PANDORA CLOUD
UNPACKING COMPLEXITY

Cloud Compliance Foundation Worksheet

Score your cloud foundation in 5 minutes. Get a 30-day path to fix what's missing.

A Pandora Cloud Buyer's Resource

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

About This Worksheet

The 20 questions below tell you, in five minutes, whether your cloud foundation will hold up under a compliance audit, an enterprise security questionnaire, or a real-world breach attempt.

It is for the small or mid-sized business owners, operations leads, and compliance owners who are about to start their first audit cycle, lost a deal because a buyer asked for documentation you did not have, or just had the unsettling realization that "our cloud is secure" is something the team says rather than something the team has verified.

Score yourself in five minutes. Spend the next fifteen reading what each tier means and which thirty-day moves matter most. Print the tear-off page at the back and bring it to your next operations meeting.

Why Your Foundation Matters

Most regulated SMBs in healthcare, finance, legal, insurance, and defense reach a moment where compliance stops being theoretical. An enterprise client asks for a System and Organization Controls 2 (SOC 2) Type II report. A regulator opens an inquiry. A new contract requires a Business Associate Agreement (BAA). The team scrambles, the consultants get expensive, and the foundation gets retrofitted under deadline pressure.

The cost difference between building the foundation correctly from day one and retrofitting it later is consistently three to ten times. That math holds across audit prep hours, cyber insurance premiums, lost deals, and remediation engineering. Strong foundations make every downstream compliance move cheaper; weak foundations make every move more expensive.

This worksheet measures the foundation. The score tells you whether you can spend the next year focused on growth or whether you should spend the next quarter shoring up the basics. Either answer is useful; not knowing is the problem.

The Five Areas That Matter Most

Compliance frameworks across Health Insurance Portability and Accountability Act (HIPAA), SOC 2, Payment Card Industry Data Security Standard (PCI DSS), and the Federal Risk and Authorization Management Program (FedRAMP) all converge on the same five operational foundations. Get these right and 80 percent of your future compliance work becomes a documentation exercise. Get them wrong and every audit becomes a forensic reconstruction.

1. Organized environments. Development, testing, and production are separated cleanly so a problem in one cannot leak into another.

2. Controlled access. Identity is centralized, multi-factor authentication is on, and access reflects job roles instead of convenience.

3. Protected data. Sensitive data is encrypted at rest and in transit, isolated from the public internet, and backed up securely.

4. Complete visibility. Every meaningful action is logged, logs cannot be tampered with, and someone is actually watching them.

5. Automated guardrails. The platform enforces compliance automatically rather than relying on the team to remember every rule.

The Worksheet

For each item below, mark Yes (fully in place), Partial (started but not complete), or No (not implemented). Count your Yes answers at the end.

Section 1: Organized Environments

A problem in your dev environment should never be able to expose production data. Most SMBs intend to keep environments separate but in practice run them with shared credentials, shared network paths, or both.

- ☐ Y ☐ P ☐ N Development and production systems run in separate, isolated environments.
- ☐ Y ☐ P ☐ N A problem in one environment cannot affect the others.
- ☐ Y ☐ P ☐ N Each environment has its own security settings and access rules.
- ☐ Y ☐ P ☐ N You know which environment holds your most sensitive data.

Section 2: Controlled Access

Access misconfigurations are the single most-cited finding category in compliance audits. The fix is not size-dependent; the controls below cost nothing to set up and prevent the highest-frequency audit findings.

- ☐ Y ☐ P ☐ N All team members log in through a single system with company credentials.
- ☐ Y ☐ P ☐ N Multi-factor authentication is required for everyone.
- ☐ Y ☐ P ☐ N Access is based on job role, not convenience.
- ☐ Y ☐ P ☐ N When someone leaves, their access is revoked within 24 hours.
- ☐ Y ☐ P ☐ N You can tell an auditor exactly who has access to sensitive data right now.

Section 3: Protected Data

Encryption settings are easy to turn on once and easy to forget about thereafter. Backups are easy to create and easy to never test. Both fail under audit pressure if they are not actively maintained.

- ☐ Y ☐ P ☐ N All sensitive data is encrypted when stored.
- ☐ Y ☐ P ☐ N All data is encrypted when it moves between systems.
- ☐ Y ☐ P ☐ N Regulated data lives in private environments not accessible from the public internet.
- ☐ Y ☐ P ☐ N Backups are encrypted and tested regularly.

