ASSET ID | NAME |	**LZB.L1.4 | Select Your Solution**
ASSET VERSION	**v0.6 | 13.09.2023**
ASSET OBJECTIVE	• Help you understand the OCI Landing Zones landscape, with the solution characteristics and maturity. • Provide you with technical guidelines on why you can consider using a solution. •
ASSET CONTENTS	[1. WELCOME NOTE] [2. UNDERSTAND THE LANDSCAPE] [3. WHY USE AND CONSIDERATIONS BEFORE USING]

1. WELCOME NOTE

Welcome to the Select Your Landing Zones Solution asset. This asset presents the OCI Landing Zones approaches and solutions available with IaC, and IaC solutions to create OCI landing zones.

Be aware that this asset might be outdated as we're not reviewing all aspects and elements weekly basis. If you find any element out of date, please don't hesitate to reach out.

Note the previous versions of the OELZ are not included.

2. UNDERSTAND THE LANDSCAPE

APPROACH		STANDARD / PRESCRIBED		TAILORED
AREA	**TOPIC**	**OELZ v2**	**CIS LZ v2**	**OCI OPEN LZ + CIS LZ ENHANCED MODULES**
SOLUTION STORY	**DESCRIPTION**	An OCI Product Management Landing Zone ready to start the OCI Journey, with hub & spokes, application-driven design with multiple workloads, using ORM and IaC.	A Secure Landing Zone to start the OCI journey with a layered approach, several network topologies (shared to hub & spoke), with top security CIS 1.2 compliance and validation, using ORM and IaC.	A framework to create and run new and all types of Landing Zones (from simple to complex ones). Includes a complete design blueprint (OCI Open LZ) and a configurable approach to IaC (CIS LZ Enhanced Modules) for running OCI.
	DOCUMENTATION	Here and here	Here and here	OCI Open LZ Blueprint + CIS LZ Enhanced Modules
	OWNER	OCI PM	TE NACE	TE NACE + EMEA
	LICENSING	UPL v1.0	UPL v1.0	UPL v1.0
	SLACK	#oci_landing_zone	#oci_cis_landing_zone	#oci_cis_landing_zone
SOLUTION SUMMARY	**CUSTOMIZATION**	Code-Driven	Code-Driven	Configuration-Driven
	ENVIRONMENTS	Prod and Non-Prod	Multiple	Multiple, Configurable
	CIS SECURITY	CIS 1.2	CIS 1.2, CIS Certified with Validations	CIS 1.2 (Embedded)
	NETWORK	Hub & Spoke, no NSGs	Shared VCN, Hub & Spoke, with NSGs.	All, Configurable
	TARGET WORKLOADS	Three-Tier Applications and ExaCS	Three-Tier Apps and ExaCS	All, Configurable
	MULTIPLE WL	Yes | ELZ Workload	Yes | By Spokes	Yes | Configurable
	GIT REPOSITORY	OCI OELZ	OCI CIS LZ + [1]	IAM, Network, Governance, Observability, and Security
SOLUTION MATURITY	**CUSTOMER BASE**	Not Disclosed	400+ Deployments with Partners	10+
	OPERATIONS INTERFACE	ORM, TF CLI	ORM, TF CLI	TF CLI, CI/CD, Config-as-Code (GitOps)
	BLUEPRINTS / PATTERNS	ExaCS	ExaCS	OCI CIS v2, OCI Open LZ Blueprint
	SOLUTION DESIGN RECOMMENDED? **(approach type)**	**YES** **(prescribed)**	**YES** **(prescribed)**	**YES** **(blueprints/tailored)**
	SOLUTION IS CUSTOMIZABLE?	**YES** **(by code)**	**YES** **(by code)**	**YES** **(configurable)**
	CUSTOMIZATION EFFORTS?	**MEDIUM-HIGH** By Code / No TF Best Practices This is a solution coded for a design, changing or customizing it can require a lot of effort. Not following Terraform's best practices pays a toll. The consequence of this it's less reuse and more effort into customizing a solution, with documentation gaps, duplication of resources, incomplete naming conventions, and the overall risk of adopting poor coding practices.	**MEDIUM** By Code / TF Best Practices The new version of his landing zones is already using the IAM modules from CIS LZ Enhanced Modules, which means that adjusting the IAM constructs is simple and no coding is required. While it doesn't get completely migrated to the new modules, you need to change the other elements with code, and this means developing efforts. This can be simpler, or more complex depending on the target solution and team expertise. Regarding the code, it's well organized with a modular approach, coded with TF best practices, and can be extended with reuse. A lot of customers are using this solution as a starting point to create their OCI IaC assets. It's also a great entry point for the IaC journey.	**LOW** By Configuration / No Coding This solution is a game change to approach OCI at the design and IaC level. Customizations are now configurations and no code is required. By using a set of Terraform modules that receive HCL JSON values it can separate configurations from code development or customizations, meaning your solution is just a set of configurations as input to the generic code. With this approach, efforts are **focused on configurations and not on coding**. This means less time to value and few implementation efforts. You can configure your own solution in no time.

