Cloud Adoption Framework

Cloud Center of Excellence

Cloud Operating Model

ORACLE

Agenda

Operational Excellence

Operational Excellence is operating your Tenancy efficiently while focusing on maximum results.
It ranges from Automating deployments to Monitoring and Managing while planning for peak events, as well as creating a culture of Reliability and D&R, Compliance, and accurate cost management.
When implemented correctly, it reduces costs, streamlines resource utilisation and prevents disruption due to human error.

Benefits

Standardise work and results:
When procedures are defined and adequately engineered, results are consistent and forecastable.

Reduced Operational Risk
Thanks to a proactive approach, unplanned events and disruptions are minimized, and when they occur, they are detected at a very early stage and their impact is vastly reduced, as all possible scenarios have been previously identified.

Reduced Operational Cost
- Automate repetitive services and configuration management
- Ensure compliance is maintained over time

Reduced time to deploy and time to Market
Improved Customer Experience

Ensure capability for accurate cost control and charge-back.

Cloud adoption considerations

Cloud adoption is a complex process that expands beyond technology implementation

- Business Strategy
- People
- Security
- Process Design
- Technology Implementation
- Management and Operations

Cloud adoption considerations

Cloud adoption is a complex process that expands beyond technology implementation

Business Strategy

- Cloud strategy
- Business case
- Business value
- KPI's
- Cloud economics processes

People

- Executive sponsorship
- Business IT alignment
- Buy in
- Cloud expertise
- Workload expertise

Security

- Cloud security understanding
- Security design
- Protection vs threats
- Security components/configuration
- Overall security approach

Process Design

- Governance
- Risk and compliance
- Enterprise Architecture
- Platform attributes
- Workload attributes

Technology Implementation

- IaaS/PaaS/SaaS
- Migration
- Tech Stack
- Workload deployment
- CI, CD

Management and Operations

- Monitoring
- Optimization
- Support and incident management
- Cost Management
- Maintenance

OCI Cloud Adoption Framework

- ✓ Standarize approach to navigate the cloud adoption and digital transformation
- ✓ Provides a blueprint to plan your journey
  - Cloud Adoption Framework

OCI Cloud Adoption Framework

Definition

OCI CAF provides thought leadership, resources, best practices, and tools to help organizations adopt the cloud with a structured approach that removes blockers and reduces time to value

Benefits

Leverage customer experiences, best practices, resources, tools, facilitates partner-customer alignment

Business strategy	People strategy	Security
Goals	Cloud center of excellence	Architecture
Business case	Change management	Deployment
Business value	Skilling and readiness	Maintenance

Process design	Technology implementation	Management and operations
Enterprise architecture	Landing zone	Monitoring
Governance	Migration	Cost Management
Risk and compliance	Modernization	Incident management

Business Strategy

Goals

Define success metrics.

Align them to business strategy and prioritize them

Consider all related economics

Business Case

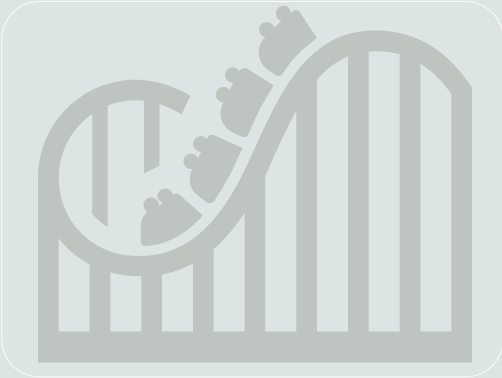
Create a strong business case to drive senior level sponsorship, align expectations, and provide a solid planning foundation for cloud adoption

Business Value

.

Evaluate how successfully the organization is accomplishing its goals for cloud adoption, review the metrics and key performance indicators (KPIs)

People Strategy



CCOE:

The CCOE is an extended multidisciplinary team that includes both business and technical stakeholders to sponsor and guide the cloud adoption initiative.

