ASSET ID			ASSET NAME	CIS Landing Zone v2 | ORM Configuration Guide		ASSET VERSION	0.3 | 11.05.2023
ASSET OBJECTIVE	Provide configuration guidelines for deploying the CIS Landing Zone v2 with Oracle Resource Manager.						
ASSET CONTENTS	[1. BEFORE YOU START] [2. RESOURCES CREATED] [3. CONFIGURATIONS DECISIONS]						

1. BEFORE YOU START

The CIS Landing Zone v2 ORM guide is a great starting point for an OCI Tenancy. Before you start take into consideration the resources that you will create, the key decisions associated with them, and the prerequisites.

If you need to learn more about Oracle Resource Manager (ORM) follow the links below.

TOPIC	ID	TRAINING
ORM - Oracle Resource Manager	1	Oracle Resource Manager Overview
	2	OCI Level 100 - Resource Manager

2. RESOURCES CREATED

Find below the summary of the resources that can be created by the OCI Security LZ stack:

- IAM. (Groups, Dynamic groups, Policies)
- Networking. (VCNs, Subnets, Route tables, Security Lists, NSGs, Internet Gateway, Nat Gateway, Service Gateway, DRGs)
- Keys
- Cloud Guard
- Logging (Log groups, Flow logs, Service connector)
- Vulnerability Scanning
- Bastion
- Events
- Alarms
- Notifications (topics and subscriptions)
- Object Storage
- Budgets
- Secure Zones

3. CONFIGURATIONS DECISIONS

Find below a summary of the key decision you will have to make during the configuration process and our configuration ready to use.

CATEGORY	TOPIC	DECISION	DEFAULT VALUE	RECOMMENDATION	REQUIRED ACTION	CONFIG #1 QS	CONFIG #2 PRD
SECURITY	ENCLOSING COMPARTMENT	Do you want to deploy the LZ under a specific compartment?	By default, CIS LZ v2 compartments are deployed under the ROOT compartment.	• **For Starters**: Use an enclosing compartment for a testing LZ. • **For Production**: Do not use an enclosing compartment, in this scenario is recommended to deploy under the root compartment.	Choose to deploy the LZ resources under an enclosing compartment or under the root depending on the LZ's purposes. Add the value of the **Service Label** attribute. This label will be used to define the name of all the stack resources that will be created. You will make this decision in step 3.1 of the ORM Deployment Guide.	YES	NO
	CIS Level	CIS Benchmark	The default value is 2.	CIS Level 1 is for basic security CIS Level 2 is for stronger security.	Leave default values, unless you have specific requirements. You will make this decision in step 3.1 of the ORM Deployment Guide.	YES	YES
	IAM	Do you want to deploy Groups included in the CIS LZ v2 stack or do you want to reuse your own Groups?	By default, CIS LZ v2 creates predefined groups.		Leave default values, unless you have specific requirements. You will make this decision in step 3.2 of the ORM Deployment Guide.	YES	YES
	CLOUD GUARD	Do you want to enable Cloud Guard monitoring?	By default, CIS LZ v2 enables Cloud Guard.	Enable Cloud Guard Service	Leave default values, unless you have specific requirements. You will make this decision in step 3.9 of the ORM Deployment Guide.	YES	YES
	SECURITY ZONES	Do you want to enable Security Zones?	By default, CIS LZ v2 does not enable the feature of Secure Zones.	Disable Secure Zones	Leave default values, unless you have specific requirements. You will make this decision in step 3.10 of the ORM Deployment Guide.	NO	NO
	VULNERABILITY SCANNING	Do you want to enable VSS?	By default, CIS LZ v2 enables VSS.	Enable Vulnerability Scanning Service	Enable Vulnerability and scanning. You will make this decision in step 3.12 of the ORM Deployment Guide.	YES	YES
NETWORK	HUB & SPOKE	Do you want to deploy a Hub & Spoke Network configuration?	By default, CIS LZ v2 does not deploy a Hub & Spoke network topology		Leave default values, unless you have specific requirements. It´s recommended to select the VCN CIDR. You will make this decision in step 3.3 of the ORM Deployment Guide.	NO	YES
	NETWORK APPLIANCE HUB	Do you want to deploy a Hub VCN for network appliance purposes (OCI network Firewall, NGFW)?	By default, CIS LZ v2 does not deploy a Hub VCN.		Leave default values, unless you have specific requirements. You will make this decision in step 3.4 of the ORM Deployment Guide.	NO	YES
	EXADATA VCN	Do you want to deploy a specific spoke VCN for ExaCS deployment?	By default, CIS LZ v2 does not deploy an EXADATA VCN.		Leave default values unless you have specific requirements. You will make this decision in step 3.5 of the ORM Deployment Guide.	NO	NO
	ON-PREM	Do you want to configure on-prem connectivity?			If you want to configure connectivity with an on-premises network provide proper values for the required attributes. You will make this decision in step 3.6 of the ORM Deployment Guide.	NO	NO

CATEGORY	TOPIC	DECISION	DEFAULT VALUE	RECOMMENDATION	REQUIRED ACTION	CONFIG #1 QS	CONFIG #2 PRD
MONITORING	BLOCK INTERNET ACCESS	Do you want to block Internet Access?	By default, CIS LZ v2 deploys an Internet Gateway and a NAT Gateway.		BLOCK Internet Access, unless you have specific requirements. If you want to deploy a Bastion Service provide proper values for the required attributes. You will make this decision in step 3.6 of the ORM Deployment Guide	NO	NO
	NOTIFICATION	Configure events and notifications	By default, CIS LZ v2 configures the notification service.		Provide Network Admin Email Endpoints and Secure Admin Email Endpoints You will make this decision in step 3.7 of the ORM Deployment Guide.	YES	YES
	LOGGING CONSOLIDATION	Do you need to deploy a service connector?	By default, CIS LZ v2 does not deploy a service connector.		Leave default values, unless you have specific requirements. You will make this decision in step 3.11 of the ORM Deployment Guide.	NO	NO
STORAGE	OBJECT STORAGE	Do you need to deploy an Object Storage?	By default, CIS LZ v2 does not deploy any object storage.		Leave default values, unless you have specific requirements. You will make this decision in step 3.8 of the ORM Deployment Guide.	NO	NO
GOVERNANCE	COST MANAGEMENT	Do you want to deploy a Cost Management Budget?	By default, CIS LZ v2 creates a budget.	• **For Starters**: Do not deploy a Cost Management Budget. • **For Production**: Deploy a Cost Management Budget.	You will make this decision in step 3.13 of the ORM Deployment Guide.	NO	NO
WORKLOADS	MULTIPLE WORKLOADS	Do you want to deploy more than one workload?	By default, CIS LZ v2 creates one compartment for the databases and one compartment for applications. Related resources will be deployed into the respective compartment.	• **For Starters**: Do not configure Multiple Workloads. • **For Production**: Configure Multiple Workloads if required.	You will make this decision in step 3.14 of the ORM Deployment Guide. If you want to improve security and manageability we recommend you check the advanced scenarios proposed.	NO	--