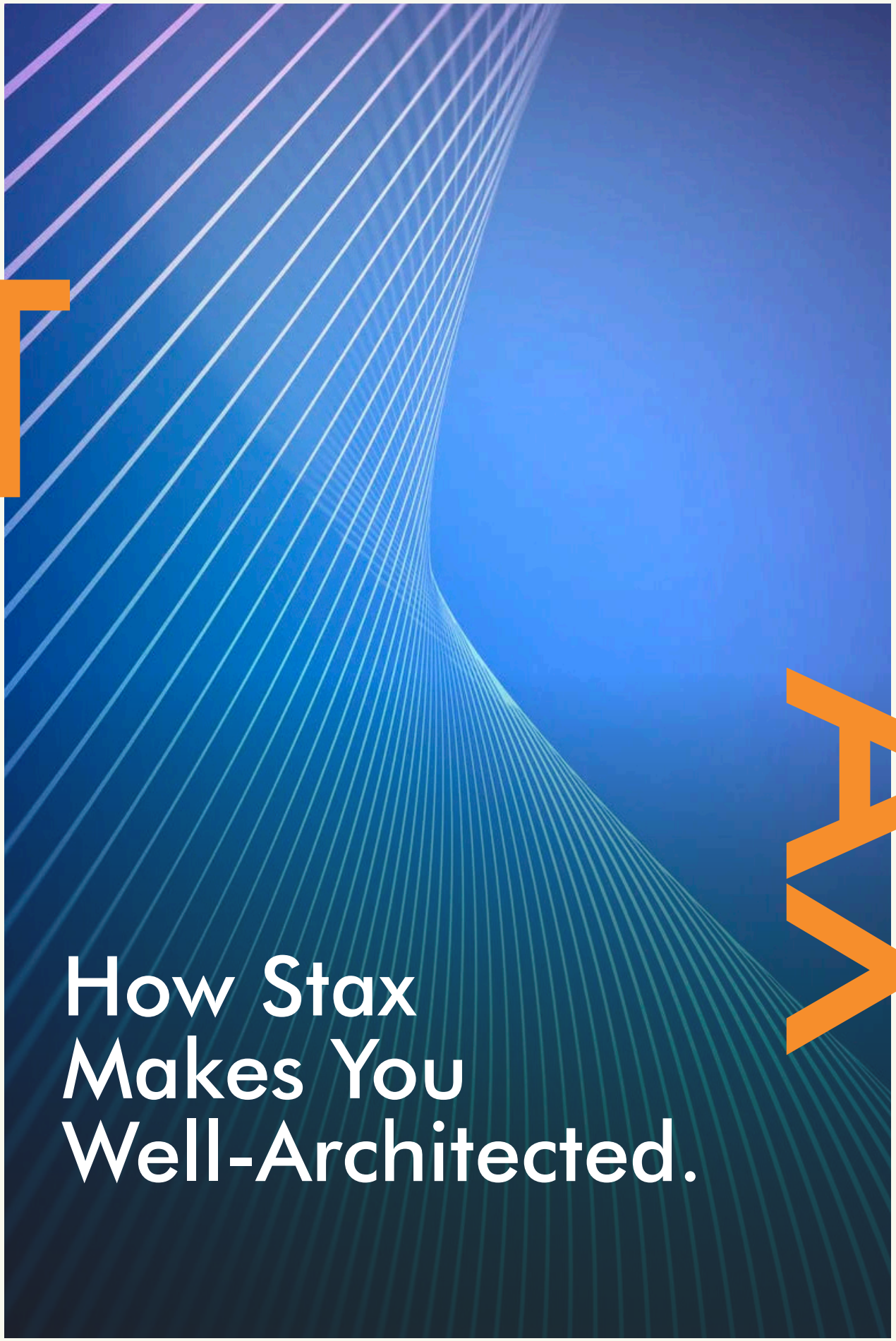
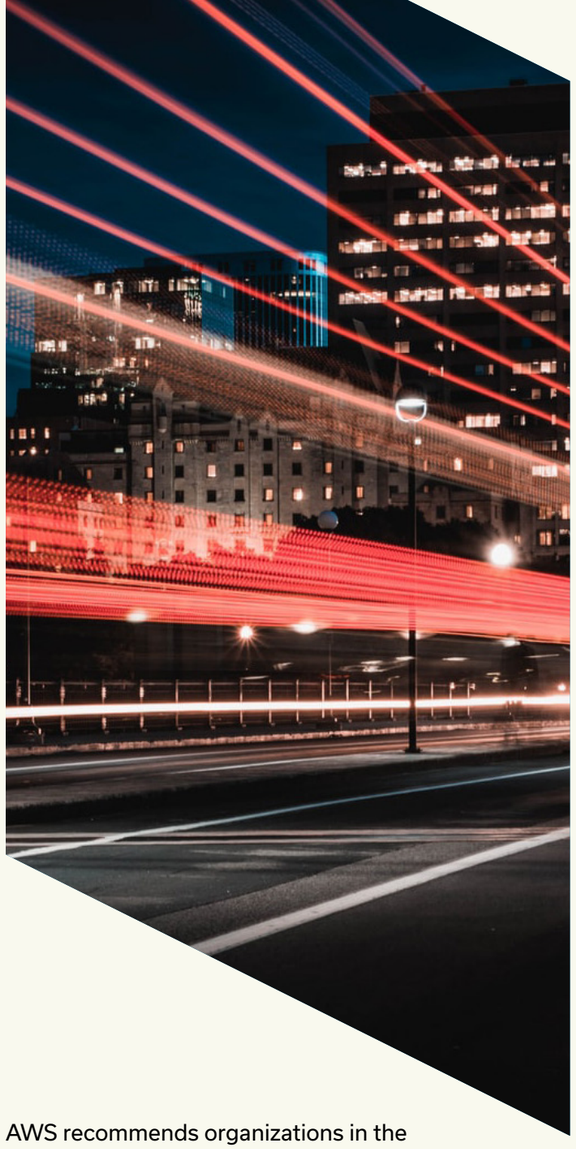


