SYMBEEO

PUBLIC

DESIGN STUDY

Landing zone for a bank's 140 AWS accounts, enrolled one window at a time

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Cloud	Financial Services	EU retail bank
DOCUMENT	**VERSION**	**DATE**
CLD-002	1.1	Oct 10, 2026

WRITTEN BY

Steve Phillips, Principal Data Center Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	CLD-002	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Cloud	Industry	Financial Services
Author	Steve Phillips	Role	Principal Data Center Architect
Credentials	CCSP, CCIE, AWS Certified Security – Specialty		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 8
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's own current page on Sep 24, 2026, or on Sep 27, 2026 where marked · [S*] figure from the vendor's page summary where the page itself could not be opened · [A] design assumption, to be confirmed by the signing engineer · [T] design target: the record's outcome figure and anything derived from it. No figure comes from any engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. Steve Phillips remains the author.

1 · Scope

Who it is for. The head of cloud platform at a retail bank whose AWS accounts grew team by team, each with its own trail, its own administrators and its own idea of a region, and whose supervisor now asks for the register of ICT arrangements and the evidence behind it, not a description of it.

Typical buyer [A]. A retail bank in the EU, one AWS organization with all features enabled, 140 member accounts: 38 production, 61 non-production, 41 sandbox or abandoned. 22 of them hold production and test in the same account. Two approved regions, Europe (Frankfurt) and Europe (Ireland). One identity provider, Microsoft Entra ID. About ten new accounts requested per month.

What is in. The landing zone (AWS Control Tower with Landing Zone Accelerator on top), the OU hierarchy, root guardrails, federated sign-in, the write-once audit archive, account vending, the enrollment of all 140 accounts with a rollback for each, and the monthly export that feeds the bank's register of information. This is SRA-CLD-001 R1–R3, R12, R17 and R18 applied to one cloud. **What is out.** Private connectivity from the bank's sites (SRA-CLD-001 §4.4); the second cloud; the SIEM (SRA-SEC-001); refactoring any workload.

Assumptions. AWS is the bank's primary cloud, decided before this document [A]. Accounts that mix environments are split by moving the production workload into a new account, not by re-labeling [A]. Change windows are Tuesday and Thursday, 19:00–23:00 [A]. The supervisor accepts an S3 Object Lock archive in compliance mode as write-once storage for the audit trail [A].

Related documents, read Sep 24, 2026.

- AWS Control Tower, key changes in landing zone 4.0 — `https://docs.aws.amazon.com/controltower/latest/userguide/key-changes-lz-v4.html`
- AWS Control Tower, about enrolling existing accounts — `https://docs.aws.amazon.com/controltower/latest/userguide/enroll-account.html`
- AWS Organizations, quotas and service limits (read Sep 27, 2026) — `https://docs.aws.amazon.com/organizations/latest/userguide/orgs_reference_limits.html`
- AWS Organizations, service control policies ("SCPs don't affect users or roles in the management account"), read Sep 27, 2026 — `https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html`
- Landing Zone Accelerator on AWS, releases (v1.16.3, September 16, 2026) — `https://github.com/awslabs/landing-zone-accelerator-on-aws/releases`

© 2026 Symbeeo. All rights reserved. · Public

- Amazon S3, locking objects with Object Lock — https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html
- ESMA, Digital Operational Resilience Act — https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- AWS, defining a multi-account strategy for a digital bank — https://aws.amazon.com/blogs/industries/defining-an-aws-multi-account-strategy-for-a-digital-bank/
- AWS, LZA Universal Configuration and Compliance Workbook — https://aws.amazon.com/blogs/security/introducing-the-landing-zone-accelerator-on-aws-universal-configuration-and-lza-compliance-workbook/

