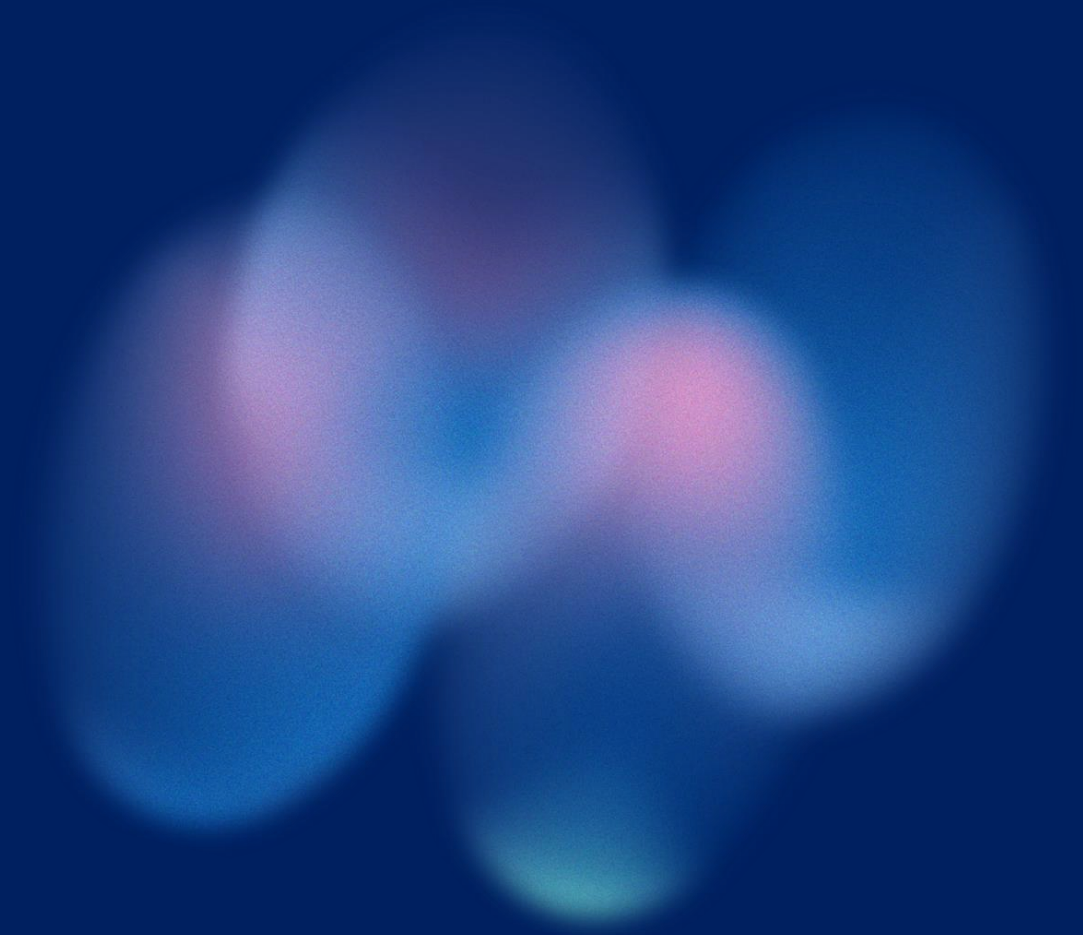
AWS SECURITY SERVICES& COMPLIANCE- FAST TRACK TO READINESS

Accelerating cloud compliance for business success

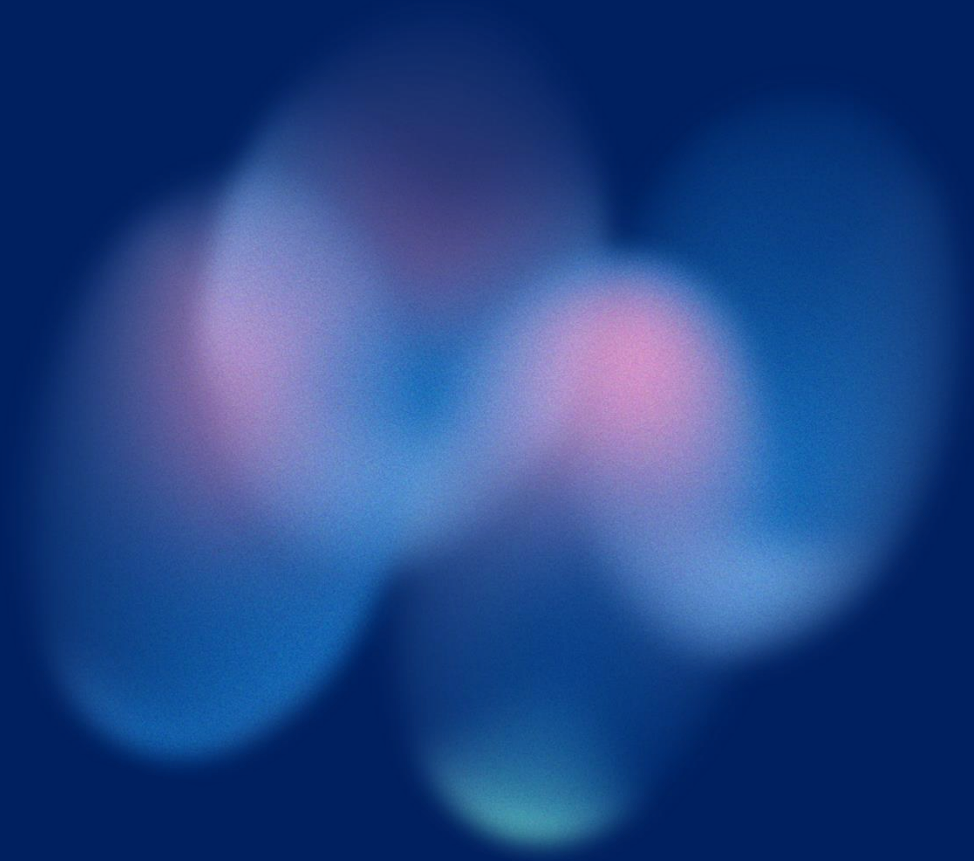


10/23/2025

INTRODUCTION

PRESENTER: Ivica Micev

WORKING AS: Senior Engineering manager @ Scalefocus



ARCHITECTING CONTINUOUS COMPLIANCE & ACCELERATION ON AWS

Shift to Continuous Compliance

Organizations must move from point-in-time audits to perpetual readiness in dynamic cloud environments.

Integrating GRC with DevSecOps

Embedding governance, risk, and compliance into DevSecOps workflows ensures security is part of daily operations.

Leveraging AWS Automation

Using AWS services to automate enforcement of security controls eliminates audit debt and enhances efficiency.

