The Cloud Landing Zones Guide

A tactical playbook for compliance-first multi-account architecture, written for regulated small and mid-sized businesses on AWS, Azure, or Google Cloud.

A Pandora Cloud Operational Guide

May 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

Foreword: Why Your Landing Zone Determines Your Compliance Trajectory

Most regulated small and mid-sized businesses (SMBs) treat their cloud landing zone as something they "got" rather than something they designed. Someone opened an Amazon Web Services (AWS) account three years ago, named it after the company, and that account has been doing every job ever since: production, development, finance, payroll, the customer-facing product, the internal HR tooling. Every new application got piled on top of the same account. Every new contractor got an Identity and Access Management (IAM) user inside it.

Then the first compliance assessment lands. The Health Insurance Portability and Accountability Act (HIPAA) audit, or the Service Organization Control 2 (SOC 2) Type II, or the Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate (ATO) preparation. The auditor asks where the production logs live and the answer is "the same place as the dev logs." They ask who has access to customer Protected Health Information (PHI) and the answer is "anyone who can log into the AWS console." They ask for evidence that test workloads cannot reach production data and there is no evidence; the architecture does not separate them.

This is not a tooling problem. The teams in this situation have access to the same AWS services as a FedRAMP-authorized vendor. What they lack is the foundational architecture decision: a deliberate landing zone that pre-decides who can touch what, where evidence accumulates, what failure modes are possible, and what frameworks the structure satisfies by default.

The central claim of this guide

Three days of foundational design at the start of a regulated SMB's cloud life saves twelve to eighteen months of remediation later. The decisions in this guide are the ones that determine whether your next compliance assessment is a review of evidence already collected or an excavation project.

We wrote this for the team that is one quarter out from their first compliance assessment and just realized their landing zone is going to be the long pole. We also wrote it for the team that already passed an audit on a fragile structure and knows the next one will not be as forgiving.

This is the tactical companion to the Pandora Cloud Foundation Worksheet. The Worksheet diagnoses what is broken in your current landing zone. This guide tells you how to fix it. Read both together.

Section 1: What a Landing Zone Actually Is (and Isn't)

A landing zone is the operational substrate of a cloud presence. It is not a single product, not a single account, and not a one-time setup task. It is the set of pre-decided answers to the questions every compliance framework will eventually ask you.

A landing zone, at minimum, pre-decides:

- Account topology: how many accounts exist, what each one is for, and how they relate to one another.
- Identity model: where users come from, how they authenticate, how access is granted, and how it expires.
- Network architecture: which networks can reach which networks, where traffic is inspected, where data crosses trust boundaries.
- Evidence collection: where logs land, who can read them, how long they are kept, and how they get to the auditor.
- Security baseline: what controls are turned on by default in every account before anyone deploys anything.

A landing zone, despite common confusion, is NOT:

- A single AWS account, even one that is well-organized internally.
- A Terraform module someone shared on GitHub.
- The result of running AWS Control Tower one time and never touching it again.
- Something the cloud provider gives you for free at signup.
- A static configuration that gets set up once and runs unchanged.

The landing zone is alive. It evolves as your compliance posture matures, your workload count grows, and your team structure changes. The mistake most regulated SMBs make is treating it as a one-time engineering task rather than a continuously-tended operational layer.

The economic argument for a deliberate landing zone is straightforward: every compliance framework that matters to regulated SMBs (HIPAA, SOC 2, Payment Card Industry Data Security Standard (PCI DSS), FedRAMP, National Institute of Standards and Technology (NIST) 800-53 Rev 5, Cybersecurity Maturity Model Certification (CMMC) 2.0) presumes a particular pattern of separation, evidence, and control. A landing zone that pre-satisfies that pattern means the audit is a review of evidence already accumulated. A landing zone that does not means the audit is an excavation project.

Section 2: The Five Architectural Decisions That Make or Break Compliance

Every regulated SMB landing zone reduces to five decisions. The teams who get these right at the start move through audits without scrambling. The teams who get them wrong (or worse, do not make them deliberately) build technical debt that compounds with every new workload.

Decision 1: Account Separation Strategy

The wrong answer: One AWS account that does everything. Separation is enforced by Identity and Access Management (IAM) policy inside a single account, which depends on policy correctness rather than architectural impossibility.

The right answer: A multi-account structure where separation is enforced by the account boundary itself. Account boundaries are the strongest isolation primitive AWS offers; a user in account A cannot accidentally read data from account B because the architecture makes the failure mode impossible.

The baseline structure for most regulated SMBs (six to ten accounts):

- Management account (Organizations root): holds the AWS Organizations structure. No workloads ever live here. Access restricted to a small number of named administrators.
- Security tooling account: runs Security Hub, GuardDuty, Inspector, AWS Config aggregator, and any third-party security tools. Receives findings from every other account.
- Log archive account: the only account with write access for centralized logs. Locked down so that even production engineers cannot delete or modify logs. This is the account the auditor will care about most.
- Identity account: runs AWS IAM Identity Center (formerly AWS Single Sign-On). All human access to every other account flows through here.
- Shared services account: hosts cross-workload infrastructure (centralized Domain Name System (DNS), shared container registries, golden machine images, build pipelines).
- Workload accounts (one per environment per major workload): dev, test, and production accounts for each distinct application. Production and non-production must always be in separate accounts.

