Compliance-Aware Platform Engineering

Scaling Hybrid Cloud Automation in Regulated Financial Environments

Satish Manchana | UBS

Today's Agenda

01

The Compliance Challenge

Understanding the unique regulatory pressures in financial environments

02

Platform Engineering Evolution

From DevOps to DevSecOps to ComplianceOps

03

Implementation Blueprint

Practical approaches to embedding compliance into your infrastructure

04

Case Studies & Takeaways

Real-world examples and actionable insights

By the end of this session, you'll have a comprehensive roadmap for automating compliance at scale in hybrid cloud environments.

The Financial Services Compliance Landscape

Beyond Traditional IT Concerns

In financial services, infrastructure must address security, traceability, and regulatory alignment alongside uptime and performance metrics.

Regulatory Framework Complexity

SOX, MiFID II, MAS, GDPR, and industry-specific requirements create a multi-dimensional compliance matrix that must be systematically addressed.

Audit Readiness

Financial institutions must maintain continuous audit readiness with comprehensive documentation and evidence of controls.

The stakes are exceptionally high: non-compliance can result in significant financial penalties, reputational damage, and regulatory restrictions.

The Evolution of Platform Engineering

DevOps

Initial focus on deployment speed, automation, and breaking down dev/ops silos

DevSecOps

Security integration into pipelines with vulnerability scanning and SAST/DAST testing

ComplianceOps

Systematic embedding of regulatory requirements into every infrastructure component

The financial sector requires this final evolution to ComplianceOps, where compliance isn't a checkpoint but embedded throughout the entire infrastructure lifecycle.

Building Secure, Hybrid IaaS Provisioning Frameworks

Policy Definition

Translate regulatory requirements into technical specifications and controls

Infrastructure as Code

Implement controls using HashiCorp Terraform, CloudFormation, etc.

Compliance Validation

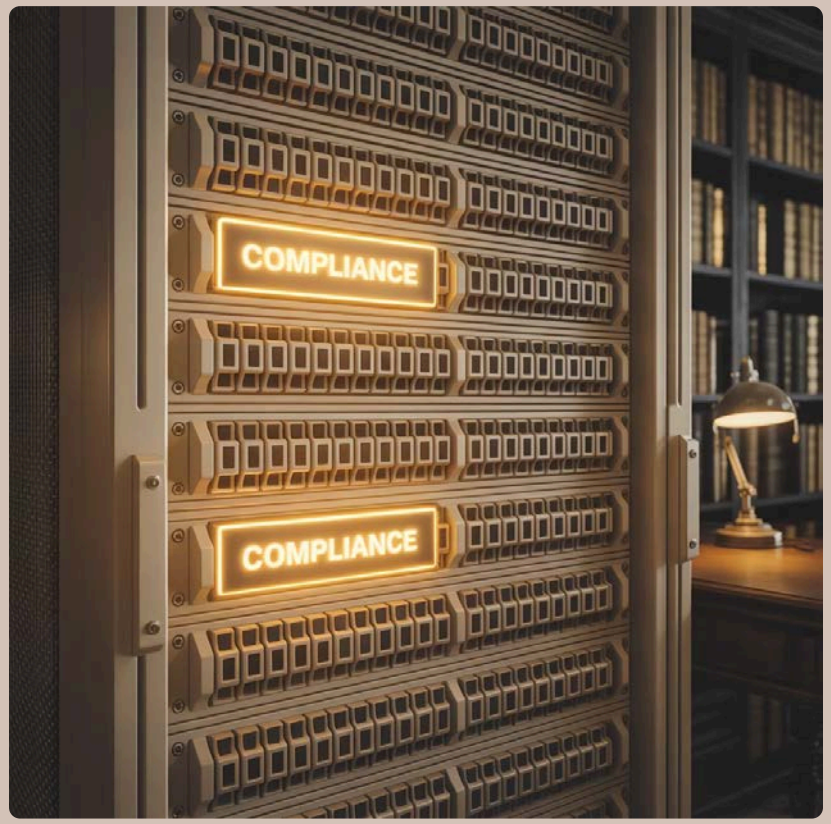
Automated testing of controls against defined policies

Evidence Generation

Automatic documentation and audit trail creation

By establishing this framework, organizations can provision compliant infrastructure consistently across public cloud (AWS, Azure, GCP) and private cloud environments, maintaining control while enabling agility.

Golden Image Creation with Compliance Baked In



Automated Image Pipeline

Using HashiCorp Packer to create standardized, compliant images for all deployment environments:

- CIS/IHSA baseline hardening automatically applied
- Security agents pre-installed and configured
- Logging and monitoring tools pre-configured
- Versioned and immutable for auditability
- Distributed via Azure Compute Gallery or AWS AMI

Golden images eliminate drift and ensure every deployed workload starts from a verified, compliant baseline, reducing security gaps and audit exceptions.

Automated Compliance Gates in CI/CD

1 **Code Commit**

Infrastructure code checked against policy templates using pre-commit hooks

2 **Build Pipeline**

Jenkins/Odyssey workflows validate compliance with regulatory requirements

3 **Approval Gates**

Automated or manual approvals based on compliance scan results

4 **Deployment**

PowerShell automation ensuring proper documentation and evidence generation

5 **Runtime Monitoring**

Continuous validation of compliance posture post-deployment

By integrating compliance validation at each stage, violations are caught early when they're easier and less expensive to remediate.