3. WHY USE AND CONSIDERATIONS BEFORE USING

APPROACH	STANDARD / PRESCRIBED		TAILORED
SOLUTIONS	**OELZ v2 (see other versions)**	**CIS LZ v2**	**OCI OPEN LZ + CIS LZ ENHANCED MODULES**
WHY USE	PM Ownership This is the solution proposed by OCI Product Management.	Worldwide Adoption It is a solution **adopted worldwide** in NA, EMEA, and JAPAC. The customer base is high and growing. The partner community is using this solution.	A Complete OCI Design Blueprint With this approach, you don't start a tailored design with an empty whiteboard. The OCI Open LZ Blueprint contains a **complete and public OCI**

APPROACH	STANDARD / PRESCRIBED		TAILORED
	Note that the licensing is UPL 1.0 and the support channel is GitHub Issues. Simple Applications Onboard The solution has an application-driven design, ready to onboard **multiple workloads into OCI with a simple/flat landing zone structure.** Each workload can have its responsible team, with a dedicated compartment and a spoke VCN. The workload layers are isolated with Subnets. Prod/Non-Prod Environments The solution is ready for landing zone **Non-production** and **Production environments.** To confirm your understanding of this topic, please read "**Approach to Environments**" for **OELZ v2** and **CIS LZ v2,** as there are several different approaches to this feature. IaC Modular Approach The modular design based on **Terraform modules** provides flexibility to optimize a Landing Zone design. With this model, this solution is a simple entry point for the **IaC journey**, simple to learn and start coding.	Strong Security (CIS Embedded) **Security-centric solution** implementing CIS OCI Foundations Benchmark version 1.2. The solution implements the recommendations and contains a script to validate any tenancy against the recommendations on the benchmark. In terms of design, the solution ensures the segregation of duties for a set of pre-defined personas, delivering operationally ready-to-use environments. At the network level, there is strong network isolation with VCNs, Subnets, and NSGs. It also lets users choose OCI security services to enable. Three-tier & Segregation of Duties The basic design is suitable for three-tier apps, deploying one VCN with one public subnet and two private subnets. A public subnet is used for the load balancers and bastion servers. The application and database tiers are attached to separate private subnets. The solution can also create VCNs to support the deployment of specific workloads, like Oracle Exadata Database Service. The segregation of duties is implemented with several management groups, including groups for security, network, database, and applications, among others. Strong Network Isolation **Several network topologies** are supported, from shared to a hub and spoke, including **using NSG**. No Initial Consumption Cost The deployment of this solution creates resources that initially don't trigger consumption costs. The following optional and paid components can incur costs: 1. Object Store, is not configured by default. 2. OCI Logging, is configured by default and will be paid after 10 gigabytes of Log Storage per month. 3. OCI Notifications, the Service Connector is not configured by default. This service will be paid over 1 million Delivery Operations Per Month Regarding 2 and 3, the deployment of these services configured doesn't incur an immediate cost as you will be far billable thresholds. Be aware that to use this solution you need a paid tenancy due to the limitations of the Always Free tenancies. Modular IaC with Best Practices The **code is well organized** with a **modular approach** and **coded with** **TF best practices** and can be **extended with reuse.** Several customers are using this solution as a starting point to create their own OCI IaC assets. It's also a great entry point to start or continue an IaC journey. Multiple Environments This solution provides a simple approach to multiple environments: "1 environment - 1 deployment". To be able to do this, you will deploy a **non-production environment in an enclosed compartment**. Note that we recommend the **production environment should be at the root level** and deployed in a second iteration. A lot of our customers prefer this separation of environments by deployment, but there are several alternatives for this feature. For example, the **OELZ v2** solution provides you with the landing zone environment concept. To confirm your understanding of this topic, please read "**Caution with Environments**" for **OELZ v2** and **CIS LZ v2,** as there are several different approaches to this feature. Incremental Versioning The CIS LZ v2 is an incremental update over the v1, and it shares the same repository. Multi-Region Deployment This solution provides you the ability to extend an existing landing zone into several more regions. IAM, IDCS & Identity Domains This solution works with OCI Local IAM (in combination with IDCS) or the OCI Default Identity Domain.	**design** full of **OCI best practices**, including a functional view, security view, network view, operations view, and runtime view. Artifacts such as **drawio** and a **design documen**t are made available, to drive the same design journey with our customers, simplifying the design phase, with higher value and reduced efforts. • The **security view** covers the tenancy structure, IAM, and security posture. • The **network view** covers the network structure, isolation and security, connectivity and NS/EW traffic scenarios, and DSN. • The **operations view** covers the cloud operating model, proposing a gitops approach to run the blueprint, using the CIS LZ Enhanced Modules as the automation engine. • The **runtime view** presents the operator's view with json/tfvars IaC configuration using the CIS LZ Enhanced Modules. Focus on Configs, not Code With this approach, efforts are **focused on