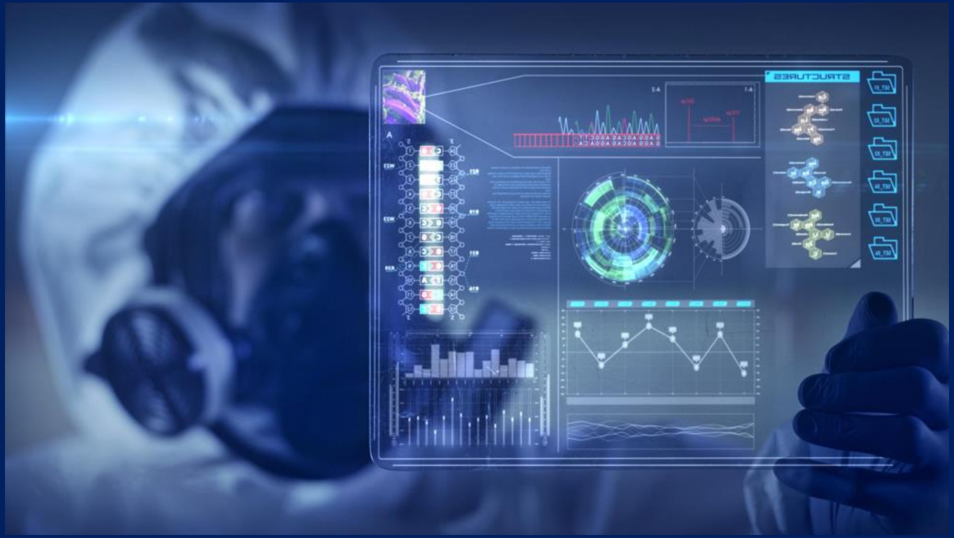
Benefits of Continuous Compliance

Continuous compliance improves security, reduces manual audit burdens, and increases operational efficiency.

COMPLIANCE PARADIGM SHIFT

10/23/2025

COMPLIANCE IS CONTINUOUS, NOT A CHECKPOINT



Shift to Continuous Compliance

Compliance has evolved from static audits to a dynamic, continuous readiness model with ongoing monitoring.

Automation and Integration

Automated tools and integrating compliance into operations reduce manual effort and streamline audits.

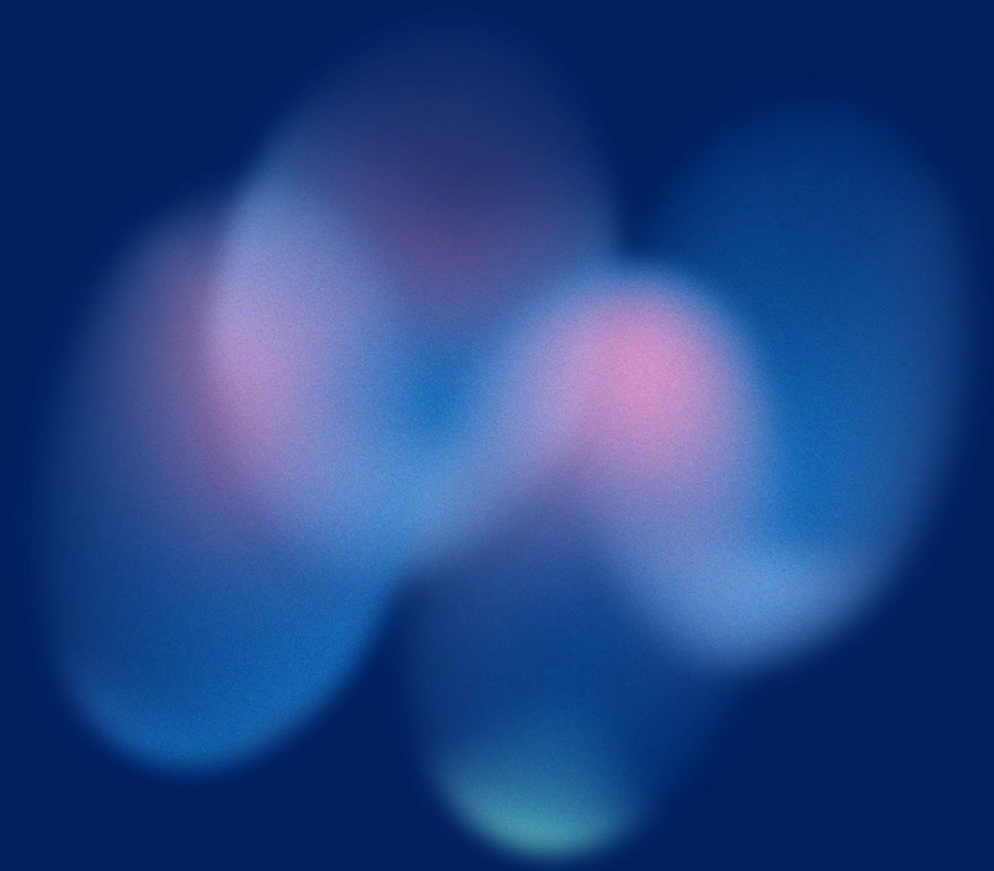
AWS FSBP Standard

Adopting AWS Foundational Security Best Practices ensures a mandatory security baseline for compliance readiness.

