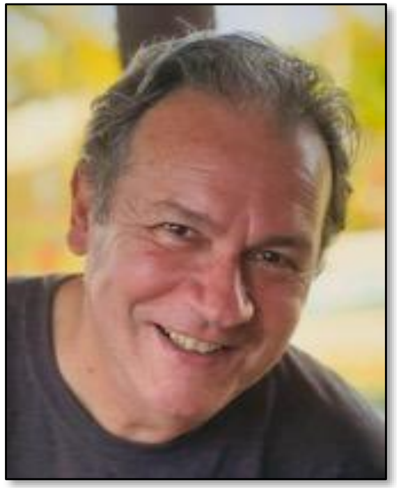
AWS Digital Sovereignty TTM
Building the Offering

Gustavo Annarumma

gustavo@advanceconsulting.com.br

Gustavo Annarumma



Executive with more than 30 years of experience in **Sales, Service and Operations** in global technology companies such as **IBM, Microsoft, SAP, Siebel Systems, Claro/Embratel**, and others.

He developed an international career **leading cross-functional teams in Latin America** and the U.S., being responsible for **strategic contracts and P&Ls** in excess of **200 million dollars**, with a strong focus on sustainable growth, digital transformation and adoption of emerging technologies, such as **Cloud, Analytics, Artificial Intelligence and CRM/ERP**.

At **Claro/Embratel**, he acted as **Sales Director of Digital Solutions**, leading a team of +50 professionals and driving double-digit growth in revenues. At **Microsoft**, he led Office 365 and Analytics adoption initiatives, combining technical skills with change management. During his career at **IBM**, he held leadership positions in **Cloud, Support Services, Financial Solutions and Strategic Outsourcing**, always with significant results in revenue growth and portfolio expansion.

As **Director of Strategic Alliances** at BAAN, structured and innovative models of channels and joint ventures. He acted as a **Customer Services Manager at SAP** and led technical teams in Latin America.

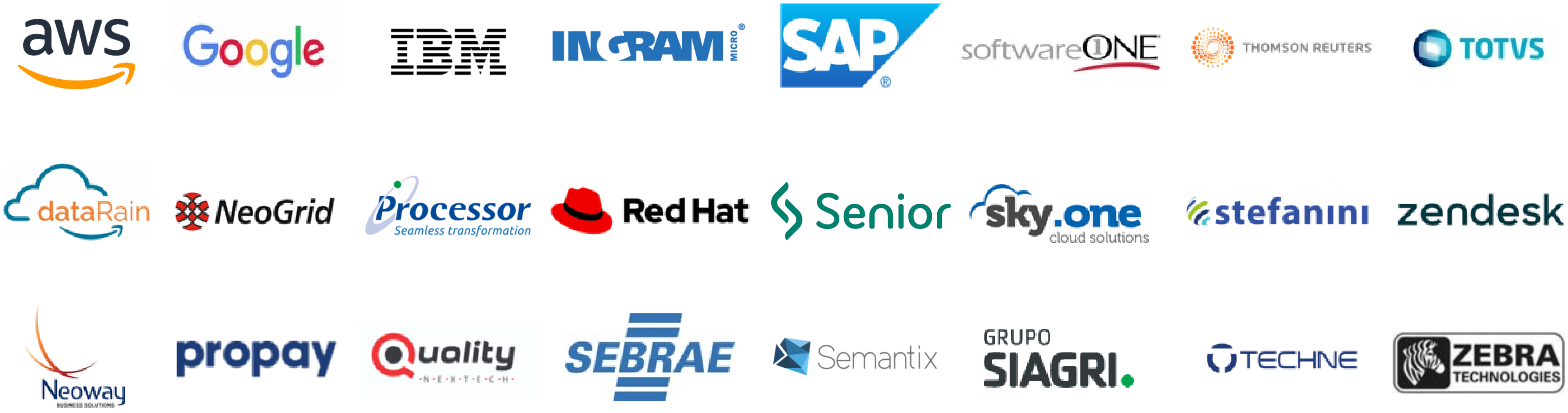
He graduated in **Electronic Engineering and Master's Degree in Engineering from PUC-RJ**, with an **International Executive MBA from FIA/USP**.

aws Digital Sovereignty SPECIALIZED PARTNER

ADVANCE Consulting

With more than **2,500 clients**, **500 consulting projects**, and **20,000 trained professionals**, **ADVANCE** is a consulting and training company in SALE$.

We are proud to serve everyone from large corporations to startups, including:



Our clients say that we stand out in solving complex situations and boosting sales.

ADVANCE Consulting

Consulting firm selected by AWS to assist partners in the US, Canada, Latin America, UK, Spain, South Africa, and Israel

AWS programs include:

- PTP (Partner Transformation Program)
- TTM (Targeted Transformation Module)

Introduction and Objectives

AWS Digital Sovereignty TTM - Objectives

By the end of this module, you should have an Assessment tools and automated reference architectures templates that addresses Digital Sovereign market needs on the AWS cloud

- Consolidate understanding of **Digital Sovereignty** and its implications to your context
- Review the **Partner and AWS roles and responsibilities** in supporting Digital Sovereignty
- Set **the importance of having an Assessment methodology and tool** focused on Digital Sovereignty and on AWS best practices
- Review guiding **designing principles** for sovereignty implementations
- Review the **Landing Zones Accelerator** as foundation for new sovereign offerings and new markets
- Create a **90-day plan** to build a Digital Sovereign Assessment, automated sovereign templates and/or adapt a LZA to a digital sovereign scenario

AWS Digital Sovereign

Before the Workshops

Pre-work - the partner will fill out a form so that we can better understand their situation and expectations

Initial interviews - we will interview the partner to better understand his company, objectives, strategies, superpowers and verticals they focus

During the Workshops

Session duration

- Session 1 will take 2:00 hours
- Session 2 will take 2:00 hours
- We recommend session 2 after 2 days off session 1
  - Our experience shows that partners need some time between session to "mature the ideas", do some "homework", and think about questions to ask

Workshop format

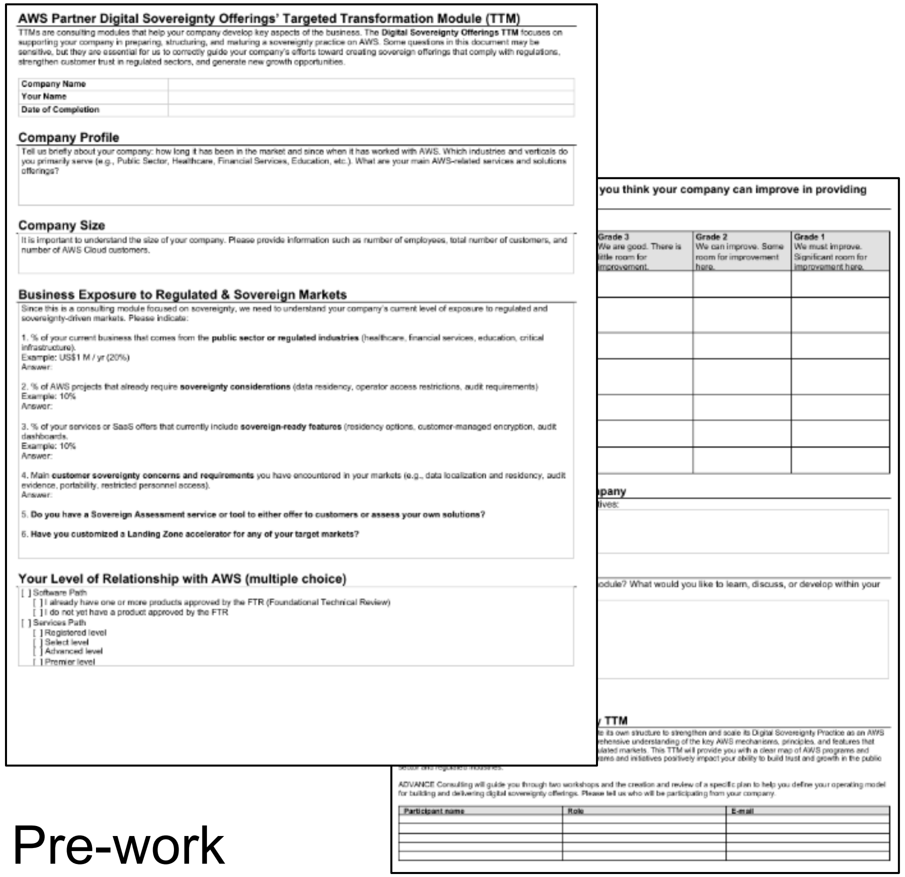
- For each topic in the workshop agenda, we will:
  - Present the concepts and best practices
  - Discuss how the partner will apply the concepts
  - Register all the ideas, discussions and decisions
  - Define actions and activities to implement

After the Workshops

Three 60-minute sessions will be scheduled after the workshops. In this sessions we will review the action plan, including:

- Planned x performed actions
- Actions not taken, with the reasons and ways to catchup
- What obstacles are encountered and how to remove them to succeed in executing the plan
- What can be done differently and better (best practices that can help in the execution of the plan activities)

Supporting materials



AWS Partner Digital Sovereignty Offerings' Targeted Transformation Module (TTM)

TTMs are consulting modules that help your company develop key aspects of the business. The **Digital Sovereignty Offerings TTM** focuses on supporting your company in preparing, structuring, and maturing a sovereignty practice on AWS. Some questions in this document may be sensitive, but they are essential for us to correctly guide your company's efforts toward creating sovereign offerings that comply with regulations, strengthen customer trust in regulated sectors, and generate new growth opportunities.

Company Name	
Your Name	
Date of Completion	

Company Profile

Tell us briefly about your company: how long it has been in the market and since when it has worked with AWS. Which industries and verticals do you primarily serve (e.g., Public Sector, Healthcare, Financial Services, Education, etc.). What are your main AWS-related services and solutions offerings?

Company Size

It is important to understand the size of your company. Please provide information such as number of employees, total number of customers, and number of AWS Cloud customers.

Business Exposure to Regulated & Sovereign Markets

Since this is a consulting module focused on sovereignty, we need to understand your company's current level of exposure to regulated and sovereignty-driven markets. Please indicate:

1. % of your current business that comes from the **public sector or regulated industries** (healthcare, financial services, education, critical infrastructure).
Example: US$1 M / yr (20%)
Answer:

2. % of AWS projects that already require **sovereignty considerations** (data residency, operator access restrictions, audit requirements)
Example: 10%
Answer:

3. % of your services or SaaS offers that currently include **sovereign-ready features** (residency options, customer-managed encryption, audit dashboards.
Example: 10%
Answer:

4. Main **customer sovereignty concerns and requirements** you have encountered in your markets (e.g., data localization and residency, audit evidence, portability, restricted personnel access).
Answer:

5. **Do you have a Sovereign Assessment service or tool to either offer to customers or assess your own solutions?**

6. **Have you customized a Landing Zone accelerator for any of your target markets?**

Your Level of Relationship with AWS (multiple choice)

[ ] Software Path
  [ ] I already have one or more products approved by the FTR (Foundational Technical Review)
  [ ] I do not yet have a product approved by the FTR
[ ] Services Path
  [ ] Registered level
  [ ] Select level
  [ ] Advanced level
  [ ] Premier level

you think your company can improve in providing

Grade 3 We are good. There is little room for improvement.	Grade 2 We can improve. Some room for improvement here.	Grade 1 We must improve. Significant room for improvement here.

pany

tives:

odule? What would you like to learn, discuss, or develop within your

y TTM

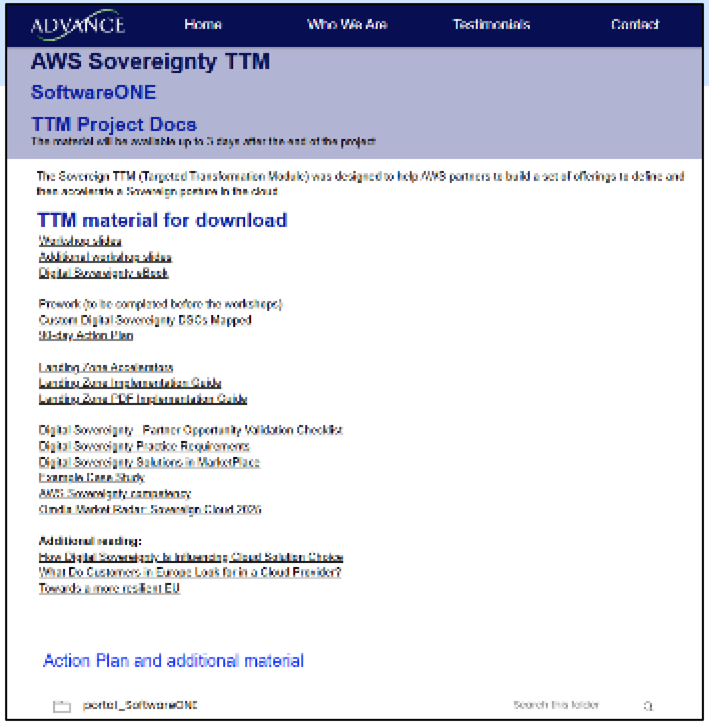
te its own structure to strengthen and scale its Digital Sovereignty Practice as an AWS rehensive understanding of the key AWS mechanisms, principles, and features that ulated markets. This TTM will provide you with a clear map of AWS programs and rams and initiatives positively impact your ability to build trust and growth in the public sector and regulated industries.

ADVANCE Consulting will guide you through two workshops and the creation and review of a specific plan to help you define your operating model for building and delivering digital sovereignty offerings. Please tell us who will be participating from your company.