How Stax Makes You Well-Architected.

By following the AWS Well-Architected Framework, you can be confident you are well-placed for success in the cloud. Learn how Stax makes it easier.

STAX

The AWS Well-Architected Framework



Follow the Framework, and you can be confident you're building a secure, high-performing, resilient cloud ecosystem that can scale as your business grows.

When you're building and running a sophisticated cloud ecosystem, it can be hard to know where to focus your team's energy to avoid problems and maximize results. Unless your team is resourced with an abundance of cloud experts, you may find yourself reinventing the wheel, making costly mistakes, or leaving your business open to security or compliance issues. Many companies need an idea of what "best practice" looks like, so they can make sure they're headed in the right direction. In the case of AWS, this takes the form of the AWS Well-Architected Framework.

The AWS Well-Architected Framework provides guideline on where to focus your efforts. The Framework offers a set of questions, developed by AWS Solutions Architects, that ensures you follow cloud best practices.

AWS recommends organizations in the cloud conduct a Well-Architected Review every 12-18 months.

Adhering to the Framework should be a priority for any organization in the cloud, no matter its size or business focus.

The challenge can be the time and resources required to adhere to this Framework.

And that's where Stax comes in.

Contents

What is the AWS Well-Architected Framework?

While it began as a single white paper, the Framework is now a sprawling collection which includes "lenses", hands-on labs and a Well-Architected Tool to automate reviews of your workloads. Lenses apply the Framework to domains or industries, such as Financial Services, SaaS, Analytics and Serverless.

The Serverless Lens focuses on designing, deploying, and architecting your serverless application workloads in the AWS Cloud. This lens covers scenarios such as RESTful microservices, mobile app backends, stream processing, and web applications. Using this lens helps you apply best practices when building serverless application workloads on AWS.

The SaaS Lens focuses on designing, deploying, and architecting your software as a service (SaaS) workloads in the AWS Cloud. Using this lens helps you apply best practices when building SaaS workloads on AWS.

The FTR Lens is designed for independent software vendors (ISVs) preparing for a Foundational Technical Review (FTR) in the AWS Partner Network (APN). It provides a set of specific questions for ISVs to perform a workload self-assessment before requesting a review.

The Framework consists of five pillars, each focused on a different area of business and technology tools and processes. Within each pillar are design principles, definitions, and best practices. Let's briefly look at the pillars to get an overview of their focus and their design principles.