Why this matters for compliance

HIPAA requires PHI to be segregated. SOC 2 requires logical separation between production and non-production environments. FedRAMP and NIST 800-53 Rev 5 require separation between authorization boundaries. A single-account architecture cannot demonstrate any of these by design.

Decision 2: Identity Strategy

The wrong answer: Creating IAM users directly in every account. This produces an explosion of long-lived credentials that no one rotates, no one inventories, and no one can revoke quickly when someone leaves the company.

The right answer: Federated identity. AWS IAM Identity Center is the modern default. Users authenticate once against your identity provider (Microsoft Entra ID, Google Workspace, Okta, or AWS Identity Center's built-in directory for very small teams). Their AWS access is short-lived, scoped to permission sets, and centrally manageable.

Non-negotiable rules:

- Multi-factor authentication (MFA) is mandatory for every human user, no exceptions.
- No long-lived IAM access keys for humans, ever.
- Just-in-time elevation for sensitive operations (production access, billing changes, IAM modifications).
- A documented break-glass account for emergency access, with separate MFA, audit logging on every action, and quarterly access review.
- Service-to-service authentication uses IAM roles, never IAM access keys.
- Every access grant has an expiration date.

This is the single highest-leverage change a regulated SMB can make. Identity findings are the most common Authority to Operate finding across every defense and federal engagement we have observed. They are also the cheapest to fix.

Decision 3: Network Architecture

The wrong answer: A single Virtual Private Cloud (VPC) per account with default routing and security groups managed by individual application teams. Lateral movement between workloads becomes trivial; a compromise in one workload exposes every workload.

The right answer: Hub-and-spoke networking via AWS Transit Gateway. A central networking account owns the Transit Gateway and the network address space. Workload VPCs attach to it. Inter-VPC traffic is inspected (AWS Network Firewall, third-party next-generation firewall, or a managed equivalent). Internet egress is centralized through a single inspection point. Sensitive data zones sit in dedicated VPCs with explicit allow-listed connectivity.

Non-negotiable rules:

- Production VPCs have no direct internet access; they egress only through the central inspection account.
- Development VPCs are isolated from production VPCs at the Transit Gateway routing layer, not just at the security group layer.
- Bastion or jump-host patterns are replaced by AWS Systems Manager Session Manager.
- VPC Flow Logs are enabled in every VPC, sent to the log archive account.
- DNS queries are logged via Amazon Route 53 Resolver query logs.

For SMBs that need to support Department of Defense (DoD) workloads at Impact Level 2 (IL2), Impact Level 4 (IL4), or Impact Level 5 (IL5), the network architecture also pre-decides whether you can run in AWS GovCloud (US) or commercial regions. That decision should be made before you build, not after.

Decision 4: Logging and Evidence Strategy

The wrong answer: Each account managing its own logs in its own Amazon Simple Storage Service (S3) buckets. The same engineers who deploy code can also delete the evidence of what they deployed. No auditor accepts this.

The right answer: Centralized, write-once, separately-administered logging. All trails land in the dedicated log archive account where production engineers have no write or delete permissions.

Non-negotiable rules:

- AWS CloudTrail enabled in every account, organization-wide, sent to a dedicated S3 bucket in the log archive account.
- The log archive S3 bucket has S3 Object Lock in compliance mode with a retention period that matches your longest applicable framework (six years for HIPAA documentation per 45 CFR 164.316(b)(2)(i), at minimum the SOC 2 Type II audit period plus the engagement's evidence-retention policy, indefinitely for some FedRAMP scenarios).
- VPC Flow Logs from every VPC, also to the log archive account.
- AWS Config configuration history, enabled organization-wide.
- Application logs aggregated to Amazon CloudWatch Logs in each account, then forwarded to the log archive account via Kinesis Data Firehose.
- Database audit logs (Amazon Relational Database Service (RDS) audit logs, Amazon Aurora audit, Amazon DynamoDB streams where applicable).
- Read access to the log archive account is tightly restricted; only the security team and a named audit role can read it.
- Write access is fully automated; no human can write to or modify the log buckets directly.

The most common audit finding in this area is not "you didn't enable logging," it is "you cannot demonstrate that the logs are tamper-resistant." Object Lock in compliance mode is the answer to that finding.

Decision 5: Security Baseline

The wrong answer: Leaving baselining to individual workload teams. Inconsistency is the result; some workloads have GuardDuty, some do not, some have AWS Config, some do not. Audit prep becomes a tour through fourteen different configurations.

The right answer: A baseline enforced by AWS Organizations Service Control Policies (SCPs), automatically deployed via AWS Control Tower customizations or AWS Landing Zone Accelerator, and continuously enforced via AWS Config conformance packs.

Non-negotiable rules:

- Amazon GuardDuty enabled in every account, in every region you operate in (and ideally in all regions, since attackers do not respect your region preferences).
- AWS Security Hub enabled with the AWS Foundational Security Best Practices standard, the Center for Internet Security (CIS) AWS Foundations Benchmark, and any framework-specific standard (PCI DSS, NIST 800-53).
- AWS Config enabled in every account, with conformance packs for each applicable framework.