Participant name	Role	E-mail

Pre-work

Partner portal



AWS Sovereignty TTM

SoftwareONE

TTM Project Docs

The material will be available up to 3 days after the end of the project

The Sovereign TTM (Targeted Transformation Module) was designed to help AWS partners to build a set of offerings to define and then accelerate a Sovereign posture in the cloud

TTM material for download

Workshop slides
Additional workshop slides
Digital Sovereignty eBook

Prework (to be completed before the workshops)
Custom Digital Sovereignty DSCs Mapped
90-day Action Plan

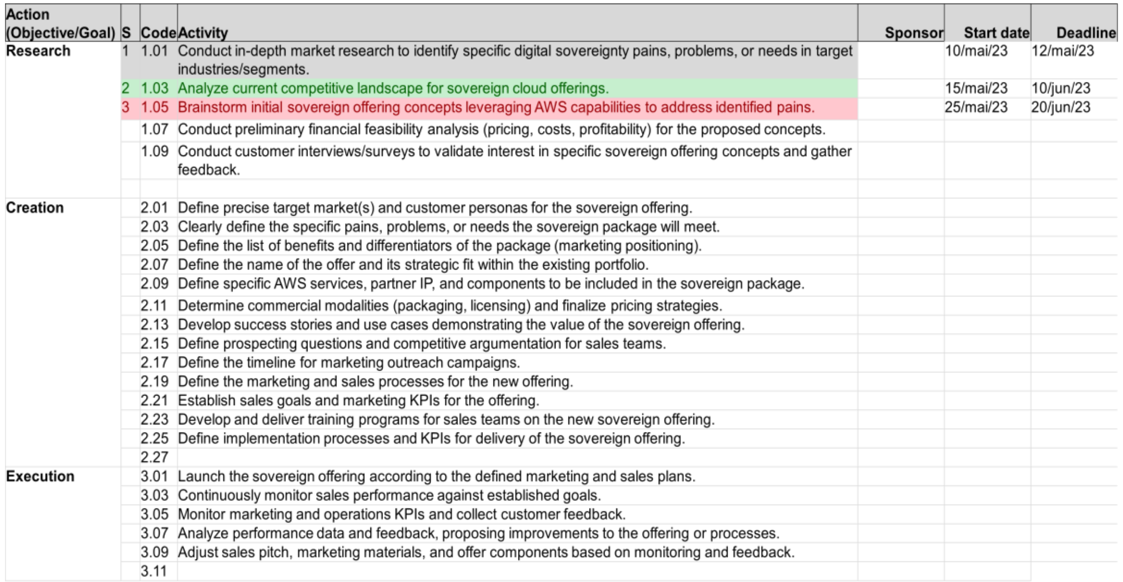
Landing Zone Accelerators
Landing Zone Implementation Guide
Landing Zone PDF Implementation Guide

Digital Sovereignty - Partner Opportunity Validation Checklist
Digital Sovereignty Practice Requirements
Digital Sovereignty Solutions in MarketPlace
Example Case Study
AWS Sovereignty competency
Omdia Market Radar: Sovereign Cloud 2025

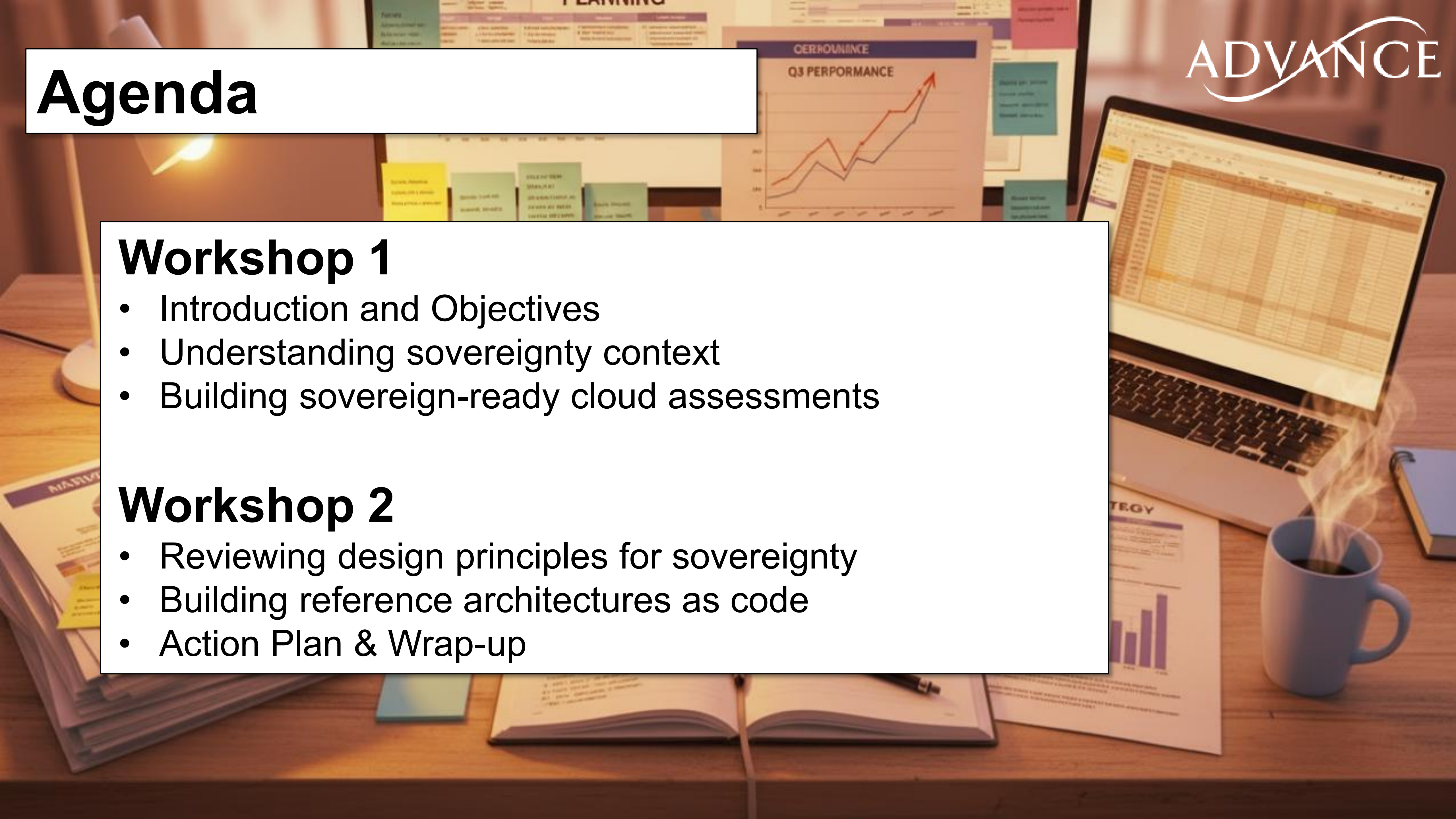
Additional reading:
How Digital Sovereignty Is Influencing Cloud Solution Choice
What Do Customers in Europe Look for in a Cloud Provider?
Towards a more resilient EU

Action Plan and additional material

Action Plan



Action (Objective/Goal)	S	Code	Activity	Sponsor	Start date	Deadline
Research	1	1.01	Conduct in-depth market research to identify specific digital sovereignty pains, problems, or needs in target industries/segments.		10/mai/23	12/mai/23
	2	1.03	Analyze current competitive landscape for sovereign cloud offerings.		15/mai/23	10/jun/23
	3	1.05	Brainstorm initial sovereign offering concepts leveraging AWS capabilities to address identified pains.		25/mai/23	20/jun/23
		1.07	Conduct preliminary financial feasibility analysis (pricing, costs, profitability) for the proposed concepts.			
		1.09	Conduct customer interviews/surveys to validate interest in specific sovereign offering concepts and gather feedback.			
Creation		2.01	Define precise target market(s) and customer personas for the sovereign offering.			
		2.03	Clearly define the specific pains, problems, or needs the sovereign package will meet.			
		2.05	Define the list of benefits and differentiators of the package (marketing positioning).			
		2.07	Define the name of the offer and its strategic fit within the existing portfolio.			
		2.09	Define specific AWS services, partner IP, and components to be included in the sovereign package.			
		2.11	Determine commercial modalities (packaging, licensing) and finalize pricing strategies.			
		2.13	Develop success stories and use cases demonstrating the value of the sovereign offering.			
		2.15	Define prospecting questions and competitive argumentation for sales teams.			
		2.17	Define the timeline for marketing outreach campaigns.			
		2.19	Define the marketing and sales processes for the new offering.			
		2.21	Establish sales goals and marketing KPIs for the offering.			
		2.23	Develop and deliver training programs for sales teams on the new sovereign offering.			
		2.25	Define implementation processes and KPIs for delivery of the sovereign offering.			
		2.27				
Execution		3.01	Launch the sovereign offering according to the defined marketing and sales plans.			
		3.03	Continuously monitor sales performance against established goals.			
		3.05	Monitor marketing and operations KPIs and collect customer feedback.			
		3.07	Analyze performance data and feedback, proposing improvements to the offering or processes.			
		3.09	Adjust sales pitch, marketing materials, and offer components based on monitoring and feedback.			
		3.11				



ADVANCE

Agenda

Workshop 1

- Introduction and Objectives
- Understanding sovereignty context
- Building sovereign-ready cloud assessments

Workshop 2

- Reviewing design principles for sovereignty
- Building reference architectures as code
- Action Plan & Wrap-up

Understanding the sovereignty context

What does Digital Sovereignty mean to you ?

What is your understanding of the term DIGITAL SOVEREIGNTY ?
[You may select more than 1 option]

1. It is about ensuring customer data stays within a region
2. It is about identifying and selection the right "Sovereign Cloud" solution
3. It is mostly to do with geo-politics and is best taken care of by compliance and legal teams
4. It is not an important topic of conversation. I have not heard many customers talk about this

Digital Sovereignty means different things to different people

Geopolitical Perspective

Data flows have become as strategically important as traditional physical assets, like ports, roads, or energy resources

Legal Perspective

Complex and constantly evolving, with countries implementing data localization laws, creating new regulatory frameworks, and establishing digital rights frameworks

Technology Perspective

Building domestic capabilities in critical areas,

Government Clouds,

Local network infrastructures,

Data Protection & Privacy

- Focus: Personal data classification, rights, and consent.

Data Localization & Flow Controls

- Focus: Keeping sensitive/critical data within jurisdiction or tightly controlling transfers.

Critical Infrastructure & Security

- Focus: Protecting healthcare, energy, finance, telecom, and other critical sectors.

Sector-Specific Rules

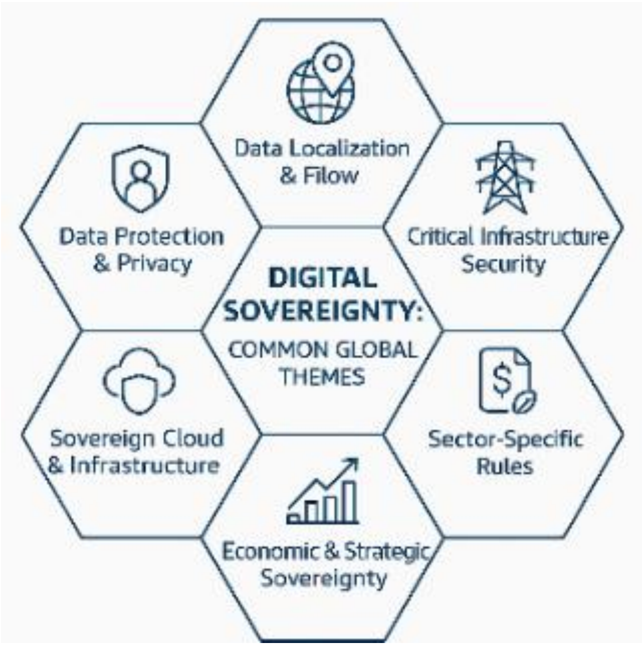
- Focus: Tailored safeguards for sensitive domains (health, finance, defense).

Sovereign Cloud & Infrastructure Independence

- Focus: Building trusted cloud infrastructure free from foreign influence.

Economic & Strategic Sovereignty

- Focus: Limiting foreign dominance, fostering local innovation, securing strategic industries.


Data Localization & Filow
Data Protection & Privacy
Critical Infrastructure Security
DIGITAL SOVEREIGNTY: COMMON GLOBAL THEMES
Sovereign Cloud & Infrastructure
Sector-Specific Rules
Economic & Strategic Sovereignty

Digital Sovereign Domains (an example)

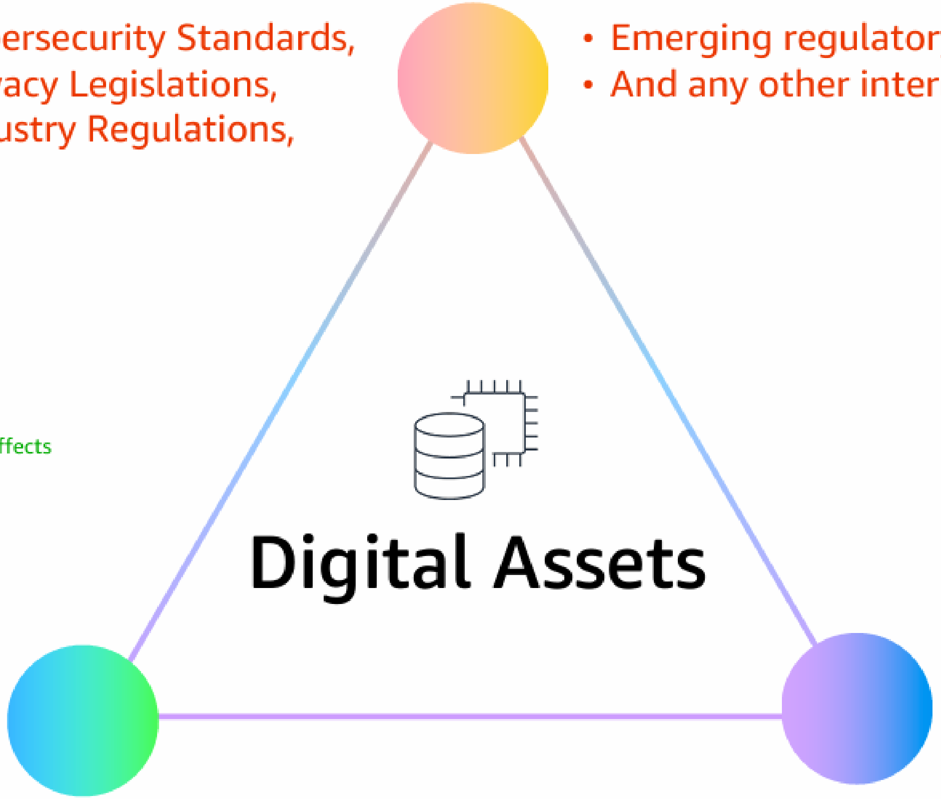
Primary Domain	Purpose / Description
1. Data Sovereignty	Ensure that the customer retains lawful control over all data (localization, storage, processing, sharing, transfer, encryption)
2. Infrastructure Sovereignty	Maintain jurisdictional and operational control over hosting location, networking infrastructure, reducing interference and dependence on foreign providers
3. Operational Sovereignty	Limit and govern who (including provider operators) can access, manage, or interfere with workloads or data.
4. Governance & Compliance Sovereignty	Ensure transparent, auditable, and enforceable compliance aligned with law and standards
5. Continuity & Portability Sovereignty	Guarantee operation survivability under disruption, failure, or exit
6. Organizational & Supply Chain Sovereignty	Ensure that the organizations, people, and vendors involved in the ecosystem operate under sovereign control and accountability.

Digital Sovereignty, the 3Cs

HOW NATIONS ASSERT SOVEREIGNTY OVER THE DIGITAL ASSETS THEY OWN OR REGULATE.

COMPLIANCE

- Cybersecurity Standards,
- Privacy Legislations,
- Industry Regulations,
- Emerging regulatory standards
- And any other internal compliance needs



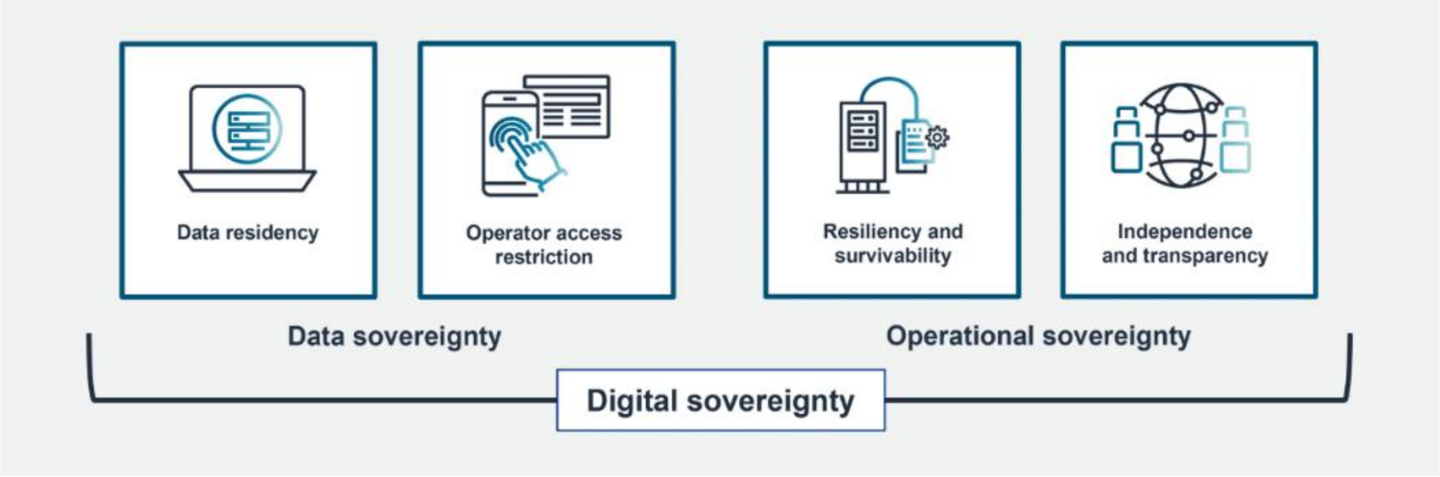
CONTINUITY

- Survivability, Resiliency
  Survive large scale infrastructure outages, or adverse effects of geo-political events.
- Independence, Choice
  Freedom to deploy and run your workloads anywhere.
- Becoming Self-Sufficient
  Successfully manage and mitigate risks around skills shortage, energy supply and supply chain constraints.

