cprime

aws

Amazon Web Services

AWS Well-architected Review

Optimizing Your AWS Cloud Architecture for Maximum Scalability, Reliability, and Security

In this guide, we're going to take a deep-dive into optimizing a corporate AWS Cloud Architecture for maximum scalability, reliability and security. We'll begin with some background information and then move on to describing the Well-Architected Framework, which is the basis for conducting Well-Architected Reviews. Finally, we'll do a deep dive into the findings from reviews that have been conducted.

Part 1: Why and How to Move to the Cloud

One of the primary reasons organizations consider the Cloud is the cost efficiency potential. AWS provides remarkable economies of scale, due to the fact that equipment purchases are not required. Payment is only necessary for services that are actually utilized, which becomes a tremendous advantage in subsequent environment spin-off capabilities, including spin-up and spin-down. The flexibility of the Cloud enables the usage of new technologies and the exploitation of the consequential advantages, which oftentimes, are faster than what is possible with on-premise situations without having to make costly up-front investments.

The scalability of the Cloud enables rapid scale-up and scale-down to be done automatically and on demand. For example, a flash sale may result in a rapid surge in demand. The possibility to automatically scale applicable systems up to accommodate this demand, and then scale them back down upon completion of the sale is an example of the flexibility and scalability of the Cloud's resources. This includes higher availability to sustain business continuity, global presence, multiple regions and zones of availability, thus enabling the achievement of primary business goals.

One of the most common methods for moving to the Cloud is called "Lift and Shift," where a business takes inventory of what they have in their on-premise situation, then move and replicate it into the Cloud.

While this is one good way to initially achieve a move to the Cloud, it has one key drawback: the on-premise architecture which worked well before may not be the best architecture when moving into AWS. Once this has been completed, a Well Architect Review would uncover issues and potential improvements.

Recognizing that "Lift and Shift" has this weakness, a modification can be made resulting in a unique "Lift and Reshape" process. Most of the on-premise situation is still moved but with selected changes applied. For example, to move a Database to RDS can include taking advantage of some of the other managed AWS services. This procedure requires a strong understanding of the numerous additional services that are available in AWS, and the ability to assume responsibility of all of the trade-offs that result. This can be a challenge, particularly to new AWS users since some of those trade-offs can be fairly confusing.

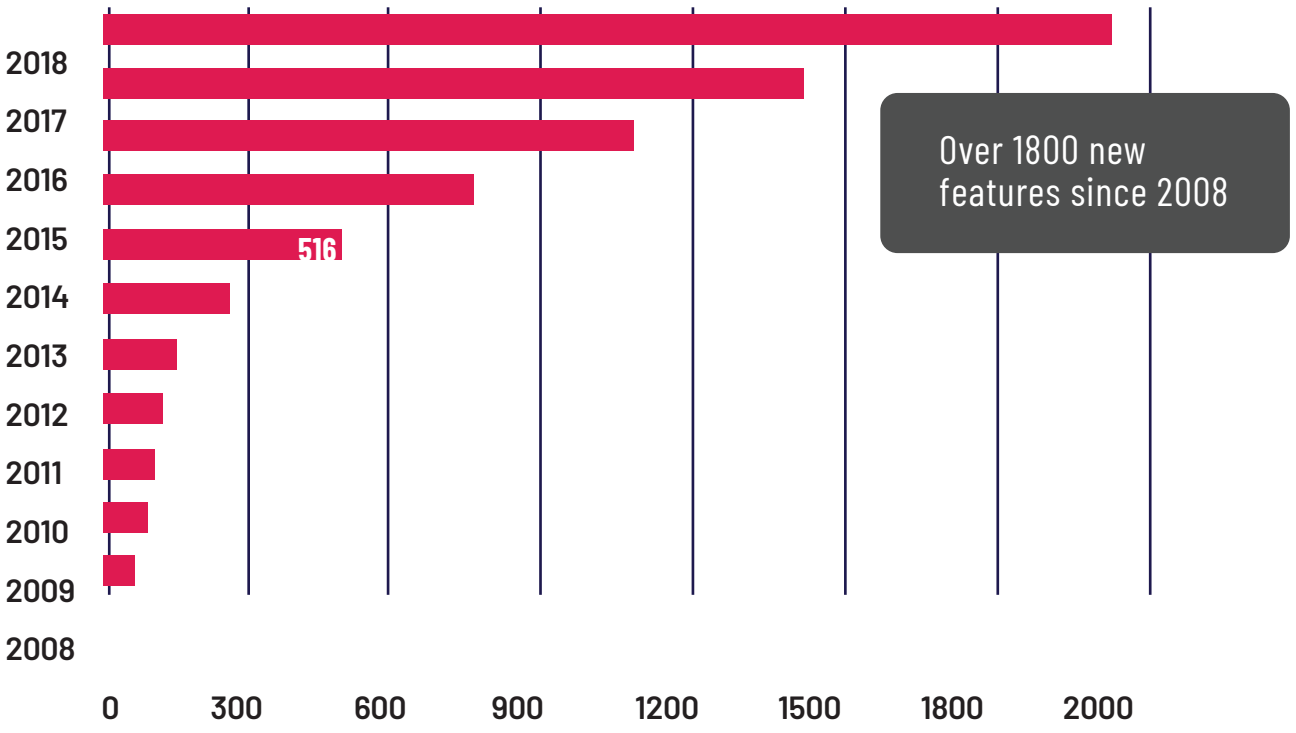
Initially, going through and trying to fully understand all the AWS services, the differences, pros and cons, and why one is preferable over another can be a very big challenge. Some businesses that start this process from scratch decide to re-architect completely, which is a valid option. The challenge here is to decide whether the company is moving to AWS or to the Cloud.

