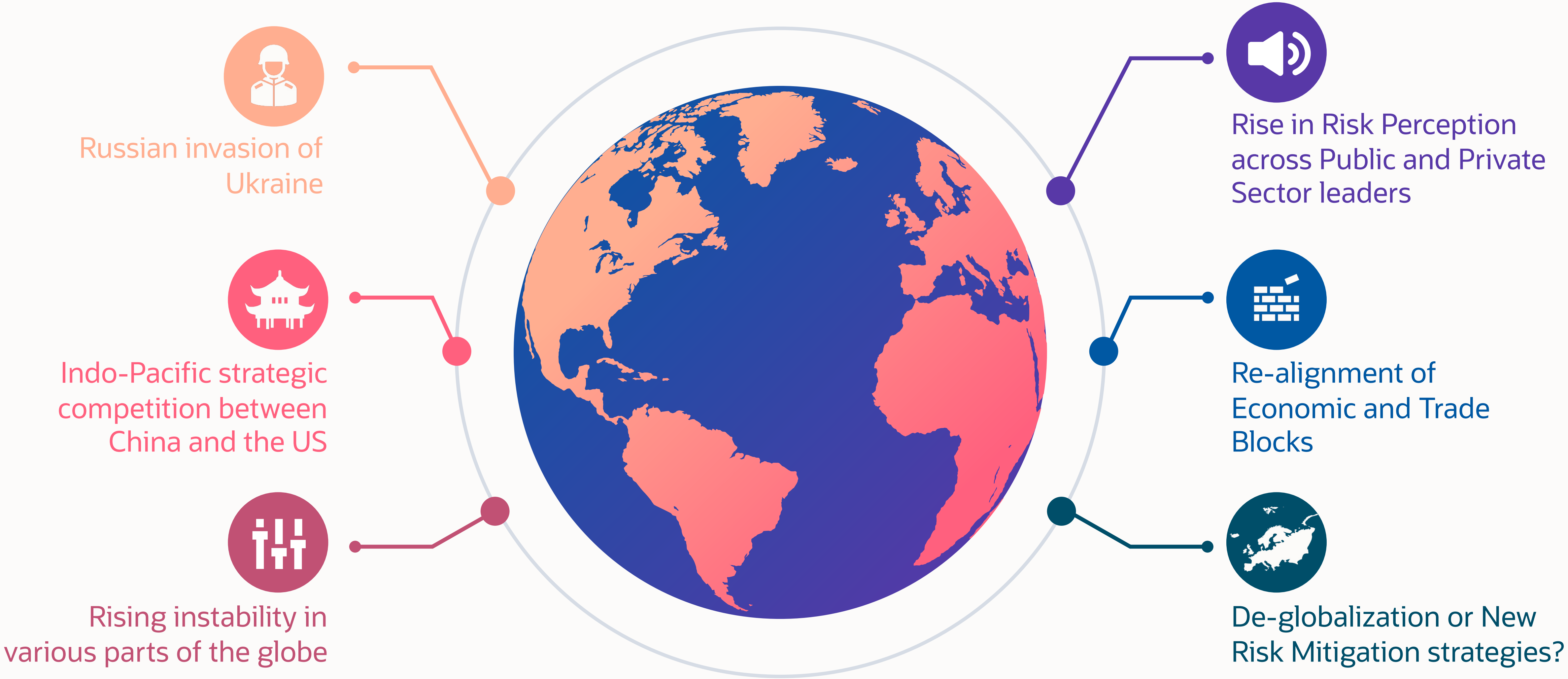
Meeting Cloud Sovereignty expectations: sharing lessons learned

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?

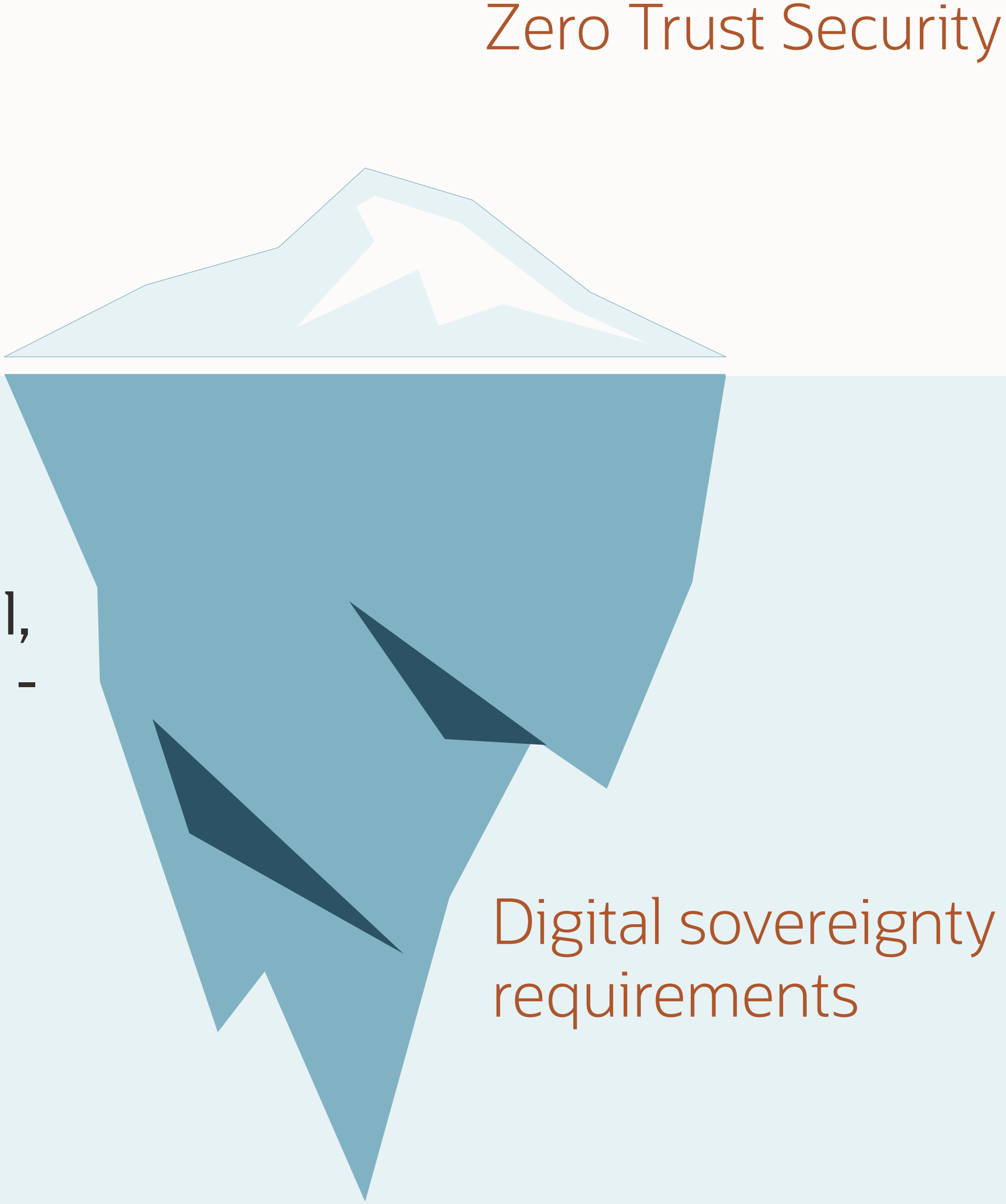
Security alone cannot bring Sovereignty

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

	Data Sovereignty	Technological Sovereignty
WHERE?	Data Access and processing	Region location including disaster recovery
WHO?	Who operates and supports regions	Open Source, External Key Mgt, Knowledge
HOW?	Laws and regulations	Contractual clauses over operations and hardware