CONTROL

- Data Residency Requirements
- Data Export Controls
- Data Protection
  Cryptography Controls, Encryption Standards, Protecting Confidentiality of Compute Operations
- Operator Access Restrictions
- Privacy Protection
  Privacy Enhancement Technologies (PETs) such as pseudonymization.

AWS Digital Sovereignty Core Pillars


Data residency
Operator access restriction
Resiliency and survivability
Independence and transparency
Data sovereignty
Operational sovereignty
Digital sovereignty

- Data Residency and Location

Control over where data is stored, processed, moved and who has access to it.

- Operator Access Restriction

Ensure neither cloud providers nor unauthorized entities can access sensitive information of infrastructure without explicit permission

- Resiliency and Survivability

Build digital systems that maintain operational continuity despite disruptions – without loss of control, data or service

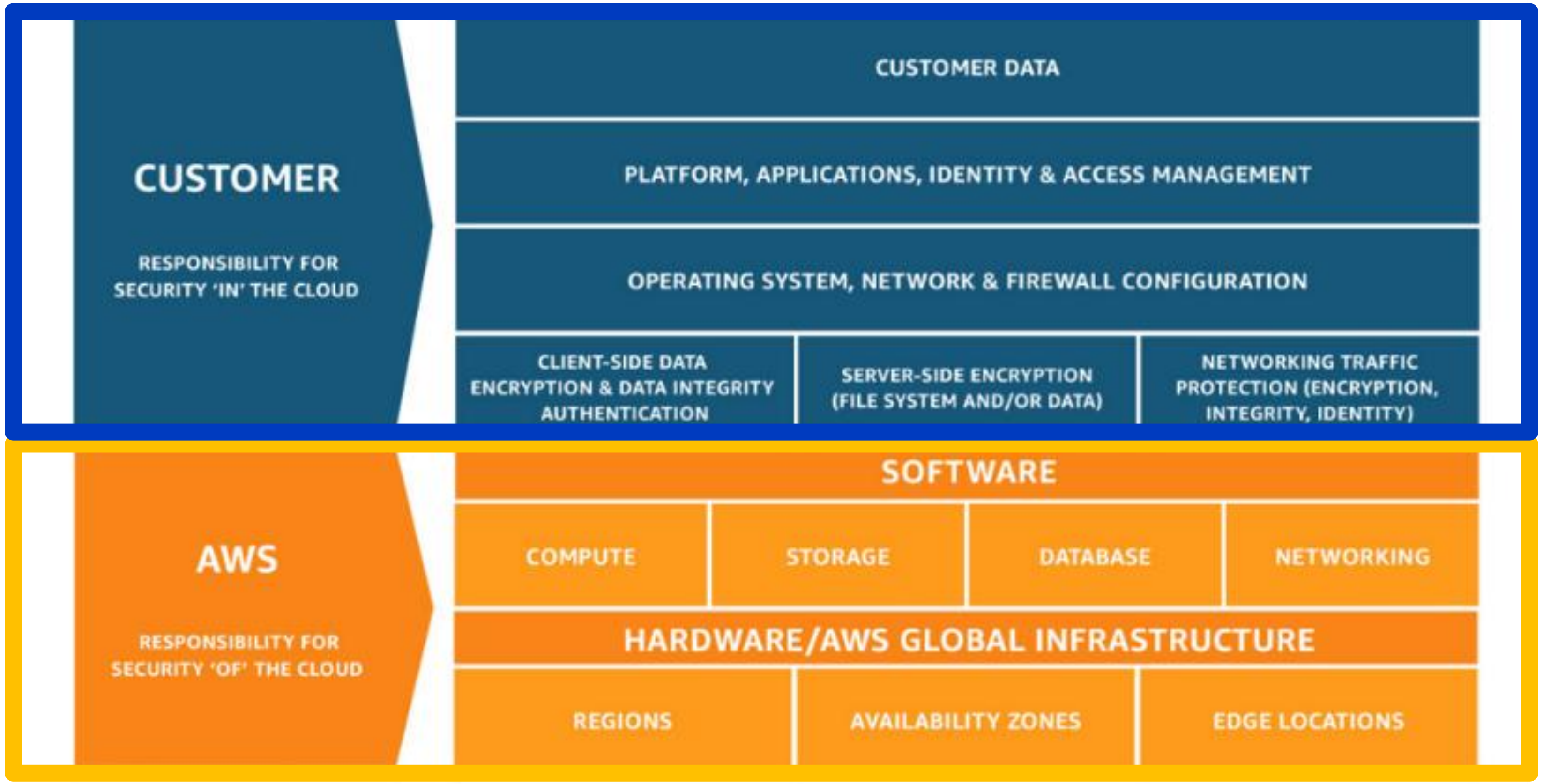
- Independence and Transparency

Local governance ower technology choices, ownership control, and visibility into how systems operate

Digital Soverignty is a Shared Responsibility

AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

Customer/Partner chose the AWS services and the Regions, the integration of those services into their IT environment, and the laws, regulations, and customer sovereign requests are applicable to their organization and workload.


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Chapter discussion

What did you see in this chapter:

- Digital Sovereignty has multiple interpretations and goes beyond just regulatory compliance
- Laws and regulations are many, with common grounds, and subject to a certain level of interpretation.
- Partners create value by clarifying, standardizing, and operationalizing what Digital Sovereignty is in practice for customers

What are we going to write in the action plan?

Suggested actionable items

- Define a Digital Sovereignty focal point for your organization.

- Create a partner value proposition on digital sovereignty

- Evaluate your solution requirements, architecture, and operational decisions against the full spectrum of Digital Sovereignty

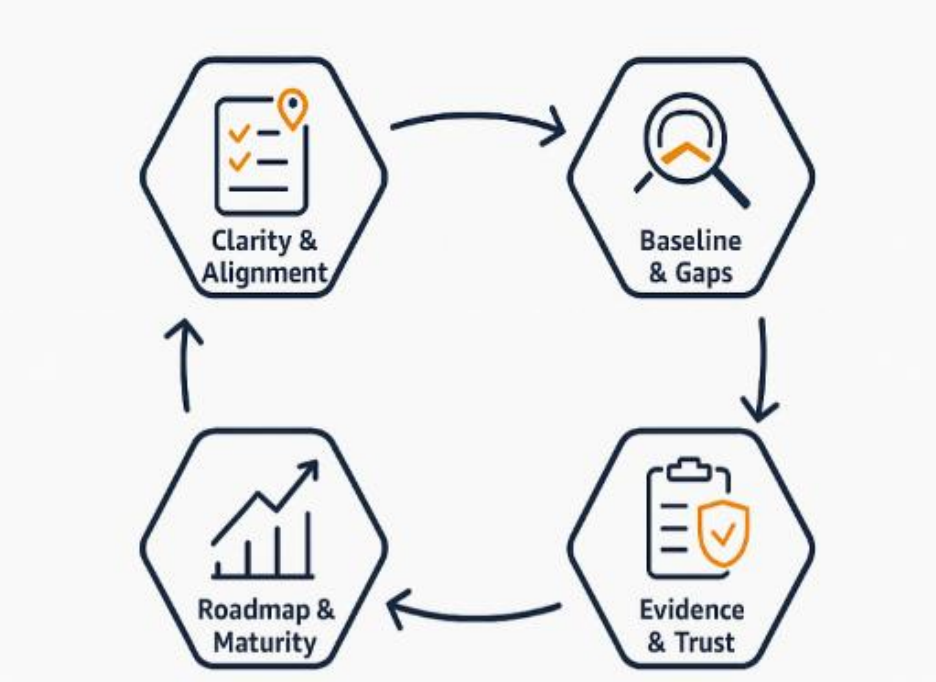
- Conduct training for sales and technical teams on the aspects of digital sovereignty, enabling more informed customer conversations and address customer objections

Building sovereign-ready assessments

Why do Assessments Matter in Digital Sovereignty Solutions ?

Assessments are the bridge from abstract regulation to concrete designs

- Measures formal alignment with sovereignty principles
- Identify regulatory gaps against proven frameworks
- Map compliance and sovereignty outcomes to concrete controls from AWS
- Build trust with customer and regulators
- Differentiates Partner and creates proprietary IP



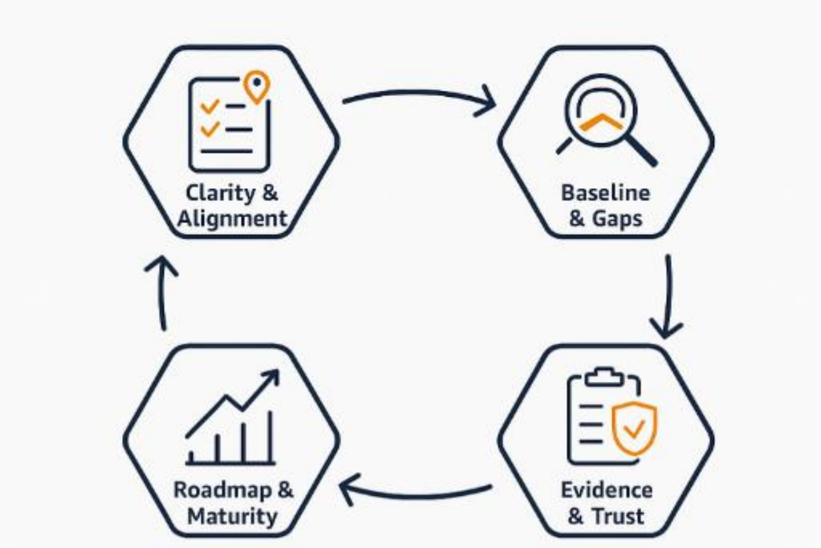
Building assessment tools

1. Define the Scope and Sovereignty Requirements
    a. Identify critical assets and business process (focus)
    b. Identify customer's sovereign goals
    c. Map jurisdictional, regulatory requirements, and sovereign design principles
    d. Define best practice reference frameworks + custom sovereign lens

2. Categorize requirements into Sovereign Domains / Sub-domains

3. Develop Assessment Instrument
    a. Create a **traceability matrix** for the requirement scope
    b. Group questions per domain, tied to the best practices frameworks
    c. Define maturity levels and scoring scales
    d. Define reports and dashboards

4. Validate against real scenarios (PoC)



Example of Digital Sovereign Domains to Assess

Primary Domain	Purpose / Description	Subdomains
1. Data Sovereignty	Ensure that the customer retains lawful control over all data (storage, processing, sharing)	• **Data Residency & Localization** — physical and logical location of data and processing. • **Data Classification & Sensitivity** — defining and labeling personal, sensitive, or regulated data types. • **Data Lineage** — traceability of data origin, movement, and transformation. • **Encryption & Key Management** — customer control of cryptographic keys, lifecycle, and jurisdictions. • **Data Sharing & Cross-Border Transfers** — contractual and technical control over how data is exchanged between entities or regions.
2. Infrastructure Sovereignty	Maintain jurisdictional and operational control over hosting and networking infrastructure	• **Hosting Location & Jurisdiction** — ownership, control, and physical location of data centers or cloud regions. • **Network & Connectivity Control** — network isolation, routing policies, and interconnect sovereignty. • **Hardware & Virtualization Control** — assurance of hardware provenance, firmware integrity, and hypervisor isolation.
3. Operational Sovereignty	Limit and govern who (including provider operators) can access, manage, or interfere with workloads or data.	• **Identity & Access Management** — authentication, authorization, and federated identity governance. • **Operator Access Control** — least-privilege, just-in-time, dual-control, and privileged access restrictions. • **Policy-as-Code & Governance Automation** — codification of compliance and security rules for automated enforcement.

Example of Digital Sovereign Domains to Assess

Primary Domain	Purpose / Description	Subdomains
4. Governance & Compliance Sovereignty	Ensure transparent, auditable, and enforceable compliance aligned with law and standards	• **Continuous Audit & Monitoring** — logging, telemetry, and continuous compliance validation. • **Regulatory Mapping & Compliance Evidence** — traceability of legal or regulatory requirements to implemented controls. • **Transparency & Accountability** — operational reporting, documentation, and oversight of third-party participation.
5. Continuity & Portability Sovereignty	Guarantee sovereignty under disruption, failure, or exit	• **Resilience & Continuity Management** — sovereign disaster recovery, fault tolerance, and resilience planning. • **Data & Workload Portability** — ability to migrate data and workloads without dependency on a non-sovereign provider. • **Open Standards & Interoperability** — use of open APIs, formats, and frameworks to preserve autonomy.
6. Organizational & Supply Chain Sovereignty	Ensure that the organizations, people, and vendors involved in the ecosystem operate under sovereign control and accountability.	• **Service Provider & Vendor Governance** — supplier selection, onboarding, and compliance alignment. • **Contractual & Legal Readiness** — data processing agreements, jurisdiction clauses, SLAs, and regulatory certifications. • **Personnel & Citizenship Control** — employee nationality, security clearance, and access conditions for sensitive workloads. • **Supply Chain Transparency & Risk Management** — traceability of software, hardware, and service components across the chain. • **Third-Party Dependency Control** — cloud service sub-processors, subcontractors, or software dependencies under jurisdictional risk review.