configurations and not on coding**. This means less time to value and fewer implementation efforts. You can configure your own solution quickly. The solution uses a set of Terraform modules that receive HCL JSON values, separating configurations from code development/customizations, meaning your solution is just a set of configurations as input to the generic Terraform modules. Suitable for DC Exits DC Exits normally involve a **high number of workloads** landing on OCI, with **different characteristics**, with specific **separations of duties** across the organization, and very fine-tuned **isolation of resources** - possibly different by workload type. As this solution is **configuration-driven**, it makes it easier to set up the target solution with **less effort focusing on configurations** and little coding. See the bullets below on organization and cloud operating models, as they are normally associated with large movements of workloads into OCI. Several Workload Types If you need **different workload types** to land on OCI, meaning several resource structures, and potentially different security or network topologies, this solution is a great fit because it allows you to configure a landing zone with these workload patterns at a fast pace and reduce efforts - as you will not be required to code it. Onboarding Enterprise Organizations You need to **onboard your organization** into OCI (Operating Entities, OpCos, LoB, Departments, etc.) and you need to reflect that into the Landing Zone. Use the OCI Open LZ Blueprint for these cases. Customized Operating Model You need a highly **tuned cloud operating model**, having **several team**s operating **different types of resources** or **areas** of the landing zone, or even having **shared areas** where some resources are operated by one team and other elements are operated by another team. Operations at Scale - GitOps This solution is a perfect fit if you're **operating at scale,** with a **high number of resource configurations,** for **different workloads and teams,** and you apply a best practice on **versioning and operating IaC configurations,** in a different lifecycle than the IaC itself. This is also commonly known as GitOps. Use the OCI Open LZ Blueprint for these cases. Follow TF Best Practices IaC solution is coded according to TF best practices, therefore it has the necessary ingredients to grow OCI IaC skills in your organization. Strong Security (CIS Embedded) **Security-centric solution** implementing CIS OCI Foundations Benchmark version 1.2. The solution implements the recommendations and contains a script to validate any tenancy against the recommendations on the benchmark. Existing Patterns/Blueprints Several blueprints will be available for you to start using this solution. These should be used as a reference design, that you can use out-of-the-box, or tailor. There are already examples on each module [1] [2] [3] [4] [5] for you to start using. The CIS LZ v2 solution configuration will be available soon, in the same repository as the existing solution, with v3 tagging. The OCI Open LZ Blueprint is also available, and more patterns will be published soon.
CONSIDERATIONS **BEFORE USE**	No Terraform best practices. To customize or extend the solution you need IaC Terraform skills. **The code doesn't follow all TF best practices,** with no documentation on several modules, duplication of resources, incomplete naming conventions, and no tagging. The consequence of this can be **more effort into customizing a solution** and higher code complexity as it gets more customized. Approach to Environments Caution when using the **Landing Zone environments** as these **don't** necessarily **match non-production and production project/application environments**. These two entities have normally different lifecycles. If you do not require two landing zone environments you can change the configuration to deploy only one environment. If you require a simple approach to environments, such as "1 environment - 1 deployment", you can also consider using **OCI CIS v2**.	Requires Terraform Skills To customize/extend the solution you need IaC Terraform skills. If you have no IaC skills and no partner responsible for this, consider using **CIS LZ Enhanced Modules**. Approaches to Org. Structures This solution design is not prepared to reflect organization structures (LoB, BU, OEs, OpCos, Departments, etc.) in the separation of duties and operating model. To onboard organizations' structures you mainly have three approaches: 1. Use a simple approach and **deploy one landing zone instance per organization**. The drawback of this approach is higher maintenance because shared resources at the security and network levels have to be operated separately. 2. **Customize this solution** with the organization's concepts at the compartment, groups, and policies level, having centrally operated shared resources for all organizations. Note that this requires customizations and coding efforts.	Customer Approach to IaC If you have an **existing strong IaC practice**, or predetermined way of using IaC (e.g., already having existing core Terraform modules for OCI, or using a procedural approach such as Ansible, etc.) and you want to follow the same approach for landing zones, weight the pros & cons of using this solution as it can enhance or break you existing IaC approach. In the case of a simpler Terraform approach in place, you can potentially reuse **CIS LZ v2** modules to expand existing capabilities. Code Customizations Requires TF Skills The Terraform skills required for just using the modules are very low as it's configuration-driven. The solution comes with highly structured Terraform written with best practices, but it's essential to be aware that to customize or change the module code you should have proficiency in Terraform and teams responsible for those tasks.