- AWS CloudTrail with management events, S3 data events, and Lambda data events.
- Amazon Inspector enabled for continuous vulnerability scanning of Elastic Compute Cloud (EC2) instances and container images.
- AWS IAM Access Analyzer enabled at the organization level.
- Tag policies enforcing required tags (environment, data-classification, owner) on every resource.

This baseline is non-negotiable. It does not need to be optimized. It needs to be on, everywhere, by default, before anyone ships code.

Section 3: AWS-Native Landing Zone Patterns

The decisions above describe the destination. AWS gives you three patterns for getting there. Each has trade-offs.

Pattern A: AWS Control Tower

When to use it: Most regulated SMBs starting their landing zone from scratch should start here. The setup is fast, the maintenance burden is low, and the guardrails are well-tested. Account Factory makes new account provisioning consistent.

When to skip it: If you already have a mature multi-account structure and migrating into Control Tower would require disruptive account moves, the migration cost may exceed the benefit. Control Tower also has region constraints; if you need to operate in regions Control Tower does not yet support, you will be patching around it.

Specific recommendations:

- Enable both mandatory and strongly recommended guardrails from day one.
- Customize the Account Factory to bake in your tagging policy, baseline security tooling, and network attachments.
- Do not let Account Factory be the only way accounts get provisioned; document the manual provisioning path for edge cases.
- Plan for the Control Tower update cadence; AWS releases new versions roughly quarterly.

Pattern B: AWS Landing Zone Accelerator on AWS

When to use it: SMBs with DoD, federal, or other regulated workloads that exceed what Control Tower's opinionated structure allows. Specifically, if you need Impact Level 4 (IL4) or Impact Level 5 (IL5) landing zones, the Accelerator is the right starting point because it is explicitly architected for Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide (CC SRG) alignment. For FedRAMP High workloads in AWS GovCloud (US), Control Tower is now available and remains a valid choice; the Accelerator is the path for the higher Impact Levels Control Tower does not officially support.

When to skip it: If Control Tower meets your needs, the Accelerator's additional flexibility is overhead you will not use.

Pattern C: Custom Landing Zone via AWS Organizations

When to use it: Mature engineering teams with strong Infrastructure as Code (IaC) discipline, specific architectural requirements that neither Control Tower nor the Accelerator satisfy, or existing landing zones that have evolved organically and would be disrupted by adopting a managed solution.

When to skip it: SMBs with limited engineering capacity. The maintenance burden of a custom landing zone is significant; every AWS service update, every new account pattern, every change in compliance requirements is your problem to solve.

Recommended order for most regulated SMBs

Control Tower first, Landing Zone Accelerator if you outgrow Control Tower or need DoD landing zones, custom only if you have a specific reason that the first two cannot satisfy.

Section 4: Azure and Google Cloud Parallels

For SMBs operating in Microsoft Azure or Google Cloud Platform (GCP), the same five decisions apply with different primitives.

Microsoft Azure

- Account topology becomes Management Group hierarchy plus subscriptions. The Enterprise Scale Landing Zone reference architecture is the Azure equivalent of Control Tower; deploy via the Azure Landing Zones accelerator.
- Identity is Microsoft Entra ID (formerly Azure Active Directory) with Conditional Access policies, Privileged Identity Management for just-in-time elevation, and Azure role-based access control (RBAC) at the subscription and resource group level.
- Networking is hub-and-spoke with Azure Virtual WAN or Virtual Network peering, Azure Firewall for inspection, and Private Endpoints for service connectivity.
- Logging is Azure Monitor and the Microsoft Sentinel Log Analytics workspace for centralized collection. Diagnostic settings push logs to a central subscription with immutable storage policies.
- Security baseline is Microsoft Defender for Cloud enabled at the management group root with regulatory compliance dashboards, Azure Policy for enforcement, and Microsoft Sentinel as the Security Information and Event Management (SIEM) layer.

Google Cloud Platform

- Account topology becomes the Organization, Folder, and Project hierarchy. Set up via the Google Cloud Architecture Framework's enterprise foundations blueprint.
- Identity is Cloud Identity or Google Workspace federated with your identity provider, plus Identity-Aware Proxy for zero-trust access patterns.
- Networking is Shared Virtual Private Cloud (VPC) for centralized network ownership, Cloud Armor for inspection, and Private Service Connect for service-to-service connectivity.
- Logging is Cloud Logging with logs routed to a centralized project, plus Cloud Audit Logs for the management plane.
- Security baseline is Security Command Center Premium tier with the relevant compliance dashboards, Organization Policy Service for enforcement, and continuous Asset Inventory.

The principles transfer; the primitives change. SMBs running multi-cloud should pick one cloud's landing zone as the primary pattern and replicate its philosophy in the other.

Section 5: The Pandora Cloud Reference Architecture

For regulated SMBs that want a named starting point, here is the architecture we deploy as a baseline. Variations exist for specific compliance frameworks; this is the common substrate.