Operational Excellence

This pillar focuses on running workloads effectively, with insight into how they operate, as well as continuously improving processes and procedures. For this pillar, AWS recommends the following design principles:

- Perform operations as code
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failures

Security

The security pillar is focused on protecting your data, systems and assets and taking advantage of cloud technologies to improve security. The six Security design principles are:

- Implement a strong identity foundation
- Enable traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data and prepare for security events

Reliability

Reliability is focused on the ability of a workload to perform its function correctly, consistently and when it's expected to. Design principles for Reliability:

- Automatically recover from failure
- Test recovery procedures
- Scale horizontally to increase aggregate system availability
- Stop guessing capacity
- Manage change in automation

Performance Efficiency

This pillar focuses on using computing resources efficiently and maintaining this as demand changes and technologies evolve. When designing for Performance Efficiency, AWS recommends:

- Democratize advanced technologies by pushing difficult technologies into the cloud vendor's domain
- Go global in minutes
- Use serverless architectures to help you quickly deploy your system in multiple Regions and remove the need to traditionally run and maintain servers.
- Experiment more often
- Consider mechanical sympathy

Cost Optimization

The Cost pillar's focus is simple: the ability to run systems that deliver business value at the lowest price point. Design principles for cost optimization:

- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on "undifferentiated heavy lifting" i.e. focus on your business and customers rather than IT infrastructure
- Analyze and attribute expenditure

The Benefits of Being Well-Architected

By asking the right questions at the right time, you and your team won't have to learn some lessons "the hard way" and can benefit from the experience of others on AWS.

The Framework is not an audit, and it's not a test in which you can be given a grade or a pass/fail mark. Neither is the Framework a means to expose failure in your team, or an excuse for finger-pointing.

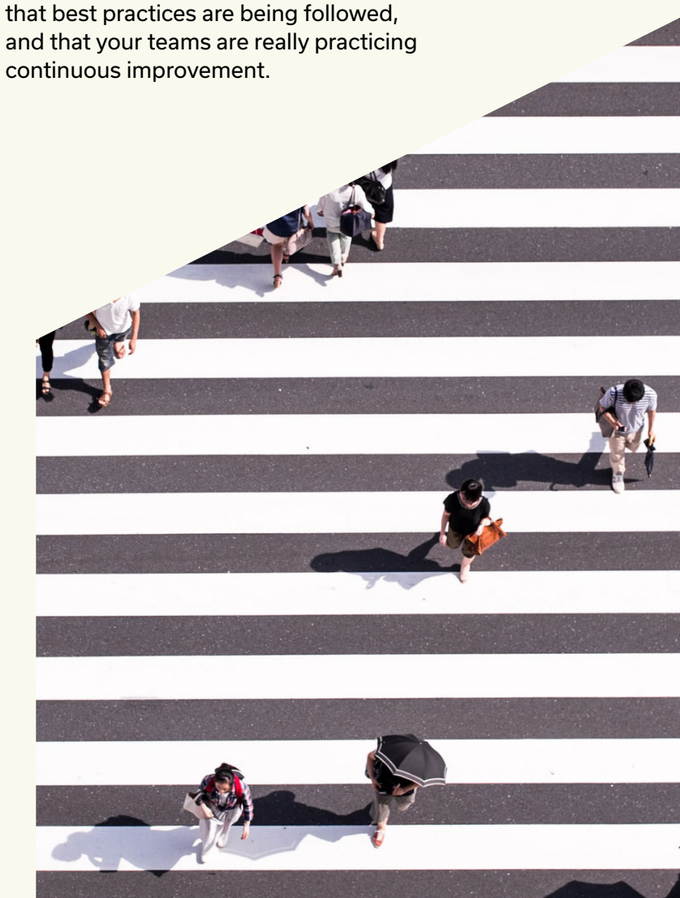
Rather, it's a way to prompt and frame your team's thinking.

If you have sat down and gone through the pillars and questions that make up the Framework, you can be confident you have asked the most important questions to ensure your success.

As your workload and experience matures on AWS, you and your team will be well placed to make improvements and avoid costly mistakes.

Well-Architected Reviews can help your teams avoid unconscious and unintentional technical debt by asking the right questions at the right time. With the right visibility and the attention to detail the Framework encourages, you can control and manage your technical debt.

While you can be Well-Architected without doing a review, a periodic review makes it easy for you to prove to your stakeholders that best practices are being followed, and that your teams are really practicing continuous improvement.



The Risks of Not Being Well-Architected

Ultimately, the Well-Architected Framework is designed to protect your business, and your customers, from experiencing problems with security, reliability, performance, and cost management in the cloud.