Digital Sovereignty

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

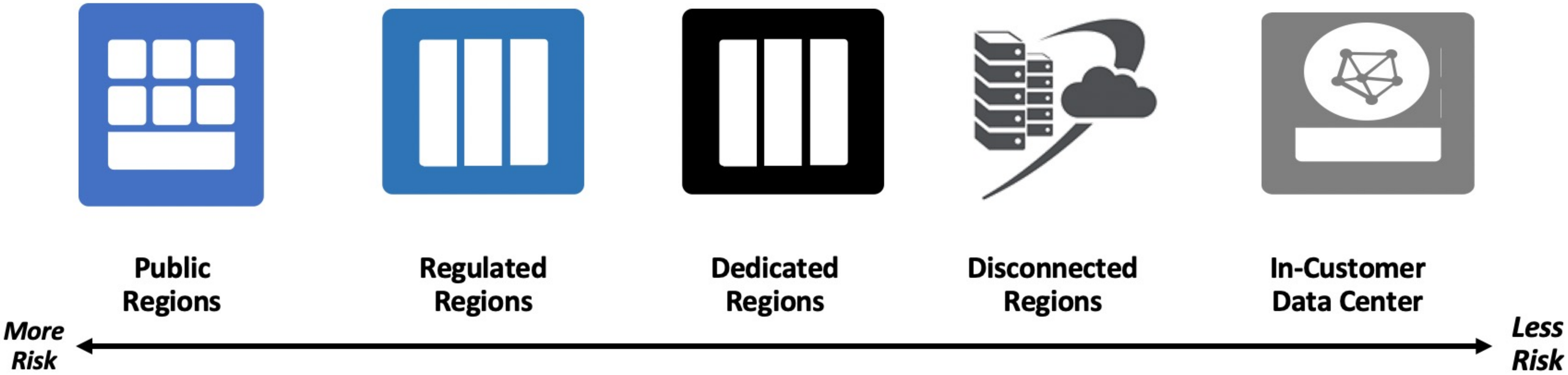
Customers can bring a key from their own key management infrastructure to Oracle and use it with any integrated OCI services or from within their own applications.

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



Public Regions

Regulated Regions

Dedicated Regions

Disconnected Regions

In-Customer Data Center

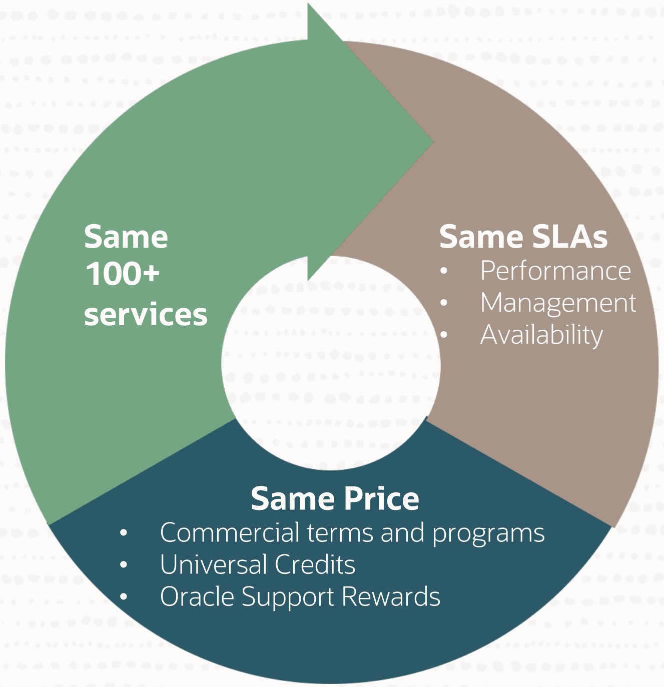
More Risk

Less Risk

Multi-Customer	*Single-Customer*		
Internet-Connected		*Air Gapped*	
Shared Ops Team		*Dedicated Ops Team*	*Customer Ops Team*

