

Blog 1: The Multi-Cloud Skills Gap

Why One Certification Isn't Enough Anymore

By TekSol Global | Cloud

Most enterprises today aren't running on a single cloud. Flexera's 2026 State of the Cloud Report found that 73% of organizations now operate hybrid cloud environments, with multi-cloud adoption continuing to climb as well, often driven by mergers, siloed application teams, or infrastructure inherited along the way rather than a deliberate strategy. A team might deploy on AWS, manage identity through Microsoft Azure, and run analytics on Google Cloud, often within the same project. Yet most cloud certification programs are still built around a single platform.

That gap is becoming a real business risk.

Why Multi-Cloud Is the Default, Not the Exception

Organizations rarely choose multi-cloud on purpose from day one. It happens through acquisitions that bring in a second vendor's infrastructure overnight, procurement teams negotiating better pricing by keeping two providers competitive, regulatory requirements that mandate data residency a single vendor can't fully cover, or simply because different teams picked different tools before anyone coordinated a strategy.

By the time leadership notices, the environment is already multi-cloud in practice, even if no one signed off on it as a plan. Retrofitting governance, security, and skills onto an environment that grew organically is far harder than building them in from the start, which is exactly the position most mid-size and enterprise IT teams find themselves in today.

The result is that professionals who can only speak one cloud's language are limited in how much of the environment they can actually support. A DevOps engineer who's deep in AWS but has never touched Azure Resource Manager can't meaningfully support a workload that migrated in through an acquisition. A security analyst fluent only in AWS IAM policies can review half the environment's access controls and has to hand off the rest, which is exactly where blind spots and misconfigurations tend to live.

Hiring managers have noticed. Job postings increasingly list two or three cloud platforms as "nice to have", a signal that will likely shift to "required" as multi-cloud architectures mature and as more of the workforce is expected to operate across vendor lines.

What a Single-Platform Team Actually Risks

It's worth being concrete about what happens when an organization's cloud skills don't match its cloud footprint:

- **Slower incident response.** When something breaks in the platform nobody was trained on, the team either escalates to an expensive contractor or works the problem cold, extending downtime.
- **Security gaps at the seams.** Multi-cloud environments create more integration points, identity federation between providers, cross-cloud networking, and shared data pipelines. These seams are where misconfigurations concentrate, and they require someone who understands both sides of the connection, not just one.
- **Vendor lock-in by default, not by design.** Teams that only know one platform tend to architect everything to that platform's specific services, even when a more portable approach would serve the business better. This isn't a strategic choice; it's a skills limitation dressed up as an architecture decision.
- **Bottlenecks around a small number of people.** If only one or two people on a team can operate the second cloud environment, they become single points of failure for incident response, for onboarding new services, and for basic vacation coverage.

None of these are hypothetical. They're the predictable outcome of skills that haven't kept pace with infrastructure decisions made elsewhere in the business.

What Cross-Platform Skills Actually Look Like

Being multi-cloud literate doesn't mean holding every certification available on every platform. It means understanding the concepts of transfer, identity and access management, networking fundamentals, cost governance, security posture, infrastructure-as-code, and knowing precisely where each platform's implementation diverges.

A professional who understands AWS IAM will pick up Azure Active Directory faster than someone starting from zero. The underlying logic of least-privilege access is the same; the console, terminology, and default behaviours differ. Someone who's built Well-Architected Framework reviews on AWS can apply the same rigour to Azure's or Google Cloud's equivalent frameworks, adjusting for the specific tools each provider gives you to enforce it.

Training that emphasizes these transferable concepts, rather than pure platform trivia, produces people who can move between environments without a steep relearning curve every time a new system lands on their desk.

A Practical Certification Pathway

The most effective route is usually sequential depth, not parallel breadth from day one:

1. **Build a strong foundation in one platform.** For most teams, this means starting with something like the **AWS Solutions Architect Associate (SAA-C03)**, which forces a solid grounding in resilient, cost-aware architecture, EC2, S3, VPC, IAM, and the Well-Architected principles that transfer conceptually to every other cloud.
2. **Layer in a second platform with the overlap in mind.** The **Azure Administrator (AZ-104)** or **Azure Solutions Architect (AZ-305)** are natural next steps, since so much of the identity, networking, and governance logic maps directly onto what was learned in AWS, just implemented differently.
3. **Add a third only where the business actually needs it.** If your organization runs analytics or ML workloads on Google Cloud, the **Professional Cloud Architect** or **Professional Data Engineer** paths round out a genuinely cross-platform skill set rather than adding certification for its own sake.
4. **For security-focused roles,** pairing platform-specific certifications with a vendor-neutral credential like the **CSA CCSK v5** builds the kind of cloud security judgment that holds up regardless of which provider a new workload lands on.

This sequencing matters. Professionals who try to learn two or three platforms simultaneously from scratch tend to retain less of any of them. Depth first, then breadth, produces people who genuinely understand the architecture underneath, not just where the buttons are in each console.

The Business Case for Investing in This Now

Teams with cross-platform capability are more resilient. They can respond to a vendor price change, a compliance requirement that favors a specific provider, or a merger that brings a second cloud environment into the fold, without scrambling to hire externally or leaning entirely on outside consultants who don't know the organization's specific environment.

For individuals, multi-cloud fluency is one of the more durable ways to future-proof a career in infrastructure, DevOps, and security roles. Platforms will keep evolving, new services, new pricing models, new AI-native tooling, but the professionals who understand the shared architecture underneath will keep adapting with them, rather than starting over every time the market shifts.

Where to Start

The most practical path is usually sequential, not simultaneous: build depth in one platform first, then layer in a second with a focus on where the concepts overlap and where they don't. Structured, practitioner-led

training accelerates this because it comes with real scenarios and real failure modes instead of generic theory built for passing an exam.

TekSol Global's cloud programs cover all three major providers, AWS, Microsoft Azure, and Google Cloud, with instructors who have implemented these platforms in production, not just taught the certification exam.

Interested in building multi-cloud capability on your team? [Explore TekSol Global's cloud training programs](#).

Source: Flexera, [2026 State of the Cloud Report](#).