GRC in DevSecOps

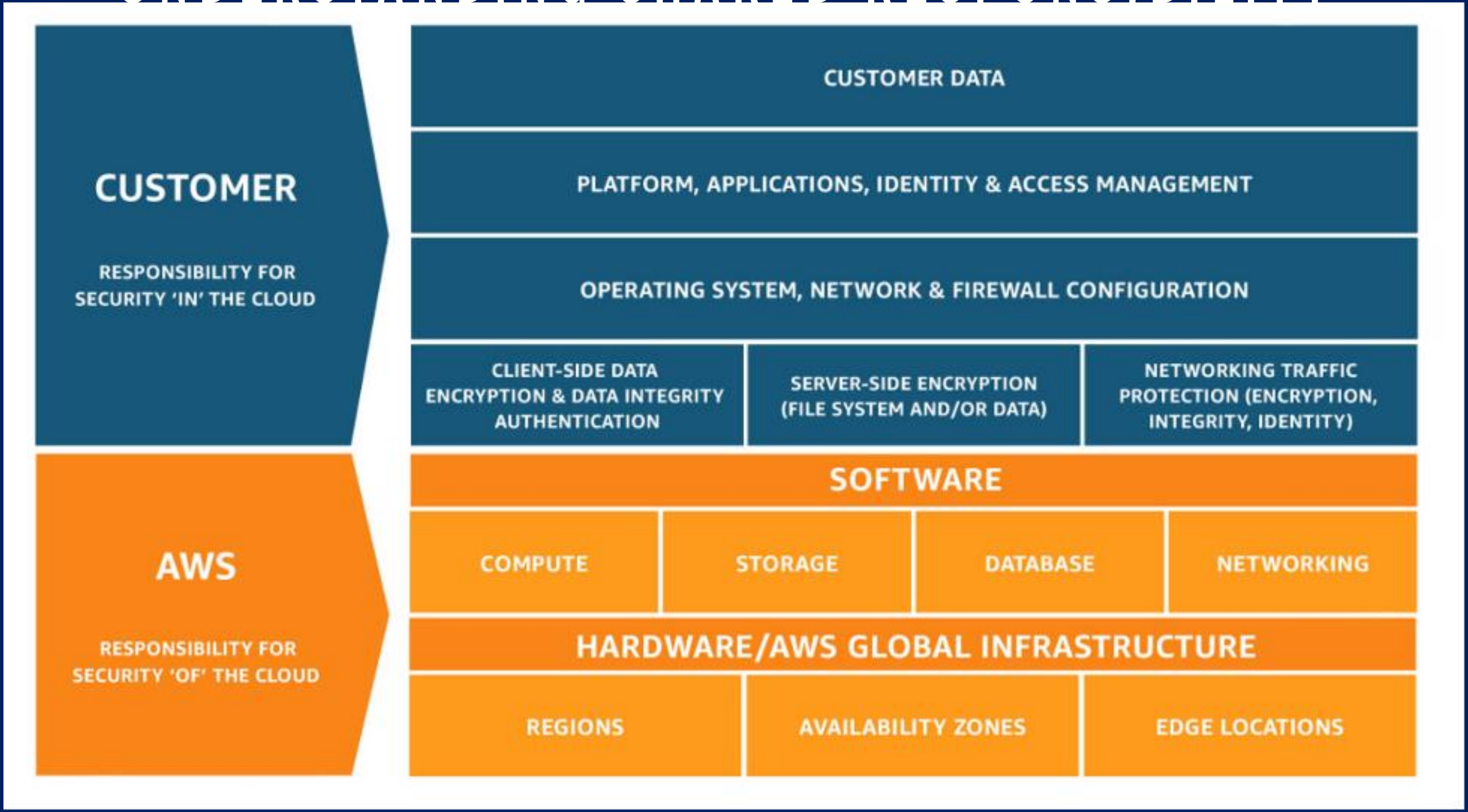
Integrating Governance, Risk, and Compliance into DevSecOps fosters a compliance-ready system with verifiable proof.