Account structure (eight accounts)

- Management (Organizations root, no workloads).
- Security tooling (Security Hub aggregator, GuardDuty master, Config aggregator, Inspector findings).
- Log archive (immutable centralized logs, S3 Object Lock, restricted read access).
- Identity (IAM Identity Center, permission sets, external Identity Provider (IdP) federation).
- Network (Transit Gateway, central VPC inspection, egress filtering).
- Shared services (DNS, container registries, golden Amazon Machine Images (AMIs), Continuous Integration / Continuous Deployment (CI/CD)).
- Workload-dev (development environments for each application).
- Workload-prod (production environments for each application; test environments often live in their own account between these two).

Identity model

- IAM Identity Center as the authentication front door.
- Permission sets aligned to job functions (Developer, Operator, SecurityAuditor, BillingViewer, BreakGlass).
- All access provisioned through groups, never direct user assignments.
- MFA enforced at the IdP layer; AWS does not see un-MFA'd authentication.
- Production access requires explicit approval through AWS Systems Manager Change Manager or equivalent.

Network architecture

- Hub-and-spoke with Transit Gateway in the Network account.
- Workload VPCs in /16 ranges within a planned /8 address space.
- Centralized egress through the Network account with AWS Network Firewall inspection.
- Production-to-development network paths are explicitly denied at the Transit Gateway route tables.
- Session Manager for any human-to-instance access; no Secure Shell (SSH) or Remote Desktop Protocol (RDP) bastions.

Logging

- Organization-wide CloudTrail to the log archive account, with S3 Object Lock in compliance mode for six years (HIPAA documentation retention floor; extend further for FedRAMP or industry-specific requirements).
- VPC Flow Logs from every VPC.
- AWS Config configuration history aggregated to the security tooling account.
- Application logs via CloudWatch Logs forwarded to the log archive account via Kinesis Data Firehose.
- Read access to the log archive bucket is restricted to two named roles: the security auditor role and the break-glass role.

Security baseline (enforced via SCPs and Config conformance packs)

- GuardDuty, Security Hub, AWS Config, IAM Access Analyzer enabled in every account, every active region.
- Inspector for container and EC2 vulnerability scanning.
- Required tags on every resource (environment, data-classification, owner, cost-center).
- Encryption at rest mandatory (Amazon Key Management Service (KMS) keys, managed per-account).
- Encryption in transit mandatory (Transport Layer Security (TLS) 1.2 minimum, 1.3 preferred).
- S3 public access blocked at the account level for every account.

Defense-specific extensions

For DoD workloads (Pandora Cloud's Bridge platform handles IL2, IL4, and IL5 workloads), this baseline is extended with AWS GovCloud (US) accounts, FedRAMP Moderate or High control inheritance, and CMMC 2.0 Level 2 alignment. The same five-decision framework applies; the parameters tighten.

Section 6: The Build Sequence

The right landing zone is not built in a day. It is built in a deliberate sequence where each step makes the next step possible.

Day 1 (the first four hours after deciding to build a landing zone)

Goal: Document the current state and commit to a target topology before any new accounts are provisioned.

- **Hour 1:** Document your current state: how many AWS accounts, what is in each, who has access, what logging exists.
- **Hour 2:** Decide on a target account topology (use Section 5 as a starting point).
- **Hour 3:** Choose the deployment pattern: Control Tower, Landing Zone Accelerator, or custom (see Section 3).
- **Hour 4:** Identify the people who will own each account (one named owner per account) and schedule the next thirty days of work.

Week 1

Goal: Stand up the foundation accounts and turn on organization-wide logging before any workload moves.

- **Day 1-2:** Enable AWS Organizations in your management account (or migrate your existing accounts under a new Organizations root).
- **Day 3:** Deploy AWS Control Tower or AWS Landing Zone Accelerator into the management account.
- **Day 4:** Provision the security tooling, log archive, and identity accounts.
- **Day 5:** Set up IAM Identity Center, integrated with your existing identity provider where applicable. Enable organization-wide CloudTrail to the log archive account. Configure S3 Object Lock in compliance mode on the CloudTrail bucket.

Month 1

Goal: Migrate or recreate workloads into separated accounts; turn on the security baseline organization-wide.

- **Week 2:** Migrate or recreate your existing workloads into the new workload accounts (production and non-production separated).
- **Week 3:** Enable GuardDuty, Security Hub, AWS Config, IAM Access Analyzer organization-wide.
- **Week 4:** Deploy the network account with Transit Gateway. Migrate or attach workload VPCs to the Transit Gateway. Apply the baseline SCPs: deny root user access, deny disabling of CloudTrail / Config / GuardDuty, deny S3 public access, deny encryption-not-enabled deployments. Document everything in an internal landing zone reference document.

Quarter 1

Goal: Tune the baseline based on real findings; apply framework-specific overlays; establish operating cadence.

Month 2: Tune the baseline based on the first month of findings. Apply framework-specific overlays (HIPAA, SOC 2, FedRAMP, NIST 800-53, CMMC).

Month 3: Run the first internal audit dry-run against the landing zone. Establish the operating cadence: weekly Security Hub review, monthly Config conformance review, quarterly access review. Begin training the team on the new operating model.