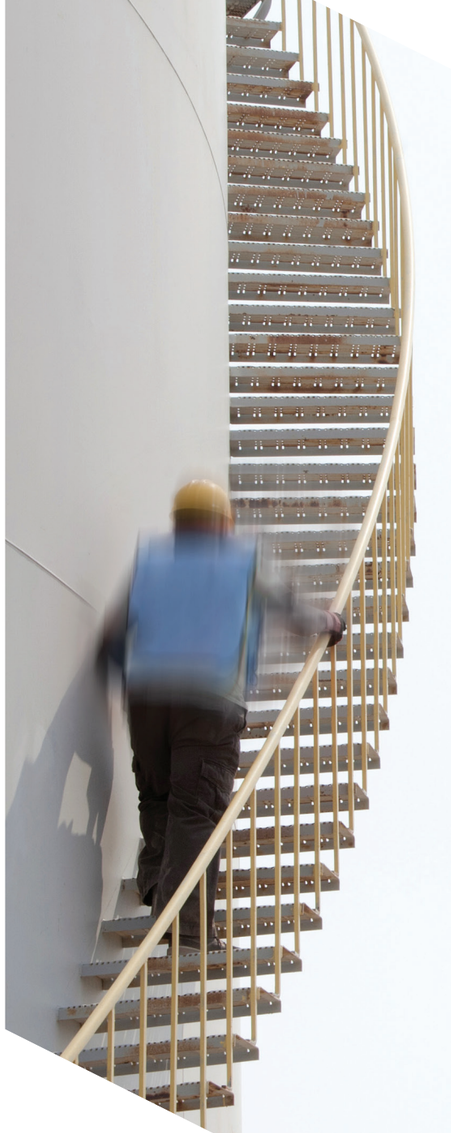
If you fail to consider the questions posed by the Framework, you may miss some obvious methods for improvement and start to experience problems. For example:

- Your cloud architecture, which you may have initially built to support a particular business purpose or team, may no longer be fit-for-purpose as your team, or your investment in the cloud grows.
- By not considering automation, your business may experience slower deployments and more downtime.
- If you fail to deploy small changes frequently, your delivery cycle will be correspondingly slower.
- And if you don't plan ahead for failure, any issues will be correspondingly larger.
- It's more likely that your business' cloud security will be weaker, as you are running minimal monitoring and reporting and reliant on manual processes, which are vulnerable to human error.
- Meanwhile, your cloud ecosystem will be vulnerable to attacks and data breaches.
- You will be more vulnerable to cost overruns, as you lack processes to measure and optimize your cloud usage.

How to Be Well-Architected

Being Well-Architected starts with the Framework but doesn't end there. Just as the Framework is updated periodically, you should be checking in on your most important workloads periodically (usually annually or bi-annually) to ensure that your standards are being maintained or improved.

"While the Framework gives you the right prompts, you must supply the answers."



Aim for Cloud "Fluency"

Teams that are able to quickly and easily give answers to the Framework's questions are more likely to give good answers. An understanding of your workload and visibility into its operation goes a long way to making it Well-Architected.

Be Proactive

A proactive team is another leading indicator that your workload will be Well-Architected. Teams that have time for proactive work are also usually not busy "putting out fires". Automation is a key part of being proactive and avoiding repeated issues, especially on a platform with automation capabilities like AWS provides.

Establish the Right Processes

Processes that support technology and workloads also play a big part. While process alone is not enough to make a workload Well-Architected, the wrong kind of processes can definitely stop one from being Well-Architected! The most productive processes empower workload operators with the right level of access and support so that they can make the right technical decision at the right time.

How Stax Helps Make You Well-Architected

A key part of the Stax mission is to make it easier for customers to do the right thing on AWS.

Given how important the Well-Architected Framework is to AWS, the team at Stax knew that it was crucial we aligned. This means that customers can build workloads on Stax and know that they're heading in the right direction and are avoiding common pitfalls and mistakes on AWS.

Automated

Maintaining best practices at scale is only possible by taking advantage of the automation that AWS makes available. Stax leverages the best of the AWS services to ensure that your AWS foundations are secure and compliant, no matter how large or complex.

Provides Visibility

Knowing what's going on in your environment is the first step towards improving it. Without visibility into your entire AWS footprint, you run the risk of being surprised by blind spots or gaps. Stax shines a light in to your AWS environment so you can see clearly what's going on.