SHARED RESPONSIBILITY MODEL



10/23/2025

UNDERSTANDING SHARED RESPONSIBILITY



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION	SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)	NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE	STORAGE	DATABASE	NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS	AVAILABILITY ZONES	EDGE LOCATIONS

BASELINE ENFORCEMENT

AWS FOUNDATIONAL SECURITY BEST PRACTICES (FSBP)

Mandatory Security Floor

FSBP establishes a mandatory security baseline for all AWS resources ensuring consistent protection.

Continuous Monitoring

AWS Security Hub enforces FSBP by continuously monitoring technical configurations and compliance status.

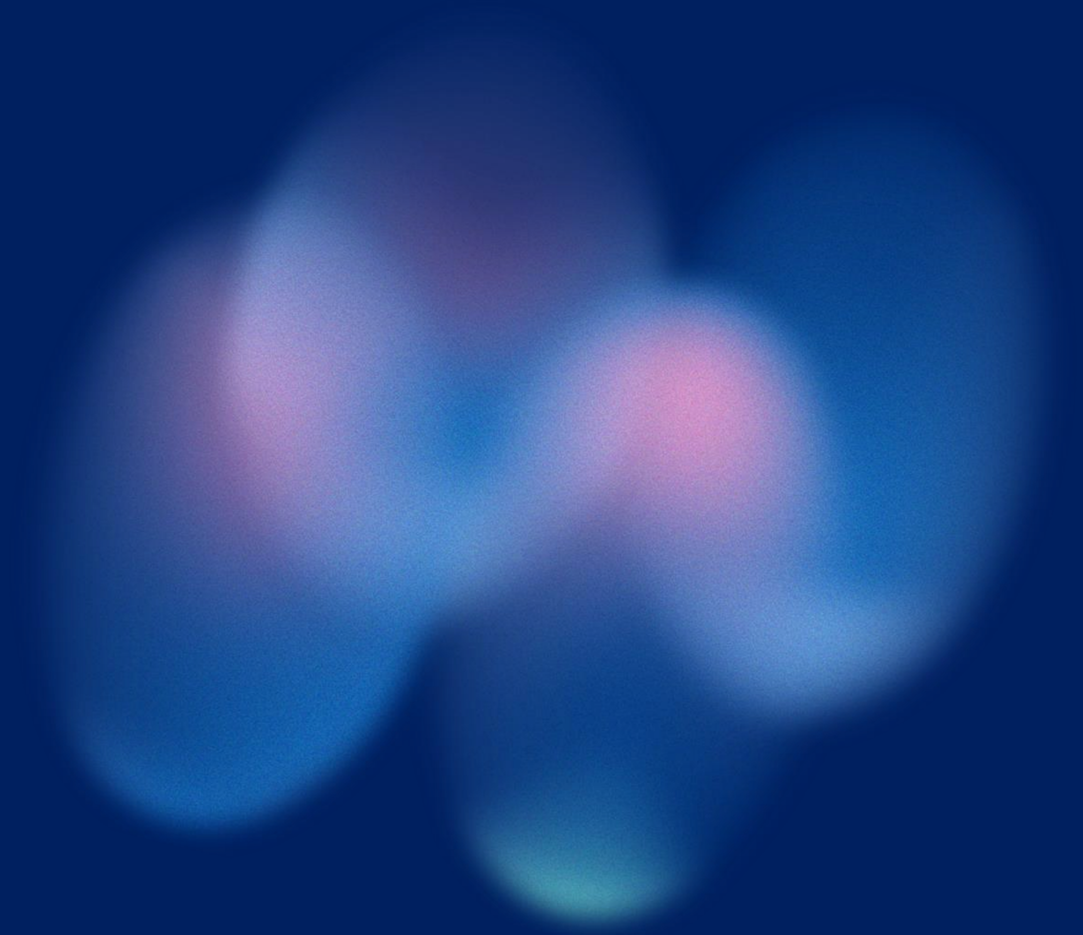
Key Security Controls

Controls include encrypting data at rest, enforcing key lengths, security contacts, and firewall associations.

Compliance and Risk Reduction

Adopting FSBP reduces vulnerabilities and simplifies compliance with regulatory requirements.

CONTINUOUS MONITORING



10/23/2025

SECURITY BACKBONE: DATA TRIANGULATION FOR AUDITING

Central Security Management

Security Hub centralizes posture management by running compliance checks and aggregating security findings in real time.

Resource Configuration Tracking

AWS Config tracks resource states over time, providing a detailed configuration history critical for auditing.