Example of a Traceability Matrix

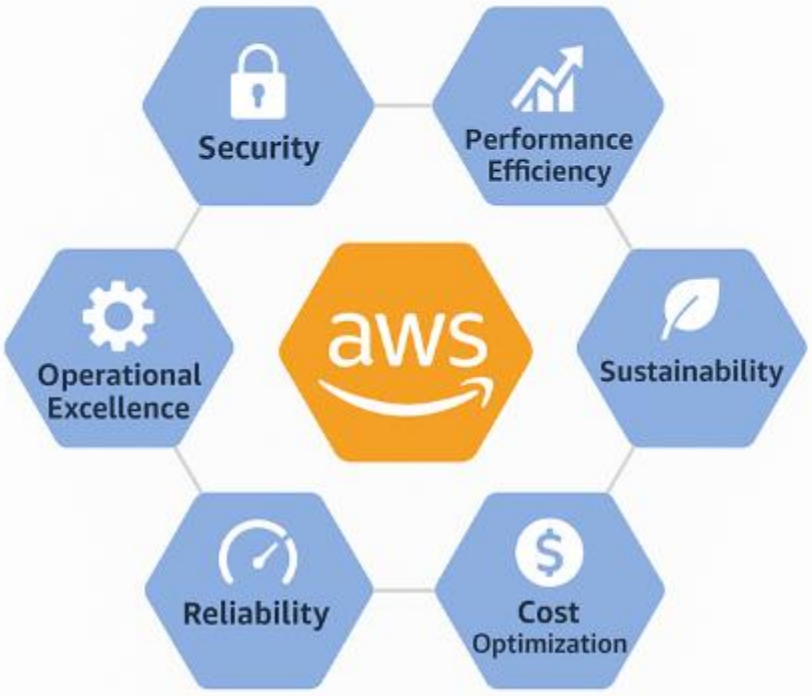
Requirement ID	Sovereignty Domain	Requirement (The "Why")	Mapped WAF Question	Technical Control (The "How")	Status	Evidence
GDPR-32.1.a	Data Sovereignty	Art. 32(1)(a) — Pseudonymisation and encryption of personal data	SEC 7: How do you classify your data?	The application code contains a function that replaces PII fields (e.g., user_name) with a non-identifiable token (pseudonym) before storing the record in the database.	Compliant	• Link to the specific code repository and file containing the pseudonymisation function. • Reference to the application's software design document. • Results of a code review that validated this function.
			SEC 8: How do you protect your data at rest?	All Amazon RDS instances storing personal data are configured with encryption enabled, using a Customer Managed Key (CMK) from AWS KMS.		• Screenshot of the RDS instance configuration showing "Encryption: Enabled" and the specific KMS Key ID. • Output of the aws rds describe-db-instances CLI command showing "StorageEncrypted": true. • Link to the compliant status of the rds-storage-encrypted rule in AWS Config·

Disclosure: This traceabilty matrix is for illustration purposes only. AWS services and controls informed here must be reviewed and validated

Well-Architected Framework and the [WAF Tool]

Well-Architected Framework (WAF)

- Globally recognized design principles and best practices based on 6 pillars
- Stimulates critical thinking of your architecture choices
- Identifies High and Medium Risks of your workloads
- Provides implementation guidelines
- Extendable with Lens for industry- and application-focus best practices



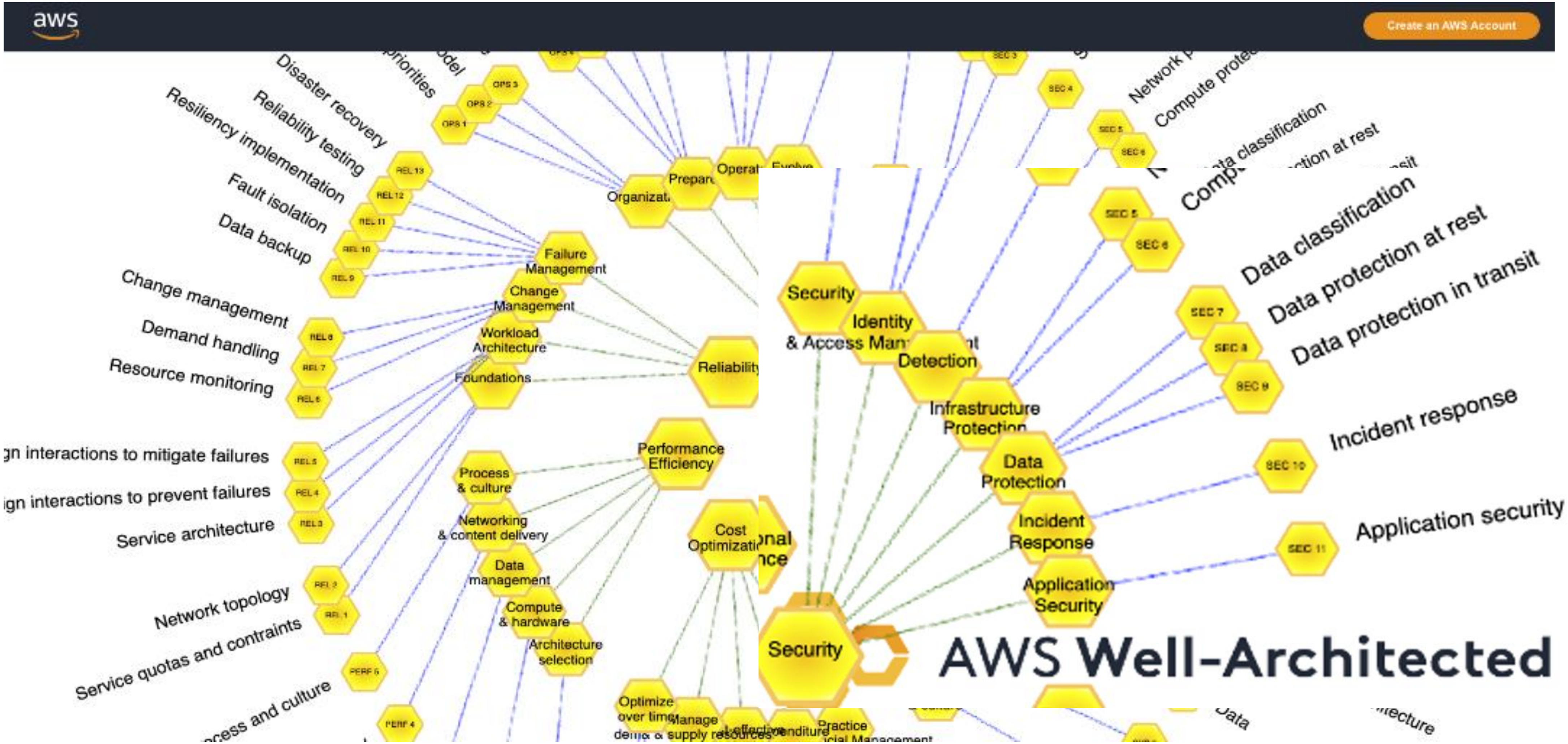
Well-Architected Framework Tool

- Service in the cloud to help reviews against the WA framework
- Allows Custom Lens (e.g. Digital Sovereignty Lens)

You can use WAF assessments to demonstrate compliance maturity and differentiate solutions in regulated sectors

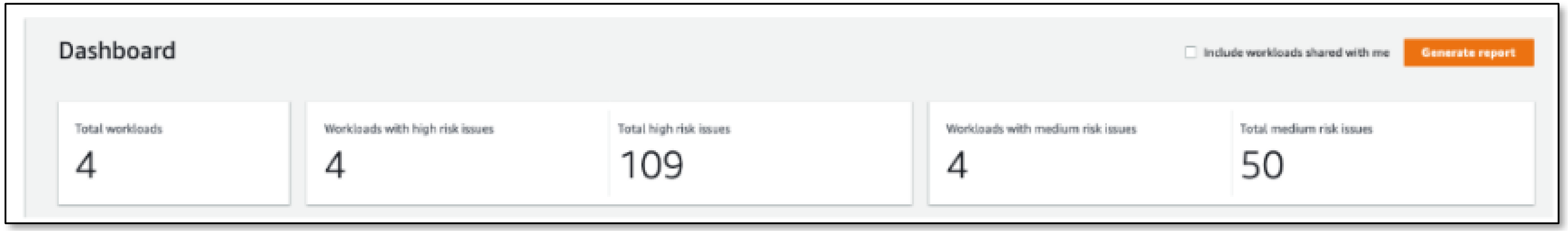
https://docs.aws.amazon.com/wellarchitected/latest/userguide/lens-catalog.html

Well-Architected Framework and the WAF Tool



https://wa.aws.amazon.com/wat.map.en.html

Well-Architected Framework Report

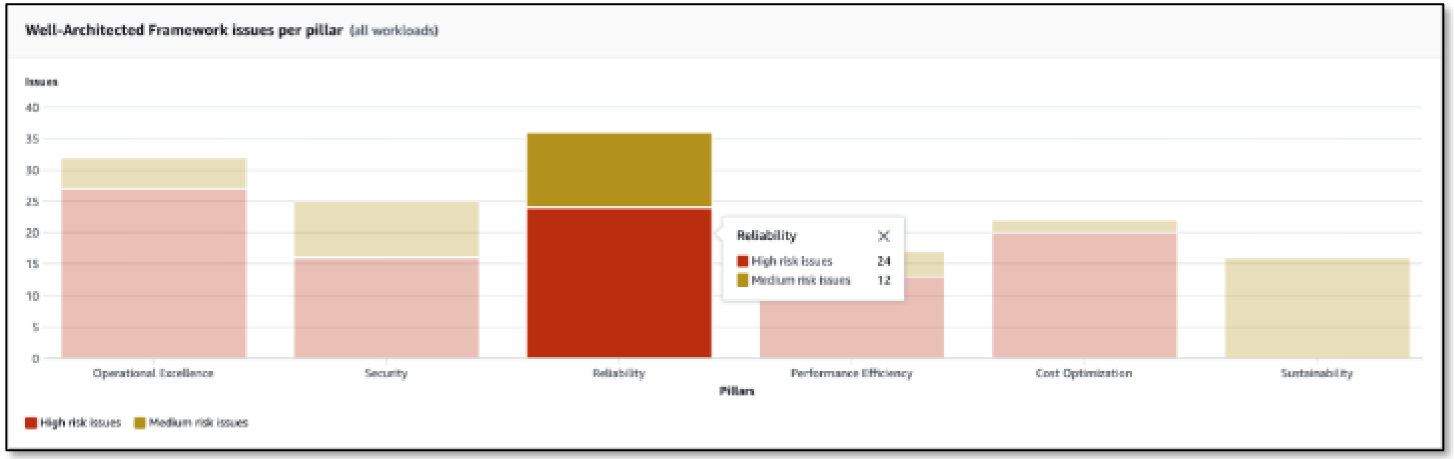


Dashboard

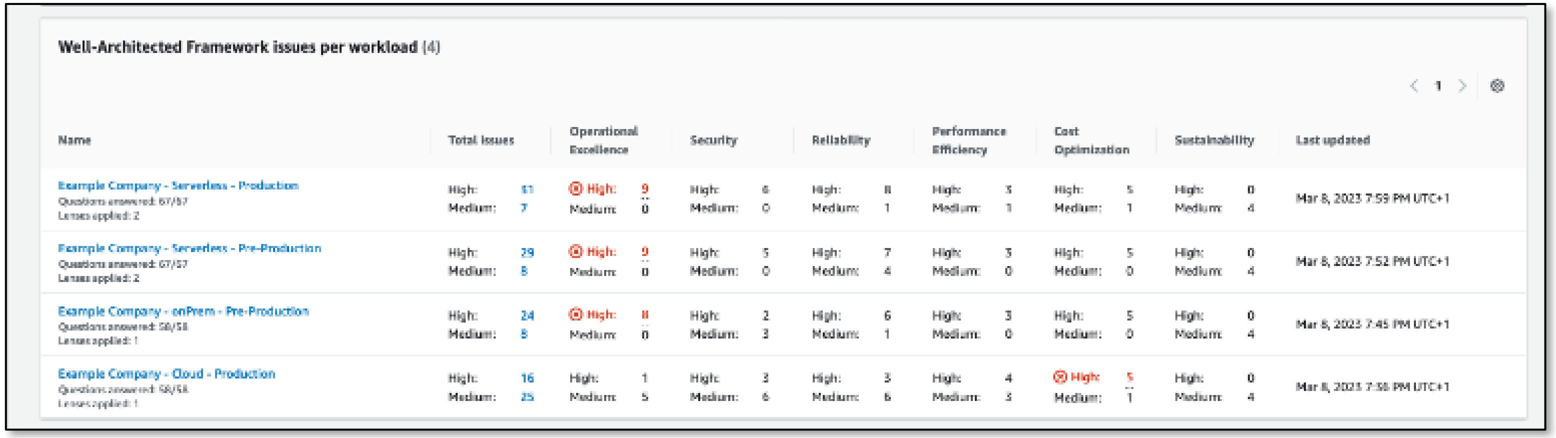
☐ Include workloads shared with me

Generate report

Total workloads	Workloads with high risk issues	Total high risk issues	Workloads with medium risk issues	Total medium risk issues
4	4	109	4	50



Well-Architected Framework issues per pillar (all workloads)



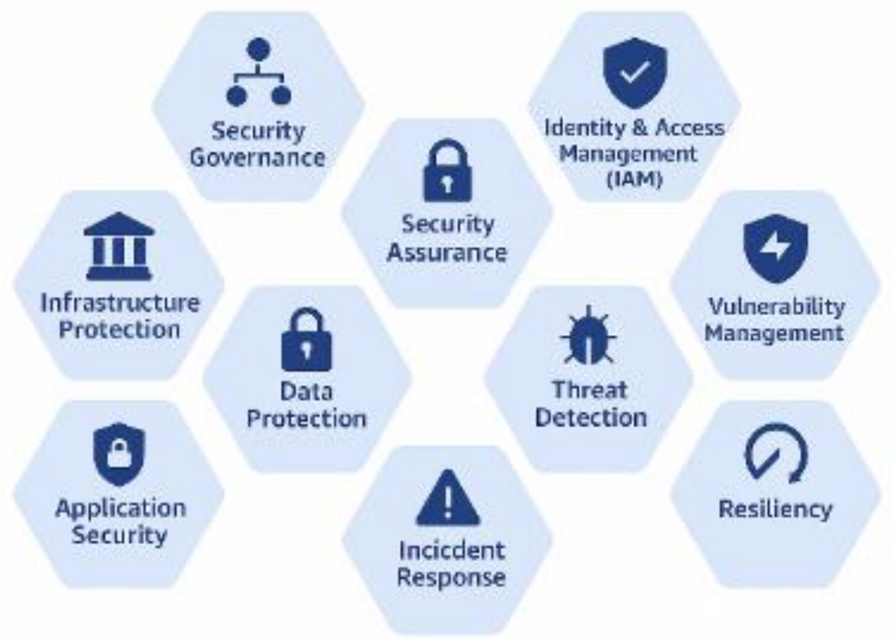
Well-Architected Framework issues per workload (4)

Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Example Company - Serverless - Production Questions answered: 57/57 Lenses applied: 2	High: 31 Medium: 7	⊗ High: 9 Medium: 0	High: 6 Medium: 0	High: 8 Medium: 1	High: 3 Medium: 1	High: 5 Medium: 1	High: 0 Medium: 4	Mar 8, 2023 7:59 PM UTC+1
Example Company - Serverless - Pre-Production Questions answered: 57/57 Lenses applied: 2	High: 29 Medium: 8	⊗ High: 9 Medium: 0	High: 5 Medium: 0	High: 7 Medium: 4	High: 3 Medium: 0	High: 5 Medium: 0	High: 0 Medium: 4	Mar 8, 2023 7:52 PM UTC+1
Example Company - onPrem - Pre-Production Questions answered: 58/58 Lenses applied: 1	High: 24 Medium: 8	⊗ High: 8 Medium: 0	High: 2 Medium: 3	High: 6 Medium: 1	High: 3 Medium: 0	High: 5 Medium: 0	High: 0 Medium: 4	Mar 8, 2023 7:45 PM UTC+1
Example Company - Cloud - Production Questions answered: 58/58 Lenses applied: 1	High: 16 Medium: 25	High: 1 Medium: 5	High: 3 Medium: 6	High: 3 Medium: 6	High: 4 Medium: 3	⊗ High: 5 Medium: 1	High: 0 Medium: 4	Mar 8, 2023 7:38 PM UTC+1

- Provide clear visibility into risks (HRIs) and a roadmap to fix them
- Create trust with regulators, executives, and customers by embedding sovereignty controls

