☐
4.1	Ensure default tags are used on resources	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts	☐	☐
4.3	Ensure a notification is configured for Identity Provider changes	☐	☐
4.4	Ensure a notification is configured for IdP group mapping changes	☐	☐
4.5	Ensure a notification is configured for IAM group changes	☐	☐
4.6	Ensure a notification is configured for IAM policy changes	☐	☐
4.7	Ensure a notification is configured for user changes	☐	☐
4.8	Ensure a notification is configured for VCN changes	☐	☐
4.9	Ensure a notification is configured for changes to route tables	☐	☐
4.10	Ensure a notification is configured for security list changes	☐	☐
4.11	Ensure a notification is configured for network security group changes	☐	☐
4.12	Ensure a notification is configured for changes to network gateways	☐	☐
4.13	Ensure VCN flow logging is enabled for all subnets	☐	☐
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.17	Ensure write level Object Storage logging is enabled for all buckets	☐	☐
5.1.1	Ensure no Object Storage buckets are publicly visible.	☐	☐
6.2	Ensure no resources are created in the root compartment	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure service level admins are created to manage resources of particular service	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days	☐	☐
1.6	Ensure IAM password policy prevents password reuse	☐	☐
1.7	Ensure MFA is enabled for all users with a console password	☐	☐
1.8	Ensure user API keys rotate within 90 days	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users	☐	☐
1.13	Ensure all OCI IAM user accounts have a valid and current email address	☐	☐
1.14	Ensure Instance Principal authentication is used for OCI instances, OCI Cloud Databases and OCI Functions to access OCI resources.	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage.	☐	☐
2.1	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22	☐	☐
2.2	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.3	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.5	Ensure the default security list of every VCN restricts all traffic except ICMP	☐	☐
2.6	Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources.	☐	☐
2.7	Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network.	☐	☐
2.8	Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network	☐	☐
4.1	Ensure default tags are used on resources	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts	☐	☐
4.3	Ensure a notification is configured for Identity Provider changes	☐	☐
4.4	Ensure a notification is configured for IdP group mapping changes	☐	☐
4.5	Ensure a notification is configured for IAM group changes	☐	☐
4.6	Ensure a notification is configured for IAM policy changes	☐	☐
4.7	Ensure a notification is configured for user changes	☐	☐
4.8	Ensure a notification is configured for VCN changes	☐	☐
4.9	Ensure a notification is configured for changes to route tables	☐	☐
4.10	Ensure a notification is configured for security list changes	☐	☐
4.11	Ensure a notification is configured for network security group changes	☐	☐
4.12	Ensure a notification is configured for changes to network gateways	☐	☐
4.13	Ensure VCN flow logging is enabled for all subnets	☐	☐
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.17	Ensure write level Object Storage logging is enabled for all buckets	☐	☐
5.1.1	Ensure no Object Storage buckets are publicly visible.	☐	☐
5.1.2	Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK).	☐	☐
5.2.1	Ensure Block Volumes are encrypted with Customer Managed Keys (CMK).	☐	☐
5.2.2	Ensure boot volumes are encrypted with Customer Managed Key (CMK).	☐	☐
5.3.1	Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK)	☐	☐
6.2	Ensure no resources are created in the root compartment	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.11	Ensure user IAM Database Passwords rotate within 90 days	☐	☐
3.1	Ensure Compute Instance Legacy Metadata service endpoint is disabled	☐	☐
3.2	Ensure Secure Boot is enabled on Compute Instance	☐	☐
3.3	Ensure In-transit Encryption is enabled on Compute Instance	☐	☐
4.15	Ensure a notification is configured for Oracle Cloud Guard problems detected	☐	☐