Upskilling & Readiness:

Develop a comprehensive workforce readiness plan

Change Management

Create a change management plan to make a company-wide engagement

People- Strategy CCOE

Executive Team

CEO
CIO/CTO
CFO
COO

Drive the focus on the organizational goals pursued with cloud adoption
Validate and sponsor the cloud adoption business case
Sponsor the changes in people, processes, and technology
Achieve stakeholder buy-in across IT and business
Move the cloud strategy forward and remove resistance to move to the cloud
Remove financial inhibitors
Remove organizational inhibitors
Validate business value

Business Team

HR
IT Security
Finance
Legal
Procurement

Evangelize the value of cloud adoption for each business unit
Free up internal resources and allocate them to the cloud adoption initiative
Drive consensus between the business and IT
Ensure that the right skills are deployed in the areas of business, architecture, and implementation

Technical Team

Program Manager
Enterprise Architect
Cloud Architect
DevOps Architect
Infrastructure Architect
IT Leadership Team
Cybersecurity Architect
Compliance Architect
Infrastructure Architect
Networking Architect
Security Architect

Coordinate with the on-premises IT team
Define the scope of adoption
Define the enterprise architecture
Define the IT solution
Define the execution timeline
Remove siloed teams, siloed releases, and siloed operations
Iteratively mature the cloud governance and security model

People Strategy – Upskilling & Readiness

Start

Mapping of current roles to cloud roles, adjusting where needed

Assessment

Current capabilities
Current capacity
Talent development plan
Talent attraction plan
Talent retention plan