AWS Security Maturity Model v2

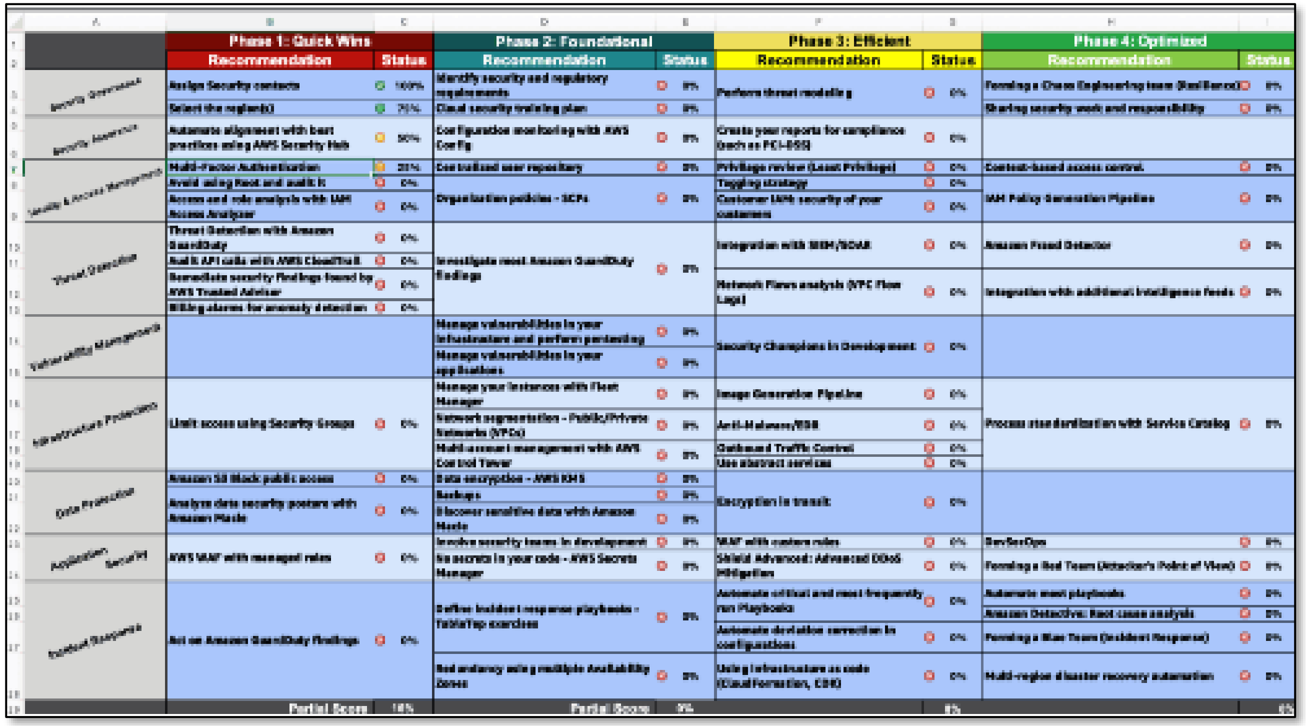
- A framework AWS to **assess and improve the cloud security posture over time (processes, people and technology)**
- It’s structured into **10 capabilities (CAFs)** that cover the full security lifecycle.
- Provides **maturity levels** (from quick wins → optimized) to benchmark current state and define a roadmap for improvements
- Integrate to **WAF,** giving both a **roadmap** and **evidence** for security and compliance improvement.



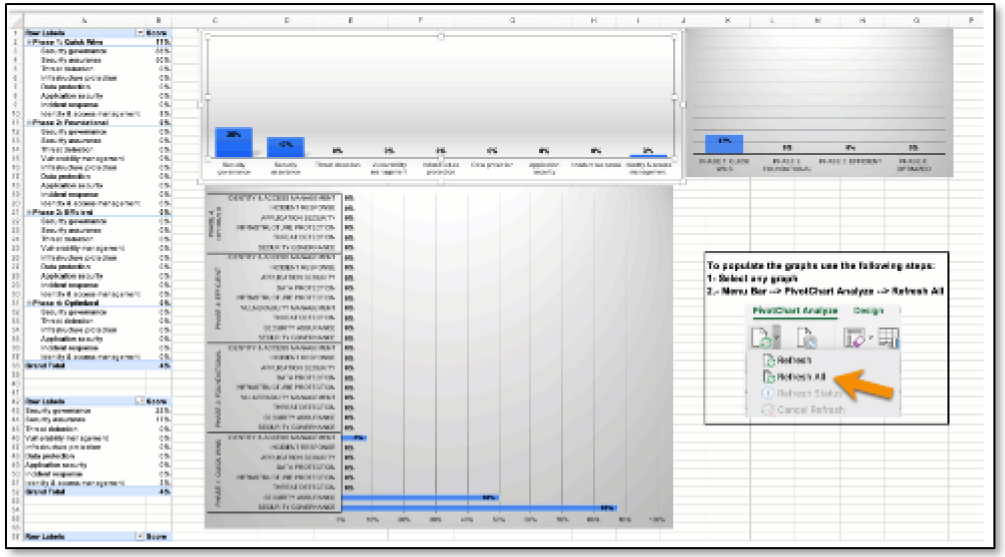
https://maturitymodel.security.aws.dev/en/assessment-tools/

- Benchmark current security posture
- Prioritize roadmap for improvement

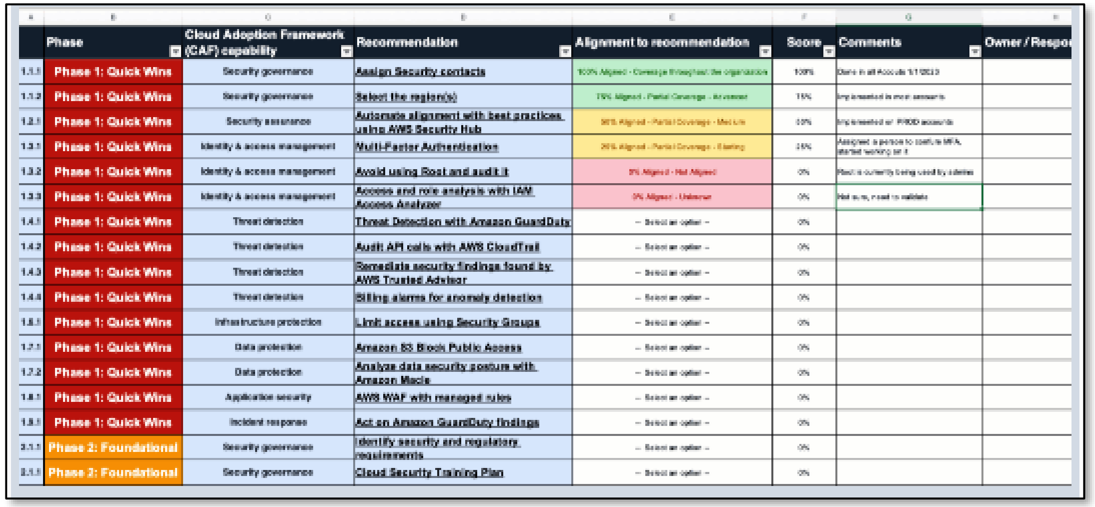
AWS Security Maturity Model v2



	Phase 1: Quick Wins		Phase 2: Foundational		Phase 3: Efficient		Phase 4: Optimized	
	Recommendation	Status	Recommendation	Status	Recommendation	Status	Recommendation	Status
Security Governance	Assign Security contacts	100%	Identify security and regulatory requirements	0%	Perform threat modeling	0%	Forming a Chaos Engineering team (Resilience)	0%
	Select the region(s)	75%	Cloud security training plan	0%			Sharing security work and responsibility	0%
Security Assurance	Automate alignment with best practices using AWS Security Hub	50%	Configuration monitoring with AWS Config	0%	Create your reports for compliance (such as PCI-DSS)	0%		
Identity & Access Management	Multi-Factor Authentication	25%	Centralized user repository	0%	Privilege review (Least Privilege)	0%	Context-based access control	0%
	Avoid using Root and audit it	0%	Organization policies - SCPs	0%	Tagging strategy	0%	IAM Policy Generation Pipeline	0%
	Access and role analysis with IAM Access Analyzer	0%			Customer IAM: security of your customers	0%		
Threat Detection	Threat Detection with Amazon GuardDuty	0%	Investigate most Amazon GuardDuty findings	0%	Integration with SIEM/SOAR	0%	Amazon Fraud Detector	0%
	Audit API calls with AWS CloudTrail	0%						
	Remediate security findings found by AWS Trusted Advisor	0%			Network Flows analysis (VPC Flow Logs)	0%	Integration with additional intelligence feeds	0%
	Billing alarms for anomaly detection	0%						
Vulnerability Management			Manage vulnerabilities in your infrastructure and perform pentesting	0%	Security Champions in Development	0%		
			Manage vulnerabilities in your applications	0%				
Infrastructure Protection	Limit access using Security Groups	0%	Manage your instances with Fleet Manager	0%	Image Generation Pipeline	0%	Process standardization with Service Catalog	0%
			Network segmentation - Public/Private Networks (VPCs)	0%	Anti-Malware/EDR	0%		
			Multi-account management with AWS Control Tower	0%	Outbound Traffic Control	0%		
					Use abstract services	0%		
Data Protection	Amazon S3 Block public access	0%	Data encryption - AWS KMS	0%	Encryption in transit	0%		
	Analyze data security posture with Amazon Macie	0%	Backups	0%				
			Discover sensitive data with Amazon Macie	0%				
Application Security	AWS WAF with managed rules	0%	Involve security teams in development	0%	WAF with custom rules	0%	DevSecOps	0%
			No secrets in your code - AWS Secrets Manager	0%	Shield Advanced: Advanced DDoS Mitigation	0%	Forming a Red Team (Attacker's Point of View)	0%
Incident Response	Act on Amazon GuardDuty findings	0%	Define incident response playbooks - TableTop exercises	0%	Automate critical and most frequently run Playbooks	0%	Automate most playbooks	0%
							Amazon Detective: Root cause analysis	0%
					Automate deviation correction in configurations	0%	Forming a Blue Team (Incident Response)	0%
			Redundancy using multiple Availability Zones	0%	Using infrastructure as code (CloudFormation, CDK)	0%	Multi-region disaster recovery automation	0%
	Partial Score	18%	Partial Score	0%		0%		0%



To populate the graphs use the following steps:
1- Select any graph
2.- Menu Bar --> PivotChart Analyze --> Refresh All

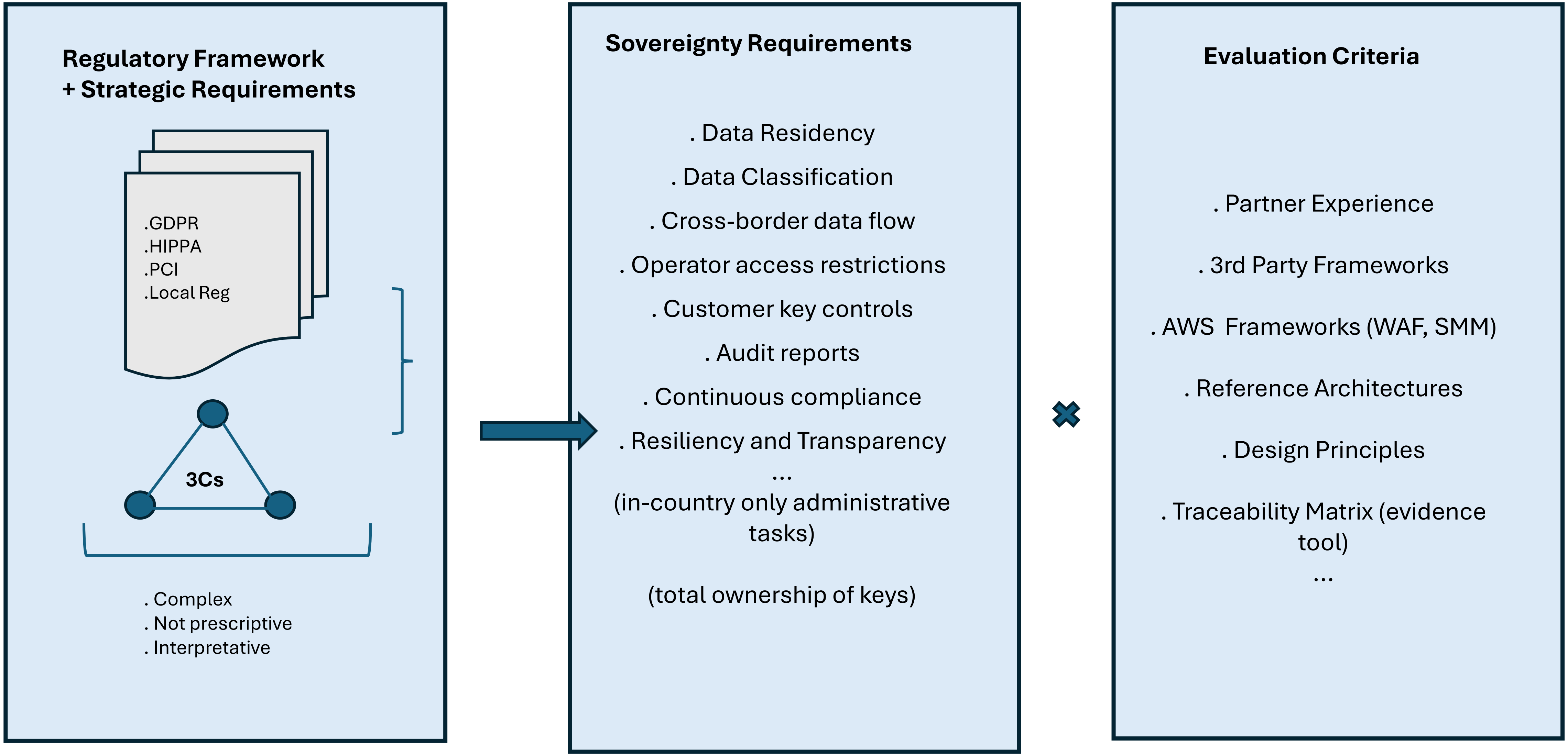


	Phase	Cloud Adoption Framework (CAF) capability	Recommendation	Alignment to recommendation	Score	Comments	Owner / Respo
1.1.1	Phase 1: Quick Wins	Security governance	Assign Security contacts	100% Aligned - Coverage throughout the organization	100%	Done in all Accounts 1/1/2023	
1.1.2	Phase 1: Quick Wins	Security governance	Select the region(s)	75% Aligned - Partial Coverage - Advanced	75%	Implemented in main accounts	
1.2.1	Phase 1: Quick Wins	Security assurance	Automate alignment with best practices using AWS Security Hub	50% Aligned - Partial Coverage - Medium	50%	Implemented on PROD accounts	
1.3.1	Phase 1: Quick Wins	Identity & access management	Multi-Factor Authentication	25% Aligned - Partial Coverage - Starting	25%	Assigned a person to configure MFA, started working on it	
1.3.2	Phase 1: Quick Wins	Identity & access management	Avoid using Root and audit it	0% Aligned - Not Aligned	0%	Root is currently being used by admins	
1.3.3	Phase 1: Quick Wins	Identity & access management	Access and role analysis with IAM Access Analyzer	0% Aligned - Unknown	0%	Not sure, need to validate	
1.4.1	Phase 1: Quick Wins	Threat detection	Threat Detection with Amazon GuardDuty	-- Select an option --	0%		
1.4.2	Phase 1: Quick Wins	Threat detection	Audit API calls with AWS CloudTrail	-- Select an option --	0%		
1.4.3	Phase 1: Quick Wins	Threat detection	Remediate security findings found by AWS Trusted Advisor	-- Select an option --	0%		
1.4.4	Phase 1: Quick Wins	Threat detection	Billing alarms for anomaly detection	-- Select an option --	0%		
1.6.1	Phase 1: Quick Wins	Infrastructure protection	Limit access using Security Groups	-- Select an option --	0%		
1.7.1	Phase 1: Quick Wins	Data protection	Amazon S3 Block Public Access	-- Select an option --	0%		
1.7.2	Phase 1: Quick Wins	Data protection	Analyze data security posture with Amazon Macie	-- Select an option --	0%		
1.8.1	Phase 1: Quick Wins	Application security	AWS WAF with managed rules	-- Select an option --	0%		
1.9.1	Phase 1: Quick Wins	Incident response	Act on Amazon GuardDuty findings	-- Select an option --	0%		
2.1.1	Phase 2: Foundational	Security governance	Identify security and regulatory requirements	-- Select an option --	0%		
2.1.2	Phase 2: Foundational	Security governance	Cloud Security Training Plan	-- Select an option --	0%		

https://maturitymodel.security.aws.dev/en/assessment-tools/

- Benchmark current security posture
- Prioritize roadmap for improvement

Assessments Matter for Digital Sovereignty



Regulatory Framework
+ Strategic Requirements

.GDPR
.HIPPA
.PCI
.Local Reg

3Cs

. Complex
. Not prescriptive
. Interpretative

Sovereignty Requirements

. Data Residency

. Data Classification

. Cross-border data flow

. Operator access restrictions

. Customer key controls

. Audit reports

. Continuous compliance

. Resiliency and Transparency

...

