Meeting Cloud Sovereignty expectations: sharing lessons learned
The Hyperscaler’s perspective - Oracle

Damien Rilliard
Senior Director, EMEA Sovereignty Lead
Oracle EMEA Sovereign Cloud and Public Sector CoE
Geo-political context is the key driver of Digital Sovereignty globally...

... foreign risk is rising, leading to the need for more control over critical systems and data.

- Russian invasion of Ukraine
- Indo-Pacific strategic competition between China and the US
- Rising instability in various parts of the globe
- Rise in Risk Perception across Public and Private Sector leaders
- Re-alignment of Economic and Trade Blocks
- De-globalization or New Risk Mitigation strategies?
“Every government is going to want a sovereign cloud.”

Larry Ellison
CNBC Analysis
April 7, 2024
A Sovereign Cloud addresses the sovereignty requirements of a region, country, or organization.

Sovereignty is a political and economic topic as much as a technical one. It relates to how the cloud provider implements and delivers the cloud platform and it may involve technical, contractual, organizational, and legal requirements.
What about Security and Sovereignty?

*Security alone cannot bring Sovereignty*

All public clouds offer tools that help with (Zero Trust) Security...

...but alone it cannot address Sovereignty.

Reaching Sovereignty goals requires organizational, technical, legal and contractual steps from the CSP - this represents the hidden tip of the iceberg.

That’s what you should pay attention to in relation with each of your “Sovereignty goals”
Primary components of digital sovereignty

**WHERE?**
- Data Sovereignty
  - Data Access and processing
  - Region location including disaster recovery

**WHO?**
- Technological Sovereignty
  - Who operates and supports regions
  - Open Source, External Key Mgt, Knowledge

**HOW?**
- Laws and regulations
  - Contractual clauses over operations and hardware

Digital Sovereignty

Copyright © 2024, Oracle and/or its affiliates | Restricted
Oracle’s approach to Sovereignty: OCI Sovereign Cloud Principles
Six key capabilities to address our customers Sovereignty requirements

**PRINCIPLE 1: LOCATION**
Control data localization, including into your own data center.

**PRINCIPLE 2: ISOLATION**
Control barriers to data movement, such as separated realms, isolated networks, and disconnected operation.

**PRINCIPLE 3: ACCESS MANAGEMENT**
Restrict tenancies in a cloud to specific geographies, users, company, or organization.

**PRINCIPLE 4: PERSONNEL REQUIREMENTS**
Set criteria for operations and support personnel, including residency or additional security clearances.

**PRINCIPLE 5: ENCRYPTION**
Customers can bring a key from their own key management infrastructure to Oracle and use it with any integrated OCI services or from within their own applications.

**PRINCIPLE 6: DATA ACCESS REQUESTS**
Oracle can establish special legal entities, alone or through partners, along with contractual and operational business practices to meet local sovereignty needs.
One size does not fit all.
Multiple deployment options, supporting each region’s specific requirements
Example: deployment on an independent, dedicated Cloud for EU customers

Key features of Oracle EU Sovereign Cloud

- Customers can rely on the same enterprise-grade support at no extra cost
- No joint venture or partnership complexities in time to market, operations, features set, or depth of support
- Strong set of organizational, technical and contractual controls
Oracle Cloud Infrastructure Europe Footprint

2024
15 regions in Europe
3 Azure Interconnect Regions

100% renewable energy by 2025
Oracle Cloud Infrastructure Europe Footprint

2024
15 regions in Europe
3 Azure Interconnect Regions

EU Sovereign Central
(Frankfurt)

EU Sovereign South
(Madrid)

Newport
(UK West, UK Gov)

London
(UK South, UK Gov)

Paris
(France Central)

Madrid
(Spain Central)

Marseille
(France South)

Milan
(Italy Northwest)

Amsterdam
(Netherlands Northwest)

Stockholm
(Sweden Central)

Zurich
(Switzerland North)