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

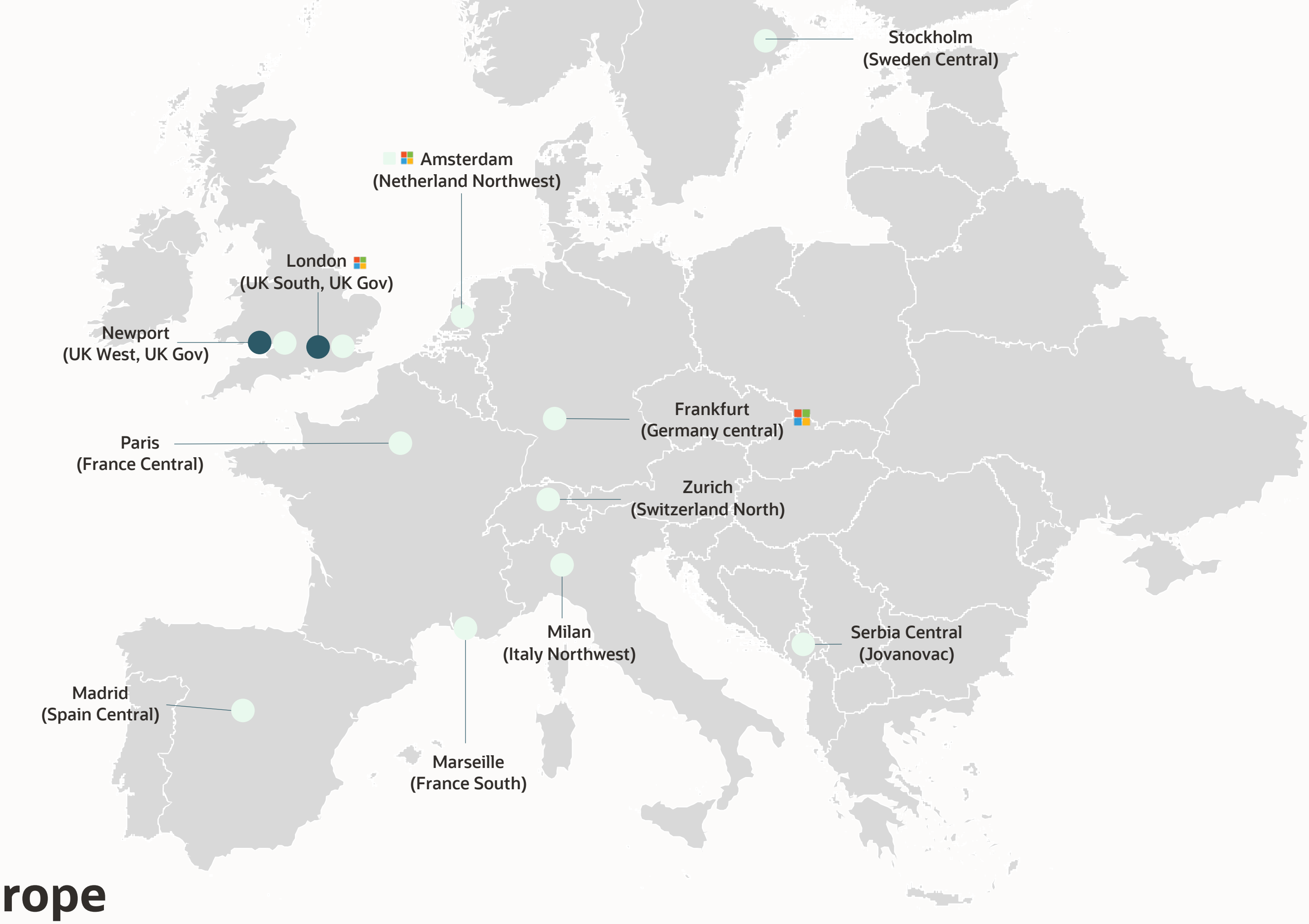
Cloud regions located in the EU

Different ownership

Compliance and governance

Security and sovereignty

Oracle Cloud Infrastructure Europe Footprint


Stockholm (Sweden Central)
Amsterdam (Netherland Northwest)
London (UK South, UK Gov)
Newport (UK West, UK Gov)
Frankfurt (Germany central)
Paris (France Central)
Zurich (Switzerland North)
Milan (Italy Northwest)
Serbia Central (Jovanovac)
Madrid (Spain Central)
Marseille (France South)