Section 4: Complete Visibility

Logs are the backbone of every compliance framework. If they are not collected continuously, retained for the required period, and protected from tampering, your evidence chain breaks. The auditor cannot verify what you cannot show.

☐ Y	☐ P	☐ N	Every action in your cloud is logged (who did what, when).
☐ Y	☐ P	☐ N	Logs are stored securely and cannot be tampered with.
☐ Y	☐ P	☐ N	Logs are retained long enough to meet your compliance requirements.
☐ Y	☐ P	☐ N	You review logs regularly or have automated alerts for unusual activity.

Section 5: Automated Guardrails

The strongest foundations enforce compliance through the platform itself, not through the team's memory. Every cloud platform offers services that block non-compliant configurations or flag them automatically; most SMBs have these services available and disabled.

☐ Y	☐ P	☐ N	Your cloud prevents non-compliant configurations from being deployed.
☐ Y	☐ P	☐ N	If someone creates a resource that violates security policies, the system catches it.
☐ Y	☐ P	☐ N	Compliance is enforced automatically, not manually checked by your team.

Scoring

Total Yes answers (out of 20):

🟢 **16 to 20 Yes**	Strong foundation. Your cloud is set up to support compliance frameworks with minimal retrofit. Focus on automation, continuous monitoring, and the framework-specific overlays your buyers ask for.
🟠 **10 to 15 Yes**	Good start, but gaps could cause problems during an audit or under buyer scrutiny. The 30-day roadmap below tells you which gaps to close first.
🔴 **Below 10 Yes**	Significant gaps. The foundation is not yet ready for any framework audit, and the cost of retrofitting later will be three to ten times higher than building it in now. Start with the Days 1-10 priorities below.

What to Do With Your Score

The score is only useful if it points you to a specific next move. Use the path that matches your tier.

If you scored 16-20 (Strong): Your foundation will hold under audit. The next investment is the framework-specific overlay your buyers actually ask for. Most regulated SMBs at this tier move next to either the HIPAA and PCI Readiness Checklist (for healthcare or payment-handling teams) or the SOC 2 Readiness

Checklist (for legal, insurance, and enterprise-facing teams). Both are free and live at pandoracloud.net.

If you scored 10-15 (Good Start): The foundation is partially in place. The fastest path forward is the 30-day roadmap below: pick the area where you have the lowest score, work through the day-by-day plan, then re-take this worksheet at the end of the month. Most SMBs at this tier move from Yellow to Green inside one focused quarter.

If you scored below 10 (Significant Gaps): Compliance is currently a risk you are carrying without realizing the size of it. The foundation needs work before any framework audit will pass. Start with Days 1-10 of the roadmap below; the early items are the cheapest to fix and the most consequential.

Watch your inbox in seven days

The Cloud Landing Zones Guide is the tactical companion to this worksheet. A 28-page playbook walking through how to actually build the foundation correctly the first time, with worked architecture examples and the order of operations that compresses retrofit timelines. Available now at pandoracloud.net/cloud-landing-zones-guide. We will also email it to you seven days from now in case you want to revisit it then.

Your 30-Day Foundation Roadmap

This roadmap targets teams scoring Yellow or Red. Strong-foundation teams can compress it; teams with significant gaps can spread it across two months.

Days 1 to 10: Identity and access (the cheapest wins)

Goal: Centralized identity with Multi-Factor Authentication (MFA) enforced. Quarterly access reviews scheduled. Departing-employee deprovisioning under 24 hours.

- **Day 1-2:** Inventory every system that holds sensitive data. List the people who have access to each. This is the document everything else depends on.
- **Day 3-5:** Stand up a centralized identity provider (Okta, Microsoft Entra, Google Workspace, or AWS IAM Identity Center) if you do not have one. Move every cloud account, every Software-as-a-Service (SaaS) app, and every internal tool behind it.
- **Day 6-7:** Enforce MFA for every account. Privileged accounts, contractor accounts, service accounts. No exceptions.
- **Day 8-9:** Review every account's permissions. Remove anything that does not match the person's current role. Document who approved each remaining elevated access.
- **Day 10:** Schedule the first quarterly access review on the calendar. Document the deprovisioning procedure and have one person own it.

Days 11 to 20: Encryption and data protection

Goal: Encryption at rest and in transit verified across all sensitive data stores. Public-access risks remediated. Backup integrity tested.