Why this sequence wins

The teams who execute this sequence in ninety days are the teams who pass their next audit without scrambling. The teams who spread it across twelve months are the teams who arrive at the audit and discover the gaps.

Section 7: Common Landing Zone Failure Modes (and the Fix for Each)

These are the patterns we see most often in regulated SMB landing zones. Each one is fixable. None of them is rare.

Failure mode 1: One account does everything.

Why it breaks: No isolation between production, development, and shared services. Every IAM mistake is a production incident.

The fix: Split into the multi-account structure described in Section 2 Decision 1. Migrate workloads progressively; production-to-its-own-account is the highest-priority move.

Failure mode 2: IAM users instead of federated identity.

Why it breaks: Long-lived credentials accumulate, no one rotates them, no one inventories them, no one can revoke them quickly.

The fix: Deploy AWS IAM Identity Center, federate it with your existing identity provider, deprecate every human IAM user. The migration takes one to two weeks for a typical SMB.

Failure mode 3: Logs live in the workload account.

Why it breaks: The engineer who deployed the bug can delete the evidence of the deployment. Auditors do not accept self-administered logs.

The fix: Centralize all logs to a dedicated log archive account with Object Lock. Read access is restricted to security and audit roles only.

Failure mode 4: No audit account.

Why it breaks: When the auditor asks "show me what you saw," there is no read-only role that has visibility across the organization without being able to change anything. Granting the auditor production access is not acceptable.

The fix: Create a dedicated SecurityAuditor permission set in IAM Identity Center, with read-only access across the organization, scoped via Organizations.

Failure mode 5: Developers have admin in dev (and prod looks the same).

Why it breaks: The production account has the same permissions surface as dev, even if the actual access list is different. One configuration mistake bridges them.

The fix: Production is its own account with its own permission set. Developer access to production is mediated through change management, not through standing access.

Failure mode 6: Console access everywhere, no Session Manager.

Why it breaks: SSH bastions and console-by-default access produce logs that are hard to attribute and access patterns that are hard to audit.

The fix: AWS Systems Manager Session Manager for all instance access. Console access is restricted to specific permission sets that require explicit elevation.

Failure mode 7: Implicit trust between accounts.

Why it breaks: Cross-account roles are created ad-hoc without a documented trust model. Over time, the trust graph becomes impossible to reason about.

The fix: Document every cross-account role with its purpose, its trust policy, and its review cadence. Use IAM Access Analyzer findings as the inventory.

Failure mode 8: Compliance is "on the security team."

Why it breaks: The security team can configure controls but cannot enforce architectural decisions made by other teams. Compliance becomes a bolt-on rather than a property of the landing zone.

The fix: Bake compliance into the landing zone itself via SCPs, Config conformance packs, and CI/CD-enforced IaC scans. The architecture makes non-compliant deployments impossible, not just discouraged.

Failure mode 9: No tagging discipline.

Why it breaks: When the auditor asks "which resources hold PHI," the answer requires a manual review of every resource. Cost allocation, security scoping, and incident response all suffer.

The fix: Enforce required tags (environment, data-classification, owner, cost-center) via Tag Policies at the Organizations level. Block deployments of resources that are missing required tags.

Failure mode 10: The landing zone is a one-time setup, not a tended garden.

Why it breaks: AWS releases new services and features continuously. The landing zone configured on day one is out of date within a quarter.

The fix: Establish a quarterly landing zone review cadence. New services that affect the baseline get evaluated, adopted, or explicitly declined. The landing zone gets versioned.

Section 8: Compliance Framework Mapping

The same landing zone, configured correctly, satisfies most of the architectural controls of the major frameworks regulated SMBs face. The table below maps landing zone elements to the framework control families they primarily support.

Landing zone element	HIPAA	SOC 2	PCI DSS 4.0	NIST 800-53 Rev 5	CMMC 2.0 L2	FedRAMP
Multi-account separation	164.308(a)(3)	CC6.1, CC6.6	Req 1, Req 7	AC-3, AC-4, SC-7	AC.L2-3.1.1	SC-7
Federated identity + MFA	164.308(a)(5), 164.312(a)(1)	CC6.1, CC6.2	Req 8	IA-2, IA-5	IA.L2-3.5.3	IA-2
Centralized immutable logging	164.312(b)	CC7.2, CC7.3	Req 10	AU-2 to AU-12	AU.L2-3.3.1	AU-2, AU-9
Encryption at rest and in transit	164.312(a)(2)(iv), 164.312(e)(1)	CC6.7	Req 3, Req 4	SC-8, SC-13, SC-28	SC.L2-3.13.8	SC-8, SC-28
Continuous monitoring baseline	164.308(a)(1)(ii)(D)	CC7.1, CC7.2	Req 10, Req 11	CA-7, SI-4	CA.L2-3.12.3	CA-7
Network segmentation	164.308(a)(4)	CC6.6	Req 1, Req 6	SC-7, AC-4	SC.L2-3.13.1	SC-7
Configuration baseline	164.308(a)(1)(ii)(B)	CC8.1	Req 2	CM-2, CM-6, CM-7	CM.L2-3.4.1	CM-2, CM-6
Access reviews and least privilege	164.308(a)(4)	CC6.3	Req 7	AC-2, AC-6	AC.L2-3.1.5	AC-2, AC-6

This is not a substitute for a control implementation document. It is a map of which landing zone investments produce evidence for which framework families. A landing zone that lands every row in this table cleanly is a landing zone where the audit becomes evidence collection, not gap remediation.