Training Plan

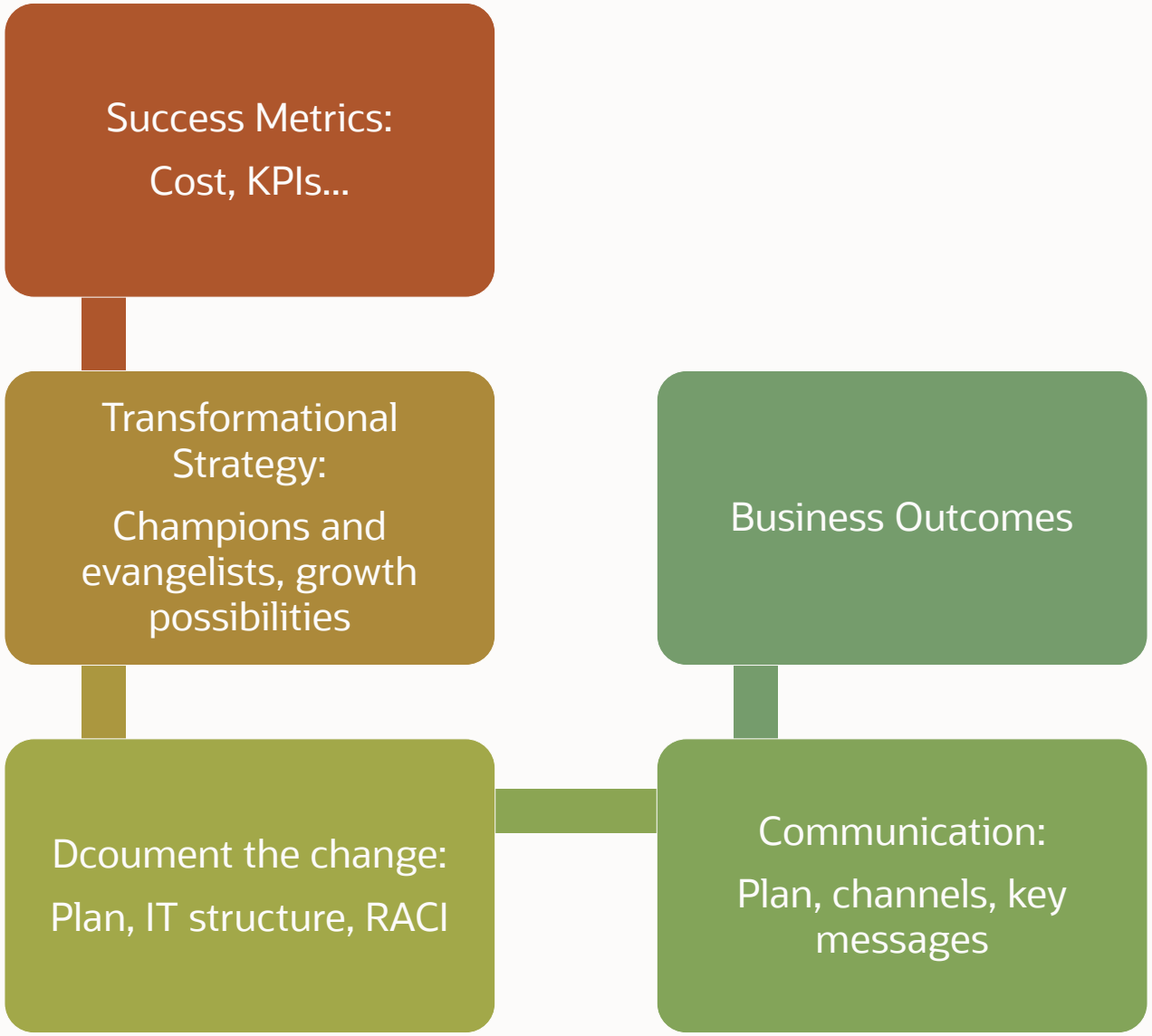
Business users

OCI Foundations

IT users

- Security (third party)
- Architect Associate
- Architect Professional
- Cloud Operations Associate
- Developer Associate

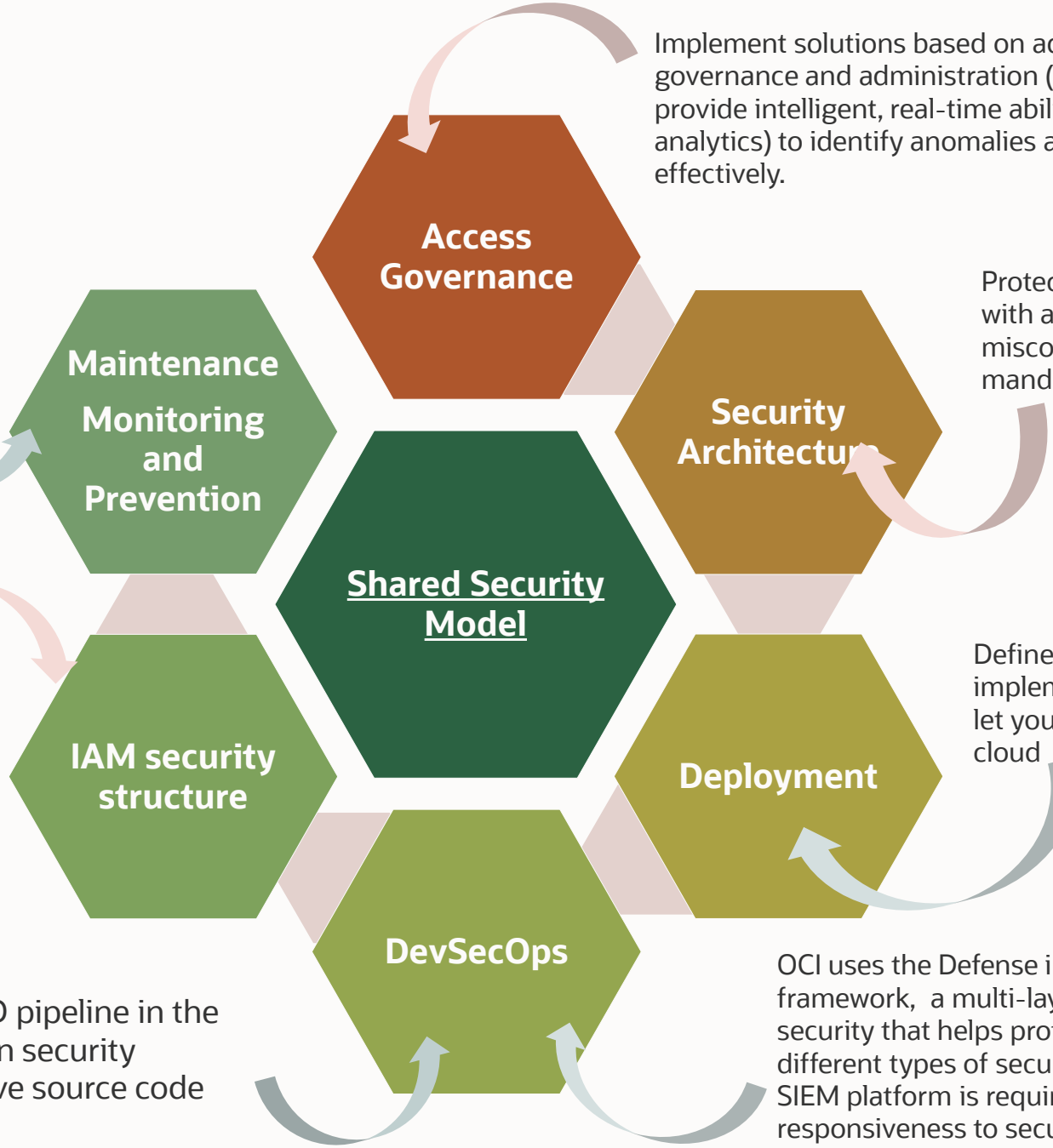
People Strategy – Change Management Plan