Cloud-native architectures can be a completely new paradigm shift, especially in how architecting is initially approached. This analysis includes changes in how CI/CD pipelines are handled, environmental provisioning, or how operations are run. All of these pose unique architectural challenges when moving to the Cloud.

Part 2: AWS Evolution

AWS is growing very quickly. Back in 2004, with a simple queuing service, AWS followed up with S3 storage service and EC2. Today AWS continues in its tremendous growth rate, accelerating beyond expectations. AWS continues to introduce so many new features that it becomes challenging just to keep up. As a result, what is understood to be good architecture today may no longer be considered the best architecture in 6 months to a year.

For businesses currently using AWS, one of the prime benefits of a review is the realization that while their systems may have been deemed well-architected two or three years ago, it would now be economically beneficial to consider re-architecting in order to take advantage of the new features and capabilities that AWS has since made available.



Part 3: Real World Consequences of AWS and Cloud

When moving to AWS and the Cloud, it is not uncommon that businesses make some missteps which result in real world consequences. For example, if a company misconfigured its Web Firewall, thus exposing a large amount of credit information, this would reveal a lack of understanding of public S3 buckets. Any company data left in a public subnet could be exposed and exploited. AWS has made it much more difficult to have public S3 buckets, making it more difficult for hackers to go in and skim corporate data from this area.

Real world consequences can also include simpler issues like wasted costs. Businesses may over-provision or ignore the advantages of the correct pricing model. Either of these circumstances could result in potential costs savings being less than predicted.

Reviewing empowers companies to identify oversights and achieve forecasted cost savings. Not being well architected can result in the business not being as scalable and reliable as initially believed, becoming vulnerable to system outages due to large load hits. Reviewing can help eliminate those load hit outages.

Part 4: The Well-architected Framework

From years of experience developing architectures within its own infrastructure, AWS has created what is commonly referred to as the Well-Architected Framework. This is not exclusively for external customers since AWS itself has built on top of existing AWS implementations. As a result, the personnel at AWS have plenty of experience in putting together good architecture that they must apply to their own work as they continue to develop services.

The Well-Architected Framework provides very specific advice on how to build and operate Cloud architecture for any business. This entails 34 design principles and nearly 250 best practices. All of which are organized into five distinct pillars. Each of these pillars contains questions that can be used to evaluate the architecture of a business against the best practices previously referenced.