Lightweight

The Infrastructure-as-Code approach that AWS has delivered offers fantastic potential for business success. The reality is that every line of code your team writes is a line of code they need to test, troubleshoot, maintain, and improve over time. Stax takes work off your team's plate, so they can get up the stack and focus on business-critical tasks that provide value to you and your customers, quicker and easier than building from scratch.

Evergreen

AWS releases a huge number of services and features every year. Unlike the on-premises world, the platform underneath your workloads is always changing and evolving. Stax helps you take advantage of foundational improvements from AWS, without needing your teams to be distracted from their day-to-day work. Updates and improvements will be applied to your environment when they've been tested and verified.

Show, Don't Tell

Now we've looked at the background of the Framework, and some of the high-level benefits, let's take a closer look at a few example questions from the Framework, to see the difference Stax can make when ensuring your workloads are Well-Architected.

1. Operational Excellence

OPS 6

How do you mitigate deployment risks?

Not every change goes as planned. Making sure you are aware of the risks during the deployment of changes is the first step in addressing, and ideally avoiding them. As the saying goes "failing to plan is planning to fail".

While you can leave it up to individual teams to manage their deployment approaches, you run the risk of having them all learn the same lessons and mistakes "the hard way". Without proper controls in place, deployments might rely on manual intervention that can delay or prevent future fixes in the event of failures.

Stax Workloads helps you follow infrastructure-as-code best practices, ensuring that your deployments are controlled, automated, repeatable, and easy to roll-back if needed. Workloads are packages of infrastructure-as-code that can be deployed to one or more AWS accounts from a single location. You only need to define your AWS resources and Stax will manage the orchestration of deployment, versioning, and termination.

By providing a consistent deployment management system and making it easy to test and validate your changes in multiple AWS accounts, Workloads encourage teams to deploy frequently, small, and reversible changes that can be more easily tested and validated.

2. Security

SEC 1

How do you securely operate your workload?

While you can use many of the AWS native security services yourself, the next challenge becomes doing it consistently at scale. Running workloads and applications in AWS doesn't mean your teams need to "reinvent the wheel". Ensuring that your security baseline, once set, does not regress or decay is also a frequent challenge that creeps up for most teams, usually when they're busy with something else. AWS is always releasing new features and services that need to be assessed, experimented with, and eventually integrated with if you're going to keep up.

Stax makes a multi-account workload easy on AWS. It establishes and maintains a security baseline, as well as keeps you up to date with new security services and features from AWS. By assessing your environments according to industry standards and service-level best practices continuously, Stax puts your teams on the front foot when it comes to managing the security of your workloads on AWS.

"Failing to plan is planning to fail."

SEC 2

How do you manage authentication for people and machines?

Ensuring that the right access is granted at the right time is a big step towards reducing the attack surface of your workloads in and environments in AWS. By clearly defining and controlling access permissions you can have confidence in your controls for both human and machine identities in your environment.

Setting up a robust identity perimeter can take time and unpicking existing access can be troublesome and encourage less secure behaviors in your developers.

Stax takes care of your access management, so that you don't have to rely on long-lived credentials. By integrating with your existing identity provider (e.g. Azure AD/Office 365, Okta, Ping, etc.) Stax allows you to take advantage of workload centralized identity provider.

3. Cost

COST 3

How do you monitor usage and cost?

The elastic, hyperscale cloud that AWS provides fantastic opportunities to optimize your spend on computing resources and services, but you need to actually take advantage of them. They don't do it for you. While developers usually mean well, the complicated nature of AWS billing makes it hard to know how much your workloads and application are going to cost when they're running. Finding out you overspent after a day is very different from finding out a month later when you get the bill from AWS!

While AWS provides some useful services in the cost management space, there are challenges when using them at scale and across many AWS accounts. The native AWS interface isn't always the easiest for non-technical users (like finance departments, etc.) to use easily.

The first step in managing your spend is to measure it. Stax's Cost features make it easy to attribute and categorize your costs, so that you and your teams are aware of where your AWS spend is going. All the reports in Stax are updated as soon as updated cost and usage report data is available from AWS, and the notification options (email, Slack, Teams, and webhooks) mean you can quickly and easily integrate your cost and usage alerts into your existing tooling.

COST 6

How do you meet cost targets when you select resource type, size and number?