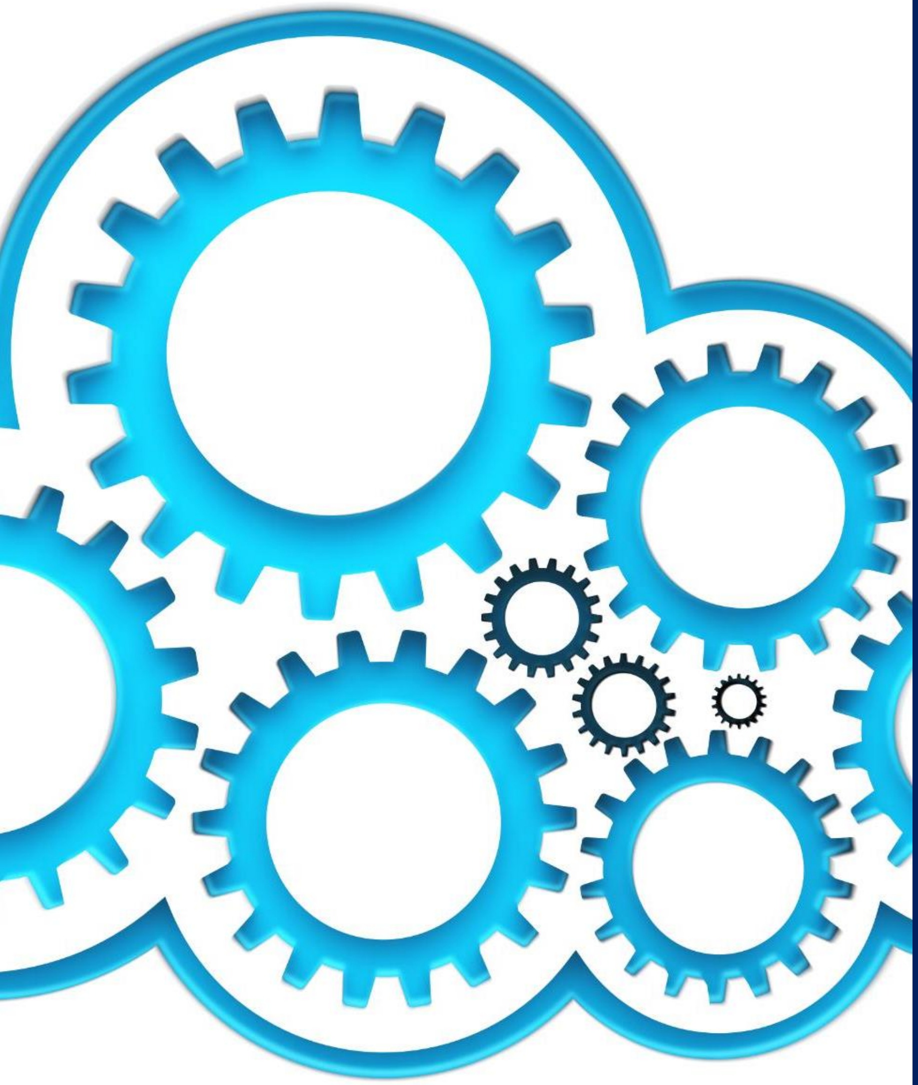
User Activity Logging

CloudTrail logs user activities, providing non-repudiation evidence of user actions for audit trails.

Automated Audit Reporting

AWS Audit Manager compiles data from services into audit-ready reports for compliance and monitoring.

ARCHITECTURAL ACCELERATION



AUTOMATED GOVERNANCE WITH CONTROL TOWER & CFCT

Automated Governance

Control Tower and CfCT automate governance to ensure compliance from account creation.

Preventative Guardrails

Service Control Policies block high-risk actions like disabling CloudTrail to maintain security.

Standardized Configurations

CloudFormation StackSets deploy standardized resource stacks for logging and IAM roles.

Lifecycle Event Workflow

The Control Tower Lifecycle Event Workflow triggers CfCT pipelines to apply compliance automatically.

EVIDENCE LAYER

AUTOMATED AUDITING WITH AUDIT MANAGER

SERVICE	GRC FUNCTION	OUTPUT/VALUE PROPOSITION
Security Hub	Continuous Monitoring	Findings used as evidence of control effectiveness.
Audit Manager	Automated Evidence Collection	Generates audit-ready assessment reports against standards (e.g., HIPAA, PCI DSS).
AWS Artifact	Documentation Retrieval	Provides proof of Inherited Controls (AWS's compliance).

STRATEGIC COMPLIANCE MAPPING

MEETING GLOBAL STANDARDS WITH AWS CERTIFICATIONS

Healthcare Compliance Support

AWS supports HIPAA/HITECH compliance using Business Associate Agreements and Audit Manager frameworks tailored for healthcare.

Retail and Finance Certifications