A business could ask “How does my system withstand component failure?” An analysis of the best practices applicable could show that the following should be implemented:

- System monitoring at all layers
- Loosely coupled architectural dependencies to enhance failure resistance
- Multiple location workload deployment to allow for the failure of one location and the immediate bail over to another location, thus improving resilience

These are only a few of the best practices that could be utilized. The questions that are provided enable effective evaluations. They can also be applied in the context of a Well-Architected Tool, which we'll detail in the following pages.

Part 5: Well-architected Framework Pillars

Operational Excellence

Concerns Operations Management, monitoring DevOps, monitoring the CICD pipeline, Incident Management and impacting Customer Support.

Security

Concerns access control, data protection, encryption, dealing with denial of service attacks and similar web-related issues.

Reliability

Concerns high availability, rapid scale-out to avoid outages due to the inability to scale accordingly, back-up and recovery, failure recovery.

Performance Efficiency

Concerns utilizing appropriate resources to effectively manage architectural services, determining trading off EC2 instances vs. Container usage, and validating the database type being used and Event-Driven architecture vs. alternative methodologies.

Cost Optimization

Principally for Finance concerns, regards right-sizing of resources, over-provisioning considerations, and under-utilization of resources which result in the wasting of costs.

Part 6: Benefits of a Well-architected Framework

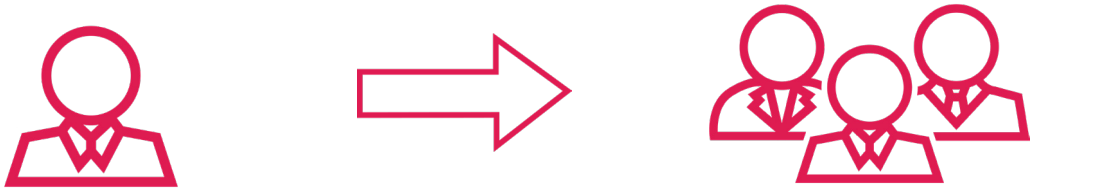
The Well-Architected Framework not only aides in avoiding costly mistakes, but improves internal efficiency, team engagement, and customer satisfaction. The customers of a business are not only better served due to faster, more responsive services, but with appropriate monitoring, logging and alerting, improves incident response and the reliability of maintaining system availability.

Additional benefits include:

- Architecting new implementations result in better informed decisions
- Greater security from reduced exposure to compromised data access
- Automated tasks and processes result in smoother deployments
- Application response time improvements
- Greater system up-time from faster operational responses to system incidents
- Dynamic ability to acquire demand-driven computing resources
- Efficient usage and maintenance of computing resources as requirements, demand and technologies evolve
- Reduced on-going costs and fewer monthly billing surprises

Part 7: The Well-architected Review

- Structured non-confrontational conversation
- Gain understanding of state of workload relative to Well-Architected Framework
- Use Well-Architected Tool
- Focus on single workload
- Address pillars in order of business priority



SOLUTION ARCHITECT

BUSINESS AND TECHNICAL STAKEHOLDERS

Part 8: AWS Well-architected Tool

The principle tool used in a Well-Architected Review is called the Well-Architected Tool. For businesses with AWS experience, this tool is available through the AWS Management Console under the Management section in the Management Tools area. All of the pillars are already there, including all of the related questions for those pillars. In practice, a reviewer would open one question then look at which of the various best practices apply.

This methodology was developed by AWS. AWS encourages businesses to use this tool during a review, while noting that this tool does not replace the discussion. Checking off boxes does not mean the review is done. AWS strongly encourages actual face-to-face discussion, which is critical to bringing up many of the issues that may require attention. The tool is not a substitute by itself for the review.

Part 9: Who Benefits From the AWS Review

Security

The review typically reveals security issues that had not been considered or fully understood. It is not uncommon for a review to identify numerous security issues.

Operations

The review can reveal potential reductions in overhead, specifically, whether or not the business is overpaying for its existing architecture. This business segment can become more efficient, leading to smoother deployments. You can improve blue-green deployments and complete a Cloud migration more efficiently when exploiting the advantages of the AWS services available.

Customer Support

The review can aid in improvements to customer response when problems occur, as well as tackling similar problems before they occur in the first place.

Product Management and Developers

Deployments and testing can always be more efficient. The Well-Architected Review benefits units all across the organization. This is a key reason why businesses conduct such reviews. Because of the well-architected nature of the business, there are less fires to fight leaving more time to add value to the existing system.