4.16	Ensure customer created Customer Managed Key (CMK) is rotated at least annually	☐	☐
5.1.3	Ensure Versioning is Enabled for Object Storage Buckets	☐	☐
6.1	Create at least one compartment in your tenancy to store cloud resources	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure service level admins are created to manage resources of particular service	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days	☐	☐
1.6	Ensure IAM password policy prevents password reuse	☐	☐
1.7	Ensure MFA is enabled for all users with a console password	☐	☐
1.8	Ensure user API keys rotate within 90 days	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less	☐	☐
1.11	Ensure user IAM Database Passwords rotate within 90 days	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users	☐	☐
1.13	Ensure all OCI IAM user accounts have a valid and current email address	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage.	☐	☐
2.1	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22	☐	☐
2.2	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.3	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.6	Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources.	☐	☐
2.7	Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network.	☐	☐
2.8	Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network	☐	☐
3.2	Ensure Secure Boot is enabled on Compute Instance	☐	☐
4.1	Ensure default tags are used on resources	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts	☐	☐
4.3	Ensure a notification is configured for Identity Provider changes	☐	☐
4.5	Ensure a notification is configured for IAM group changes	☐	☐
4.6	Ensure a notification is configured for IAM policy changes	☐	☐
4.7	Ensure a notification is configured for user changes	☐	☐
4.8	Ensure a notification is configured for VCN changes	☐	☐
4.9	Ensure a notification is configured for changes to route tables	☐	☐
4.10	Ensure a notification is configured for security list changes	☐	☐
4.11	Ensure a notification is configured for network security group changes	☐	☐
4.12	Ensure a notification is configured for changes to network gateways	☐	☐
4.13	Ensure VCN flow logging is enabled for all subnets	☐	☐
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy	☐	☐
4.15	Ensure a notification is configured for Oracle Cloud Guard problems detected	☐	☐
4.17	Ensure write level Object Storage logging is enabled for all buckets	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
5.1.1	Ensure no Object Storage buckets are publicly visible.	☐	☐
6.1	Create at least one compartment in your tenancy to store cloud resources	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure service level admins are created to manage resources of particular service	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days	☐	☐
1.6	Ensure IAM password policy prevents password reuse	☐	☐
1.7	Ensure MFA is enabled for all users with a console password	☐	☐
1.8	Ensure user API keys rotate within 90 days	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less	☐	☐
1.11	Ensure user IAM Database Passwords rotate within 90 days	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users	☐	☐
1.13	Ensure all OCI IAM user accounts have a valid and current email address	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage.	☐	☐
2.1	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22	☐	☐
2.2	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.3	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.4	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.5	Ensure the default security list of every VCN restricts all traffic except ICMP	☐	☐
2.6	Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources.	☐	☐
2.7	Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network.	☐	☐
2.8	Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network	☐	☐
3.1	Ensure Compute Instance Legacy Metadata service endpoint is disabled	☐	☐
3.2	Ensure Secure Boot is enabled on Compute Instance	☐	☐
4.1	Ensure default tags are used on resources	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts	☐	☐
4.3	Ensure a notification is configured for Identity Provider changes	☐	☐
4.5	Ensure a notification is configured for IAM group changes	☐	☐