2024

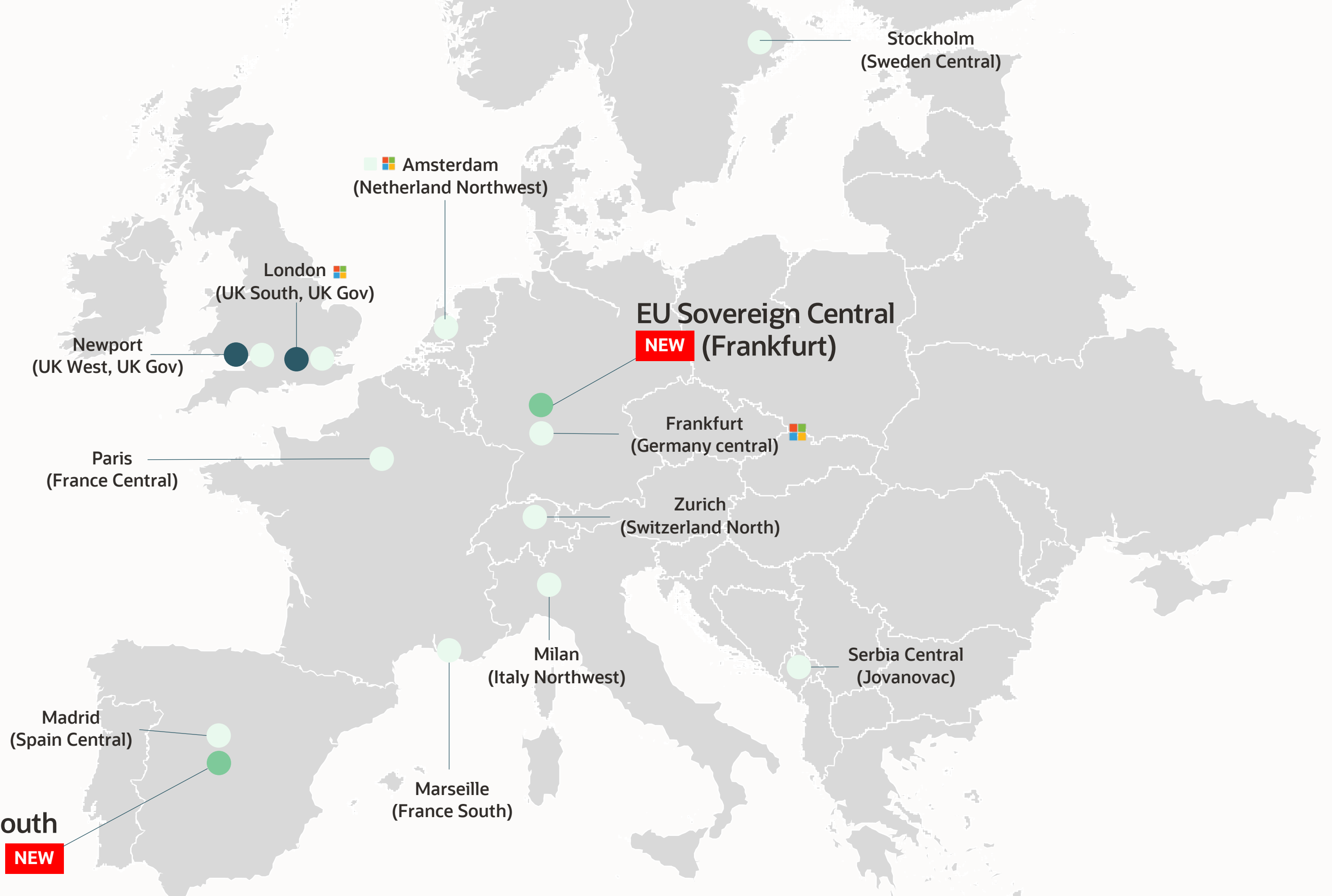
15 regions in Europe

3 Azure Interconnect Regions

100% renewable energy by 2025

⬜ Commercial	🟩 Sovereign
⬛ Government	⊞ Microsoft Interconnect Azure

Oracle Cloud Infrastructure Europe Footprint



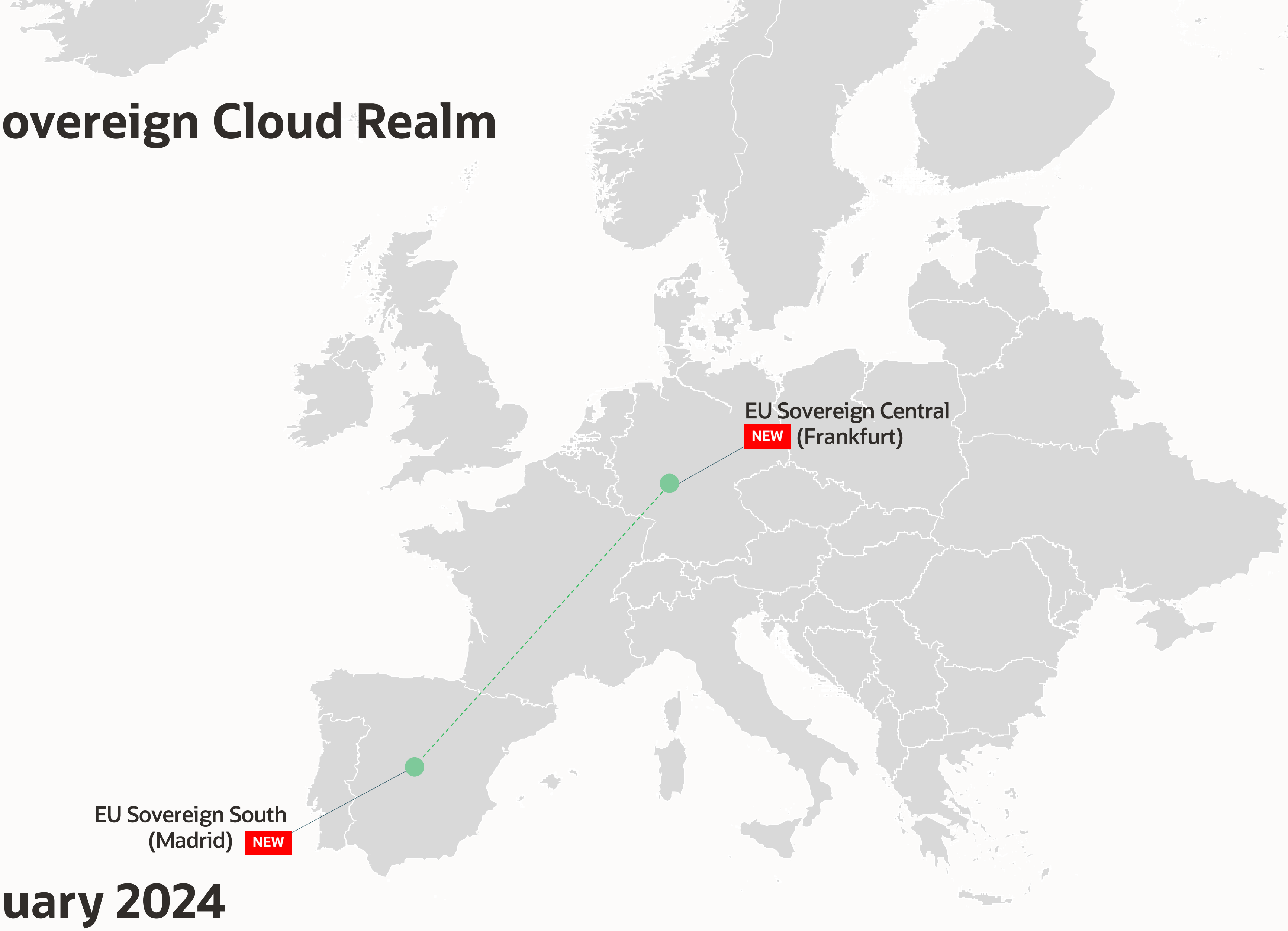
2024

15 regions in Europe

3 Azure Interconnect Regions

100% renewable
energy by 2025

EU Sovereign Cloud Realm



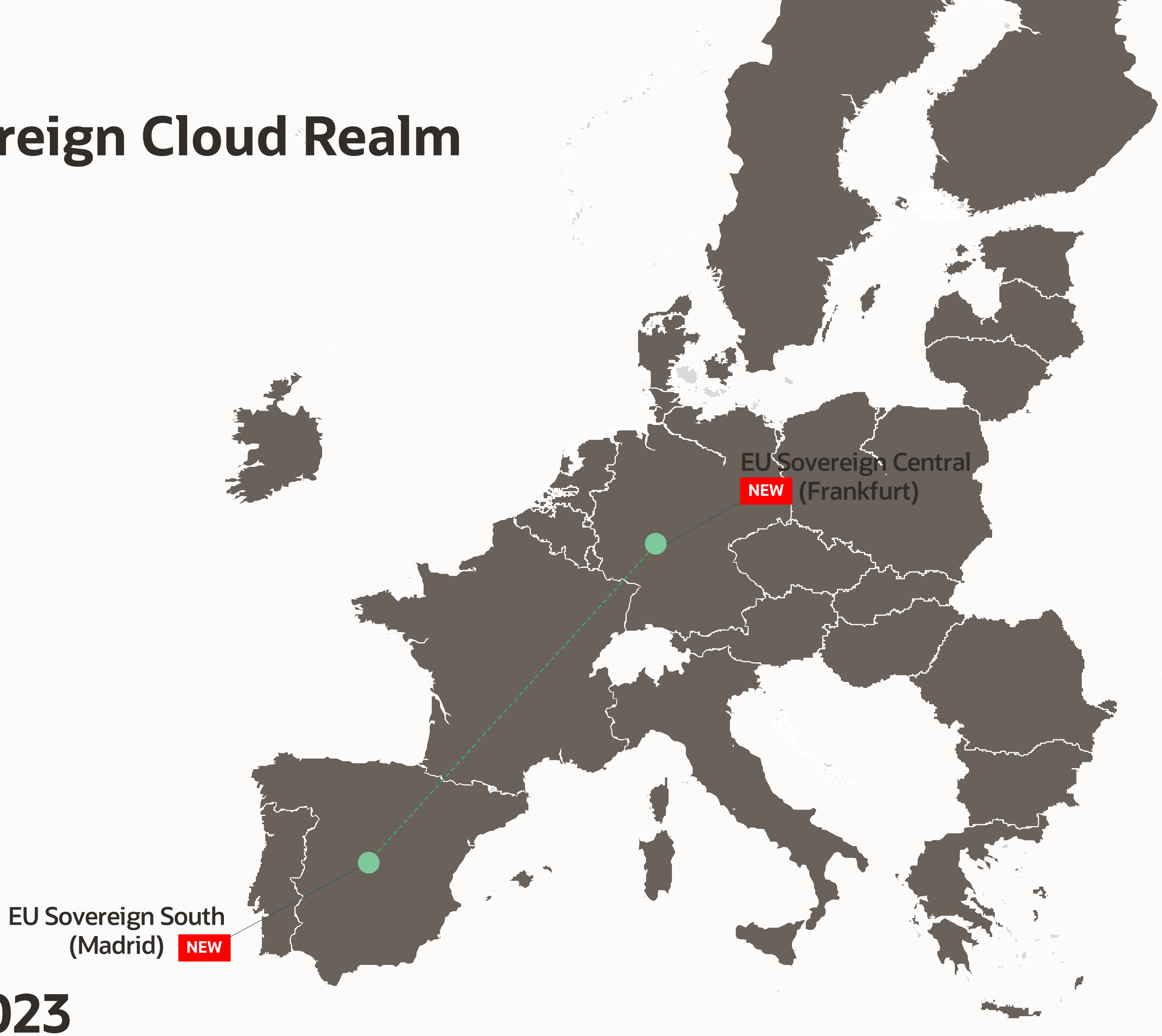
January 2024

2 Sovereign Regions in Europe

🟩 Sovereign

100% renewable energy by 2025

EU Sovereign Cloud Realm



🟩 Sovereign

100% renewable energy by 2025

June 2023

2 Sovereign Regions in Europe