Finance

This department, of course appreciates costs being kept low as a direct result of the benefits of the Well-Architected Framework.

Part 10: AWS Well-architected Review Options

SELF SERVICE

Business & Technical Stakeholders + **Whitepapers** + **Well-Architected Tool**

- Review at own pace
- Internally define remediation plan

Business & Technical Stakeholders + **Partner Solution Architect** + **Well-Architected Tool**

- Single review meeting
- SA provides findings, recommendations, action plan
- Brings outsider perspective to review

Self-Service Review

One option for doing a review is a business doing the review by itself. It is encouraged for AWS savvy business staff to read as much as they can about the self-service review before attempting to conduct one. Remember to organize the review and use the Well-Architected Tool. Include discussions by gathering the business and technical stakeholders together to objectively go over the architecture then derive an appropriate remediation plan as a result of the review insights.

AWS Partner Review

When a business does not have internal staff needed for a self-service review,

they can bring in an AWS partner, such as Cprime. Cprime's Solution Architects can conduct these reviews on-site and provide a much needed outsider perspective. Our reviewers apply the Well-Architected Tool and then convene a Review meeting with the business and technical stakeholders to examine the review. Afterwards, they provide their findings, recommendations and an action plan for moving forward on the results of the review.

Part 11: The AWS Well-architected Review Process

Step 1: Preparation

The key part of preparation is to have the Solution Architect review the accounts. If the account review is conducted by Cprime or an internal Solution Architect, read access will be required to analyze the accounts properly. From a security perspective, the Solution Architect should have sufficient access to be able to probe the IAM portion to determine what policies are in place, which users are in place, and what other security policies are active.

In addition, the Solution Architect will be able to probe how the different subnets are setup, how information is distributed across the nets and the availability zones, as well as review scaling capabilities and how they have been configured. As part of the initial portion, AWS also encourages a business to fill out the Well-Architected Tool.

Step 2: Review Meeting

The Review meeting should be, depending upon the amount of preparation invested, approximately 2 to 4 hours in duration. This meeting will not be a tremendously in-depth analysis.

When conducted by the business itself, there is the risk to drill-down to excessive levels of detail. When conducted with an outside partner, the partner typically recommends a 2 to 4 hour meeting after the analysis of the current architecture's content and status. The Solution Architect walks through the framework, what was examined and asks questions concerning architectural issues that require any additional clarification.

Step 3: Read-Out

After the Review meeting is completed, a Read-out is held. It is vital to hold this within a few days of the Review, so that during the Read-out, findings and any proposed recommendations or remediation fixes are all still fresh. A business gathers the key people concerned and presents the summary of what was found and what was proposed to address those findings. Any business decision-makers empowered to approve actions and fix issues should be in attendance.

Step 4: Quick Wins

AWS encourages implementation of some of the proposed changes as soon as possible, within a week or two after the review. This provides the business with the benefit of some quick wins and affirms that the Review had value. Further, it will help gain business support to make any larger changes deemed necessary. The business can note the value of what was changed right after the Review, and see the larger benefit of investing as necessary to implement the larger changes the Review findings uncovered.

Step 5: Follow-Up Review

AWS further encourages businesses to do a follow-up review after 30 to 60 days to determine how well the implementations were conducted, and whether implementations improved the architecture. One of the AWS benefits of a review is that it may qualify a business for some funding programs for remediation. AWS has several different funding programs to assist businesses with some of the costs of doing changes, using services that are available. While these are eminently worth looking into, the caveat is that AWS is constantly changing their programs. Again, this is but one use of a review that may qualify businesses for some of the funding programs that might become available in the future.

Part 12: Reviews are Not a One-time Event

Reviews are not a one-time event. AWS strongly encourages businesses to conduct reviews periodically. The reason being, architectures tend to drift over time. Businesses make changes to the architecture, incorporating new features and adding new capabilities. During these times, it can be difficult to keep things well-architected. AWS constantly introduces new services. This may result in the situation that what is a good architecture today won't necessarily be optimal in another 6 or 9 months.