APPROACH	STANDARD / PRESCRIBED		TAILORED
	Note also that the Landing Zones environments might have different lifecycles, different target tenancies, or target compartments, or even managing their configurations in other places. For this type of requirement, you can consider two options: 1. Customize the code with the environment and project/workload entities, for the proper operation of these elements. This implies coding efforts. 2. If you require highly customized environments, from landing zones to project environments, we recommend using the t**ailored approach.** The OCI Open LZ Blueprint presents an example to help you drive into these scenarios. Approaches to Org. Structures This solution design is not prepared to reflect organization structures (LoB, BU, OEs, OpCos, Departments, etc.) in the separation of duties and operating model. To onboard organizations' structures you mainly have three approaches: 1. Use a simple approach and **deploy one landing zone instance per organization**. The drawback of this approach is higher maintenance because shared resources at the security and network levels have to be operated separately. 2. **Customize this solution** with the organization's concepts at the compartment, groups, and policies level, having centrally operated shared resources for all organizations. Note that this requires customizations and coding efforts. 3. Consider using the **tailored approach** to **onboard enterprise organizations and their organization structures** into OCI focusing on configurations and not code customizations, reducing your efforts drastically. You can **leverage the OCI Open LZ Blueprint** to simplify this process. Identity Domains are Required This solution requires the use of OCI IAM with **Identity Domains**, and it will create resources on the default Domain and several resources related to workloads on the new Identity Domains. If you have an older tenancy without Identity Domains we recommend that you use **CIS LZ v2**. Caution with CIDRs There is a "Workload - VCN" match, so the more workloads, the more complex it gets to manage the CIDR blocks For highly complex landing zones for DC-Exits situations, we recommend using the **tailored approach** with the **OCI Open LZ Blueprint,** which uses shared VCN and subnets for several workloads with NSG isolating each layer. Limited Network Security The use of Network Security Groups (NSG) is considered an OCI best practice, and **NSGs are not available** out-of-the-box with this solution**.** If you require higher levels of network isolation or higher security postures, you can **customize** the solution with these elements, or use **CIS LZ v2.** Requires Terraform Skills To customize/extend the solution you need IaC Terraform skills. If you have no IaC skills and no partner responsible for this, consider using **CIS LZ Enhanced Modules** from the **tailored approach.** Home Region Deployment The Oracle Enterprise Landing Zone should be deployed to the tenancy's Home Region. Different Codebase from V1 This solution is a completely new approach in terms of design and code, and it doesn't propose an incremental update from **OELZ v1**. It has a dedicated new code repository from the previous version. In other words, If v1 is already in use, the v2 approach is disruptive.	3. Consider using the **tailored approach** to **onboard enterprise organizations and their organization structures** into OCI focusing on configurations and not code customizations, reducing your efforts drastically. You can **leverage the OCI Open LZ Blueprint** to simplify this process. Approach to Environments The approach to environments with the rule "1 environment - 1 deployment" is very flexible as it allows multiple landing zone environments. You can therefore decide the scope and content for each. If the above model is not enough and you require that a landing zone instance contains different project environments, you can have two options: 1. Customize the code with the environment and project/workload entities, for the proper operation of these elements. This implies coding efforts. 2. If you require highly customized environments, from landing zones to project environments, we recommend using the **tailored approach.** The OCI Open LZ Blueprint presents an example to help you drive into these scenarios. If you require a solution with OOTB two landing zone environments, please review the two **OCI OELZ v2** environments entries on the left. Caution with CIDRs Spokes in this solution are one VCN with three subnets, one for each layer. Deciding on the spoke granularity is key to scaling the use of this landing zone for several workloads. Note that if the decision is "1 Workload - 1 VCN", the more workloads on the landing zone, the more complex it gets to manage the CIDR blocks. For highly complex landing zones for DC-Exits situations, we recommend using the **tailored approach** with the OCI Open LZ Blueprint**,** which uses shared VCN and subnets for several workloads with NSG isolating each layer.	