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

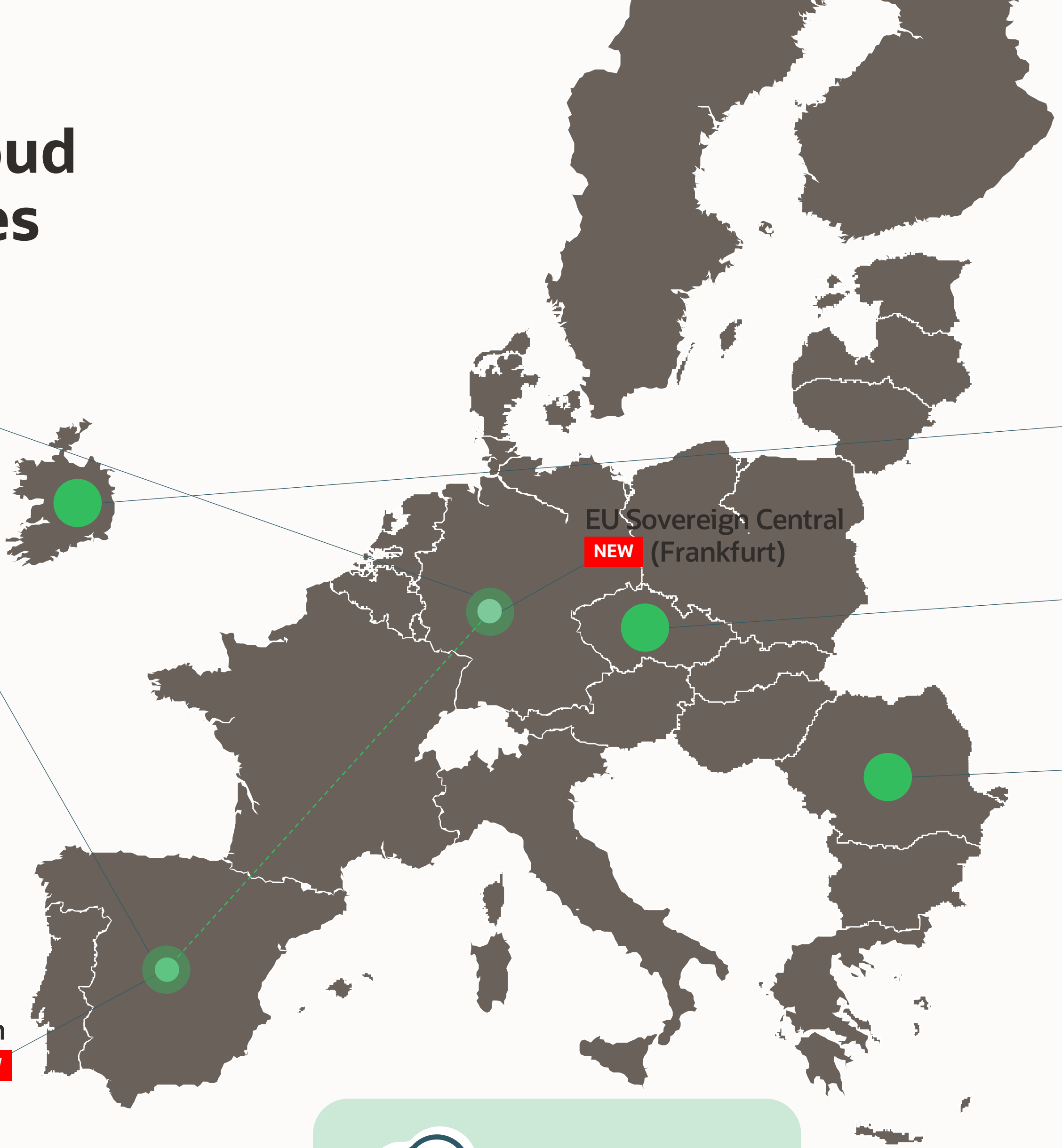
Support and operations are delivered within EU borders by EU residents employed by EU legal entities isolated from Oracle global cloud operations

EU Sovereign Cloud Dedicated Entities

Oracle Sovereign Cloud
Germany GmbH

Oracle Sovereign Cloud
Spain, SRL

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



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

COMPLETE EU OPERATIONS

Technical Controls

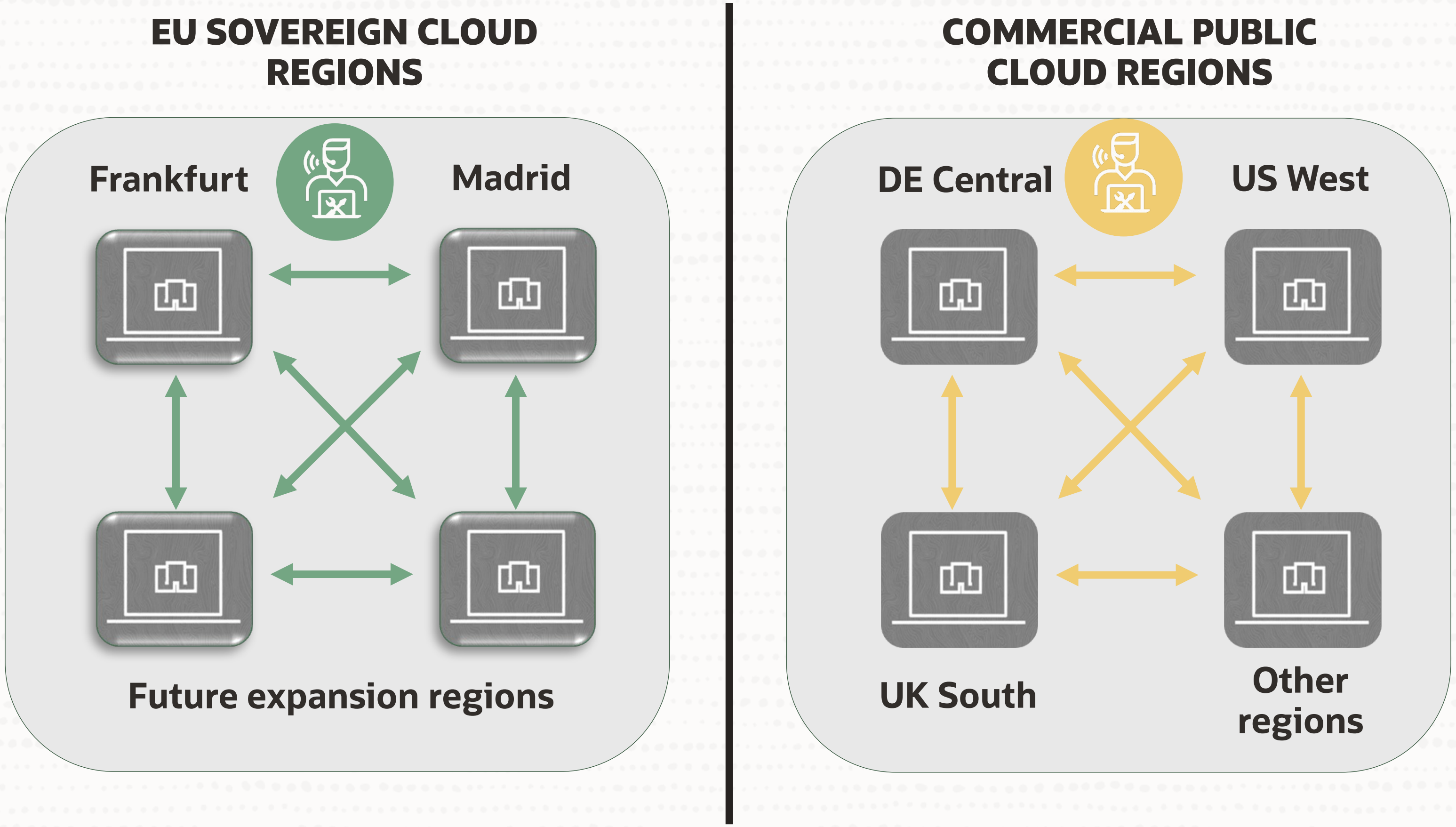
Data residency by design makes sovereign cloud deployments quicker and simpler