1c · Public implementations this design follows

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Digital-bank OU pattern: foundational OUs (Infrastructure, Security, Deployment, Policy Staging, Sandbox, Suspended) plus workload OUs, one account per workload	AWS Industries blog · Sep 27, 2021 · vendor documentation, used to build our own design	§4.1: the bank-shaped form of the SRA-CLD-001 hierarchy; Policy Staging kept as the guardrail test OU	https://aws.amazon.com/blogs/industries/defining-an-aws-multi-account-strategy-for-a-digital-bank/
LZA Universal Configuration: a security baseline "developed from field experience with highly regulated customers"; the Compliance Workbook maps it to 12 frameworks	AWS Security blog · Nov 20, 2025, updated Apr 4, 2026 · vendor documentation, used to build our own design	R7 and §4.2: LZA on top of Control Tower instead of a home-built pipeline	https://aws.amazon.com/blogs/security/introducing-the-landing-zone-accelerator-on-aws-universal-configuration-and-lza-compliance-workbook/

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Accounts in scope	140 existing · about 10 new per month	[A]
R2	Environment isolation	0 accounts holding more than one environment (22 at the start)	[T]; [A] count
R3	Human sign-in	100 % through the IdP; ≤ 2 alarmed break-glass users for the organization	[T]
R4	Root guardrails	five SCPs: region allow-list (Frankfurt, Ireland), deny leaving the organization, deny trail changes, require encryption at rest on new storage, protect the account-level S3 Block Public Access setting; in force before a workload lands	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R5	Guardrail budget	≤ 10 SCPs directly attached per root, OU or account, the AWS-managed FullAWSAccess included; inherited policies do not count; ≤ 10,240 characters per SCP; ≤ 5 RCPs per target	[S] AWS Organizations quotas, read Sep 27, 2026
R6	Hierarchy depth	≤ 5 OU levels under the root	[S] AWS Organizations quotas
R7	Landing zone	Control Tower landing zone 4.0, integrations for Config, CloudTrail, SecurityRoles and Backup enabled	[S] LZ 4.0 makes each integration configurable
R8	Drift alerts	drift events routed from EventBridge in the management account to platform on-call	[S] LZ 4.0 sends drift to EventBridge, not SNS
R9	Enrollment pre-check	AWSControlTowerExecution role present; no AWS Config recorder or delivery channel in the account	[S] enrollment guide
R10	Audit archive	organization trail to S3 Object Lock in compliance mode, 400 days	[S] compliance mode; [A] 400 days
R11	Account vending	new account with R2–R4 and R10 applied ≤ 1 working day after approval	[T]
R12	Enrollment impact	0 workload outages during enrollment or rollback	[T]
R13	Enrollment pace	6 accounts per window, 2 windows per week, 12 weeks	[A]
R14	Declared state	100 % of OUs, SCPs, RCPs and baselines match the configuration repository, checked every 24 h	[T]
R15	Register feed	monthly export of every account with owner, environment, criticality and ICT service, for the register of information	[T]; [S] DORA applies as of January 17, 2025

Fifteen rows; seven carry a vendor or regulator figure, three are design assumptions, five are design targets.

