AWS Well-Architected Framework Made Easy with Kion

Since establishing a partnership with AWS in 2016, Kion has been at the forefront of cloud governance and management best practices. Kion was a key contributor to the identification of Cloud@Scale requirements and helped develop the predecessor to the AWS Well-Architected Framework (WAF), "AWS Governance at Scale".

This matrix provides guidance for organizations aiming to achieve and maintain a Well-Architected posture, facilitating continuous improvement as they scale and evolve in the cloud. Below we've highlighted key best practice areas - Operational Excellence, Security and Cost Optimization - where Kion can help you adhere to and meet WAF requirements.

Kion is your trusted partner in your pursuit towards building and maintaining a Well-Architected cloud. To speak with a Kion technical expert on establishing Well-Architected Cloud Operations processes, click here.

Operational Excellence

OPS 01: How do you determine what your priorities are?

Best Practice ID: OPS01-BP03 Evaluate governance requirements

Action Items	Verification	Kion Value Add
Identify organizational governance requirements and incorporate them into workload planning	Regular audits and AWS configuration for continuous governance monitoring	Cloud Rules ensure governance standards are automatically applied to new and existing workloads, eliminating manual intervention and supporting multiple AWS organizations.

Best Practice ID: OPS01-BP04 Evaluate compliance requirements

Action Items	Verification	Kion Value Add
Align workload with compliance frameworks relevant to the industry and regulatory standards.	Use AWS Audit Manager to automate evidence collection and ensure continuous compliance.	Kion's compliance engine can scan your AWS environment against a number of different built in frameworks from HIPAA, NIST, ISO27001, and custom frameworks to give you an instant baseline of where gaps exist in your current configuration.

Best Practice ID: OPS01-BP07 Manage benefits and risks

Action Items	Verification	Kion Value Add
Balance decision benefits against associated risks, considering business impact.	Risk assessment meetings and documentation of risk mitigation strategies.	Kion mitigates tradeoffs around cloud operations to enable strategies that would otherwise need to be disregarded.

OPS 05: How do you reduce defects, ease remediation, and improve flow into production?

Best Practice ID: OPS05-BP03 Use configuration management systems

Action Items	Verification	Kion Value Add
Document and define all configurations as code where possible	Use AWS Config to continuously monitor environment and resource configurations	By using Kion's centralized policy management, organizations can create, manage, and apply IAM policies, service control policies (SCPs), and permissions boundaries efficiently across their entire AWS organization.

Best Practice ID: OPS05-BP06 Share design standards

Action Items	Verification	Kion Value Add
Share and enforce design standards using AWS Service Catalog, allowing teams to use approved and standardized resources. Enforce the use of standardized AMIs for compute resources.	Verify that Kion Cloud Rules with Service Catalogs are present. If necessary, develop Kion compliance checks to verify the presence of Service Catalogs and deviations from things like standard AMIs.	Kion provides a way to standardize the AWS Service Catalog configurations available across multiple accounts and in multiple AWS Organizations to ensure standards and best practices are adopted.

Best Practice ID: OPS05-BP08 Use multiple environments

Action Items	Verification	Kion Value Add
Set up separate environments (development, testing, production) using AWS Elastic Beanstalk or AWS CloudFormation.	Validate environment setup and isolation by deploying different stacks in AWS CloudFormation and managing them via AWS Elastic Beanstalk environments.	Kion can manage and segregate multiple environments across development, testing, and production stages. Kion allows you to create and enforce policies, such as IAM policies and service control policies (SCPs), across different AWS accounts organized within its Organizational Units (OUs), ensuring isolated, secure, and controlled sandbox, development, and production environments.