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

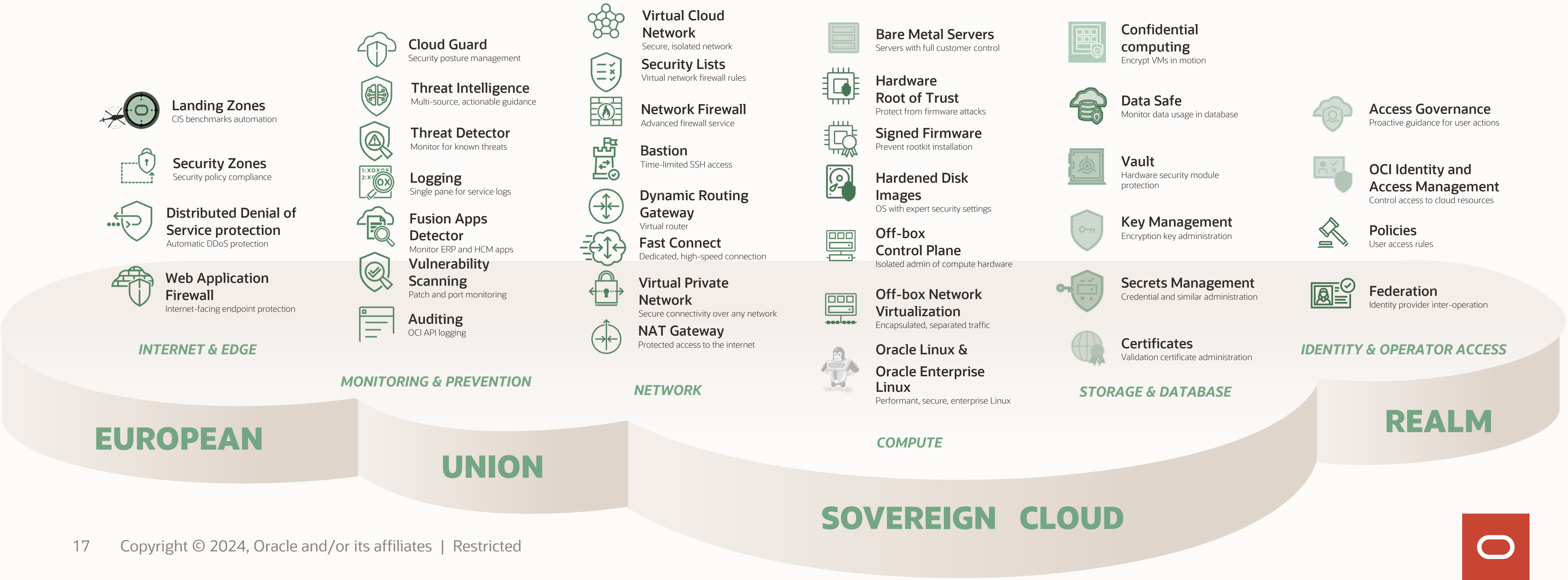


Physical and logical isolation between realms

Full stack of sovereign cybersecurity, access and governance capabilities

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

Prevent	Monitor	Mitigate	Protect	Encrypt	Access
Block attacks and malicious traffic	*Log, analyze, and audit activity*	*Isolate comms with secure, reliable networks*	*Hardware-enabled security built into the architecture*	*Encrypt and protect all data*	*Authentication, authorization, and governance*



INTERNET & EDGE

- **Landing Zones** – CIS benchmarks automation
- **Security Zones** – Security policy compliance
- **Distributed Denial of Service protection** – Automatic DDoS protection
- **Web Application Firewall** – Internet-facing endpoint protection

MONITORING & PREVENTION

- **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 ERP and HCM apps
- **Vulnerability Scanning** – Patch and port monitoring
- **Auditing** – OCI API logging

NETWORK

- **Virtual Cloud Network** – Secure, isolated network
- **Security Lists** – Virtual network firewall rules
- **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 rootkit installation
- **Hardened Disk Images** – OS with expert security settings
- **Off-box Control Plane** – Isolated admin of compute hardware
- **Off-box Network Virtualization** – Encapsulated, separated traffic
- **Oracle Linux & Oracle Enterprise Linux** – Performant, secure, enterprise Linux

STORAGE & DATABASE

- **Confidential computing** – Encrypt VMs in motion
- **Data Safe** – Monitor data usage in database
- **Vault** – Hardware security module protection
- **Key Management** – Encryption key administration
- **Secrets Management** – Credential and similar administration
- **Certificates** – Validation certificate administration

IDENTITY & OPERATOR ACCESS

- **Access Governance** – Proactive guidance for user actions
- **OCI Identity and Access Management** – Control access to cloud resources
- **Policies** – User access rules
- **Federation** – Identity provider inter-operation