The wide variety of EC2 instances provide great potential to craft a highly focused server that is ideal for your workload's requirements, which allows you to get the most "bang for buck" no matter the focus of your application. Unfortunately, all this choice can sometimes make it hard to make the *right* choice.

Using AWS native tools and services is possible, but needs to be done at the account level, and makes for reactive, repetitive work. If you don't do it, you're leaving money on the table, and if you do, it's tedious and slow.

Stax provides wastage recommendations so that you can be confident that you've sized your resources correctly. By integrating your usage reports and performance metrics, we can quickly show you the instances that need your attention. Stax wastage recommendations also provides suggestions for other common services and resources, like RDS, EBS, and S3.

For more examples of how Stax can enable you to be Well-Architected, read the full list in the appendix.

Interested?

Maybe your organization is considering the cloud but is unclear about the right path to follow to guarantee the business outcomes that were promised. Or maybe you're already in the cloud and you've found yourself going around in circles.

Either way, the AWS Well-Architected Framework can help you ask the right questions of your team to help guarantee success. But if you use Stax, you can also provide the correct answers.

If your organization has made being Well-Architected a business priority, get in touch to learn more about how our secure cloud management platform can make it a reality.

Visit **stax.io** and book a no obligation demonstration today.

STAX

Appendix A

Well-Architected Review Questions and Stax

Security

Enforce best-practice policies or apply ones specific to a customer's needs.

SEC 1 — How do you securely operate your workload?

Stax makes a multi-account workload easy on AWS. It establishes and maintains a security baseline, and keeps you up to date with new security services and features from AWS.

SEC 2 — How do you manage authentication for people and machines?

Stax takes care of your access management and integrates with your existing identity provider, so that you don't have to rely on long-lived credentials.

SEC 3 — How do you manage permissions for people and machines?

Stax provides default roles for you to use and customize to provide least privileges to your environment, as well as preventing when permissions are used.

SEC 4 — How do you detect and investigate security events?

Stax ensures that foundational security logging is always enabled (e.g., VPC flow logs, Session Manager logs, etc.), and sends events to the Stax EventBridge to make it easy to manage your security events centrally.

SEC 5 — How do you protect your network resources?

Stax Networks provides you with a best-practice, multi-tiered (i.e., layers) approach to AWS networking.

SEC 8 — How do you protect your data at rest?

Stax Rules can be configured to alert if data is not encrypted at rest anywhere in your AWS footprint.

SEC 10 — How do you anticipate, respond to, and recover from incidents?

Stax frees your team up from low-level work so that they can focus on the processes and planning need to respond to critical incidents, that can't be automated.

Operational Excellence

Develop and run workloads effectively, gain insight into their operation, and continuously improve processes.

OPS 6 — How do you mitigate deployment risks?

Stax Workloads helps you follow infrastructure-as-code best practices, ensuring that your deployments are controlled, automated, repeatable, and easy to roll-back if needed.

Cost Optimization

Run systems to deliver business value at the lowest price point.

COST 1 — How do you implement cloud financial management?

Stax Cost helps you manage your cost budgeting, forecast, optimization, and monitoring proactively.

COST 2 — How do you govern usage?

Stax Cost gives you visibility in to your AWS usage across your entire footprint, and helps you manage your usage and spend targets.

COST 3 — How do you monitor usage and cost?

Stax makes it easy to attribute and categorize your costs, so that you and your teams are aware of where your AWS spend is going.

COST 4 — How do you decommission resources?

By making it easy to see your AWS spend in one place, Stax helps you keep on top of any active resources, so that you can decommission them in a timely manner, and not waste money.

COST 6 — How do you meet cost targets when you select resource type, size and number?

Stax Cost provides wastage recommendations so that you can be confident that you've sized your resources correctly.

Reliability

Ensure workloads can perform their intended functions correctly and consistently when they are intended to.

REL 2 — How do you plan your network topology?

Stax Networks gives you a hub-and-spoke topology, takes care of IP subnet allocation for multi-AZ networks, and makes it easy to use DNS and VPC Endpoints in your network.

www.stax.io

Consistency | Confidence | Velocity

Find out more
www.stax.io

aws partner network — solution provider

aws partner network — accredited reseller

aws partner network — ISV accelerate member

Level 19, 8 Exhibition Street,
Melbourne, VIC 3000

www.stax.io