- **Day 11-12:** Audit every storage bucket, database, and file share for encryption-at-rest status. Turn on encryption for any unencrypted store.
- **Day 13-14:** Verify Transport Layer Security (TLS) 1.2 or higher is enforced on every public endpoint and every internal service connection. Disable weak cipher suites.
- **Day 15-16:** Audit every cloud resource for public-internet exposure. Anything holding regulated data should not be reachable from the public internet without authentication.
- **Day 17-18:** Test backup restore procedures. Pick one critical system, attempt a full restore from yesterday's backup, document the result.
- **Day 19-20:** Document the encryption policy and the backup retention policy. These are the artifacts an auditor will ask for.

Days 21 to 30: Logging and guardrails

Goal: Continuous logging across all in-scope systems with retention meeting your framework requirements. At least one automated guardrail active. Re-take the worksheet to measure progress.

Day 21-23: Enable cloud-native logging (AWS CloudTrail, Azure Activity Logs, Google Cloud Audit Logs) across every account. Centralize the destination. Configure retention to meet your compliance framework's minimum (typically 1 year for PCI DSS, 6 years for HIPAA).

Day 24-25: Make logs tamper-resistant. Use immutable storage with versioning enabled and write-protect the destination from your normal admin accounts.

Day 26-27: Turn on configuration drift detection (AWS Config, Azure Policy, Google Cloud Security Health Analytics). Start with one rule that maps to a control you care about; expand from there.

Day 28-29: Configure alerts for the highest-risk events: changes to encryption status, public-access changes, MFA being disabled, log sources going silent.

Day 30: Re-take the worksheet. Compare scores. The improvement tells you whether the program is working; any persistent low-score areas are the next quarter's priorities.

Common Patterns We See

Across SMBs in healthcare, finance, legal, insurance, and defense, the same four foundation gaps show up over and over. None of them are technically hard to fix; all of them are routinely missed.

1. The "we have MFA on, mostly" gap. MFA is enabled for some users, sometimes, but not enforced for everyone. Service accounts and contractor accounts are usually the gap. The fix is enforcement, not just availability.

2. The "we will deprovision them next week" gap. A former employee retains access for weeks because deprovisioning is owned by no one specifically. The longer the delay, the larger the audit finding and the higher the breach risk.

3. The "the cloud handles backups" assumption. Cloud platforms handle infrastructure availability, not your data backups. Your databases, file shares, and configurations need explicit backup with tested restore procedures. Many teams discover this only when they need to restore.

4. The "we will turn on logging when we need it" gap. Logging that started capturing midway through an audit period creates an evidence gap that cannot be retroactively fixed. Turn it on before you need it; even six months of clean logs is more useful than zero.

If you scored Yellow or Red, at least two of these patterns are almost certainly the cause. Address them in the order above.

A Worked Example

A 40-person healthtech SMB scored 7 of 20 on its first run through this worksheet. The leadership team was surprised; they had been telling enterprise prospects for two years that the cloud was "secure and compliant."

The seven items they had in place were the obvious ones: development and production were separated, MFA was enforced for the senior team, sensitive data was encrypted at rest, and logs were captured for the main application database. The thirteen items they were missing included MFA enforcement for service accounts (gap), departing-employee deprovisioning (gap), centralized identity (partial), backup restore testing (never done), and any form of automated guardrails (gap).

They ran the 30-day roadmap exactly as written. Days 1-10 closed seven items. Days 11-20 closed three more. Days 21-30 closed two more. By day 30 they scored 19 of 20; the remaining gap was automated guardrails for non-production environments, which they deferred to the next quarter.

The cost: roughly 40 hours of engineering time spread across one operations lead and two engineers, plus one Saturday for the centralized-identity migration. The result: a clean SOC 2 readiness assessment two months later, and the enterprise prospect they had been losing to a larger competitor signed a $180,000 annual contract within the same quarter. The foundation paid for itself in week one of the new contract.

This worksheet is the diagnostic. The roadmap is the prescription. The example is what running the prescription actually looks like.

Where to Go From Here

The Foundation Worksheet is the entry point of a longer compliance journey. Depending on your score and your industry, the natural next moves are below.

If you scored Yellow or Red: Grab the Cloud Landing Zones Guide. The 28-page tactical companion to this worksheet, it walks through how to build the foundation correctly the first time, with worked architecture examples, pitfalls to avoid, and the order of operations that compresses retrofit timelines. Free at pandoracloud.net/cloud-landing-zones-guide. We will also email it to you seven days from now.

If you handle Protected Health Information (PHI) or process credit cards: Pick up the HIPAA & PCI Readiness Checklist next. It builds on the foundation here with framework-specific items. Free at pandoracloud.net/compliance-checklist.