EUROPEAN UNION SOVEREIGN CLOUD REALM

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

kubernetes
MANAGED CONTAINERS

docker
CONTAINERS

HashiCorp Terraform
INFRASTRUCTURE AS CODE

ORACLE
AUTONOMOUS LINUX

MySQL
DATABASE

hadoop
BIG DATA

APACHE Spark
ANALYTICS ENGINE

redis
CACHING DATABASE

fluentd
DATA COLLECTION

cloudevents
EVENT DELIVERY

kafka
STREAMING

DATABASE

fn
SERVERLESS PLATFORM

OpenSearch
SEARCH AND ANALYTICS

OPEN API INITIATIVE
INTERFACE DEFINITION

Run the technologies you already use

Red Hat
Oracle Linux
Ubuntu
CentOS
Debian
SUSE
LINUX OS

Microsoft
WINDOWS SERVER OS

vmware
VIRTUAL ENVIRONMENT

OpenJDK
PROGRAMMING LANGUAGE

GraalVM
PROGRAMMING LANGUAGE

mongoDB
DATABASE

APPLICATION FRAMEWORK

cassandra
NOSQL DATABASE

helidon.io
APPLICATION FRAMEWORK

HYPERLEDGER
BLOCKCHAIN

PyTorch
MACHINE LEARNING FRAMEWORK

Native integrations with the dev tools you're used to

GitHub
DEV-OPS

AUTOMATION

DEV-SEC-OPS

ANSIBLE
AUTOMATION

kubernetes
CONTAINER MANAGEMENT

HELM
PACKAGE MANAGEMENT

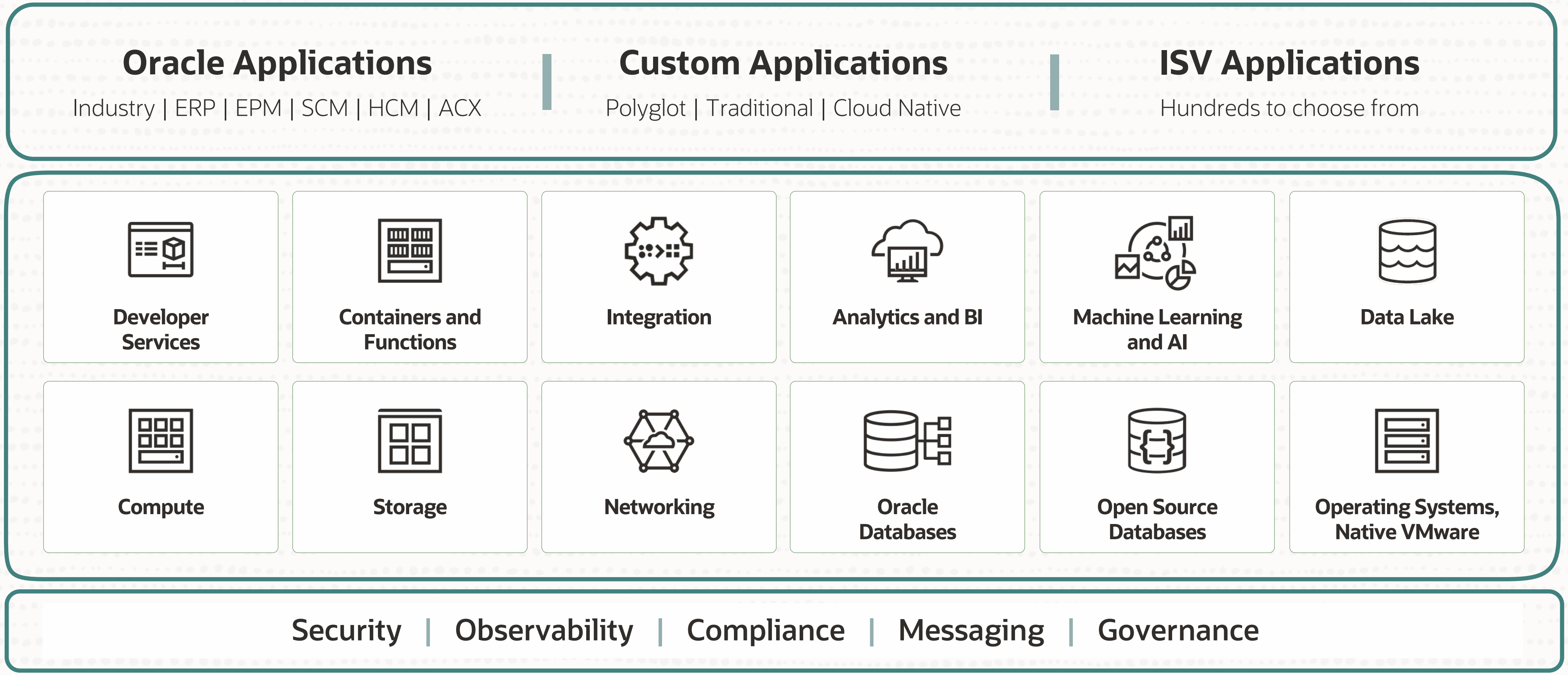
HashiCorp Terraform
INFRASTRUCTURE AS CODE

ATLASSIAN
TEAM COLLABORATION

RISK MANAGEMENT

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

- **Developer Services**
- **Containers and Functions**
- **Integration**
- **Analytics and BI**
- **Machine Learning and AI**
- **Data Lake**
- **Compute**
- **Storage**
- **Networking**
- **Oracle Databases**
- **Open Source Databases**
- **Operating Systems, Native VMware**