Frankfurt
(Germany central)

Serbia Central
(Jovanovac)

Oracle Cloud Infrastructure Europe Footprint

100% renewable energy by 2025

Copyright © 2024, Oracle and/or its affiliates  |  Restricted
January 2024

2 Sovereign Regions in Europe

EU Sovereign Cloud Realm

EU Sovereign Central (Frankfurt)

EU Sovereign South (Madrid)

100% renewable energy by 2025
June 2023
2 Sovereign Regions in Europe

EU Sovereign Cloud Realm

EU Sovereign South (Madrid)
EU Sovereign Central (Frankfurt)

100% renewable energy by 2025
Organizational Controls
EU Sovereign Cloud Entities, Operations and Support

Operated by new, EU based legal entities created for this EU Sovereign region purpose. These entities own:
- Hardware and assets
- Data Center leases
- Cloud operations
- Customer Support

The isolation of the EU Sovereign Cloud realm allows Oracle to restrict support and operations personnel to EU residents employed by the EU legal entities, including physical and logical access to the realm.

The EU-based legal entities are backed by a governance committee to ensure integrity and alignment with current and future regulations.

Support and operations are delivered within EU borders by EU residents employed by EU legal entities isolated from Oracle global cloud operations.
EU Sovereign Cloud Dedicated Entities

Oracle Sovereign Cloud Germany GmbH

Oracle Sovereign Cloud Spain, SRL

Oracle Sovereign Cloud Ireland Ltd

Oracle Sovereign Cloud Czech Republic S.R.O

Oracle Sovereign Cloud Romania S.R.L

Responsible for providing support, hosting, and maintenance services for Oracle Sovereign Cloud Entities and for procuring EU Sovereign Cloud data centers

EU Sovereign South (Madrid) NEW

Complete EU Operations

Copyright © 2024, Oracle and/or its affiliates | Restricted
Technical Controls
Data residency by design makes sovereign cloud deployments quicker and simpler

**Physically and logically separated**
Oracle EU Sovereign Cloud is housed in physically isolated data center space and has no backbone network connection to Oracle’s other cloud regions.

**Independent operations**
EU Sovereign cloud operations and customer support are carried out within the EU by dedicated teams of EU residents, and are distinct from Oracle’s commercial operations.

---

**EU SOVEREIGN CLOUD REGIONS**
- Frankfurt
- Madrid
- Future expansion regions

**COMMERCIAL PUBLIC CLOUD REGIONS**
- DE Central
- US West
- UK South
- Other regions

Physical and logical isolation between realms
Full stack of sovereign cybersecurity, access and governance capabilities

Customers can easily implement their own controls to achieve their Sovereign security goals

**Prevent**
Block attacks and malicious traffic

**Monitor**
Log, analyze, and audit activity

**Mitigate**
Isolate comms with secure, reliable networks

**Protect**
Hardware-enabled security built into the architecture

**Encrypt**
Encrypt and protect all data

**Access**
Authentication, authorization, and governance

---

**INTERNET & EDGE**
- **MONITORING & PREVENTION**
  - Cloud Guard
  - Threat Intelligence
  - Threat Detector
  - Logging
  - Fusion Apps Detector
  - Vulnerability Scanning
  - Auditing
  - OCI API logging

**NETWORK**
- Virtual Cloud Network
- Secure, isolated network
- Network Firewall
- Advanced firewall service
- Bastion
- Time-limited SSH access
- Dynamic Routing Gateway
- Virtual router
- Fast Connect
- Dedicated, high-speed connection
- Virtual Private Network
- Secure connectivity over any network
- NAT Gateway
- Protected access to the internet

**COMPUTE**
- Bare Metal Servers
  - Servers with full Customer control
- Hardware Root of Trust
  - Protect from firmware attacks
- Signed Firmware
  - Prevent malware installation
- Hardened Disk Images
  - OS with expert security settings
- Off-box Control Plane
  - Isolated domain of compute hardware
- Off-box Network Virtualization
  - Encapsulated, separated traffic
- Oracle Linux & Oracle Enterprise Linux
  - Performant, secure, enterprise Linux