3 · Architecture overview

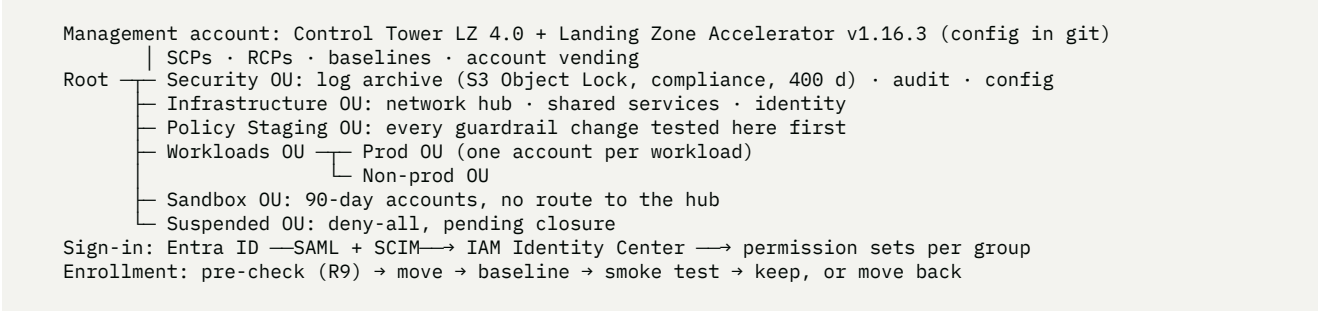


Figure 1. Organization hierarchy and account enrollment

© 2026 Symbeeo. All rights reserved. · Public

One organization, one hierarchy two levels deep, one configuration repository that the pipeline applies and nobody edits in the console. The 140 accounts are not rebuilt; they are enrolled into the hierarchy six at a time, and each one can be moved back to where it was inside the same window.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Landing zone	AWS Control Tower, landing zone 4.0	1 organization	140 accounts, about 280 in 12 months: 140 + 22 from the splits + about 120 new [A]	integrations configurable, drift to EventBridge [S]
Configuration pipeline	Landing Zone Accelerator on AWS v1.16.3	1	every OU and account [T]	released Sep 16, 2026 [S]; baseline for regulated workloads [S]
Organization policy	AWS Organizations SCPs and RCPs	6 of 10 SCPs at root (5 of ours + FullAWSAccess), ≤ 3 of ours per OU	root and 8 OUs [T]	quotas in R5 [S]
Sign-in	AWS IAM Identity Center with Microsoft Entra ID	1	all human access [T]	one federation for 140 accounts [A]
Audit archive	Amazon S3 with Object Lock, compliance mode	1 bucket in the log archive account	400 days of the organization trail [A]	WORM; assessed by Cohasset for SEC 17a-4, CFTC and FINRA [S]

4 · Design by subsystem

4.1 Hierarchy.

The SRA-CLD-001 shape in AWS terms, following the digital-bank pattern: Security, Infrastructure, Policy Staging, Workloads (Prod, Non-prod), Sandbox, Suspended [S]. Under landing zone 4.0 Control Tower no longer creates the Security OU; the OU that holds the service-integration accounts becomes the designated Security OU [S], so the design creates it first and places the log archive and audit accounts there. Deepest path: root → Workloads → Prod, two levels of five allowed [S]. Rejected: business lines at the top level — environment becomes the second key, so each production guardrail is attached once per business line and the 10-SCP budget per OU (R5) runs out.

4.2 Guardrails.

Five SCPs at the root (R4) [T]: region allow-list with the global-service exemptions, deny leaving the organization, deny stopping or deleting CloudTrail, require encryption on new storage, and deny changes to the account-level S3 Block Public Access setting, which is turned on in every account [A]. The AWS-managed FullAWSAccess SCP stays attached and counts toward the root's ten, so the root holds six of ten [S] (quotas read Sep 27, 2026). On each OU, FullAWSAccess and the Control Tower controls SCP take two slots [A], leaving up to three of ours and five spare. One RCP restricts S3 and KMS access to principals inside the organization [A]; the RCPFullAWSAccess policy counts toward the five-RCP quota [S], leaving three. Every change is merged to the repository, applied to the Policy Staging OU and its test account, then promoted by the pipeline (R14). Rejected: SCPs written in the console per incident — that is how the 140 accounts reached their current state, and it fails R14.

4.3 Identity.

Entra ID federated to IAM Identity Center by SAML, groups provisioned by SCIM [A]; permission sets per group, none per person. Control Tower provisions permission sets for the Logging and SecurityRoles accounts but not for the Config

© 2026 Symbeeo. All rights reserved. · Public

or Backup accounts [S]; those two are created by the pipeline. Two break-glass users in the management account carry hardware MFA, and any sign-in raises an EventBridge alarm to the on-call [A] (R3). IAM users with console passwords in workload accounts are listed at pre-check and removed after enrollment [A]. Rejected: one SAML application per account — 140 trust relationships to rotate.

