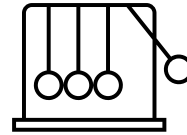




OCI Security Health Check

Why OCI Security Health Check ?



Did you know ?!

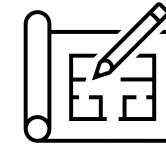


- ✓ 40% of businesses experienced a data breach in their cloud environment.
- ✓ 45% of breaches are cloud-based
- ✓ Data breaches exposed more than 8 million records in 2023, highest single loss was 125 million data sets were breached
- ✓ Facebook lost 530 millions user's personal data, LinkedIn lost 700 Million Data, Toyota exposed 260k customers' data, Microsoft exposed 30000 Business due to cyber attack , Real Estate Wealth Network leaked 1.5 billion records
- ✓ 69% of organizations admitted to experiencing data breaches due to exposures to multi-cloud security configurations
- ✓ 80% of companies have experienced cloud security incidents last year
- ✓ More than 4,000 attacks per day, US organizations lost more than \$20 billion in 2023, 19-day average downtime, Average total cost per breach: \$3.86M, Cost of one lost record: \$150, Average size of data breach: 25,575 records, Average total remediation cost \$1.85M
- ✓ According to Cloud Security Alliance Release /CSA/ top 5 risks :
 1. Misconfiguration and inadequate change control
 2. Identity and Access Management (IAM)
 3. Insecure interfaces and APIs
 4. Inadequate selection/Implementation of cloud security strategy
 5. Insecure third-party resources

OCI Security Health Check Standard Edition

- ✓ Developed based on latest CIS /Center of Internet Security/ Oracle Cloud Infrastructure Foundations Benchmark : https://www.cisecurity.org/benchmark/Oracle_Cloud
- ✓ The CIS Benchmark is the product of a **community consensus** process and consists of secure configuration guidelines developed for Oracle Cloud Infrastructure
- ✓ Customers can run the assessment as a self-service. We recommend to run with experienced Oracle specialist or certified OCI partner. Why ? See previous slide..
- ✓ Everybody can benefit from implementing cybersecurity processes and stronger defence to stop cyber-attacks
- ✓ Generic controls are applicable to many scenarios
- ✓ It is not industry specific
- ✓ Assessment is non-intrusive, assessing OCI configuration and will not affect performance
- ✓ **Out of scope** : *covers the OCI platform as specified in the CIS Oracle Cloud Infrastructure Foundations Benchmark, only. Any workload provisioned in Databases, Compute VMs (running any Operating System), the Container Engine for Kubernetes, or in the VMware Solution is out of scope of the OCI Security Health Check.*

OCI Security Health Check Standard. What it brings ?

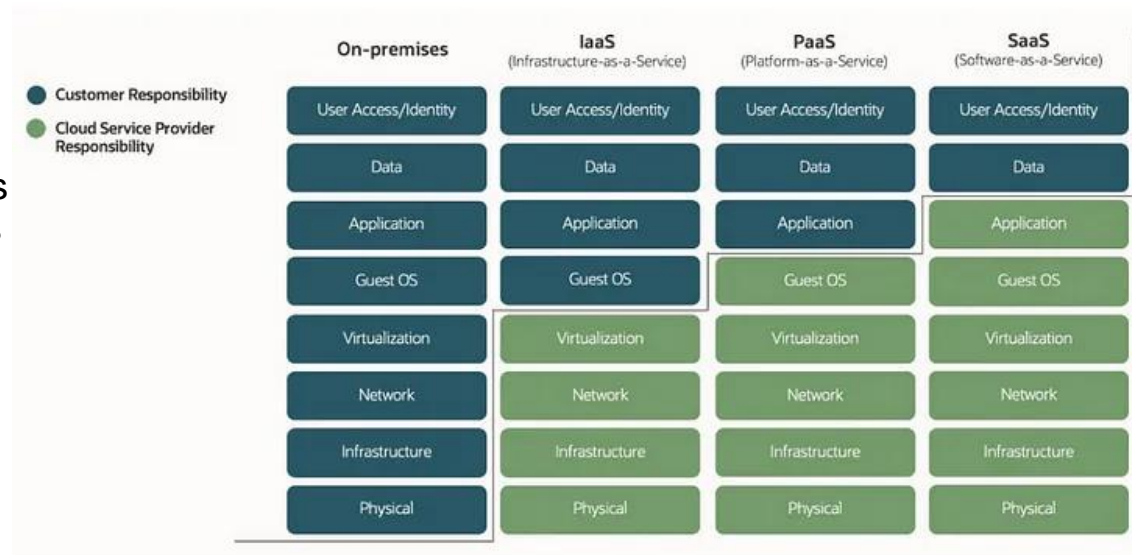


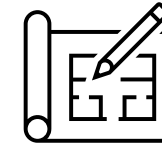
OCI Security Health checks brings you :

- ✓ Enables OCI best practises
- ✓ increase OCI stickiness
- ✓ Better adoption of OCI security services
- ✓ Reduce risks of OCI Tenancy Breaches

Focus areas :