(in-country only administrative tasks)

(total ownership of keys)

✖

Evaluation Criteria

. Partner Experience

. 3rd Party Frameworks

. AWS Frameworks (WAF, SMM)

. Reference Architectures

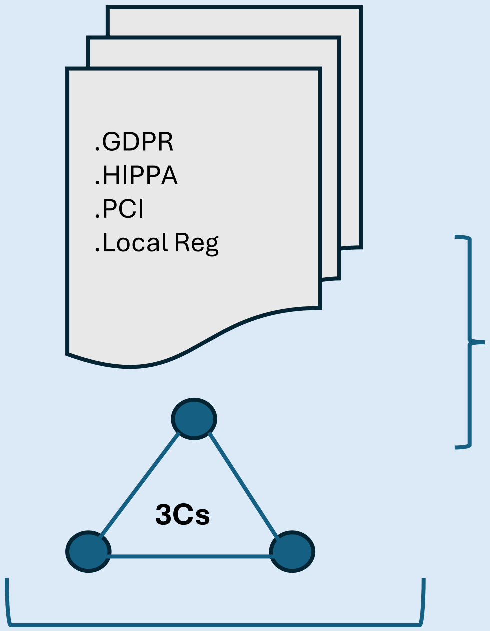
. Design Principles

. Traceability Matrix (evidence tool)

...

Assessments Matter for Digital Sovereignty

Regulatory Framework
+ Strategic Requirements



.GDPR
.HIPPA
.PCI
.Local Reg

. Complex
. Not prescriptive
. Interpretative

GDPR Art. 9
LGPD Art 11

Sovereignty Requirements

. Data Residency

. Data Classification

. Cross-border data flow

. Operator access restrictions

. Customer key controls

. Audit reports

. Continuous compliance

. Resiliency and Transparency

…

(in-country only administrative tasks)

(total ownership of keys)

Evaluation Criteria

WAF Security Pillar
. Data Protection
.Sec7- How do you classify your data?
. Sec07-BP01:"Understand your data classification scheme"
. Sec07-BP02: "apply data protection controls based on data sensitivity"

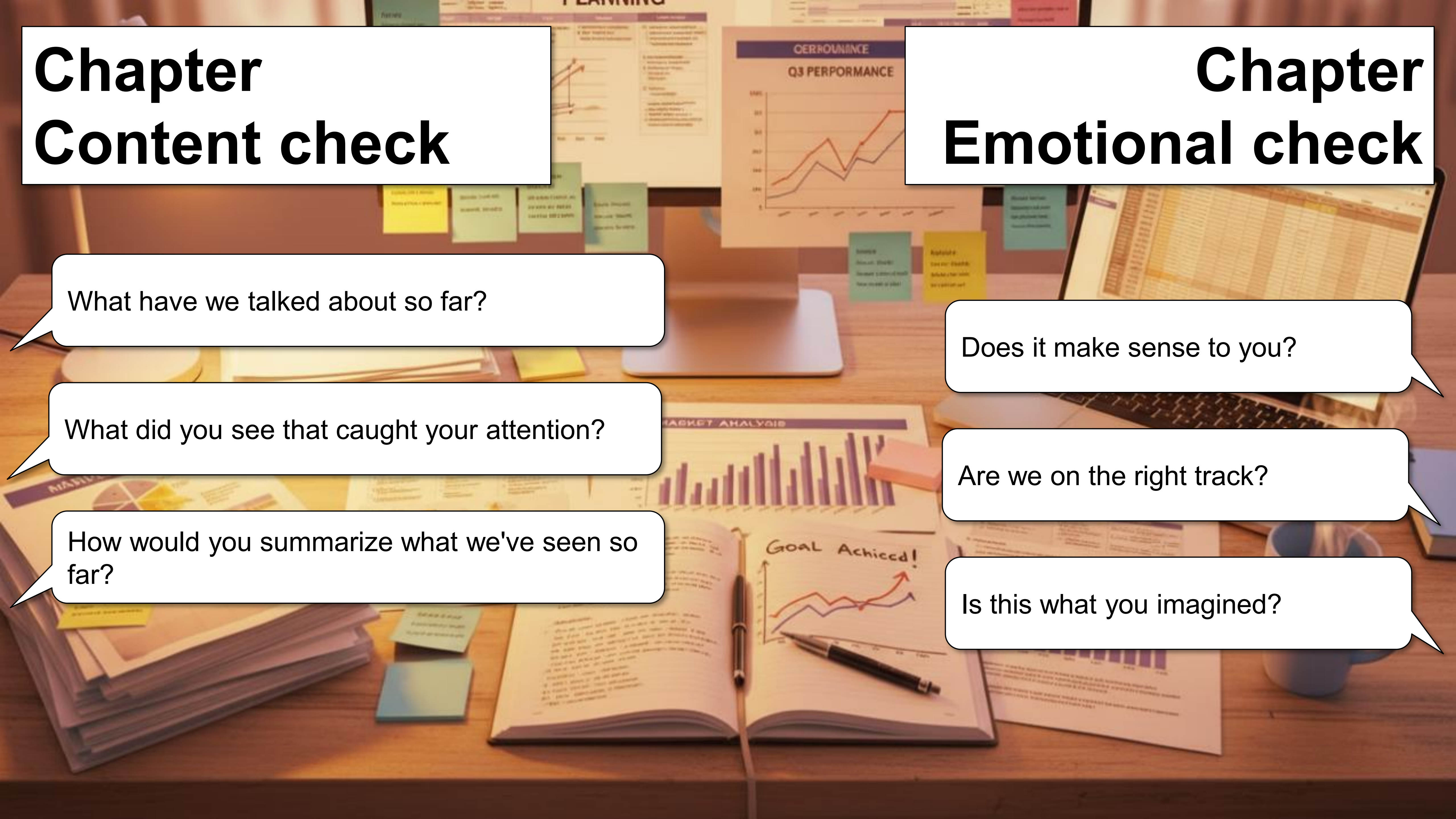
. Design Principles

Traceability Matrix (

HRI (No automated tagging for data classification) – fails SEC07-BP01

…

. Implementation guidance : xxx
. AWS Services and Controls



Chapter
Content check

What have we talked about so far?

What did you see that caught your attention?

How would you summarize what we've seen so far?

Chapter
Emotional check

Does it make sense to you?

Are we on the right track?

Is this what you imagined?

Chapter discussion

What did you see in this chapter:

- An Assessment Tool based sovereign-by-design principals positions partners as trusted advisors and create value
- Tools based on proven principles and frameworks (like AWS WAF, SMM) bridge regulatory requirement into concrete sovereign architecture decisions

What are we going to write in the action plan?

Suggested actionable items

- Create a **traceability matrix** listing the sovereign regulations requirements to architecture best practices and to AWS services and features, for your target markets
- Create a **Digital Sovereignty Lens** to customize the WAF tool to improve the assessment of architectures
- Create/Adapt a **Digital Sovereignty Assessment methodology** to use internally and/or to productize
- **Integrate Design Principles into Offerings:** Review your solution architecture best practices and integrate the "Sovereign by Design" principles (e.g., design for continuous compliance, interoperability) into your standard solution blueprints and development processes

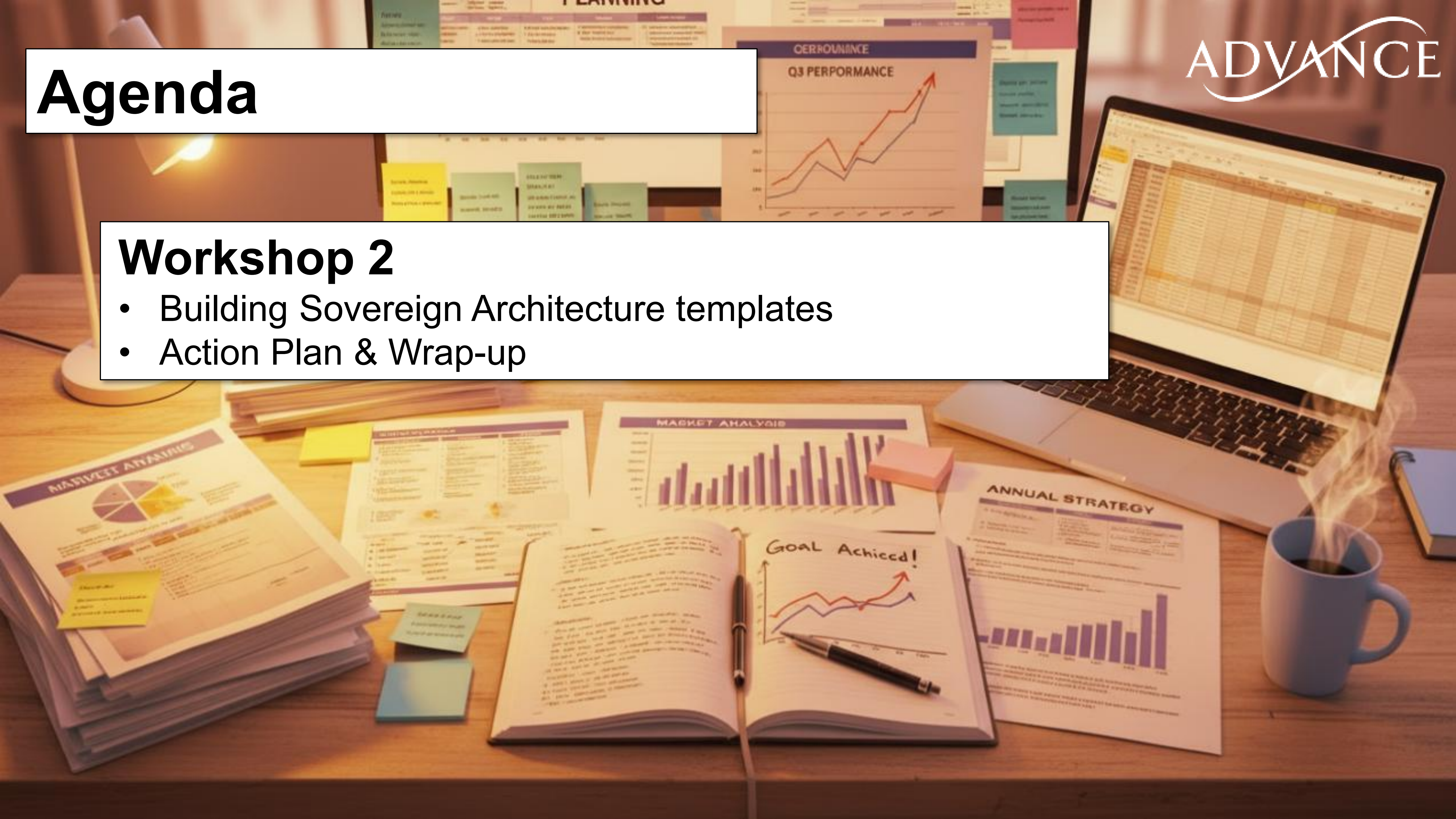
ADVANCE
ADVANCE Your Sales

AWS Digital Sovereignty TTM
Building the Offering

Gustavo Annarumma
gustavo@advanceconsulting.com.br

Workshop 2

Agenda



Workshop 2

- Building Sovereign Architecture templates
- Action Plan & Wrap-up

Building Sovereign Architecture templates

This section addresses the creation of sovereign offerings, highlighting Landing Zone Accelerators (LZAs) to build secure and compliant cloud infrastructures-as-code, enabling partners to differentiate themselves and create recurring value

Recap from Workshop # 1

- Review Digital Sovereignty definitions and domains
    - Sovereignty for SoftwareOne BR and for customers
    - Compliant ≠ Sovereign
    - SoftwareOne Brasil to appoint a Digital Sovereighty focal-point

- The importance of Assessments
    - SoftwareOne has a Digital Sovereign security assessment offer
    - Traceability matrix as a fundamental IP for assessment and deployment
    - Education could be a focus vertical to adapt the assessment tool

Why Landing Zone Accelerators Matter for SI Partners?

Advantage	How it Drives Partner Growth
• **New Revenue Stream**	Implements an IP play (differentiation) and a Service play (recurring revenue)
• **Reusable IP**	Partners use it as a *pre-sales entry point* to uncover customer concerns, map opportunities, and demonstrate thought leadership.
• **Accelerate Time-to-Value**	Automates complex, customer-specific configurations. Reduces deployment times
• **Asset Reusability**	Operational efficiency and scalability
• **Reduce Delivery Risk**	Automation reduces errors
• **Competency & Recognition**	Supports achievement of Competency as it demonstrates capability maturity.