As previously indicated, a review prior to launch is worth considering, especially if a major refactoring is being conducted. On existing workloads, reviews should be done periodically, about every 6 months.

Part 13: Common Findings in AWS Well-architected Review

Cprime has conducted a large number of Well-Architected Reviews. From discussions with AWS and other organizatios, various issues are often found as a result of these reviews. While each workload is unique and the reviews will differ, there are some common issues that have been identified.

Common Findings - Security

Protecting Data	Examples of Potential Problems Identified in Review
Managing Credentials and Access Keys	• Credentials of former employee still enabled • MFA not enabled on root account • Access key used by application is stored in code or on disk
Protecting Data	• Sensitive data not encrypted • Using insecure protocol for transmission of sensitive data • S3 buckets unnecessarily public
Protecting the Network	• Ports open unnecessarily to Internet • Application servers or databases in public subnet • No protection against DDOS attack
Handling Security Invidents	• Security tracing or logging not enabled • No automated alerts from security breach

As previously noted, Security is not always at the forefront of people's mind in a business. Numerous issues are often identified in this area. This includes credential management, data protection and how a business can support handling security incidents.

One common finding concerns credentials not being periodically purged. This applies not just for former employees. Staff members may have changed roles as well. It is not uncommon to find User IDs that have been inactive for a few years and access keys that have not been utilized in over a year. Lingering credentials such as this are potential security holes. As the AWS Console is accessible via the web, if business staff with access leave the company and their credentials have not been purged, they will still be able to log in. It is imperative to have a reliable method of constantly purging credentials, rotating keys and rotating passwords.

Some businesses still have public S3 buckets that may need to be either shut or protected in some manner. AWS currently makes it more difficult to have public buckets, yet there are businesses with existing architectures that are public. Issues involving the database and public subnets are actually common occurrences. One reason for this is that sometimes business staff needs to have a Developer go in and look at the log files or to go in and probe the database themselves. As a result, they determine that the database or application service resides on a public subnet. This exposes work open to them to the internet to be able to get in and examine various aspects of their data.

AWS emphatically discourages this. AWS encourages businesses to put all such things in a private subnet using a bastion host. And yes, there are means to tunnel through a bastion host to access the database. AWS does not recommend putting databases in a public subnet, despite having security groups to protect the data; it is still an inadequate practice. If a business has logs, the logs should be collected in Cloud formation or a third party product such as Log Aggregation. These methods can provide effective ways of looking through the logs, when necessary. This means that there is no good reason for putting something in a pubic subnet, other than either a bastion host or a gateway.

Such issues are the sort of things that keeps CSO's from getting a good night's sleep. AWS is serious about looking at security.

Common Findings - Reliability

Areas Examined	Examples of Potential Problems Identified in Review
Scaling to Meet Unexpected Demands	• No auto-scaling in place • No monitoring of load to detect when reaching capacity • Load testing not performed
Supporting Expansion	• Subnet CIDR ranges are too narrow • Service limits are not being monitored • VPCs have overlapping CIDR blocks

Handling Component Failures	• Single point of failure in architecture • Load balancer not properly distributing traffic across multiple AZs • Failure recovery is not automated
Recovering from Major Failures	• No defined RTD and RPO • Backups not saved to a second AWS region • Restore from backups has not been tested in a long time (if ever)

AWS considers if a business is going to be able to scale for unexpected demand, if they can handle expansion, and if they can handle unexpected failures and recover. For example, some businesses do not have monitoring; some have it but without any alerting. Or, they have alerting but without any automated responses. As a consequence, when thing sstart to fail they do not automatically re-start servers that may have failed.

The VPCs, overlapping CIDR blocks, and having subnets with too narrow ranges are all considered during the review. One of the strengths of AWS is its ability to spin up multiple VPCs for different purposes.

Caution is advised because while a business may believe those VPCs don't have to talk to each other today, another six months from now there may be a reason to peer the VPCs together. Unfortunately, this results in conlficts on the IP ranges within those subnets. As a result, AWS encourages business to not have overlapping CIDR blocks within those VPCs.

