kualitee

www.kualitee.com



CASE STUDY

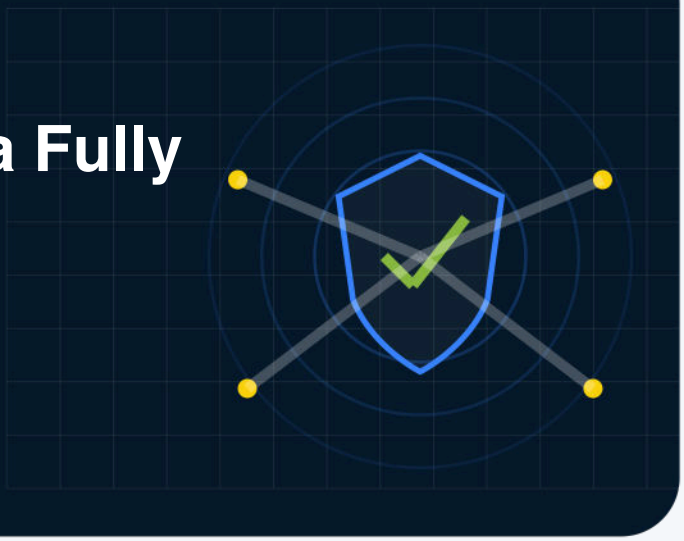
A Gulf Bank Moves to a Fully On-Premise Kualitee Deployment

How a regulated bank kept all of its test data within its own infrastructure while meeting strict banking compliance requirements.

INDUSTRY	REGION	DATA MIGRATION
Banking	Gulf	No added cost

kualitee

A Gulf Bank Moves to a Fully On-Premise Kualitee Deployment



Client Snapshot

The client is a bank operating in the Gulf region, where financial institutions are held to strict security and data protection standards.

As with most banks in this market, the client's IT and compliance teams operate under a mandate that any core software infrastructure, including tools used for internal test management, must meet a specific set of regulatory and security requirements before it can be adopted.

Background

Before approaching Kualitee, the client had no dedicated test management platform in place that could satisfy their security posture. Given the nature of their business, a standard cloud-hosted SaaS solution was not an option.

Banks in the Gulf region typically operate under regulatory frameworks that require sensitive data, including test data tied to core banking systems, to remain within infrastructure the institution directly controls. This ruled out any vendor whose only offering was a shared, cloud-hosted product.

The Challenge

The client's requirements were shaped almost entirely by their regulatory environment rather than by feature gaps in any specific competing tool. Their problem statement centered on two connected needs:

On-premise deployment for security reasons.

As a bank, the client could not have their test data, requirements, or defect records hosted on third-party cloud servers. Any test management solution had to be deployable entirely within their own infrastructure, under their own security controls.

A compliant testing infrastructure.

Beyond simply being on-premise, the platform had to be set up in a way that satisfied the compliance obligations specific to banking institutions in the Gulf, including PCI-DSS for payment data security, GDPR for data protection given their international customer base, the SAMA Cybersecurity Framework, and additional regional regulatory requirements banks in the Gulf are held to.

For a bank, these aren't preferences but hard requirements. Any vendor unable to deploy on-premise, or unable to demonstrate alignment with these compliance frameworks, would have been disqualified from consideration regardless of feature set.

Why They Moved to Kualitee

Kualitee was brought in specifically because it could offer a genuine on-premise deployment model rather than a cloud-only product with limited configuration options. This made it one of the few test management platforms able to meet the client's non negotiable security and compliance requirements from the outset.



The Solution

Kualitee's team worked directly with the client to stand up a fully on-premise instance of the platform, built around their compliance obligations:

- **On-premise infrastructure setup.** Kualitee's team deployed the platform's servers locally within the client's own environment, rather than relying on any external hosting. This gave the client full control over where their testing data lived and how it was secured, satisfying the core requirement that drove them to seek an on-premise solution in the first place.
- **Compliance-aligned deployment.** The infrastructure was set up in a way that supported the client's obligations under PCI-DSS, GDPR, and the SAMA Cybersecurity Framework, along with the other regional regulatory requirements the client operates under as a Gulf-based bank.
- **Free data migration.** As with other clients transitioning to Kualitee, the client's existing test data was migrated onto the new on-premise instance at no additional cost, minimizing the burden of the switch on their internal teams.

Ongoing Maintenance for On-Premise Deployments

Unlike cloud-hosted clients, who receive new features automatically as Kualitee rolls them out, on-premise clients such as this one operate under a different update model by necessity. Kualitee cannot push updates directly into infrastructure it does not host. Instead:

- Feature updates are deployed manually into the client's local infrastructure.
- Updates are typically delivered on a biannual or annual basis, or whenever the client specifically requests a new set of features.
- No update or new feature is deployed to the client's on-premise environment without their explicit consent, given the sensitivity of the systems involved.

This model gives the client full control over when and how their environment changes, which matters considerably for an institution operating under strict change management and compliance obligations.

The Outcome

With Kualitee deployed on-premise, the client now has a test management platform that operates entirely within infrastructure they control, without compromising on functionality relative to Kualitee's cloud offering:



- A fully self-hosted testing environment that keeps all test data within the client's own security perimeter
- A deployment aligned with PCI-DSS, GDPR, the SAMA Cybersecurity Framework, and other applicable regional banking regulations
- Existing test data migrated in at no cost, with no gap in the team's ability to continue their testing work
- A predictable, consent-based update model that respects the change-control requirements of a regulated banking environment

Looking Ahead

The relationship with this client continues on Kualitee's manual update cycle, with new features deployed into their on-premise environment as they request them. This ongoing, opt-in approach reflects the level of control a banking client in a highly regulated market needs to maintain over their own core systems.