4.6	Ensure a notification is configured for IAM policy changes	☐	☐
4.7	Ensure a notification is configured for user changes	☐	☐
4.8	Ensure a notification is configured for VCN changes	☐	☐
4.9	Ensure a notification is configured for changes to route tables	☐	☐
4.10	Ensure a notification is configured for security list changes	☐	☐
4.11	Ensure a notification is configured for network security group changes	☐	☐
4.12	Ensure a notification is configured for changes to network gateways	☐	☐
4.13	Ensure VCN flow logging is enabled for all subnets	☐	☐
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.15	Ensure a notification is configured for Oracle Cloud Guard problems detected	☐	☐
4.17	Ensure write level Object Storage logging is enabled for all buckets	☐	☐
5.1.1	Ensure no Object Storage buckets are publicly visible.	☐	☐
5.1.2	Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK).	☐	☐
5.2.1	Ensure Block Volumes are encrypted with Customer Managed Keys (CMK).	☐	☐
5.2.2	Ensure boot volumes are encrypted with Customer Managed Key (CMK).	☐	☐
5.3.1	Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK)	☐	☐
6.1	Create at least one compartment in your tenancy to store cloud resources	☐	☐
6.2	Ensure no resources are created in the root compartment	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure service level admins are created to manage resources of particular service	☐	☐
1.2	Ensure permissions on all resources are given only to the tenancy administrator group	☐	☐
1.3	Ensure IAM administrators cannot update tenancy Administrators group	☐	☐
1.4	Ensure IAM password policy requires minimum length of 14 or greater	☐	☐
1.5	Ensure IAM password policy expires passwords within 365 days	☐	☐
1.6	Ensure IAM password policy prevents password reuse	☐	☐
1.7	Ensure MFA is enabled for all users with a console password	☐	☐
1.8	Ensure user API keys rotate within 90 days	☐	☐
1.9	Ensure user customer secret keys rotate every 90 days	☐	☐
1.10	Ensure user auth tokens rotate within 90 days or less	☐	☐
1.11	Ensure user IAM Database Passwords rotate within 90 days	☐	☐
1.12	Ensure API keys are not created for tenancy administrator users	☐	☐
1.13	Ensure all OCI IAM user accounts have a valid and current email address	☐	☐
1.14	Ensure Instance Principal authentication is used for OCI instances, OCI Cloud Databases and OCI Functions to access OCI resources.	☐	☐
1.15	Ensure storage service-level admins cannot delete resources they manage.	☐	☐
2.1	Ensure no security lists allow ingress from 0.0.0.0/0 to port 22	☐	☐
2.2	Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.3	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22	☐	☐
2.4	Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389	☐	☐
2.5	Ensure the default security list of every VCN restricts all traffic except ICMP	☐	☐
2.6	Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources.	☐	☐
2.7	Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network.	☐	☐
2.8	Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network	☐	☐
3.1	Ensure Compute Instance Legacy Metadata service endpoint is disabled	☐	☐
3.2	Ensure Secure Boot is enabled on Compute Instance	☐	☐
4.1	Ensure default tags are used on resources	☐	☐
4.2	Create at least one notification topic and subscription to receive monitoring alerts	☐	☐
4.3	Ensure a notification is configured for Identity Provider changes	☐	☐
4.5	Ensure a notification is configured for IAM group changes	☐	☐
4.6	Ensure a notification is configured for IAM policy changes	☐	☐
4.7	Ensure a notification is configured for user changes	☐	☐
4.8	Ensure a notification is configured for VCN changes	☐	☐
4.9	Ensure a notification is configured for changes to route tables	☐	☐
4.10	Ensure a notification is configured for security list changes	☐	☐
4.11	Ensure a notification is configured for network security group changes	☐	☐
4.12	Ensure a notification is configured for changes to network gateways	☐	☐
4.13	Ensure VCN flow logging is enabled for all subnets	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.14	Ensure Cloud Guard is enabled in the root compartment of the tenancy	☐	☐