Businesses are usually effective when scaling out their computer instances and having database replication, but sometimes they put a single instance of a queue, which is now a single point of failure without clustering occurring. It may be better to use AWS services such as AWS MQ which is a way of having MQ compatibility, including high availability without having to manage an entire MQ cluster on their own.

There can be some improvements from automating the provisioning of things. Auto-Scaling is one effective way, even if it is not deemed necessary to have dynamic scaling, and even if the business only needs to add new capabilities every few months.

Auto-Scaling can actually be an easier way to expand one's capability by simply removing one more manual step. Auto-Scaling groups can eliminate having to do manual restarts.

Even businesses with fixed scalability or that don't need scalability benefit from auto-scaling groups. They use these groups to strictly restart failed instances automatically. This removed a bit of manual operational work without having to exploit the auto-scaling groups for any other scaling purposes. This is one example of exploiting a partial feature in an interesting way.

Common Findings - Perfomrance Efficiency

Protecting Data	Examples of Potential Problems Identified in Review
Scaling to Meet Unexpected Demands	• No auto-scaling in place • No monitoring of load to detect when reaching capacity • Load testing not performed
Supporting Expansion	• Subnet CIDR ranges are too narrow • Service limits are not being monitored • VPCs have overlapping CIDR blocks
Handling Component Failures	• Single point of failure in architecture • Load balancer not properly distributing traffic across multiple AZs • Failure recovery is not automated
Recovering from Major Failures	• No defined RTD and RPO • Backups not saved to a second AWS region • Restore from backups has not been tested in a long time (if ever)

Auto-Scaling can actually be an easier way to expand one's capability by simply removing one more manual step. Auto-Scaling groups can eliminate having to do manual restarts. Even businesses with fixed scalability or that don't need scalability benefit from auto-scaling groups. They use these groups to strictly restart failed instances automatically. This removed a bit of manual operational work without having to exploit the auto-scaling groups for any other scaling purposes. This is one example of exploiting a partial feature in an interesting way.

Serverless technology is an effective way of being able to take advantage and achieve scalability, reliability, and high availability.

Simply dealing with performance issues when customers call isn't beneficial to anyone. AWS prefers to apply perfomrance monitoring in order to get in front of customer issues rather than reacting to customer complaints afterwards.

Frequently a review will reveal many unused instances that are literally eating up dollars unnecessarily. This is not just a money issue, but also clutter issue. The problem comes from the fact that this makes debugging other system issues more difficult.

For instance, imagine a scenario where a Lambda function is in places and extended efforts are spent to debug that particular part of the system containing the Lambda function. It's determined that the Lambda function is not even being used. This comes after wasting time (and resources) on trying to analyze something that is, in effect, dead code (an unused resource within AWS). Clutter inhibits understanding the architecture of a business. Consequently, AWS strongly encourages businesses to have effective decommissioning processes in order to be able to shut down unused components.

Common Findings - Operational Excellence

Areas Examined	Examples of Potential Problems Identified in Review
Deployment Operations	• Manual deployments & provisioning of environments and changes • Production environment configuration is not version controlled • Making large changes at once • Ad hoc rollback strategy

Monitoring of Workload & Operations	• KPIs not well defined • "Normal" behavior of workload not base-lined • No automated alerts from metrics
Incident Response	• No run-books for known incidents • No automatic Customer alerts on incident status and resolution

Businesses conduct numerous manual operations that could be reduced by exploiting some of the AWS features to avoid manual processes. This results in improved Operational Excellence.

AWS strongly encourages either using CloudFormation in AWS or, another third party application. Automation is singularly important to a business, allowing it to help with multiple environments. For example, when an additional QA environment is needed it can be as easy as spinning one up for a few hours, then conducting the required test, and afterwards spinning it down. Automation enables this ability to have environments available for short bursts of time, on demand, based upon need.

Another typical finding is that KPIs are not well defined. Businesses consider KPIs in terms of release frequency, mean time to fix production issues, and other similar statistics. This is in accord with the idea that a business cannot really improve what they cannot measure. AWS analyzes how to implement monitoring regarding these areas and help a business to achieve improved operational excellence.

