Atlassian Cloud in a Bank

Secure migration from Atlassian Data Center in the context of regulations (including DORA) and operational practice

Version: 1.0 | **Date:** 2026-01-20 | **Purpose:** educational and factual (no promotional content)

Table of content

1. Why this topic is back on the table right now

In many banks, Jira and Confluence (and related Atlassian tools) are part of the organization's "circulatory system": they support software development, change management, incident handling, documentation, audits, and collaboration between IT and the business.

At the same time, pressure is increasing to move away from running self-managed application infrastructure (Data Center) toward a service model (SaaS). This shift has two main drivers:

- **Vendor product direction**
  – Atlassian is moving innovation to the cloud (including AI and new platform capabilities) and has announced a timeline for ending Data Center sales and ultimately reaching end of life.
- **Regulatory context and operational risk**
  – as of January 17, 2025, DORA is in force, tightening requirements for ICT operational resilience, incident management, and third-party oversight, including cloud services.

This whitepaper structures the fundamentals and shows how to approach the migration from a bank perspective: not as an "IT project," but as a change in the service delivery model—with consequences for risk, compliance, security, and operations.

2. What Atlassian Cloud is (in practice, not marketing)

Atlassian Cloud

is a SaaS model: the bank uses applications (e.g., Jira, Confluence, Jira Service Management), while responsibility for the infrastructure layer and a significant portion of operations sits with the service provider.

2.1 Where it runs (infrastructure and multi-cloud)

Atlassian publicly states that its cloud applications are hosted on **Amazon Web Services (AWS)**. Atlassian has also announced a partnership with **Google Cloud** as part of a multi-cloud strategy (hosting selected applications on Google Cloud in the future).

Implication for banks: in third-party risk assessment, you must evaluate not only Atlassian as a SaaS provider, but also the infrastructure dependency chain (hyperscalers).

2.2 Data residency (where the data "lives")

Atlassian Cloud includes a **data residency** mechanism that lets you select the region where "in-scope app data" is stored for selected products (including Jira, Jira Service Management, and Confluence).

Implication for banks: data residency can support data location requirements, but it does not automatically address everything (e.g., logs, metadata, Marketplace app data, integrations, and data flows to external systems).

2.3 Compliance reports and audits

Atlassian publishes information about the availability of **SOC 2** reports and its approach to compliance audits for cloud services.

Implication for banks: this is an input to vendor assessment, but the bank still needs its own control mapping: what is the provider's responsibility, and what remains the bank's responsibility **(shared responsibility model)**.

3. Data Center vs. Cloud – differences that truly matter during migration

The table below is intentionally "plain." It highlights areas that typically generate the most questions and risk in banks.

Table 1. Key operational differences

Area	Data Center (on-prem / self-managed)	Atlassian Cloud (SaaS)	What it means in a bank
Infrastructure operations	Bank responsibility	Provider responsibility	Operational model and control changes
Updates	Bank-planned (maintenance windows, testing)	Cyclical, provider-managed	Regression testing and change communication must be redesigned
Platform security	Patching and hardening by the bank	Largely provider responsibility	Control emphasis shifts from "implement" to "verify and enforce"
Configuration & customization	Often extensive (apps, scripts, modifications)	Partly limited / different logic	Must map "must-have" vs "habit"
Marketplace apps	Many DC apps	Not always 1:1 cloud equivalents	One of the most common migration blockers
Integrations	Local, often tightly coupled	API integrations + access policies	Requires review of IAM, tokens, data flows
Backups	Bank designs and tests	Provider model + options	Must align to bank RTO RPO and audit requirement

4. Data Center phase-out timeline: what is a hard date vs. a risk

Atlassian has published milestones related to ending Data Center sales and end of life (including the Data Center Marketplace).

Table 2. Key dates (per Atlassian public communications)

Milestone	Meaning
December 16, 2025	No new Data Center apps can be submitted to Marketplace
March 30, 2026	End of sales for new Data Center subscriptions and DC apps for new customers
March 30, 2028	Last date to purchase/expand Data Center licenses and apps for existing customers
March 28, 2029	Data Center end of life: subscriptions expire; products move to read-only mode

What this means for a bank "right now":

If your environment is complex (many projects, workflows, automations, apps), "we have time until 2029" can be misleading – because the biggest effort is typically not moving the data but untangling dependencies and closing risk items.

5. DORA and migration to Atlassian Cloud – connecting the dots without shortcuts

5.1 What DORA is (in one paragraph)

DORA (Digital Operational Resilience Act) is an EU regulation that has applied since **January 17, 2025**. It strengthens requirements for financial entities in ICT risk management, incident management, resilience testing, and oversight of ICT third-party providers (including cloud providers).

5.2 Why Atlassian migration is a “DORA project,” even if it starts in IT

Maciej Szostek
Competency Center Director

Because you are moving a tool that often:

- stores operational data about incidents, changes, defects, and risks,
- is part of the digital service delivery chain,
- integrates with code repositories, CI/CD pipelines, ITSM tools, and monitoring.

5.3 Third-party risk and “critical providers”

DORA introduces enhanced oversight of critical ICT third-party providers. In practice, EU regulators may designate certain entities as critical for the financial sector. In 2025, public reporting noted, among other things, the designation of major cloud providers as “critical” for the EU financial market.