4.15	Ensure a notification is configured for Oracle Cloud Guard problems detected	☐	☐
4.17	Ensure write level Object Storage logging is enabled for all buckets	☐	☐
5.1.1	Ensure no Object Storage buckets are publicly visible.	☐	☐
5.1.2	Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK).	☐	☐
5.2.1	Ensure Block Volumes are encrypted with Customer Managed Keys (CMK).	☐	☐
5.2.2	Ensure boot volumes are encrypted with Customer Managed Key (CMK).	☐	☐
5.3.1	Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK)	☐	☐
6.1	Create at least one compartment in your tenancy to store cloud resources	☐	☐
6.2	Ensure no resources are created in the root compartment	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure In-transit Encryption is enabled on Compute Instance	☐	☐
4.4	Ensure a notification is configured for IdP group mapping changes	☐	☐
4.16	Ensure customer created Customer Managed Key (CMK) is rotated at least annually	☐	☐
5.1.3	Ensure Versioning is Enabled for Object Storage Buckets	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Oct 18, 2023	2.0.0	UPDATE - Ensure user API keys rotate within 90 days or less - update audit and remediation console steps (Ticket 19277)
Oct 18, 2023	2.0.0	ADD - Compute Section (Ticket 20101)
Oct 30, 2023	2.0.0	UPDATE - Ensure no security lists allow ingress from 0.0.0.0/0 to port 22 - change to Description, Audit and Remediation sections (Ticket 18648)
Oct 30, 2023	2.0.0	UPDATE - Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389 - Minor changes to the wording in the Description, Audit Procedure, and Remediation Procedure (Ticket 18680)
Oct 30, 2023	2.0.0	UPDATE - Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22 - changing the Assessment Status from Manual to Automated (Ticket 19266)
Oct 30, 2023	2.0.0	UPDATE - Ensure no network security groups allow ingress from 0.0.0.0/0 to port 22 - Add Console steps to remediation and Audit sections (Ticket 18940)
Oct 30, 2023	2.0.0	UPDATE - Ensure the default security list of every VCN restricts all traffic except ICMP - changes to Audit and remediation procedures. (Ticket 19008)
Oct 31, 2023	2.0.0	UPDATE - Ensure default tags are used on resources - changes to Audit and Remediation console steps (Ticket 19489)
Oct 31, 2023	2.0.0	UPDATE - Ensure default tags are used on resources - change Assessment Status to Automated (Ticket 17885)
Oct 31, 2023	2.0.0	UPDATE - Create at least one notification topic and subscription to receive monitoring alerts - change Assessment Status to Automated (Ticket 17886)

Date	Version	Changes for this version
Oct 31, 2023	2.0.0	UPDATE - Ensure a notification is configured for Identity Provider changes - Change assessment status and grammatical updates (Ticket 18104)
Oct 31, 2023	2.0.0	UPDATE - Ensure a notification is configured for IdP group mapping changes - correct event names in audit and remediation (Ticket 16869)
Oct 31, 2023	2.0.0	UPDATE - Ensure a notification is configured for IdP group mapping changes - syntax corrections in audit and remediation (Ticket 18103)
Oct 31, 2023	2.0.0	UPDATE - Ensure a notification is configured for IAM group changes - Syntax updates in audit and remediation (Ticket 18105)
Nov 1, 2023	2.0.0	UPDATE - Ensure a notification is configured for IAM policy changes - Syntax changes in audit and remediation (Ticket 18106)
Nov 9, 2023	2.0.0	UPDATE - Ensure a notification is configured for user changes - syntax corrections in audit and remediation (Ticket 18107)
Nov 9, 2023	2.0.0	UPDATE - Ensure a notification is configured for user changes - Conditions are case sensitive/incorrectly cased. (Ticket 16289)
Nov 9, 2023	2.0.0	UPDATE - Ensure a notification is configured for VCN changes - syntax corrections in audit and remediation (Ticket 18108)
Nov 9, 2023	2.0.0	UPDATE - Ensure a notification is configured for changes to route tables - syntax corrections in audit and remediation (Ticket 18109)
Nov 9, 2023	2.0.0	UPDATE - Ensure a notification is configured for security list changes - Ensure a notification is configured for security list changes (Ticket 18110)
Nov 9, 2023	2.0.0	UPADATE - Ensure a notification is configured for network security group changes - syntax corrections in audit and remediation (Ticket 17920)