Section 9: The Landing Zone Maturity Ladder

Most regulated SMBs do not arrive at full landing zone maturity overnight. The ladder below describes the five levels we see in the field. Knowing where you are helps you plan where to invest next.

Level 1: Ad-hoc

Single AWS account or a small handful with no Organizations structure. IAM users, no federation. Logs are wherever each engineer put them. No centralized security tooling. This is where most SMBs start.

Audit posture: Cannot pass anything beyond an attestation. Every audit will be a remediation project.

Level 2: Documented

Multi-account structure exists but is inconsistent. Some accounts have GuardDuty, some do not. Federated identity is partially adopted. Logs are partially centralized. The architecture is documented in a Confluence page that is six months out of date.

Audit posture: Can pass SOC 2 Type I with significant prep. HIPAA possible with compensating controls. FedRAMP not feasible.

Level 3: Standardized

Multi-account structure is consistent. Control Tower or Landing Zone Accelerator deployed. Federated identity, organization-wide CloudTrail and GuardDuty, centralized logging, baseline SCPs enforced. The architecture is documented in versioned IaC.

Audit posture: SOC 2 Type II with normal prep effort. HIPAA cleanly. FedRAMP Low feasible. NIST 800-53 Rev 5 alignment demonstrable.

Level 4: Measured

Standardization extended with continuous monitoring. Config conformance packs run continuously. Security Hub findings tracked to closure with documented service-level agreements. Quarterly access reviews automated. Tagging discipline enforced. Drift detection alerts.

Audit posture: SOC 2 Type II with minimal prep effort. HIPAA, PCI DSS, FedRAMP Moderate all feasible. CMMC 2.0 Level 2 alignment demonstrable.

Level 5: Continuous

Every control is monitored continuously, drift is auto-remediated where safe, audit evidence is generated automatically from running state. Compliance is a property of the architecture, not an activity.

Audit posture: Audits run on evidence already collected. Days to weeks of audit prep, not months. FedRAMP High feasible. IL4 and IL5 workloads supportable.

Where to invest first

The leap from Level 1 to Level 3 is the highest-leverage investment a regulated SMB can make. The leap from Level 3 to Level 5 is the difference between "we pass audits" and "we ship contracts that require continuous attestation."

Section 10: Worked Example

Aurora Health Analytics is a fictional but representative regulated SMB: forty-person SaaS company, healthcare analytics product, two AWS accounts at the start of the engagement (one production, one for "everything else"), HIPAA-attested but with significant gaps, pursuing a SOC 2 Type II and a federal pilot that will require FedRAMP authorization.

Starting state (Level 1.5)

- Production account with the SaaS application, the customer database holding PHI, the CI/CD pipeline, the analytics warehouse, internal tooling, and the founder's personal IAM user.
- "Everything else" account for development, staging, finance, and HR tooling.
- Sixteen IAM users with long-lived access keys, no MFA on six of them.
- CloudTrail enabled but logs in the production account, no Object Lock.
- GuardDuty enabled in production, not in the other account.
- One VPC per account, default routing, no inspection.

Day 1 (first four hours)

The Aurora team documents the current state, sketches a target account topology of eight accounts (per the Pandora Cloud reference architecture), and decides to deploy AWS Control Tower as the entry point. They identify Kim as the management-account owner, Marcus as the security-tooling owner, and Priya as the log-archive owner. They schedule the rest of week one.

Week 1

Control Tower is deployed in the management account. The log archive, security tooling, and identity accounts are provisioned automatically. CloudTrail is re-enabled organization-wide; the log archive bucket gets Object Lock in compliance mode with a six-year retention period (the HIPAA documentation floor). The team migrates their IAM users to IAM Identity Center, federated against their existing Google Workspace. MFA becomes enforced at the IdP layer for every user.

Month 1

The Aurora SaaS application is migrated into a new workload-prod account (still HIPAA-attested under the same Business Associate Agreement (BAA), but now in a dedicated account). A workload-dev account is provisioned for development. The "everything else" account is split: development is migrated to workload-dev, internal tooling to a new shared-services account, finance and human resources tooling to a new corporate-services account that exits the AWS Organizations entirely after the data transfer (it never needed to be there).

GuardDuty is enabled in every account, every region. Security Hub aggregates to the security tooling account. AWS Config is enabled organization-wide with the HIPAA and CIS conformance packs. A network account is provisioned with Transit Gateway; workload VPCs are migrated to attach to it. Production-to-development network paths are explicitly denied.

Quarter 1

The first quarterly access review surfaces six standing access grants that are no longer needed; they get revoked. SCPs are tightened: deny root user activity, deny disabling of CloudTrail / Config / GuardDuty, deny S3 public access, deny non-encrypted resource creation. The first SOC 2 Type II preparatory engagement begins; the auditor's evidence requests map cleanly onto the landing zone.