Security Strategy

Organizations must be prepared for a variety of threats. Main issues to consider are:

- **Advanced persistent threats**
- **Porous perimeter**
- **Unsanctioned IT**



Implement solutions based on advanced identity governance and administration (IGA) capabilities that provide intelligent, real-time abilities (such as prescriptive analytics) to identify anomalies and mitigate security risks effectively.

Protect your organization's assets with a security architecture that prevents misconfiguration errors and implements mandatory security best practices.

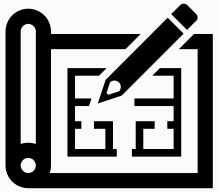
Define robust security controls and implement standard configurations that let you securely deploy resources in the cloud

OCI uses the Defense in depth (DiD) framework, a multi-layer approach to security that helps protect data by using different types of security defenses. A SIEM platform is required to increase responsiveness to security attacks.

Before creating multiple OCI cloud resources, we recommend to set up an identity and access management (IAM) security model

Analyze components of the CI/CD pipeline in the deployment process to strengthen security defenses. Consider how to improve source code and protect code repositories.

Process Design



Enterprise Architecture

EA includes several layers:

business architecture

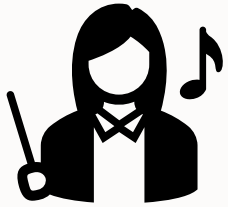
data architecture

application architecture

technology architecture

security architecture

Each layer provides a different perspective of IT systems and processes and helps to ensure that all components of the technology infrastructure work together seamlessly.

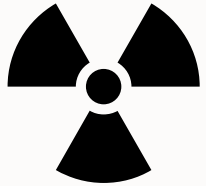


Governance

Establish a set of policies, processes, and controls to guide and manage the use of cloud computing resources within an organization. It ensures that cloud services are used in a secure, compliant, and efficient way.

Key Principles

- ✓ *Alignment with Business objectives*
- ✓ *Risk management and Security*
- ✓ *Compliance and Regulatory Adherence*
- ✓ *Cost Optimization & resource efficiency*
- ✓ *Interoperability & Integrations*
- ✓ *Communication*
- ✓ *Vendor management*
- ✓ *Change management*
- ✓ ....



Risk & Compliance

Refers to the set of policies, procedures, and practices that ensure the identification, assessment, and mitigation of risks associated with cloud-based technology solutions.

Considerations*	Examples
Regulatory Analysis	PCI. GDPR. HIPAA...
Risk Assessment	Risk Identification, Risk Register, Risk Prioritization...
Vendor Due Diligence	Conduct due diligence
Awareness & Training	Policy development
Security Control Implementation	Define encryption, implement MFA
Continuous Monitoring	Define tools, thresholds..
Incident Response planning	Establish team, policy, severity..

*these are just some considerations.
For full details visit https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/risk-and-compliance.htm

Technology Implementation

The ***technology implementation*** pillar focuses on transforming your governance and security model into a cloud environment that is deployed to meet the organization's needs.

Landing Zone

The landing zone helps customers quickly and securely create a foundation for cloud deployment based on Oracle recommendations, customer experience, and industry-standard best practices. The landing zone consists of Terraform modules, in addition to architecture and implementation information.

OCI provides multiple landing zone implementations that you can choose from. See How Do I Decide Which Landing Zone to Use?