**STORAGE & DATABASE**
- Data Safe
  - Monitor data usage in database
- Vault
  - Hardware security module protection
- Key Management
  - Encryption key administration
- Secrets Management
  - Credential and similar administration
- Certificate
  - Validation certificate administration

**IDENTITY & OPERATOR ACCESS**
- Access Governance
  - Proactive guidance for user actions
- OCI Identity and Access Management
  - Centralized access to Cloud resources
- Policies
  - User access rules
- Federation
  - Identity provider inter-operation

---

**EUROPEAN UNION**
- Landing Zones
  - IC backbone network automation
- Security Zones
  - Security policy compliance
- Distributed Denial of Service protection
  - Automatic DDoS protection

**REALM**
- Web Application Firewall
  - Internet-facing endpoint protection
- Cloud Guard
  - Security posture management
- Threat Intelligence
  - Multi-source, actionable guidance
- Threat Detector
  - Monitor for known threats
- Logging
  - Single pane for service logs
- Fusion Apps Detector
  - Monitor SBF and HCM apps
- Vulnerability Scanning
  - Tools and path monitoring
- Auditing
  - OCI API logging
EU Sovereign Cloud is supporting your open-source code
Supporting our customers choice of open-source code as a sovereignty requirement

Managed open-source services available

Run the technologies you already use

Native integrations with the dev tools you're used to
What do you need in your Sovereign Cloud?
Identical Services as in Oracle Public Cloud

Oracle Applications
Industry | ERP | EPM | SCM | HCM | ACX

Custom Applications
Polyglot | Traditional | Cloud Native

ISV Applications
Hundreds to choose from

120+ public cloud services to support your workloads

50+ Oracle Fusion and Industry applications

10,000 OCI developers

3,000 field cloud engineers

Bring all of Oracle’s 120+ public cloud services and applications, with the same rates and SLAs, to your own data center
Contractual controls

Oracle European Union Sovereign Cloud Service Description

Oracle PaaS and IaaS Public Cloud Services Pillar Document

Appendix A-Oracle European Union Sovereign Cloud and Sovereign Operations

Oracle Data Processing Agreement for Oracle European Union Sovereign Cloud

1. Scope and Applicability

This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the European Union Sovereign Cloud ("EUSC") Services specified in Your Services Agreement. Unless otherwise expressly stated, this version of the Data Processing Agreement applies to the EUSC Service(s) and the Personal Information processed for Your benefit.
Conclusion
There’s more to Sovereignty than meets the eyes
Set clear objectives and do your due diligence with your partners on the key controls areas

Organizational Controls

Technical Controls

Contractual Controls

What is your data classification? What are your regulations requirements and Data Privacy objectives?
Which cloud capabilities do you need to meet your innovation objectives? (Who said AI?)
What is your budget, schedule, internal policies?

Controls should be designed to help address your Sovereignty goals and ensure that Your Content, including Personal Information, will not leave the Cloud you have selected without Your authorization or instruction.
Sovereignty links
Take a picture to read on your way back home ;-) 

Websites:
General Worldwide Sovereign Cloud Page
https://www.oracle.com/cloud/sovereign-cloud/

Oracle EU Sovereign Cloud
https://www.oracle.com/cloud/eu-sovereign-cloud/

Isolated cloud for Governments and Defense Mission
https://www.oracle.com/government/govcloud/isolated/

Dedicated Cloud Regions for Customers
https://www.oracle.com/cloud/cloud-at-customer/dedicated-region/

Whitepaper:
Oracle Sovereign Cloud Principles
Thank you

Damien Rilliard
Senior Director, EMEA Sovereignty Lead
EMEA Sovereign Cloud and Public Sector CoE
damien.rilliard@oracle.com