Date	Version	Changes for this version
Nov 9, 2023	2.0.0	REVIEW - Ensure a notification is configured for changes to network gateways - the deletelocalpeeringgateway is invalid; has a .end. (Ticket 16290)
Nov 9, 2023	2.0.0	UPDATE - Ensure a notification is configured for changes to network gateways - syntax corrections in audit and remediation (Ticket 17921)
Nov 13, 2023	2.0.0	UPDATE - Ensure VCN flow logging is enabled for all subnets - syntax corrections in audit and remediation (Ticket 17891)
Nov 13, 2023	2.0.0	UPDATE - Ensure Cloud Guard is enabled in the root compartment of the tenancy - syntax corrections in audit and remediation (Ticket 17892)
Nov 13, 2023	2.0.0	UPDATE - Ensure customer created Customer Managed Key (CMK) is rotated at least annually - syntax corrections in audit and remediation (Ticket 17893)
Nov 13, 2023	2.0.0	UPDATE - Ensure write level Object Storage logging is enabled for all buckets - syntax corrections in audit and remediation (Ticket 17894)
Nov 13, 2023	2.0.0	UPDATE - Benchmark Description - add compliance checking script info (Ticket 20307)
Nov 13, 2023	2.0.0	DELETE - Ensure audit log retention period is set to 365 days (Ticket 18290)
Nov 15, 2023	2.0.0	UPDATE - Ensure no Object Storage buckets are publicly visible - Default Value to Private (Ticket 18791)
Nov 15, 2023	2.0.0	UPDATE - Ensure no Object Storage buckets are publicly visible - Change Assessment Status to Automated (Ticket 17869)
Nov 15, 2023	2.0.0	UPDATE - Ensure no Object Storage buckets are publicly visible - Language updates to Audit Procedure and Remediation Procedure (Ticket 18712)
Nov 15, 2023	2.0.0	UPDATE - Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK) - Change Assessment Status to Automated (Ticket 17870)

Date	Version	Changes for this version
Nov 15, 2023	2.0.0	UPDATE - Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK) - Default Value to Oracle Managed Key (Ticket 18828)
Nov 15, 2023	2.0.0	UPDATE - Ensure Object Storage Buckets are encrypted with a Customer Managed Key (CMK) - Update to Audit and Remediation Procedure (Ticket 18739)
Nov 15, 2023	2.0.0	UPDATE - Ensure Versioning is Enabled for Object Storage Buckets - Update in language to Audit and Remediation Procedures (Ticket 18754)
Nov 15, 2023	2.0.0	UPDATE - Ensure Versioning is Enabled for Object Storage Buckets - Add Default Value as Versioning Disable (Ticket 18792)
Nov 15, 2023	2.0.0	UPDATE - Ensure Versioning is Enabled for Object Storage Buckets - Change Assessment Status to Automated (Ticket 17871)
Nov 17, 2023	2.0.0	UPDATE - Ensure Block Volumes are encrypted with Customer Managed Keys (CMK). - small updates made (Ticket 18720)
Nov 17, 2023	2.0.0	UPDATE - Ensure Block Volumes are encrypted with Customer Managed Keys (CMK) - Change Assessment Status to Automated (Ticket 17872)
Nov 17, 2023	2.0.0	UPDATE - Ensure boot volumes are encrypted with Customer Managed Key (CMK) - Change Assessment Status to Automated (Ticket 17873)
Nov 20, 2023	2.0.0	UPDATE - Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK) - Change Assessment Status to Automated (Ticket 17874)
Nov 20, 2023	2.0.0	UPDATE - Ensure no resources are created in the root compartment - Change Assessment Status to Automated (Ticket 17884)
Nov 20, 2023	2.0.0	UPDATE - Create at least one compartment in your tenancy to store cloud resources - Change Assessment Status to Automated and expand audit CLI (Ticket 17883)

Date	Version	Changes for this version
Nov 20, 2023	2.0.0	UPDATE - Ensure user customer secret keys rotate within 90 days or less - changes to reduce ambiguity (Ticket 19092)
Nov 20, 2023	2.0.0	UPDATE - Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389 - Automated Auditing Alternative in additional information section (Ticket 18422)
Nov 22, 2023	2.0.0	UPDATE - Ensure permissions on all resources are given only to the tenancy administrator group - Add remediation via CLI and change to automated status (Ticket 18695)
Nov 22, 2023	2.0.0	UPDATE - Ensure IAM administrators cannot update tenancy Administrators group - change Assessment Status from Manual to Automated (Ticket 17836)