HA & DR

The first step in planning for DR involves determining the recovery time objective (RTO) and recovery point objective (RPO). Full Stack Disaster Recovery (FSDR) is an OCI native service that provides a simple and consistent interface to orchestrate DR operations for many different systems, making it easy for any authorized user in your IT operations to trigger a failover or switchover without needing to understand any of the underlying recovery processes.

-> Determine which applications require HA

-> Leverage regions and availability domains

->Chose over Active/Passive and Active/Active deployments

Scenarios for Design & Implementation

An enterprise architecture for the cloud will allow customers to benefit from:

-> Scalability

-> High reliability

-> Security

-> Agility

-> Cost effectiveness

-> Manageability

Enterprise scenarios for design and implementation of cloud adoption involve planning and executing the transformation of an organization's technology infrastructure and processes to

leverage cloud computing services.

- **Enterprise Ready**
- **Cloud Native**

Management & Operations

OBSERVE:

Know what is happening in your environment

Optimize:

Maximize Performance and minimize costs by right-sizing and decomissioning

Operate:

Maintenance

Onboarding Workloads

Oracle/Oci products lifecycle management

Multi-Cloud

Support & Incident management

Minimize service disruption

Integrate with IT service management

Management & Operations
Where do I start: Cloud Operating Model

Oracle Cloud Infrastructure (OCI) Cloud Operating Model (COM) provides actionable information to help enterprises operationalize Oracle Cloud and provides a template to define and build your organization's IT model for ongoing operations (Day2 onwards) and governance of your OCI environments.
It's a framework that identifies the most common operational and functional scenarios to consider and procedures to establish according to your requirements.

COM is generally organized in 4 areas

Security

- Onboarding new business units and users
- Environment isolation
- Handling real time security events and threats
- User administration
- Regulatory and organizational compliance

FinOps

- Cost management best practices that address questions about cost creep causes, identifying cost creep areas, and mitigating and preventing cost creep and budget overrun

New Workload Onboarding

- Choosing the right OCI PaaS/IaaS/DBaaS based on workloads and your architectural considerations
- Rationalizing between "lift and shift" versus "modernize and migrate"

Operations and Support

- Ongoing maintenance of OCI IaaS and PaaS
- Managing OCI product lifecycle
- Oracle/OCI support
- Integration with your ITSM and third-party tools
- IaaS and PaaS monitoring

Technology: components supporting security strategy, operations support and incident management, finops

Processes: Define Business and Technical processes needed to achieve business goals

People: Cloud Center of Excellence and organisational structure

Security Operations

Security

IAM Governance

- Onboarding new business units and users
- User administration

Organization and Tenancy

IAM Identity Domains

Compartments and Tagging structure for fine-grained IAM Policies

SecOps enablement

- Handling real time security events and threats
- Regulatory and organizational compliance

Cloud Guard

Enable Security Operation Teams Early

Monitor Vulnerabilities with Regular Scanning

Log Archiving and SIEM Integration

Environment isolation

Evaluate and Use Security Zones together with Cloud Guard

Management & Operations- Operations & Support

Iaas & Paas Maintenance

Upgrading to newer versions of OCI services

New Workload Onboarding

Support & Incident management

Cloud Operations Team
Operational Areas

Ongoing maintenance of IaaS and platform as a service (PaaS) in OCI
Onboarding new business units (BUs) and workloads to OCI
Incident management
IaaS and PaaS monitoring with OCI-native services
Integration with third-party observability, IT service management (ITSM), and collaboration tools
Managing OCI services that are approaching End-of-Support-Life (EOSL)
SecOps

Management & Operations- Iaas & Paas Maintenance

Iaas & Paas Maintenance

Patching

OCI VMs	Overview of OS Management
OCVS	Upgrading VMWare software in OCI
EXA	Patch and Update an Exadata Cloud Infrastructure System
DBCS	Upgrade a DB System
Oracle Products on OCI	EBS on OCI

Vulnerability Management

OCI Networking and OCI Compute	Vulnerability Scanning

Management & Operations: Upgrading to newer versions of OCI services

Upgrading to newer versions of OCI services

Upgrade

OCI Core Iaas	Plan a phased migration to newer compute shapes
OCI Paas	Architect new workloads using the newer features while planning a phased migration of existing workloads.
Oracle Databases	Deploy newer workloads on the latest Oracle Database PaaS version.
Oracle Apps running on OCI	Packaged application versions running in OCI follow a similar lifecycle to running them on premises.