Security | Observability | Compliance | Messaging | Governance

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

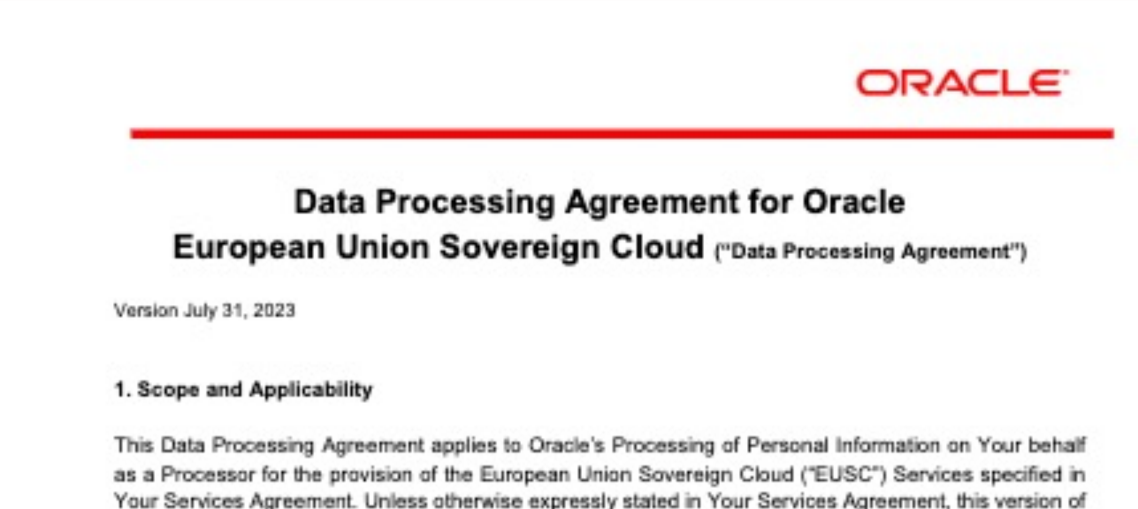
Contractual controls

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



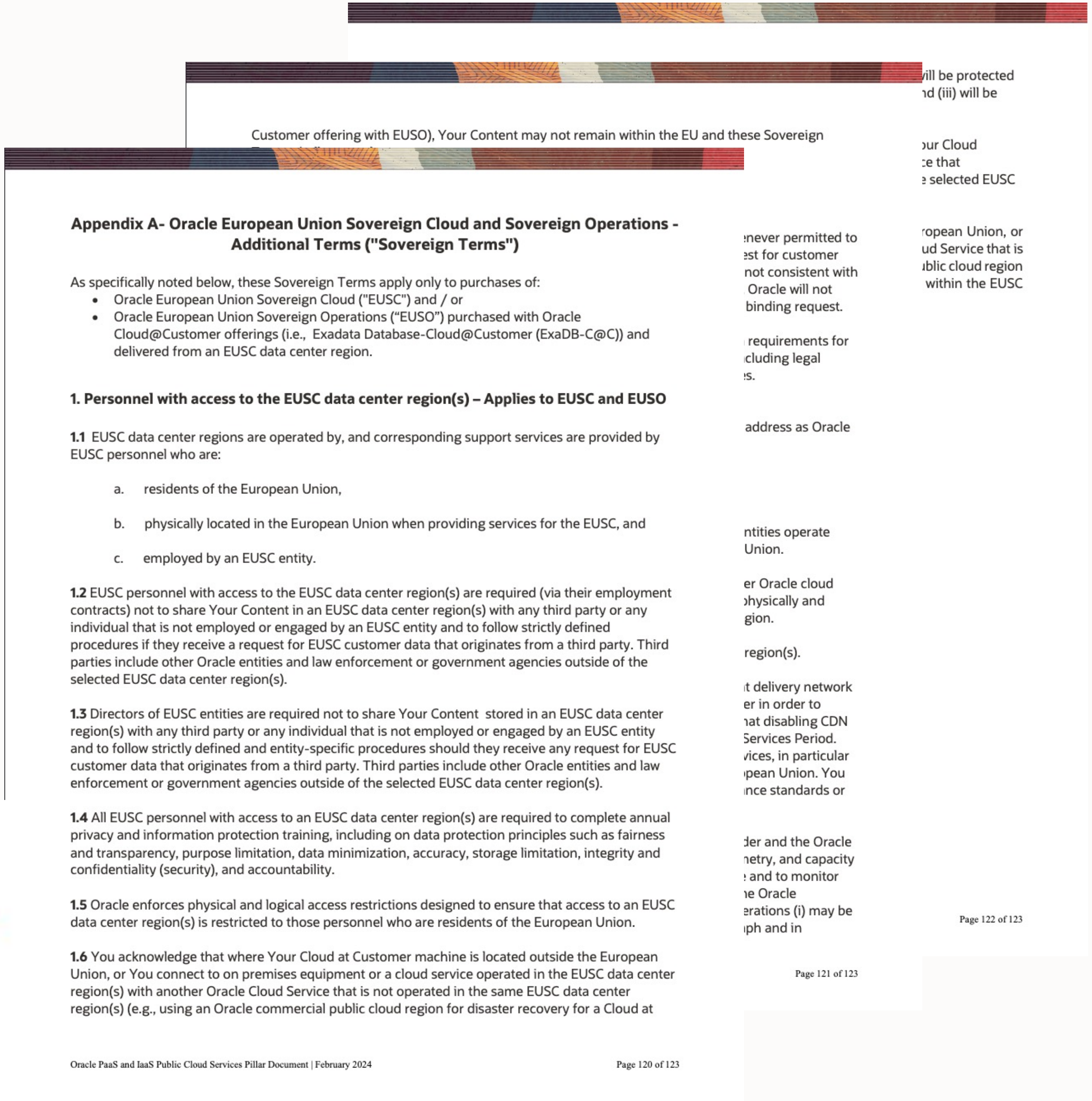
ORACLE

Data Processing Agreement for Oracle European Union Sovereign Cloud ("Data Processing Agreement")

Version July 31, 2023

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 in Your Services Agreement, this version of



vill be protected
nd (iii) will be

our Cloud
ce that
e selected EUSC

ropean Union, or
ud Service that is
ublic cloud region
within the EUSC

Page 122 of 123

Customer offering with EUSO), Your Content may not remain within the EU and these Sovereign

never permitted to
est for customer
not consistent with
Oracle will not
binding request.

requirements for
cluding legal
es.

address as Oracle

ntities operate
Union.

er Oracle cloud
physically and
gion.

region(s).

t delivery network
er in order to
hat disabling CDN
Services Period.
vices, in particular
pean Union. You
nce standards or

der and the Oracle
netry, and capacity
and to monitor
he Oracle
erations (i) may be
ph and in

Page 121 of 123

Appendix A- Oracle European Union Sovereign Cloud and Sovereign Operations - Additional Terms ("Sovereign Terms")

As specifically noted below, these Sovereign Terms apply only to purchases of:

- Oracle European Union Sovereign Cloud ("EUSC") and / or
- Oracle European Union Sovereign Operations ("EUSO") purchased with Oracle Cloud@Customer offerings (i.e., Exadata Database-Cloud@Customer (ExaDB-C@C)) and delivered from an EUSC data center region.

1. Personnel with access to the EUSC data center region(s) – Applies to EUSC and EUSO

1.1 EUSC data center regions are operated by, and corresponding support services are provided by EUSC personnel who are:

a. residents of the European Union,

b. physically located in the European Union when providing services for the EUSC, and

c. employed by an EUSC entity.

1.2 EUSC personnel with access to the EUSC data center region(s) are required (via their employment contracts) not to share Your Content in an EUSC data center region(s) with any third party or any individual that is not employed or engaged by an EUSC entity and to follow strictly defined procedures if they receive a request for EUSC customer data that originates from a third party. Third parties include other Oracle entities and law enforcement or government agencies outside of the selected EUSC data center region(s).

1.3 Directors of EUSC entities are required not to share Your Content stored in an EUSC data center region(s) with any third party or any individual that is not employed or engaged by an EUSC entity and to follow strictly defined and entity-specific procedures should they receive any request for EUSC customer data that originates from a third party. Third parties include other Oracle entities and law enforcement or government agencies outside of the selected EUSC data center region(s).

1.4 All EUSC personnel with access to an EUSC data center region(s) are required to complete annual privacy and information protection training, including on data protection principles such as fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security), and accountability.

1.5 Oracle enforces physical and logical access restrictions designed to ensure that access to an EUSC data center region(s) is restricted to those personnel who are residents of the European Union.

1.6 You acknowledge that where Your Cloud at Customer machine is located outside the European Union, or You connect to on premises equipment or a cloud service operated in the EUSC data center region(s) with another Oracle Cloud Service that is not operated in the same EUSC data center region(s) (e.g., using an Oracle commercial public cloud region for disaster recovery for a Cloud at

Oracle PaaS and IaaS Public Cloud Services Pillar Document | February 2024 Page 120 of 123

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
https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oracle-sovereign-cloud-principles.pdf

Thank you

Damien Rilliard

Senior Director, EMEA Sovereignty Lead

EMEA Sovereign Cloud and Public Sector CoE

damien.rilliard@oracle.com