Many businesses do not have run-books for incident managements. Oftentimes, staff members rspond to incidents using "tribal knowledge", where they, more or less, know what to do. AWS highly encourages businesses to have run-books. If a run-book is available, including run-book support, this can avoid having to call developers or operations staff by having tier 1 support staff resolve specific run-book documented issues. Run-books can be invaluable in these circumstances.

Common Findings - Cost Optimization

Areas Examined	Examples of Potential Problems Identified in Review
Deployment Operations	• No defined budget or cost target • Not generating Cost and Usage Reports • No cost attribution

Eliminating Waste	• Unused EC2 instances, unattached EBS volumes, etc. • No defined decommissioning process • Oversized resources instead of reactively provisioning • Test environment left in place even when not being used
Pricing Models	• Not using reserved instances for long term EC2 resources • Keeping archived files in S3 instead of Glacier • Not leveraging spot pricing for temporary increases in demand • Batch jobs not executing in low priced regions

Part 14: Key Takeaways

A Well-Architected Review can help a business to:

- Leverage accumulated collective wisdom of AWS architects
- Discover improvemetns affecting cost, performance, reliability, operations, and security.
- Accelerate remediation of most urgent and impactful issues
- Surface discrepancies in understanding of current state of workload
- Learn how workloads can take advantage of new AWS services
- Gain understanding of AWS best practice

So after reviewing the benefits of AWS WAR my question is, “Are you well architected?”

To explore more, or get help with your own AWS WAR, contact the experts.

Architecting on AWS

3 Day Classroom Session | 3 Day Live Online | Custom Onsite

Course Overview

Architecting on AWS covers the fundamentals of building IT infrastructure on AWS. The course is designed to teach solutions architects how to optimize the use of the AWS Cloud by understanding AWS services and how these services fit into cloud-based solutions.

This course emphasizes AWS cloud best practices and recommended design patterns to help students think through the prT solutions on AWS. Infrastructures and the stratervices they implemented.

You will learn how to:

- Make architectural decisions based on the AWS-recommended architectural principles and best practices.
- Leverage AWS services to make your infrastructure scalable, reliable, and highly available.
- Leverage AWS managed services to enable greater flexibility and resiliency in an infrastructure.

Individual	Custom Onsite	Request a quote online or call (877) 753-2760
$2025.00	8+ TEAM MEMBERS	

For more information on our AWS curriculum, please visit:
www.cprime.com/learning

visit www.cprime.com
or call (877) 753-2760

cprime

About the Author

Peter Panec is a DevOps Solution Architect with Cprime. Peter has over 25 years of experience in software application and delivery as a developer and technical/ engineering manager in a variety of industries. He actively champions and participates in Agile and DevOps and acts as a leader for culture and organizational transformations. His passions include the application of DevOps and Cloud technologies to support evolutionary architectures and doing whatever it takes to help organizations succeed.

About Cprime

Cprime is an industry-leading, full-service global consulting firm with a focus on providing integrated and innovative solutions around digital transformation, product, cloud, and technology. With over 20 years' experience, we provide strategic and technical expertise to businesses across more than 50 industries. Our team of advisors and technical experts have the know-how to meet organizations where they are to develop actionable solutions and solve business challenges. We also collaborate with our expansive network of partners to design, deploy, and harmonize technology stacks across organizations. Our mission is to empower visionary business leaders and teams to reimagine the future of work to achieve better outcomes.

Visit us at **www.cprime.com**

Additional Resources

[WEBINAR] AWS Well-Architected Review: Optimizing Your AWS Cloud Architecture for Maximum Scalability, Reliability and Security

www.aspetraining.com/aws-war-webinar

Cprime AWS Well-Architected Review

https://www.cprime.com/cloud/aws-well-architected-framework/

[WHITEPAPER] AWS Well-Architected Framework

https://www2.cprime.com/l/19052/2019-10-15/btvk8z/19052/222327/AWS_Well_Architected_Framework.pdf

[On-Demand Webinar] Are We Well Architected? Optimizing Your Cloud Architecture for Maximum Scalability, Reliability and Security

https://www.cprime.com/resource/webinars/are-we-well-architected-optimizing-your-cloud-architecture-for-maximum-scalability-reliability-and-security/

AWS Website

https://aws.amazon.com/architecture/well-architected/