OCI Product Lifecycle Events

End of Orderability	Capacity or service limit increases are granted only under exceptional circumstances.
End of Sale	•New Universal Cloud Credits (UCCs) don't list the SKUs for end-of-sale products. •Capacity or service limit increases aren't guaranteed for all regions. •Services continue to be supported.
End of Support Life	•Beyond a published date, there is no support for the OCI products. •You are advised to discuss migration and upgrade options with Oracle account teams. •Oracle publishes the dates for such events and products on the Oracle support portal

Management & Operations: Onboarding New Workloads

Onboarding New Workloads

Choose the Most suitable Paas and Iaas based on

- Application Charatecteristics
- Existing Licenses
- Certification of a packaged application with the appropriate OCI middleware or database
- High availability and disaster recovery considerations (RPO/RTO)
- Performance and cost objectives

Management & Operations: Optimize

Optimization Best Practises

Architect cloud-first workflows that can adjust to elastic demand with limited human intervention.

Evaluate cloud services in the context of your requirements.
Understand which cloud services best support the architecture and current business requirements.

Be data driven. Data should inform decisions and provide detailed insight into your workload performance.

Anticipate growth. Over time, your workloads might grow or expand into more geographical regions. Ensure that your architecture and the services that you use support your business growth.

Optimize spending. The cloud allows for rapid provisioning of services.
When your demand increases, it's important to have visibility into the associated costs and how to manage them.

Architect for reliability and resiliency. A robust cloud resiliency architecture must handle different types of adversities and correlated failures, such as hardware failure, data center disasters, network outages, software bugs, cyberattacks, or operational errors

Management & Operations: OCI Tools to Understand and Manage Cloud Spending

Cloud cost planning	OCI Cost Estimator
Billing and reporting	Cost Analysis Cost and usage reports
Detailed billing analysis	OCI Cost Governance and Performance Insights solution
Invoicing	Invoices Payment history Billing schedule
Forecasting	Forecasting in Cost Analysis
Tagging	Tags
Alerts and notifications	Budget alerts
Template driven deployment	Terraform
Controls	Quotas Enforcing budgets using functions and quotas
Recommendations	Cloud Advisor

Management & Operations: Observability & Management

Monitoring is a tool or a service that watches a system's state and triggers a notification when a predefined condition is met.

Observability is a tool or a solution that uses a system's telemetry data, such as metrics, logs, and traces, to debug a problem and improve performance.

Observability & Management

A top priority is to increase automation that enables scalable, predictable results. Use integrated functionality and automation for DevOps monitoring and IT operations management to prevent and solve IT problems.

Logging lets you enable, view, and manage all the logs in the tenancy, and provides access to logs from Oracle Cloud Infrastructure resources.

Logging Analytics is a unified, integrated cloud solution that enables users to monitor, aggregate, index, analyze, search, explore, and correlate all log data from their applications and system infrastructure.

Use Monitoring to query metrics and manage alarms. Metrics and alarms help monitor the health, capacity, and performance of your cloud resources

Database Management provides comprehensive database performance diagnostics and management capabilities to monitor and manage Oracle databases.

Application Performance Monitoring provides deep visibility into applications performance and enables rapid diagnostics in order to deliver a consistent level of service.

Management & Operations: Support & Incident Management

Optimization Best Practises

Architect cloud-first workflows that can adjust to elastic demand with limited human intervention.

Evaluate cloud services in the context of your requirements.
Understand which cloud services best support the architecture and current business requirements.

Be data driven. Data should inform decisions and provide detailed insight into your workload performance.

Anticipate growth. Over time, your workloads might grow or expand into more geographical regions. Ensure that your architecture and the services that you use support your business growth.

Optimize spending. The cloud allows for rapid provisioning of services.
When your demand increases, it's important to have visibility into the associated costs and how to manage them.

Architect for reliability and resiliency. A robust cloud resiliency architecture must handle different types of adversities and correlated failures, such as hardware failure, data center disasters, network outages, software bugs, cyberattacks, or operational errors

Management & Operations: Support & Incident Management