4.4 Audit archive.

The Control Tower CloudTrail integration writes the organization trail to the log archive account. The bucket uses Object Lock in compliance mode: a locked version "can't be overwritten or deleted by any user, including the root user" [S]; default retention 400 days [A]. Retention is set first in governance mode on a test bucket and moved to compliance only after the pipeline's retention check passes [A], because a compliance-mode period cannot be shortened [S]. In landing zone 4.0, disabling centralized logging deletes the associated resources from the logging account [S]. Landing-zone changes are made from the management account, where SCPs do not apply [S], so an IAM permissions boundary on every role and permission set in that account except the pipeline role denies the Control Tower landing-zone update, reset and delete actions [A]; the management account's root user sits outside IAM policy and is held under the break-glass procedure [A]. Per-account trails are deleted after enrollment to avoid duplicate CloudTrail charges [S]. Rejected: governance mode in production — a user holding `s3:BypassGovernanceRetention` can delete, which the supervisor would not read as write-once.

4.5 Enrollment of the 140 accounts.

Pre-check per account (R9): the execution role exists; AWS Config recorder and delivery channel exported to the ticket, then stopped and deleted with the guide's commands [S]; existing trails and IAM users listed [A]. Enrollment baselines the account, places it in the target OU and applies that OU's SCPs; it neither adds nor removes VPCs [S]. Order: sandbox, then non-production, then production [A]. During each window a probe calls each production application's health endpoint every 10 s [A]; a failed probe after the move sends the account back to its old OU inside the window (R12). The 22 mixed accounts are split first: production moves to a newly vended account, the old account is enrolled as non-production [T]. Six accounts per window, two windows a week: 144 slots in 12 weeks for 140 accounts, so four slots are spare for retries [A]; a fifth retry moves the last enrollment into week 13 (§6).

4.6 Vending and the register feed.

New accounts are declared in the LZA account configuration and created through the pipeline with R2–R4 and R10 applied (R11). On the first working day of each month an Organizations API export lists every account with its owner, environment, criticality and ICT-service tags (R15) — the input to the register of information that DORA requires, in force since January 17, 2025 [S]. Rejected: a register kept by hand — it drifts from the organization inside a month [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Enrollment fails: Config resources still present	enrollment stops; account unchanged in its old OU; pre-check fixed, retried next window	[S] no existing Config resources allowed; [A] retry
Workload fails its probe after the SCPs apply	account moved back to its old OU in the same window; the denying policy found in CloudTrail	[T] R12; [A] method
Guardrail changed in the console	drift event in EventBridge; pipeline restores the coded state ≤ 24 h	[S] LZ 4.0 drift to EventBridge; [T] R14

© 2026 Symbeeo. All rights reserved. · Public

Failure	Behavior	Source
Attempt to disable centralized logging	refused by the management-account permissions boundary for every role but the pipeline (SCPs do not reach that account); locked trail objects stay locked	[A] boundary; [S] SCP scope, compliance mode
Identity provider unreachable	no new sign-ins; break-glass users in the management account	[A]
SCP quota reached on one OU	new statement merged into an existing SCP inside 10,240 characters	[S] quotas; [A] merge rule

6 · Limits

- The account counts and the 22 mixed accounts are assumptions; the week-1 inventory sets the real enrollment list.
- Twelve accounts a week assumes most accounts carry no AWS Config recorder; each one that does adds an export-and-delete step. The plan has four spare slots; beyond four retries the 12 weeks become 13, and the week-1 inventory says which.
- Compliance-mode retention cannot be shortened and ends early only by closing the account [S]; a wrong period lives for 400 days.
- LZA v1.16.3 is the current release on Sep 24, 2026; the pipeline pins it and upgrades within 90 days of each release [A].
- The monthly export feeds the register of information; the register's legal completeness is the bank's compliance function's, not this design's.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

Steve Phillips

Principal Data Center Architect

CCSP, CCIE, AWS Certified Security – Specialty

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

CLD-002 · Version 1.1 · Oct 10, 2026