CASE STUDY · CHASE UK

How Chase UK Made Kubernetes Audit-Ready with Kyverno Policy as Code

Chase UK made Kubernetes audit-ready by replacing a manual compliance process with Kyverno policies enforced in every cluster from the day it is built. Policy reports feed one Grafana dashboard for developers, security teams and auditors.

46	50	<20 ms	7–8 months
KYVERNO POLICIES, UP FROM 4	CLUSTERS	AVERAGE ADMISSION LATENCY	ENGINEERING EFFORT SAVED (ESTIMATE)

CUSTOMER	LAUNCHED	PLATFORM	REPLACED	STACK
Chase UK (JPMorganChase)	September 2021	About 50 clusters and 2,000 nodes	OPA Gatekeeper	Kyverno, Prometheus, Thanos, Grafana

§01 CHALLENGE

What made compliance hard at Chase UK?

Chase UK launched in September 2021 and now has more than 2.5 million customers and over £20 billion in deposits. The platform behind it runs hundreds of services on about 50 clusters and 2,000 nodes, and independent backend teams ship to it every day.

When security or audit teams asked how the environment was configured, the platform team answered with quarterly reports, spreadsheets and the output of kubectl commands. Requirements arrived ad hoc as the bank grew, the work was manual, and no two reports looked the same.

BEFORE	PROBLEM
Reactive compliance	Questions answered only when security or audit asked
Manual auditing	Spreadsheets and kubectl output, assembled by hand
No standard reporting	Each stakeholder got a different, inconsistent answer

OPA Gatekeeper had been in place since before launch. Over roughly four years it produced four policies in production. Rego expertise was scarce, the engineers who had written those policies had left the team, and every change depended on a small group of platform and security engineers. Without reporting, there was no developer ownership of failing resources either.

> **“…didn’t have a compliance system, we actually had a compliance process.”**
>
> **Nischay Goyal** SENIOR LEAD PLATFORM ENGINEER, CHASE UK (JPMORGANCHASE)

§02 SOLUTION

The audit-ready Kubernetes stack

Chase UK chose Kyverno because it is Kubernetes-native (YAML and CRDs), has no Rego learning curve, and comes with built-in reporting, Enforce, Audit and Warn modes, and policy exceptions as first-class resources. In banking, “100% compliance” doesn’t mean every workload meets every policy. It means 100% of the risk is managed: the remaining 1% needs a documented, reviewable exception, not a back door.

The stack is deliberately simple:

LAYER	TOOL	ROLE
Enforcement	Kyverno admission controller	Part of the base cluster definition, present in every cluster from the moment it is built
Results	Kyverno policy reports	Pass, fail and skip results per resource, policy and rule
Metrics	Prometheus, Thanos	Collect and aggregate results across clusters
Reporting	Grafana	One dashboard for every audience

One Grafana dashboard, filtered per audience, serves everyone: security engineers filter by policy category, team leads by namespace, platform engineers by a single policy before rolling it out, and developers use a violations panel that lists the cluster, namespace, resource kind and name, policy, rule and category in one row.

The move started with an audit finding in 2023. Nischay took the problem from research to production in a month, which he stressed is fast for a bank. The team migrated the four existing policies and decommissioned OPA Gatekeeper the same year. Kyverno has now run in Chase UK’s clusters for almost three years, with average admission latency across the estate under 20 milliseconds.

§03 RESULTS

What Chase UK got from it

The bank has grown from 4 policies to 46 across 50 clusters. The bigger change was cultural: any developer or security engineer can open a pull request with a new policy for review, instead of filing a ticket and waiting for the platform team.

YEAR	POLICIES	FOCUS
2021	4	Chase UK launches; policies on OPA Gatekeeper
2023	6	Migration to Kyverno; engineering practices; Istio
2024	30	Pod Security Policy replacement; mutation policies
2025	44	Networking
2026	46	Multi-region compliance

Nischay estimates roughly 7–8 months of engineering effort saved: 30% from engineering best practices, 25% from self-service audits, 25% from preventing misconfigurations and 20% from automation and cleanup. Before each Kubernetes upgrade, a policy shows which applications still use deprecated APIs, and cleanup policies removed dangling resources.

And the result that mattered most: the auditors were happy, which Nischay called one of the hardest KPIs to meet.

§04 LESSONS

Three lessons for your own rollout

01. **Test policies in CI.** One policy can affect a whole cluster. Every Chase UK policy now ships with test cases, and the Kyverno CLI runs them in a pipeline.
02. **Start in enforce mode when you can.** A policy that starts in audit mode can take ages to reach enforcement. Enforcing from day one means new resources are always compliant.
03. **Keep scope and exceptions apart.** A policy's match rules skip resources outside its scope, and an exception also produces a skip. Make the two easy to tell apart in your reports.



Nirmata created Kyverno, the CNCF graduated policy engine for Kubernetes. We help platform and security teams govern clusters, workloads, and AI agents with policy as code.

WATCH THE TALK

Audit-Ready Kubernetes: How Chase UK Leveraged Policy as Code for Continuous Compliance, Jim Bugwadia and Nischay Goyal

youtube.com/watch?v=B01BQ60PLqM

READ THE FULL STORY

How Chase UK Made Kubernetes Audit-Ready with Kyverno Policy as Code

nirmata.com/2026/10/22/how-chase-uk-made-kubernetes-audit-ready-with-kyverno

TALK TO THE KYVERNO MAINTAINERS

nirmata.com/request-a-demo

© 2026 Nirmata, Inc. Kyverno is a CNCF graduated project. Kubernetes is a registered trademark of The Linux Foundation.