AWS Control Tower and the Landing Zone

- **AWS Managed Service** automates and governs well-architected, secure, compliant multi-account **foundation** environments (LANDING ZONES)

- **The physical implementation of Well-Architecture Framework best practices**

- **Orchestrates** AWS Organizations, Service Catalog, and IAM Identity Center automatically

    - **Multi-account structure** (root + OUs)
    - **Predefined guardrails (**SCPs + detective controls)
    - **Centralized logging** (CloudTrail, Config) in a Log Archive Account
    - **Audit Account** for security investigations

- **Account Factory**

- **Dashboard**

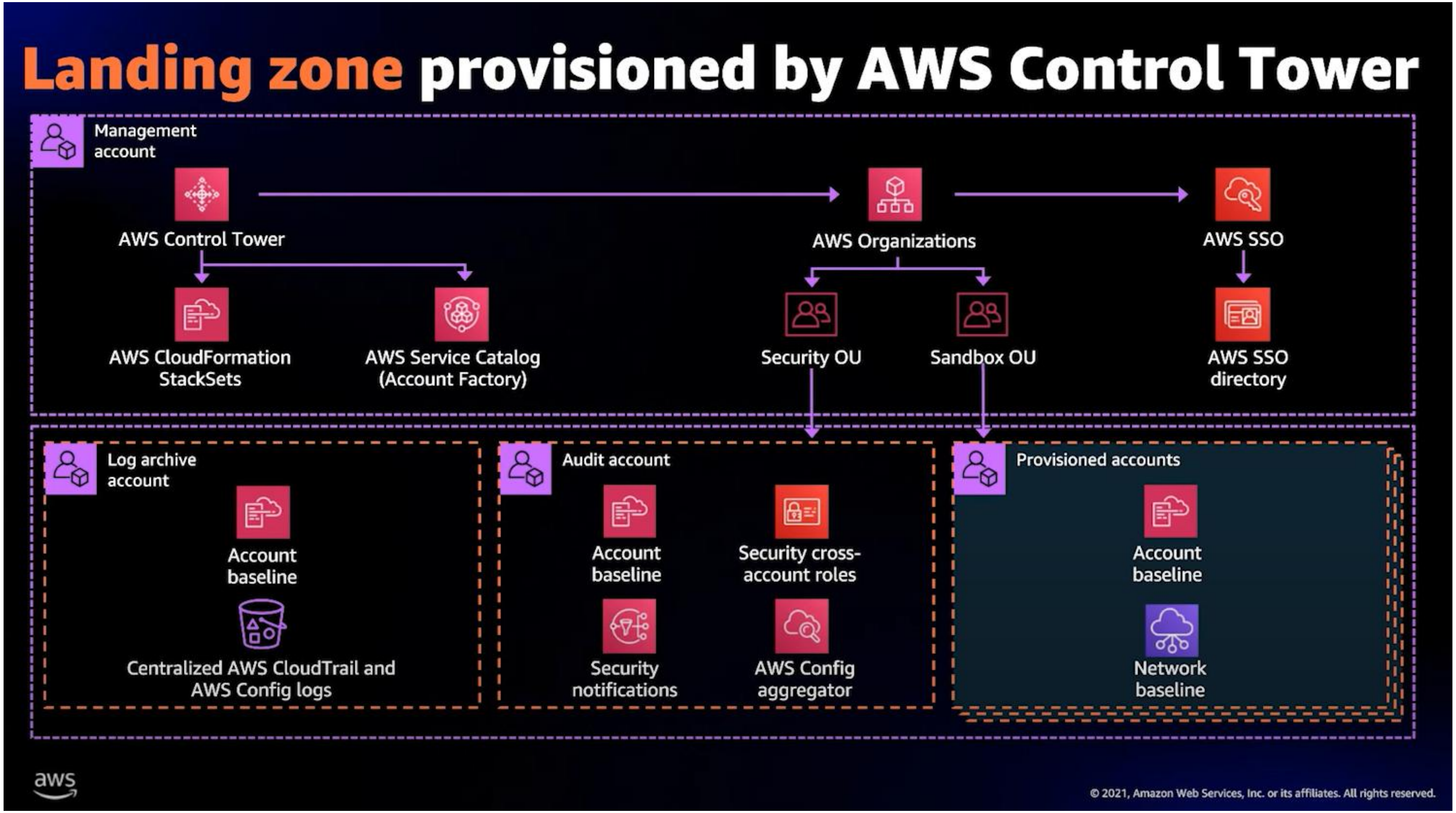
- **245+ Digital Sovereignty Controls**

- **Extendable with Customizations for Control Tower (CfCT)**

https://aws.amazon.com/blogs/aws/aws-control-tower-helps-customers-meet-digital-sovereignty-requirements/

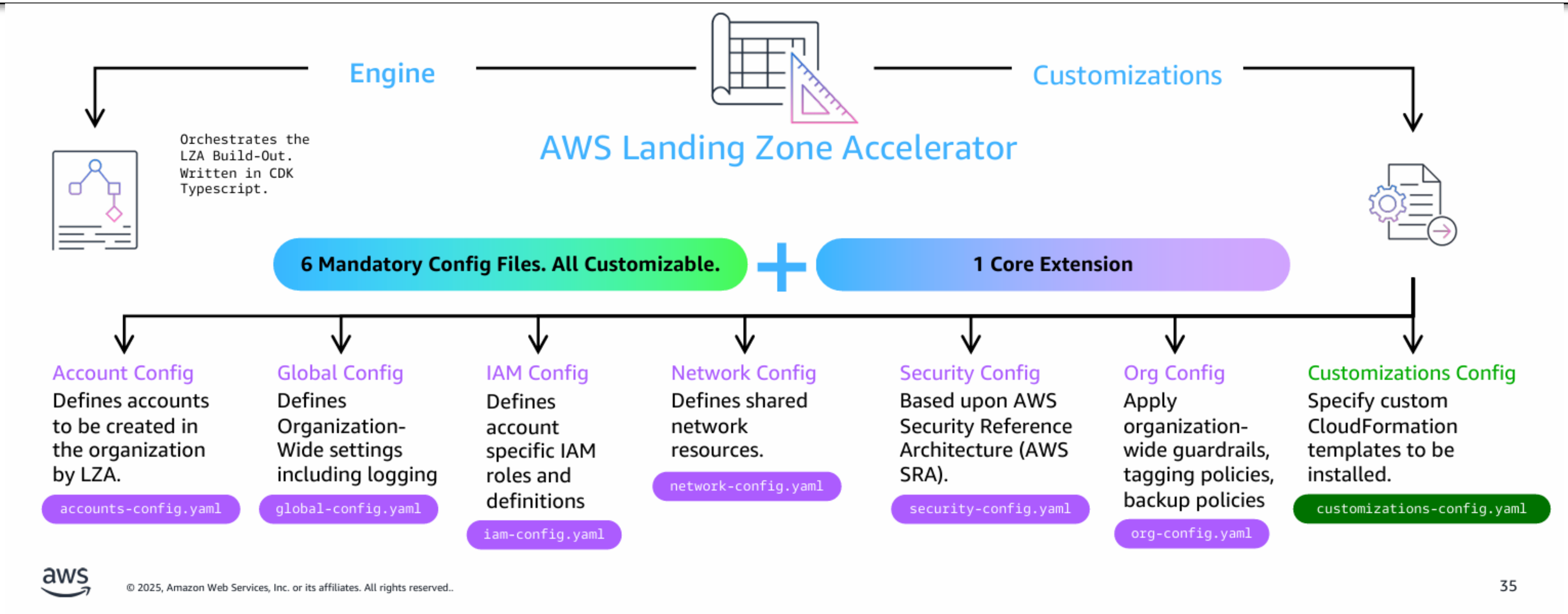
Landing Zones and AWS Control Tower

Landing Zone is a **well-architected**, **multi-account**, and **secure** AWS baseline infrastructure



Landing Zones Accelerators

- **An open-source infrastructure as code (IaC) solution**
- Automates provision of reference **secure, governed, multi-account AWS environments**, including accounts, organizational units (OUs), guardrails, networking, security services
- LZA uses configuration files (YAML) to specify the desired account structure, guardrails, network settings
- … and runs pipelines (CodePipeline / CodeBuild) to deploy the resulting stacks across accounts & regions.



Engine
Customizations
AWS Landing Zone Accelerator
Orchestrates the LZA Build-Out. Written in CDK Typescript.
6 Mandatory Config Files. All Customizable.
+
1 Core Extension

Account Config
Defines accounts to be created in the organization by LZA.
`accounts-config.yaml`

Global Config
Defines Organization-Wide settings including logging
`global-config.yaml`

IAM Config
Defines account specific IAM roles and definitions
`iam-config.yaml`

Network Config
Defines shared network resources.
`network-config.yaml`

Security Config
Based upon AWS Security Reference Architecture (AWS SRA).
`security-config.yaml`

Org Config
Apply organization-wide guardrails, tagging policies, backup policies
`org-config.yaml`

Customizations Config
Specify custom CloudFormation templates to be installed.
`customizations-config.yaml`

https://github.com/awslabs/landing-zone-accelerator-on-aws/tree/main/reference/sample-configurations

AWS LZA Universal Configuration

(https://docs.aws.amazon.com/solutions/latest/landing-zone-accelerator-on-aws/support-for-regions-and-industries.html)

- **Opinionated approach** to configuring Landing Zones
- Based on **AWS Well-Architected Framework**, **AWS Security Reference Architecture**, **AWS ProServ** vast **experience**
- **Simplifies** the complexity of establishing a well-architected landing zone
- **Pre-built set** of configurations, incorporating AWS security best practices, governance controls, and operational excellence principles
- Provides a **customization layer** to address local or organizational requirements
- Currently offers **compliance mapping** coverage for the following regional and industry implementations:
  - FedRAMP Moderate; High
  - Cybersecurity Maturity Model Certification (CMMC)
  - NIST SP 800-171r2
  - Germany’s Cloud Computing Compliance Criteria Catalogue (C5)
  - ISO/IEC 27001
  - HIPAA

(https://github.com/aws/lza-universal-configuration)

Chapter discussion

What did you see in this chapter:

- LZs + CfCT to create reference blueprints
- LZAs are more robust blueprints but customizations to specific regional and regulatory requirements may be required
- Customized LZAs are strong opportunities to gain customer trust, to create differentiation and recurring revenue

What are we going to write in the action plan?

Suggested actionable items

- **Develop Observability & Transparency Tools:** Invest in or integrate tools/practices that enhance visibility and transparency for customers (e.g., custom dashboards for audit trails, simplified access control policy visualization) to prove their control posture

- **Skills Development for Portability:** Focus skill development on technologies and practices that enable interoperability and portability (e.g., containerization, open-source adoption, multi-cloud strategy if applicable) to empower customer choice and independence

- **Develop Contractual Advisory Service:** Offer advisory services to customers on interpreting and negotiating SLA and contract clauses related to digital sovereignty, helping them ensure alignment with their mandates

- **Automate Evidence Collection:** Implement automation for continuous evidence generation (logs, config changes, audit trails) to support customer compliance and auditability, reducing manual effort

Sovereign Services opportunities

Sovereign Foundations Services

- **Digital Sovereignty Assessment:** Map customer workloads against best practices (AWS Well-Architected, Security Maturity Model, Sovereignty Design Principles).
- **Landing Zone Design & Deployment**: Build or extend Landing Zone Accelerators (LZAs) tailored to jurisdictional laws (LGPD, GDPR, HIPAA, DORA, etc.)

Compliance and Governance Services

- **Managed Sovereign Compliance Service:** Continuous monitoring, reporting, and alerting aligned to sovereign regulations.
- **Audit & Evidence Automation:** Leverage AWS Audit Manager, Config Conformance Packs, and partner accelerators for automated evidence collection.
- **Data Classification & Mapping Workshops:** Identify and classify sensitive, restricted, or regulated workloads.

Sovereign Services opportunities

Security & Key Management Services

- **BYOK / HYOK Services**: Deploy "Bring/Host Your Own Key" solutions using AWS KMS, CloudHSM, or partner external key stores for sovereign key control.
- **Operator Access Restriction**: Enforce least privilege and sovereignty boundaries with IAM, SCPs, JIT access, and monitoring of AWS operator/admin activities.

Sovereign Data Protection Services

- **Backup & Disaster Recovery Sovereign Solutions**: Ensure localized backups and cross-region replication within approved jurisdictions
- **Education Data Protection**: Sector-specific solutions such as protecting minors' data under regulations, or sovereignty-ready SaaS platforms (e.g., Moodle, Canvas).
- **Data Classification & Mapping Workshops:** Identify and classify sensitive, restricted, or regulated workloads.

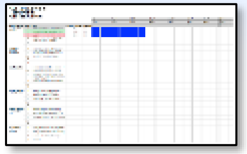
Marketplace & Ecosystem

- **Marketplace Sovereign Solutions**: Publish and certify partner solutions on AWS Marketplace with sovereignty labeling (e.g., LGPD-ready DLP tools, GDPR-ready monitoring)

Action plan & wrap-up

This final chapter consolidates all workshop content into a practical action plan, dividing it into Research, Creation, and Execution phases, providing a detailed roadmap and supporting materials for participants to implement their Digital Sovereignty strategies

Action Plan



Action (Objective/Goal)	S	Code	Activity	Sponsor	Start date	Deadline
Research	1	1.01	Conduct in-depth market research to identify specific digital sovereignty pains, problems, or needs in target industries/segments.		10/mai/23	12/mai/23
	2	1.03	Analyze current competitive landscape for sovereign cloud offerings.		15/mai/23	10/jun/23
	3	1.05	Brainstorm initial sovereign offering concepts leveraging AWS capabilities to address identified pains.		25/mai/23	20/jun/23
		1.07	Conduct preliminary financial feasibility analysis (pricing, costs, profitability) for the proposed concepts.			
		1.09	Conduct customer interviews/surveys to validate interest in specific sovereign offering concepts and gather feedback.			
Creation		2.01	Define precise target market(s) and customer personas for the sovereign offering.			
		2.03	Clearly define the specific pains, problems, or needs the sovereign package will meet.			
		2.05	Define the list of benefits and differentiators of the package (marketing positioning).			
		2.07	Define the name of the offer and its strategic fit within the existing portfolio.			
		2.09	Define specific AWS services, partner IP, and components to be included in the sovereign package.			
		2.11	Determine commercial modalities (packaging, licensing) and finalize pricing strategies.			
		2.13	Develop success stories and use cases demonstrating the value of the sovereign offering.			
		2.15	Define prospecting questions and competitive argumentation for sales teams.			
		2.17	Define the timeline for marketing outreach campaigns.			
		2.19	Define the marketing and sales processes for the new offering.			
		2.21	Establish sales goals and marketing KPIs for the offering.			
		2.23	Develop and deliver training programs for sales teams on the new sovereign offering.			
		2.25	Define implementation processes and KPIs for delivery of the sovereign offering.			
		2.27				
Execution		3.01	Launch the sovereign offering according to the defined marketing and sales plans.			
		3.03	Continuously monitor sales performance against established goals.			
		3.05	Monitor marketing and operations KPIs and collect customer feedback.			
		3.07	Analyze performance data and feedback, proposing improvements to the offering or processes.			
		3.09	Adjust sales pitch, marketing materials, and offer components based on monitoring and feedback.			
		3.11				