Implication: even if Atlassian is not a hyperscaler, the bank must assess the full-service delivery chain (SaaS + infrastructure + subcontractors + integrations).

6. Mapping DORA to real migration work (concrete, not theoretical)

Table 3. DORA → what to include in an Atlassian migration

DORA areas	Control questions	Migration project implications
ICT risk management	Are Jira/Confluence classified as supporting a critical process? What data do they process?	Data classification, permission models, data minimization, logging and monitoring
Incidents and reporting	How will the bank detect and classify incidents in a SaaS service? How does the provider report events?	Triage, escalation, supplier collaboration, audit evidence, response times
Resilience testing	How do we test outage and continuity scenarios for SaaS and integrations?	Test plan for app + IAM + integrations + dependencies + workaround procedures
ICT third-party management	Does the contract provide audit rights, subcontractor transparency, BCP requirements, SLAs?	Legal/procurement work in parallel with IT; required clause templates and an exit plan
Exit strategy	How will the bank recreate processes and data outside Atlassian? How fast? In what format?	Export and archiving design, reverse migration/alternatives, recoverability testing

7. Most common bank concerns (and how to tackle them like engineers)

This is not a reassurance list. These are topics you must work through, gather evidence for, and close with a decision.

Functionality and customization

Concern: "In DC we have X apps and Y automations. Cloud won't replicate it."

Approach:

- Inventory apps and automations (what is critical vs. "nice to have")
- Map: cloud equivalent / substitute / retire / redesign the process
- Run a proof of concept on selected projects

Third parties and contracts

Concern: "DORA requires hard commitments, while SaaS has standard terms."

Approach:

- Clause checklist (audit, subcontractors, incident communications, BCP, exit)
- Define the control model and cyclical vendor assessment
- Ensure consistency with the bank's vendor management policy

Data and compliance (including data residency)

Concern: "Where is the data, who can access it, how do we ensure auditability?"

Approach:

- Data classification (what may go into Jira/ Confluence and what must not)
- Permissions policies, SSO/MFA, admin roles
- Confirm data residency mechanisms and analyze out-of-scope data (integrations, apps)

User experience and operational change

Concern: "It won't be the same. People will lose habits; support will change."

Approach:

- Communication and training plan (admins, power users, end users)
- Migration windows vs. transition period
- A clear "definition of readiness": when the bank considers the service stable

8. A reference migration model (phases, artifacts, quality criteria)

This model is applicable regardless of scale (what changes most is the timeline and number of iterations).

PHASE 1

Analysis and inventory

Outputs (artifacts):

- Instance and project map
- List of apps and integrations
- Data and risk classification
- List of regulatory/operational requirements (including DORA)

PHASE 2

Migration design and governance

Outputs:

- Roles and responsibilities (IT, security, compliance, legal, procurement)
- Communication plan
- Success criteria definition (functional and control-related)

PHASE 3

Pre-test migration (pilot)

Outputs:

- First mapping of apps and workflows
- Captured functional gaps
- Change plan (what we redesign vs. what stays)

PHASE 4

Test migration (full control layer)

Outputs:

- Test results: permissions, integrations, reports, automations
- Verification of audit evidence and logging
- Production migration runbook

PHASE 5

Production migration

Outputs:

- Data integrity confirmation
- Stabilization and support plan
- Plan to decommission/archive DC components

PHASE 6

Stabilization and optimization

Outputs:

- Quality monitoring (performance, incidents, feedback)
- Operational processes finalized
- First revision of the exit strategy and recoverability testing

9. Bank readiness checklist (quick scan)

Table 4. Minimum to have before deciding “we’re migrating”

Area	Questions	Status
Scope	Do we have a list of instances/projects/ apps/integrations?	✓ / ✓
Data	Do we have data classification and rules for what may go into Atlassian?	✓ / ✓
IAM	Do we have a target model for SSO/MFA/admin roles?	✓ / ✓
DORA	Do we have DORA requirements mapped to controls and processes?	✓ / ✓
Contracts	Do we have a clause checklist for audit, incidents, BCP, exit?	✓ / ✓
Testing	Do we have a functional + control test plan (security/compliance)?	✓ / ✓
Migration	Do we have a runbook and a rollback/ contingency plan?	✓ / ✓
Operations	Do we know how L1–L3 support and vendor escalation will work?	✓ / ✓

10. Summary: how to think about this migration to avoid the traps

Migrating from Atlassian Data Center to Atlassian Cloud in a bank is not “moving an application.” It is a change in the operating model that impacts:

- responsibilities (shared responsibility),
- controls and audit,
- incident management,
- resilience testing,
- vendor relationship and exit strategy.

DORA strengthens these areas and makes it clear that a decision to adopt SaaS for work tools (such as Jira/Confluence) must be tightly connected to governance, vendor management, and cybersecurity – not just the IT roadmap.

Michał Żelazowski
Senior Head
of Industry

Are you looking for support? Contact Sii!

Get to know our offer

With over 7 500 Power People, Sii is the leading technology consulting, digital transformation, engineering, and business services vendor in Poland.