If you sell to enterprise buyers asking for SOC 2: Pick up the SOC 2 Readiness Checklist. Tuned for legal and insurance Small and Medium-sized Businesses (SMBs), with a 90-day audit-prep timeline and honest cost expectations. Free at pandoracloud.net/soc2-readiness-checklist.

If you are pursuing a federal Authority to Operate (ATO) or sell to defense agencies: Pick up the ATO Readiness Checklist. Free at pandoracloud.net/ato-readiness-checklist.

In every case, the Foundation Worksheet score is the single best predictor of how cleanly the next framework will go. Improve the foundation; everything downstream gets easier.

Printable Scoring Sheet

Print this page. Take it to a conference room. Walk through the 20 questions with the team and mark Y, P, or N for each. The page is designed to live on a wall or in a binder for the duration of your foundation work.

1. Organized Environments

- ☐ Y ☐ P ☐ N Dev and production isolated
- ☐ Y ☐ P ☐ N Problems contained per environment
- ☐ Y ☐ P ☐ N Each environment has own security settings
- ☐ Y ☐ P ☐ N Sensitive data location is known

2. Controlled Access

- ☐ Y ☐ P ☐ N Centralized identity for all team members
- ☐ Y ☐ P ☐ N MFA required for everyone
- ☐ Y ☐ P ☐ N Access based on job role
- ☐ Y ☐ P ☐ N Departing access revoked within 24 hours
- ☐ Y ☐ P ☐ N Auditor-ready access list available

3. Protected Data

- ☐ Y ☐ P ☐ N Sensitive data encrypted at rest
- ☐ Y ☐ P ☐ N Data encrypted in transit
- ☐ Y ☐ P ☐ N Regulated data not internet-accessible
- ☐ Y ☐ P ☐ N Backups encrypted and tested

4. Complete Visibility

- ☐ Y ☐ P ☐ N All cloud actions logged
- ☐ Y ☐ P ☐ N Logs tamper-resistant
- ☐ Y ☐ P ☐ N Log retention meets framework requirements
- ☐ Y ☐ P ☐ N Logs reviewed or alerts configured

5. Automated Guardrails

- ☐ Y ☐ P ☐ N Non-compliant configs blocked at deploy
- ☐ Y ☐ P ☐ N Policy violations caught automatically
- ☐ Y ☐ P ☐ N Compliance enforced by platform, not team memory

Total Yes (out of 20): _____

16-20: Strong foundation. Focus on automation and framework-specific overlays.
10-15: Good start; address gaps via the 30-day roadmap.
Below 10: Significant gaps; start with Days 1-10 priorities.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. We help regulated SMBs across healthcare, finance, legal, insurance, and defense build compliance-first cloud foundations and operate them as part of normal business, not as periodic audit projects.

If you scored Yellow or Red and want a second set of eyes on which gaps to prioritize, we offer free 30-minute consultations.

Want a second set of eyes on your gaps?

Schedule a free 30-minute consultation. We will walk through your scored worksheet and help you prioritize the next 30 days.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to cloud foundation vocabulary, this glossary names the most common terms used in this worksheet.

BAA (Business Associate Agreement)
Contract under HIPAA between a covered entity and a third party handling Protected Health Information (PHI). Required for any vendor that touches patient data.

Centralized Identity Provider
A single system (Okta, Microsoft Entra, Google Workspace, AWS IAM Identity Center, etc.) that handles authentication for all your applications. Replaces having separate logins for each tool.

Drift Detection
Automated monitoring that flags when a cloud configuration no longer matches your defined baseline. Critical for catching changes that introduce risk between audits.

Encryption at Rest vs. in Transit
"At rest" means encrypted while stored on disk; "in transit" means encrypted while moving over a network. Compliance frameworks require both.

MFA (Multi-Factor Authentication)
Login that requires more than just a password (e.g., password plus a phone-based code or hardware key). Single most effective control against account takeover.

Retention Period
How long logs, backups, or other evidence must be kept. Varies by framework: typically 1 year for PCI DSS, 6 years for HIPAA, sometimes longer for federal contracts.

SOC 2 (System and Organization Controls 2)
Audit framework increasingly required by enterprise buyers as a contract gate. Confirms a service organization handles customer data appropriately across security, availability, processing integrity, confidentiality, and privacy criteria.

Tamper-Resistant Storage
Storage configured so that data cannot be modified or deleted, even by an administrator account, for a defined retention period. Critical for audit log integrity.