Nov 22, 2023	2.0.0	UPDATE - Ensure MFA is enabled for all users with console password capability - CLI Changes (Ticket 18959)
Nov 22, 2023	2.0.0	UPDATE - Ensure API keys are not created for tenancy administrator users - Changes to include Audit and Remediation CLI commands (Ticket 19300)
Nov 22, 2023	2.0.0	UPDATE - Compute Section - Move Compute Section after Networking section (Ticket 20216)
Dec 4, 2023	2.0.0	UPDATE - Ensure MFA is enabled for all users with a console password - Updates for accuracy and readability (Ticket 18953)
Dec 4, 2023	2.0.0	ADD - Ensure a notification is configured for Oracle Cloud Guard problems detected (Ticket 20356)
Dec 11, 2023	2.0.0	ADD - Ensure Compute Instance Legacy MetaData service endpoint is disabled (Ticket 20112)
Dec 11, 2023	2.0.0	ADD - Ensure Secure Boot is enabled on Compute Instance (Ticket 20113)
Dec 12, 2023	2.0.0	UPDATE - Benchmark Overview - Automated Auditing Alternative (Ticket 18421)
Dec 18, 2023	2.0.0	ADD - Ensure user IAM Database Passwords rotate within 90 days (Ticket 20483)

Date	Version	Changes for this version
Dec 28, 2023	2.0.0	UPDATE - Ensure IAM password policy requires minimum length of 14 or greater - update Assessment Status from Manual to Automated and add CLI audit steps (Ticket 17838)
Dec 28, 2023	2.0.0	ADD - Ensure In-transit Encryption is enabled on Compute Instance (Ticket 20473)
Dec 29, 2023	2.0.0	UPDATE - Mutiple recommendations in Identity and Access Management section - audit and remediation steps to support tenancy with Identity Domains (Ticket 20440)
Dec 29, 2023	2.0.0	UPDATE - Ensure Dynamic Groups are used for OCI instances, OCI Cloud Databases and OCI Function to access OCI resources - change Dynamic Groups to to Instance Principal (Ticket 20499)
Dec 29, 2023	2.0.0	UPDATE - Ensure no network security groups allow ingress from 0.0.0.0/0 to port 3389 - Change the Assessment Status from Manual to Automated (Ticket 19267)
Dec 29, 2023	2.0.0	UPDATE - Ensure IAM password policy expires passwords within 365 days - Setting moved (Ticket 17889)
Dec 29, 2023	2.0.0	UPDATE - Ensure IAM password policy prevents password reuse - setting removed (Ticket 17890)
Dec 29, 2023	2.0.0	UPDATE - Ensure no security lists allow ingress from 0.0.0.0/0 to port 22 - Check port range (Ticket 20482)
Dec 29, 2023	2.0.0	UPDATE - Ensure no security lists allow ingress from 0.0.0.0/0 to port 3389 - change audit query (Ticket 18756)
Mar 29, 2022	1.2.0	ADD - Ensure Dynamic Groups are used for OCI instances, OCI Cloud Databases and OCI Function to access OCI resources. (Ticket 15247)
Mar 29, 2022	1.2.0	ADD - Ensure Oracle Integration Cloud (OIC) access is restricted to allowed sources (Ticket 15249)
Mar 29, 2022	1.2.0	ADD - Ensure Oracle Analytics Cloud (OAC) access is restricted to allowed sources or deployed within a Virtual Cloud Network (Ticket 15250)

Date	Version	Changes for this version
Mar 29, 2022	1.2.0	ADD - Ensure Oracle Autonomous Shared Databases (ADB) access is restricted to allowed sources or deployed within a Virtual Cloud Network (Ticket 15251)
Mar 29, 2022	1.2.0	ADD/UPDATE - Object Storage changed to Storage to include all storage services as subsections (Ticket 14316)
Mar 29, 2022	1.2.0	ADD - Ensure Versioning is Enabled for Object Storage Buckets (Ticket 14444)
Mar 29, 2022	1.2.0	UPDATE - Ensure a notification is configured for user changes - Syntax Error in JSON Example in CLI Audit step 3 (Ticket 12074)
Mar 29, 2022	1.2.0	ADD - Ensure storage service-level admins cannot delete resources they manage. (Ticket 14445)
Mar 29, 2022	1.2.0	UPDATE - Ensure IAM administrators cannot update tenancy Administrators group - Syntax fix Remediation Section (Ticket 12073)
Mar 29, 2022	1.2.0	ADD - Ensure Block Volumes are encrypted with Customer Managed Keys (CMK) (Ticket 15254)
Mar 29, 2022	1.2.0	ADD - Ensure boot volumes are encrypted with Customer Managed Key (CMK) (Ticket 15255)
Mar 29, 2022	1.2.0	ADD - Ensure File Storage Systems are encrypted with Customer Managed Keys (CMK) (Ticket 15256)
Apr 8, 2022	1.2.0	UPDATE - Multiple Recommendations - Add mapping CIS v8 to Foundations Benchmark (Ticket 14227)