ADVANCE
ADVANCE Your Sales

ADVANCE Consulting

Advance Your Sales

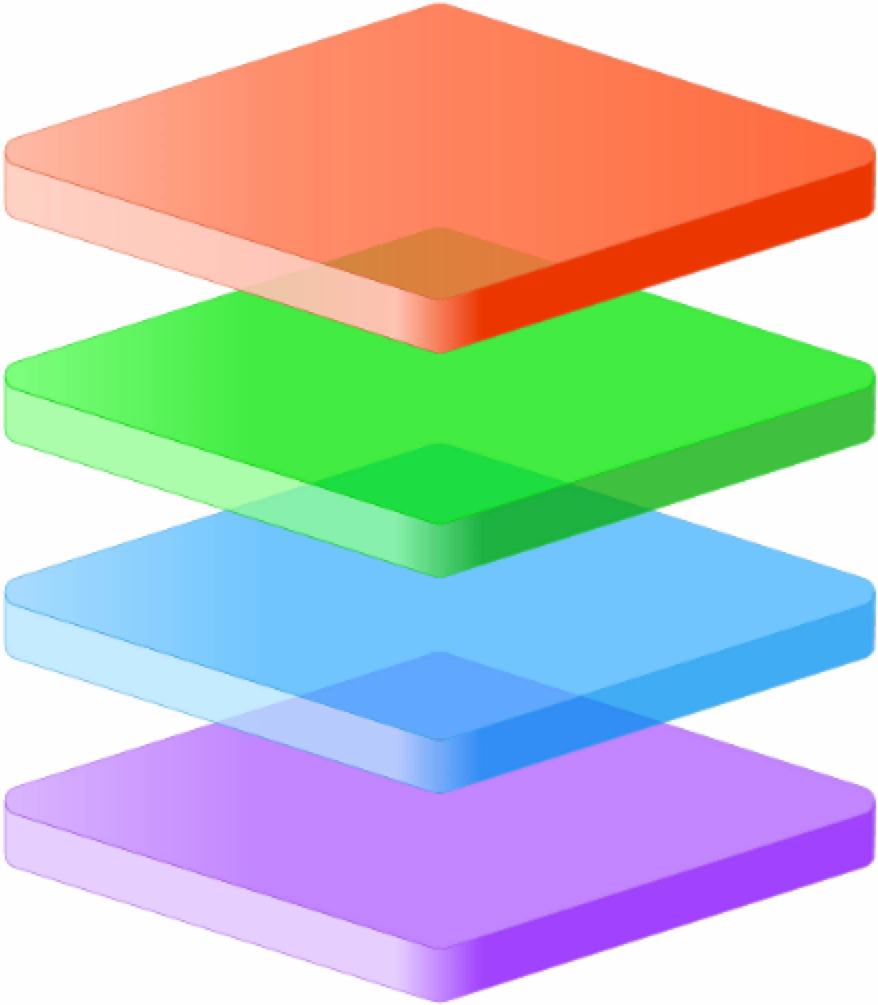
www.advanceconsulting.com.br

ADVANCE
ADVANCE Your Sales

BACK UP SLIDES

www.advanceconsulting.com.br

Visualizing Sovereignty as a Stack



VISIBILITY, TRANSPARENCY, RESILIENCY, PORTABILITY

Amazon Guard Duty
INTELLIGENT THREAT DETECTION

AWS Audit Manager
CONTINUOUS COMPLIANCE AND AUDITABILITY, WITH PRE-BUILT AUDITS

Amazon Security Lake
STORE, ANALYZE SECURITY DATA FORMATTED USING OPEN SCHEMA (OCSF)

Provable Security
IAM ACCESS ANALYZER, AMAZON VERIFIED PERMISSIONS

Improve Portability
15 PLUS OPEN-SOURCE ALIGNED SERVICES, SUPPORT FOR OPEN DATA & OPEN TABLE FORMATS

AWS Resilience Hub
MANAGE AND IMPROVE THE RESILIENCE POSTURE OF YOUR APPLICATIONS

ADDITIONAL WORKLOAD PROTECTION

AWS KMS
EXTERNAL KEY STORES CUSTOMER MANAGED HSM

Nitro, Nitro Enclaves
COMPUTE PROTECTION

Amazon Macie
DISCOVER SENSITIVE DATA

POLICIES, AUTOMATED CHECKS & ATTESTATIONS

AWS Config
PRE-BUILT POLICY PACKS MAPPED TO REGULATORY FRAMEWORKS, EXTENSIBLE, WRITE YOUR OWN RULES

AWS CloudFormation
PRE-PACKAGED PROACTIVE HOOKS, BUILD CUSTOM HOOKS OR USE A DSL TO WRITE YOUR OWN CFN-GUARD RULES

AWS Artifact
ON-DEMAND ACCESS TO SECURITY AND COMPLIANCE REPORTS FROM AWS AND ISVS

FOUNDATIONAL SECURITY

AWS Control Tower
OVER 240 PLUS DIGITAL SOVEREIGNTY ALIGNED CONTROLS, INCLUDING 23 MANDATORY CONTROLS

AWS Security Hub
PRE-CONFIGURED SECURITY STANDARDS, COMPREHENSIVE VIEW OF YOUR SECURITY SATE

Landing Zone Accelerators
PRE-BUILT TEMPLATES ALIGNING WITH MULTIPLE GLOBAL COMPLIANCE FRAMEWORKS, PARTNER BUILT LZA

Service Landscape

Apply standardized enforceable Controls

- AWS Config
- AWS Security Hub
- Amazon Verified Permissions
- VPC Reachability Analyzer
- IAM Access Analyzer
- VPC Network Access Analyzer

Design for visibility and transparency

- Amazon Macie
- AWS Network Firewall
- AWS WAF
- AWS X-Ray
- AWS Shield
- Amazon GuardDuty
- Amazon Security Lake
- Amazon Inspector

Design for continuous compliance

- AWS Config
- AWS Security Hub
- Amazon GuardDuty
- AWS Artifact
- Amazon Inspector
- AWS Audit Manager
- Amazon Detective
- AWS Systems Manager

Design for interoperability and portability

- Amazon ECS Anywhere
- Amazon EKS Anywhere
- AWS Distro for OpenTelemetry
- EKS Distro
- 15 plus open source aligned services

Design for survivability

- AWS Resilience Hub
- AWS Elastic Disaster Recovery
- AWS Fault Injection Simulator

- AWS Control Tower
- AWS Organizations
- Amazon CloudTrail Management & Data Events
- Amazon CloudWatch
- AWS IAM
- AWS IAM Identity Center
- Amazon Nitro Enclaves
- AWS KMS (XKS)
- AWS Certificate Manager

AWS : Sovereign-by-Design Principles

	Design Principles	Driving Forces
A	**Apply standardized enforceable controls**	Interpreting compliance needs and creating effective controls • Requires deep domain knowledge • Is time consuming • And is prone to potential errors
B	**Establish adequate security posture in-line with data sensitivity levels**	Customer requires • Full visibility of where data is stored • Control how and with whom data is shared • Audit who has access and for what duration
C	**Design for continuous compliance**	• Attestations and certifications are snap shots • Audits disrupt operations by requiring engineering teams to collect evidence
D	**Design for interoperability and portability**	• Customers want to be self-sufficient. This translates to uninterrupted access to infrastructure, services and skills required to support their digital footprint. • Customers want choices. They don’t want to be locked into a proprietary technologies or punitive license terms.
E	**Design for survivability**	• Customers want to be self-sufficient. This translates to uninterrupted access to infrastructure, services and skills required to support their digital footprint. • Customers want choices. They don’t want to be locked into a proprietary technologies or punitive license terms.

AWS : Sovereign-by-Design Principles

A) Apply Standardization Enforceable Controls

Initiatives	
Document	Create a compliance matrix or a traceability document that maps specific regulatory requirements to the technical controls and processes, implemented to fulfil those requirements. This provides an auditable trail tying your practices directly to mandates.
Standardize	Utilize software or services that provide standardized compliance controls out-of-the-box. Standardized controls leave no room for interpretation and reduce the risk of erroneous or inconsistent implementations. These controls must be automated and continuously monitor for misconfigurations around the clock. The deployment of standardized, automated controls is known as "policy-as-code" (PaC).
Automate	Policy-as-code, codifies compliance requirements and policies into automated tests and validations that can be integrated into CI/CD pipelines. This allows compliance to be continuously enforced through automated guardrails during software development and infrastructure provisioning. When combined with modern DevOps practices, policy-as-code can play a major role in reducing both the risks and costs associated with compliance. Develop policies-as-code, that solve a single defined problem and are verifiable. Look to package PaCs under easily recognizable compliance groups.
Shift Left	Prioritize "shifting left" by embedding preventative and proactive controls into the software development lifecycle. Embed controls directly into the Continuous Integration/Continuous Deployment (CI/CD) pipelines and infrastructure-as-code workflows to stop non-compliant resources from being deployed. When preventative controls are not feasible, deploy detective controls with automated remediation capabilities to restore compliance quickly.

AWS : Sovereign-by-Design Principles

B) Establish adequate security posture in-line with data sensitivity levels

Initiatives	
Locate	Protect sensitive data in the cloud, using automated discovery, classification and cataloging, augmented with human-in-the-loop process. AWS services like Amazon Macie automatically identify and classify sensitive data types like personally identifiable information (PII) across data stores like S3 buckets.
Protect	Define trust boundaries implementing strict access permissions. Restrict sensitive information sharing to verified accounts and environments. Apply data obfuscation techniques like tokenization, masking to balance data utility with security controls.
Verify	Use threat modelling to help verify the effectiveness and coverage of security controls placed to protect sensitive data. Integrate Amazon GuardDuty, Amazon Inspector, AWS Firewall Manager, and AWS Security Hub to automate threat detection and consolidate security findings in a unified dashboard.
Observe	Track data movement both across and within trust boundaries. Record boundary crossing using gateway and firewall logs at network edges. Monitor all traffic with Virtual Private Cloud (VPC) Flow Logs, Domain Name System (DNS) query logs, and Web Application Firewall (WAF) logs. Use data lineage solutions to track information flowing through your data pipelines and storage systems.
Evidence	Retain network flow logs, usage logs, access logs, application logs, audit trails and security findings for the long-term aligning with regulatory needs. Use immutable storage options and protect the chain of evidence.

AWS : Sovereign-by-Design Principles

B) Establish adequate security posture in-line with data sensitivity levels (cont.)

Initiatives	
Improve privacy and transparency	• Implement consent management systems to track user preferences for personal data use. • Collect only necessary data and clearly inform users about how you collect, process, and share their information. • Create data retention policies that comply with regulations and delete data promptly when no longer needed. • Build systems that support user rights protections as mandated by data privacy legislations; including data access, correction, deletion and portability. • Conduct Data Protection Impact Assessments (DPIAs) for processing activities involving personal data to identify privacy risks.

AWS : Sovereign-by-Design Principles

C) Design for Continuous Compliance

Initiatives	
Introduce a Culture of Compliance	Integrate compliance into all software development activities and operational processes rather than adding it later. Weave compliance activities into the entire software development lifecycle to identify and mitigate risks before incidents occur. Cultivate a culture of continuous compliance, ensuring systems and processes are consistently audit ready and aligned with regulatory standards. Implement regular compliance training for all staff. Without a continuous compliance mindset, organizations risk accumulating technical debt, security vulnerabilities, and regulatory violations over time. Compliance cannot be an isolated, periodic effort. It requires comprehensive integration across people, processes, and technology to be sustainable and effective long-term.
Be audit ready	Monitor compliance status continuously to reduce audit disruption and improve security posture. AWS Audit Manager collects compliance information from AWS Config and AWS Security Hub, tracks user activity through AWS CloudTrail, and captures environment snapshots automatically. This automation produces audit-ready reports that meet regulatory requirements.
Build-in remediations	Prioritize building automated remediations. When “automated remediations” are in place, “return-to compliance” is quick and predictable. Therefore, reducing the need for seeking approvals or unbudgeted expenses.

AWS : Sovereign-by-Design Principles

C) Design for Continuous Compliance

Initiatives	
Empower local teams	Local teams are best placed to understand regional regulatory needs. To improve compliance: • Make local engineers' teams self-sufficient • Engage with local law firms and regulatory authorities to reduce ambiguity around legislations • Hire local talent to better understand regional sensitiveness
Establish vendor compliance	Define specific compliance requirements for vendors based on data handling, security protocols, and regional regulations. Require vendors to demonstrate compliance through certification and regular reporting on security measures. Track vendor compliance through automated monitoring tools, regular audits, and compliance dashboards.

AWS : Sovereign-by-Design Principles

D) Design for interoperability and portability

Initiatives	
Define interoperability goals	Decide why interoperability is important and what risks need to be addressed. Risks could be related to continued availability of technical infrastructure, software, services or skills.
Build abstractions	Incorporate abstractions into your code and configurations to deploy workloads consistently across AWS Regions, AWS edge locations, or another managed infrastructure. This approach eliminates the need for significant rework when deploying to new environments. Consider aligning with open-source technologies, open standards, and open data formats to widen your portability and interoperability options. Alternatively, consider using infrastructure-agnostic ISV solutions.
Plan ahead for data portability	Evaluate data exit policies, the costs involved, tools required, and the available network bandwidth to build a data migration plan if needed. Test your workloads across multiple environments to ensure interoperability. Run identical test suites in each environment to verify consistent functionality across all deployment locations.

AWS : Sovereign-by-Design Principles

E) Design for survivability

Initiatives	
DR must support business recovery	Align with organizational business continuity goals. Define what a minimum restorable service is. Define timelines for full-service restoration
Design systems with DR as a stated goal	Document your recovery path. Test for disaster recovery. Prioritize and test all critical paths of recovery. Record outcomes of DR testing. Use Correction of Errors (CoE) to identify root causes and mitigations
Prepare for DR	In addition to stakeholders involved in performing the actual recovery from a disaster (such as engineers, technical support, and executives), you should also have a list of: • key internal stakeholders • a list of critical vendors • third-party suppliers • and even key customers who might be most affected
Report irregularities	Incorporate regulatory requirements for incident response and breach notification into your disaster recovery and business continuity plans
Plan for contingencies	Implement offline and semi-offline operation modes to maintain critical business functions during severe disruptions. Create procedures to restore workloads after periods of offline operation

Example of Digital Sovereign Domains to Assess

Primary Domain	Purpose / Description	Subdomains
1. Data Sovereignty	Ensure that the customer retains lawful control over all data (storage, processing, sharing)	• **Data Residency & Localization** — physical and logical location of data and processing. • **Data Classification & Sensitivity** — defining and labeling personal, sensitive, or regulated data types. • **Data Lineage & Provenance** — traceability of data origin, movement, and transformation. • **Encryption & Key Management** — control of cryptographic keys, lifecycle, and jurisdictions. • **Data Sharing & Cross-Border Transfers** — contractual and technical control over how data is exchanged between entities or regions.
2. Infrastructure Sovereignty	Maintain jurisdictional and operational control over hosting and networking infrastructure	• **Hosting Location & Jurisdiction** — ownership, control, and physical location of data centers or cloud regions. • **Network & Connectivity Control** — network isolation, routing policies, and interconnect sovereignty. • **Hardware & Virtualization Control** — assurance of hardware provenance, firmware integrity, and hypervisor isolation.
3. Operational Sovereignty	Limit and govern who (including provider operators) can access, manage, or interfere with workloads or data.	• **Identity & Access Management** — authentication, authorization, and federated identity governance. • **Operator Access Control** — least-privilege, just-in-time, dual-control, and privileged access restrictions. • **Policy-as-Code & Governance Automation** — codification of compliance and security rules for automated enforcement.

Example of Digital Sovereign Domains to Assess

Primary Domain	Purpose / Description	Subdomains
4. Governance & Compliance Sovereignty	Ensure transparent, auditable, and enforceable compliance aligned with law and standards	• **Continuous Audit & Monitoring** — logging, telemetry, and continuous compliance validation. • **Regulatory Mapping & Compliance Evidence** — traceability of legal or regulatory requirements to implemented controls. • **Transparency & Accountability** — operational reporting, documentation, and oversight of third-party participation.
5. Continuity & Portability Sovereignty	Guarantee sovereignty under disruption, failure, or exit	• **Resilience & Continuity Management** — sovereign disaster recovery, fault tolerance, and resilience planning. • **Data & Workload Portability** — ability to migrate data and workloads without dependency on a non-sovereign provider. • **Open Standards & Interoperability** — use of open APIs, formats, and frameworks to preserve autonomy.
6. Organizational & Supply Chain Sovereignty	Ensure that the organizations, people, and vendors involved in the ecosystem operate under sovereign control and accountability.	• **Service Provider & Vendor Governance** — supplier selection, onboarding, and compliance alignment. • **Contractual & Legal Readiness** — data processing agreements, jurisdiction clauses, SLAs, and regulatory certifications. • **Personnel & Citizenship Control** — employee nationality, security clearance, and access conditions for sensitive workloads. • **Supply Chain Transparency & Risk Management** — traceability of software, hardware, and service components across the chain. • **Third-Party Dependency Control** — cloud service sub-processors, subcontractors, or software dependencies under jurisdictional risk review.