Six months in

SOC 2 Type II report is delivered with no exceptions. The FedRAMP pilot pre-assessment identifies that the landing zone inherits approximately 40 percent of the FedRAMP Moderate control baseline from AWS (the physical, environmental, and network-perimeter controls). The remaining 60 percent, customer-implemented controls at the application, identity, data, and monitoring layers, now has a stable architectural home and is scoped cleanly because the foundational decisions are made.

Twelve months in

Aurora is at Level 3.5 on the maturity ladder. The investment in months one through three converted a "we pass HIPAA on a wish and a prayer" posture into a "we can pursue regulated SMB contracts" posture. The architectural foundation is durable; subsequent compliance work is incremental.

The cost / return arithmetic

Cost: roughly two engineer-months across the first quarter (one full-time security engineer, plus partial allocation of the founding engineer and the new platform engineer). Return: a FedRAMP pilot worth six figures and a SOC 2 report that unblocked four enterprise contracts in the pipeline. Teams who skip this work and try to retrofit it later, after their first audit failure, spend two to three times as much.

Section 11: The Fifteen-Question Landing Zone Self-Assessment

Score each question one of three ways. Green: yes, fully in place and operating. Yellow: partially in place, gaps known. Red: not in place, or not known.

Account topology

- [ ] 1. Do you have at least five distinct AWS accounts in an AWS Organizations structure, with production isolated from non-production and from internal tooling?
- [ ] 2. Is there a dedicated log archive account that production engineers cannot write to or read from directly?
- [ ] 3. Is there a dedicated security tooling account that aggregates findings from every other account?

Identity

- [ ] 4. Is human authentication federated through an identity provider (IAM Identity Center, Microsoft Entra ID, Okta, or equivalent), with no human IAM users in any AWS account?
- [ ] 5. Is MFA enforced for every human user, with no exceptions?
- [ ] 6. Are IAM access keys for humans prohibited (service-to-service auth via IAM roles only)?

Network

- [ ] 7. Do workload VPCs connect through a centralized hub (Transit Gateway or equivalent) rather than ad-hoc Virtual Private Cloud (VPC) peering?
- [ ] 8. Is production network access denied from development network paths at the route table layer, not only the security group layer?
- [ ] 9. Is human-to-instance access provided through Session Manager rather than SSH or RDP bastions?

Logging and evidence

- [ ] 10. Is organization-wide CloudTrail enabled with logs delivered to the log archive account, with S3 Object Lock in compliance mode?
- [ ] 11. Are VPC Flow Logs enabled in every VPC and centralized to the log archive?
- [ ] 12. Is the log archive bucket retention period at least as long as your longest applicable framework requires (six years for HIPAA documentation under 45 CFR 164.316; longer where FedRAMP or industry-specific rules apply)?

Security baseline

- [ ] 13. Are GuardDuty, Security Hub, AWS Config, and IAM Access Analyzer enabled in every account, in every region you operate in?
- [ ] 14. Are required tags (environment, data-classification, owner) enforced on every resource via Tag Policies?
- [ ] 15. Are Service Control Policies in place to prevent disabling of security tooling and to enforce encryption defaults?

Scoring tiers

12 or more green	Level 3 or higher on the maturity ladder; you are in good shape. Use this guide to identify the specific gaps from yellow to green.
8 to 11 green	Level 2; you have a documented structure but inconsistent execution. Prioritize the yellow items in identity and logging first.
Fewer than 8 green	Level 1 or 1.5; the landing zone needs deliberate investment before the next audit. Treat this as a quarter-long project, not a backlog item.

Section 12: The 30/60/90 Day Operational Plan

If you scored below 12 green on the self-assessment, this is the recommended execution sequence.

Days 1 to 30: Foundation

Goal: Document the current state, deploy the foundation accounts, and migrate human users to federated identity.

- **Week 1:** Document the current account topology and access map. Choose your deployment pattern (Control Tower, Landing Zone Accelerator, or custom).
- **Week 2:** Deploy the management, security tooling, log archive, and identity accounts. Enable organization-wide CloudTrail with Object Lock.
- **Week 3:** Migrate human users to federated identity with MFA enforcement.
- **Week 4:** Identify the production account migration plan (which workloads move first). Lock the next 60 days of execution sequence.

Days 31 to 60: Migration

Goal: Provision workload accounts; migrate the highest-priority workload first; turn on the security baseline organization-wide.

- **Week 5-6:** Provision workload-prod and workload-dev accounts per major application. Migrate the highest-priority workload (typically the one with the most regulated data) into its dedicated production account.
- **Week 7:** Deploy the network account with Transit Gateway. Attach the new workload VPCs to the Transit Gateway.
- **Week 8:** Enable GuardDuty, Security Hub, Config, IAM Access Analyzer organization-wide. Begin running Config conformance packs against your applicable frameworks.

Days 61 to 90: Hardening

Goal: Apply enforced policies, tagging, and tooling cadence; run the first internal compliance review.

- **Week 9-10:** Apply baseline SCPs (deny root, deny disabling security, deny encryption-off, deny public S3). Enforce tagging via Tag Policies.
- **Week 11:** Run the first internal compliance review against the landing zone.
- **Week 12:** Document the operating cadence (weekly Security Hub review, monthly Config review, quarterly access review). Schedule the first external compliance pre-assessment.