PCI DSS Level 1 certification in retail and finance is enabled by AWS infrastructure certifications and Audit Manager evidence.

GDPR and Data Protection

AWS supports GDPR compliance through ISO 27018 and encryption controls ensuring data residency and privacy.

Strategic Compliance Overlap

Overlapping controls like FSBP simplify achieving multiple certifications such as SOC 2, ISO 27001, and HIPAA.

PRESCRIPTIVE ROADMAP

FROM DEBT TO VELOCITY: 4-PHASE STRATEGY

Phase 1: Foundation Setup

Deploy Security Hub and activate FSBP standard to build a strong compliance foundation.

Phase 2: Architectural Lock-Down

Implement governance with Control Tower, CfCT, SCPs, and StackSets to secure architecture.

Phase 3: Automation Integration

Integrate Audit Manager with Config, CloudTrail, and Security Hub for automated compliance checks.

Phase 4: Acceleration & Expertise

Leverage GSCA program and partner resources to accelerate compliance and enforcement.

LONG-TERM GRC EFFICIENCY & CALL TO ACTION

Sustainable Compliance Through Automation

Automation enables continuous compliance, making it sustainable and efficient for long-term governance.

Preventative vs Reactive Measures

Prioritize preventative controls like Control Tower and CfCT instead of reactive detection and remediation.

Integrated Compliance Tools

Combining Security Hub, Config, CloudTrail, and Audit Manager creates a self-reporting and governance environment.

Pilot Deployment & Next Steps

Initiate pilot deployment on critical units and define compliance frameworks for scalable GRC efficiency.