Kion

AWS Well-Architected Framework Made Easy with Kion

Security

SEC 01: How do you securely operate your workload?			**SEC 02:** How do you manage identities for people and machines?		
Best Practice ID: SEC01-BP01	Separate workloads using accounts		**Best Practice ID:** SEC02-BP01	Use strong sign-in mechanisms	
Action Items	Verification	**Kion Value Add**	Action Items	Verification	**Kion Value Add**
Implement a multi-account strategy to isolate workloads based on function, compliance requirements, or a common set of controls. Use AWS Organizations for account management.	Verify isolation and compliance by checking the account structure and policies in AWS Organizations. Ensure workloads are separated according to the strategy.	Kion is the beating heart of a multi-account AWS strategy, enhancing AWS Organizations by simplifying the management of a multi-account strategy through automated account provisioning, budget enforcement, and compliance standards across all accounts.	Implement multi-factor authentication and enforce strong password policies	Verify MFA is enabled and check password policies for complexity requirements	Kion provides policies for enforcing password complexity requirements and compliance checks for MFA for IAM users created in accounts. Kion also provides a way to create a time-limited, managed IAM user account for AWS API access.
Best Practice ID: SEC01-BP02	Secure account root user and properties		**Best Practice ID:** SEC02-BP02	Use temporary credentials	
Action Items	Verification	**Kion Value Add**	Action Items	Verification	**Kion Value Add**
Enable MFA for the root user and remove or secure root user access keys. Use a strong password and secure the email and phone associated with the account.	Regularly audit root user access, MFA status, and check for the absence of access keys using IAM reports and AWS CloudTrail logs.	With Kion's robust IAM policy and permissions management, Kion allows for the delegation of permissions with fine granularity, eliminating the need to use the root account.	Utilize roles and temporary credentials for AWS service access instead of static keys	Check for the absence of long-term credentials and the presence of role-based access in IAM	Kion simplifies the management of temporary credentials by automating the assignment of roles and permissions, ensuring users and services are granted the minimum necessary access on a temporary basis.

AWS Well-Architected Framework Made Easy with Kion

Cost Optimization

OPS 01: How do you implement cloud financial management?

Best Practice ID: COST01-BP02 Establish a partnership between finance and technology?

Action Items	Verification	Kion Value Add
Foster collaboration between finance and technology teams to ensure alignment on cloud cost management and optimization	Validate through documented joint initiatives and meetings that demonstrate active cooperation and shared strategies	Kion's role-based access and reporting enable finance and technology teams to access relevant information, facilitating effective communication and joint decision-making on cloud cost management initiatives.

Best Practice ID: COST01-BP03 Establish cloud budgets and forecasts

Action Items	Verification	Kion Value Add
Utilize AWS Budgets and AWS Cost Explorer to create detailed budgets and forecasts that account for expected cloud usage and expenses	Ensure budgets and forecasts are reviewed and adjusted regularly, verified by change logos and budget variance reports	Kion enhances the experience found in native AWS functionalities by offering a consolidated view and management of cloud budgets across multiple AWS accounts from a single dashboard. Kion allows for automated budget tracking and notifications, and is proactive with automated financial enforcement actions to avoid budget overruns proactively.

Best Practice ID: COST01-BP05 Report and notify on cost optimization

Action Items	Verification	Kion Value Add
Set up AWS Budgets alerts and AWS Cost Anomaly Detection to monitor and report on cost optimization efforts.	Confirm the setup of alerts and regular receipt of reports that highlight optimization efforts and identify areas for improvement.	By leveraging Kion's financial management and enforcement actions, organizations can monitor and proactively manage cloud spend across AWS accounts, ensuring cost optimization recommendations are implemented and tracked over time.

Best Practice ID: COST01-BP08 Create a cost-aware culture

Action Items	Verification	Kion Value Add
Implement programs and initiatives that foster a cost-aware culture within the organization, encouraging cost-efficient practices.	Surveys, feedback, or case studies demonstrating a shift in organizational behavior towards more cost-aware practices.	Kion's policy enforcement and budgeting tools empower teams to take ownership of their cloud costs, promoting a proactive approach to cost management. Funding sources allow FinOps teams to reconcile spend back to the cost center(s).