Outcome after 90 days

A regulated SMB executing this plan moves from Level 1.5 to Level 3 on the maturity ladder. The investment is roughly one to two engineer-months of dedicated effort, ideally with a named owner who is not also responsible for product delivery during the same period.

Section 13: Common Questions Answered

1. Do we need all eight accounts, or can we start with fewer?

Start with the management, log archive, security tooling, identity, and at least one workload-prod plus one workload-dev account. Five accounts is the minimum for a defensible landing zone. The network and shared-services accounts can come in month two without losing the audit posture.

2. How long does this actually take?

Ninety days of focused execution for a Level-1-to-Level-3 transition, assuming a dedicated security or platform engineer. Twelve to eighteen months if you spread it across part-time effort.

3. Can we do this without Control Tower?

Yes, via Landing Zone Accelerator or a custom build. For most SMBs, the Control Tower starting point is faster and cheaper to maintain. Reserve custom builds for cases where Control Tower's opinionation gets in the way.

4. Does this work in AWS GovCloud (US)?

Yes. AWS Control Tower is available in AWS GovCloud (US) for FedRAMP High workloads, though it requires account creation via APIs in the commercial Region and runs against a separate AWS Organizations structure (commercial and GovCloud Organizations do not share membership). For Department of Defense workloads at Impact Level 4 (IL4) or Impact Level 5 (IL5), AWS Landing Zone Accelerator on AWS is the recommended starting point because it is explicitly architected for Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guide (CC SRG) alignment.

5. What about multi-region?

Enable the security baseline (GuardDuty, Security Hub, Config) in every region you operate in. For regions you do not use, apply SCPs that deny resource creation; this prevents shadow IT spinning up workloads in unmonitored regions.

6. How do we handle existing accounts that have been running for years?

Two paths. Path one: migrate workloads progressively into new accounts under the Organizations structure, retire the legacy accounts when empty. Path two: invite the legacy accounts into Organizations, retroactively apply the landing zone baseline. Path one is cleaner; path two is faster. Most regulated SMBs do a hybrid.

7. What does this cost in AWS spend?

The landing zone itself adds modest cost. Control Tower has no per-account fee but the underlying services it deploys (Config, CloudTrail data events, GuardDuty) add cost. For a typical regulated SMB with eight accounts and moderate workload volume, expect a few thousand dollars per month in landing-zone-attributable AWS spend. Compared to the cost of a failed audit, the calculation is straightforward.

8. How does this map to FedRAMP authorization?

A well-designed landing zone on AWS inherits approximately 40 percent of FedRAMP Moderate controls from the underlying AWS infrastructure (physical, environmental, and network-perimeter controls). Organizations are responsible for implementing the remaining 60 percent, which lives at the application, customer-data, customer-identity, and customer-monitoring layers. Pursuing FedRAMP without a deliberate landing zone is multiple years of remediation because the customer-implemented 60 percent has nowhere stable to live; with

one, it is twelve to eighteen months of disciplined execution because the foundation is already in place.

9. We are pre-revenue. Is this premature?

If you handle any regulated data (PHI, payment card data, controlled unclassified information, anything the federal government is interested in), this is not premature. The cost of retrofitting compliance into a startup that did not start compliance-first is one of the most expensive technical debt categories there is. Build the landing zone before the first customer signs the contract that requires it.

Section 14: Resources and Next Steps

This guide is one piece of a larger Pandora Cloud library for regulated SMBs. Each resource below is free.

Related lead magnets

- Cloud Compliance Foundation Worksheet: the diagnostic companion to this guide. Self-assesses where your landing zone stands today.
- Cut Your Audit Prep from Weeks to Days whitepaper: the operating model for audit prep once the landing zone is in place.
- Continuous Monitoring Toolkit: the 25-control monitoring baseline that runs on top of the landing zone.
- FedRAMP / NIST Readiness Checklist: the next layer for SMBs pursuing federal authorization.
- SBIR Compliance Sprint Plan: the operating sequence for Small Business Innovation Research (SBIR) companies whose landing zone work intersects DoD contracting.

Authoritative AWS references

- AWS Well-Architected Framework, Security Pillar.
- AWS Control Tower documentation.
- AWS Landing Zone Accelerator on GitHub.
- AWS Security Reference Architecture.
- AWS Prescriptive Guidance: Building a Secure Enterprise Multi-Account Cloud Environment.

Pandora Cloud assistance: If you read this guide and your reaction is "this is the work we need to do but we do not have the bandwidth to do it ourselves," that is exactly the engagement we run with regulated SMBs. We deploy and tune the landing zone, document it for your auditors, and hand it over with the operating runbook. Most engagements run twelve to sixteen weeks from kickoff to a Level 3 landing zone, and our clients typically maintain it themselves afterward.

Want a second set of eyes on your landing zone?

Book a free 30-minute consultation. We will identify the highest-leverage moves for your specific framework requirements and tell you whether to tackle this yourselves or bring in help.

Schedule at pandoracloud.net/#schedule-consultation