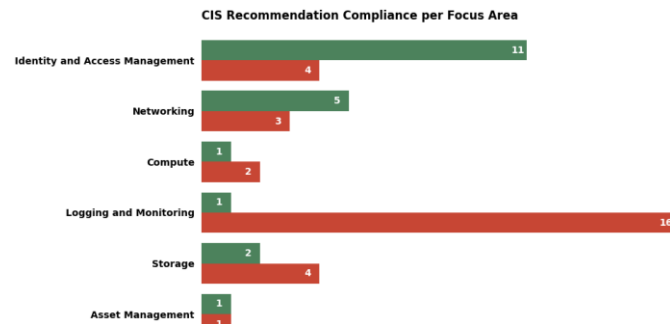
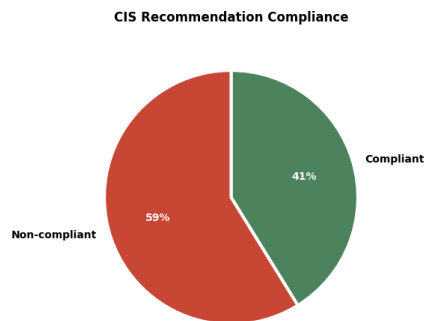
- ✓ Identity and Access Management
- ✓ Networking
- ✓ Compute
- ✓ Logging and Monitoring
- ✓ Storage
- ✓ Asset management



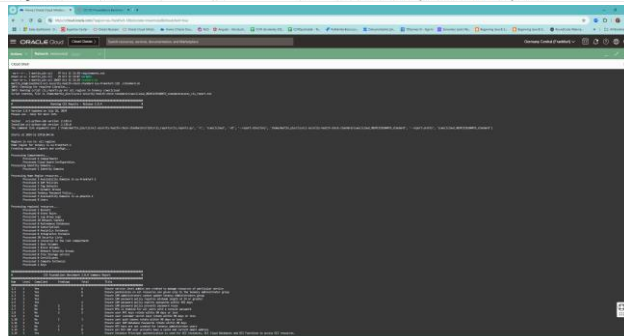


OCI Security Health Check Standard. How it goes ?

- ✓ Deploy expert for OCI Security /Oracle, Partner, Internal/
- 1. **Kick-off.** Understand the purpose , process and what is included
- 2. **Prepare** Prepare the OCI tenancy and run the script
- 3. **Execute** Run the script to retrieve the information for the assessment
- 4. **Results** Inspect the data and check the html output with the customer
- 5. **Implement.** review actionable feedback from assessment report and plan to implement changes.



Recommendation #	Section	Level	Compliant	Findings	Compliant Items	Total	Title	CIS v8	CCCS Guard Rail
1	Identity and Access Management	1	Yes	6	6	6	Ensure service level admins are created to manage resources of particular service	[5.4, 6.7]	2,3
2	Identity and Access Management	1	Yes	6	6	6	Ensure permissions on all resources are given only to the tenancy administrator group	[3.3]	1,2,3
3	Identity and Access Management	1	Yes	6	6	6	Ensure IAM administrators cannot update tenancy Administrators group	[3.3, 5.4]	2,3
4	Identity and Access Management	1	Yes	0	0	0	Ensure IAM password policy requires minimum length of 14 or greater	[4.1, 5.2]	2,3
5	Identity and Access Management	1	Yes	2	2	2	Ensure IAM password policy expires passwords within 365 days	[4.1, 5.2]	2,3
6	Identity and Access Management	1	No	2	0	2	Ensure IAM password policy prevents password reuse	[5.2]	2,3
7	Identity and Access Management	1	No	3	5	8	Ensure MFA is enabled for all users with a console password	[6.3, 6.5]	1,2,3,4
8	Identity and Access Management	1	Yes	2	2	2	Ensure user API keys rotate within 90 days or less	[4.1, 4.4]	6,7
9	Identity and Access Management	1	Yes	2	2	2	Ensure user API keys rotate within 90 days or less	[4.1, 4.4]	6,7



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.



CCW as Oracle partner has these BYC Offerings :

BYC Offering	Description	Duration
 Landing Zones implementation	OCI strategy and optimization ; landing zone design and build, workload migration and modernization – containerization and microservice adoption; DevOps modernization, Lift and Shift Migration, VMWare Workloads migration.	2-7 days
 Siebel CRM deployment to OCI	We create a new deployment of Siebel CRM in OCI or we can migrate you Siebel CRM from on premise to OCI using Siebel Cloud Manager. CCW can also design “Lift and Shift” migration from onprem to OCI. Updates to new version is seamless and easy.	4-6 weeks
 Oracle Digital Assistant Entry Pack	Design , configuration, training ,integration and deployment of the Oracle Digital Assistant (AI, genAI Chatbot) into OCI and integration with applications. Integration with OCI AI and generative AI services for upgrading the chatbot to highest industry level. Training for 20 intents, 5 workflows and 2 channels. Integration with 2 REST Webservices	2 weeks
 Oracle Digital Assistant Premium Pack	Training 50 intents, design and configuring 10 workflows, multichannel integration and 5 REST WebServices integration	5 weeks
 OCI Security Health Check	Assess your OCI security posture against best practices outlined in CIS benchmarks and receive Oracle Advisory how to close the security gaps	1-2 weeks
 OCI Cloud Native Development entry	We design and implement your workload natively in the cloud. No matter if you need backend microservice, front-end rich web client, leveraging genAI, IoT, DB processing.	4 weeks



ORACLE



Follow our <http://www.ccw.sk> where we publish our OCI innovations in blog and news section

Thank you !

CCW s.r.o.
Námestie Slobody 11
81106 Bratislava
Slovakia
<http://www.ccw.sk>

Email: martin.piekov@ccw.sk

Phone: +421 908036873

www.ccw.sk