Policy-as-Code: The Cornerstone of ComplianceOps

Key Technologies

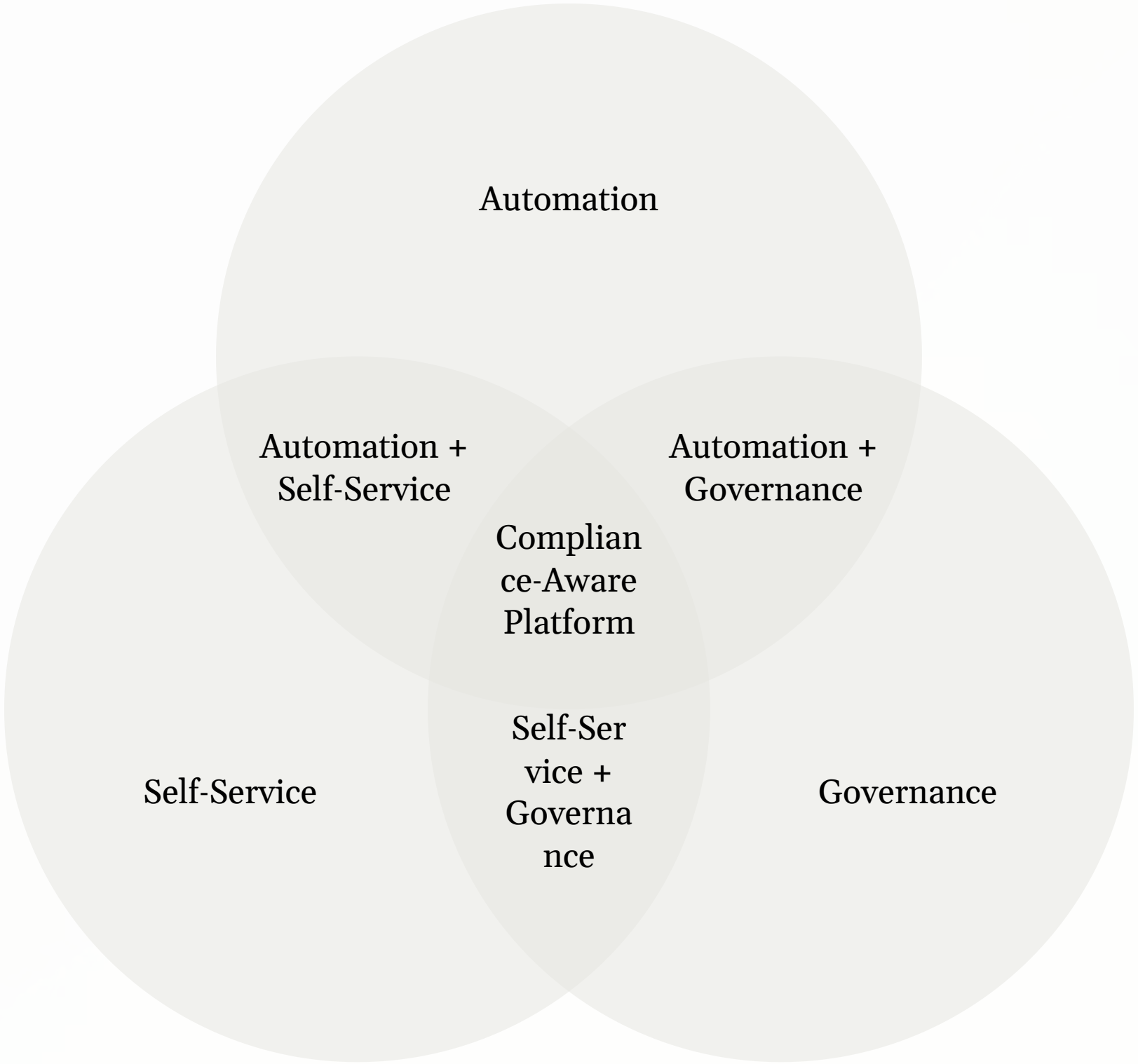
- HashiCorp Sentinel
- Open Policy Agent (OPA)
- AWS Config Rules
- Azure Policy
- Custom PowerShell compliance modules

Implementation Approach

- Create a policy registry mapped to regulatory requirements
- Version control all policies
- Implement automated testing for policy logic
- Build standardized remediation workflows
- Generate compliance evidence automatically

Policy-as-Code transforms abstract regulatory requirements into executable, testable code that can be applied consistently across environments. This approach ensures that compliance is both verifiable and scalable.

Enabling Self-Service While Preserving Compliance



The intersection of these three elements creates a powerful, scalable approach to infrastructure that satisfies both engineering and compliance teams. By embedding compliance into self-service platforms, organizations can maintain velocity while ensuring regulatory requirements are continuously met.

Case Study: Leading Financial Organization Hybrid Cloud Transformation

Challenge

Managing thousands of workloads across multiple regulatory jurisdictions while transitioning to a hybrid cloud model

Approach

Implemented a compliance-aware platform with automated golden image creation, standardized provisioning, and policy-as-code enforcement

Results

85% reduction in compliance exceptions, 60% faster infrastructure provisioning, and significantly improved audit outcomes

Implementation Roadmap

Assess Current State

Map existing compliance requirements and identify automation opportunities

Define ComplianceOps Strategy

Create a roadmap for tools, processes, and organizational changes

Implement Foundation

Establish golden image pipeline and policy-as-code framework

Scale & Integrate

Expand coverage across environments and integrate with existing workflows

Measure & Improve

Track compliance metrics and continuously enhance automation

Start small with a focused pilot project, prove the concept, then expand systematically across your infrastructure estate.

Key Takeaways

- [ ] **Compliance is a design principle, not an afterthought**

  Build regulatory requirements into your infrastructure from day one

- [ ] **Automation is essential for scalable compliance**

  Manual processes cannot keep pace with modern infrastructure demands

- [ ] **ComplianceOps is the natural evolution for regulated environments**

  Financial services must move beyond DevSecOps to remain competitive

- [ ] **Self-service and compliance can coexist**

  Well-designed platforms enable both speed and regulatory alignment