

A PRACTICAL GUIDE · AUGUST 2026

Jira Cloud migration for banks and regulated enterprises

What moves and what does not, the app estate, the regulated layer, the migration itself — and what Atlassian will help pay for. Written for platform owners and IT leaders running Jira Data Center in a regulated firm.



01

Why this guide, why now

Atlassian has put fixed dates on Data Center's life. New customers have been unable to buy Data Center subscriptions or Data Center Marketplace apps since 30 March 2026. Existing customers can renew, expand and buy apps only until 30 March 2028. On 28 March 2029, Data Center subscriptions and their Marketplace apps expire and instances become read-only. Atlassian commits to technical support and critical security fixes until that date; beyond it, extended maintenance exists only "by exception", negotiated through an Account Executive. Those dates anchor everything else in this guide — we will not keep repeating them, but every timeline below runs backwards from them.

For most organisations, 2029 sounds comfortable. For a bank, it is not — and the arithmetic is worth doing honestly.

Atlassian's own end-to-end estimates for a lift-and-shift migration are roughly four months for up to 5,000 users, roughly six months for 5,000 to 10,000, and six-plus months above that — and it does not recommend lift-and-shift at all beyond 10,000 users. Its FastShift programme was created precisely because typical enterprise migrations run 12 to 16 months. Those figures assume an organisation that can simply decide and go.

A regulated enterprise cannot simply decide and go. Before a single project moves, you need vendor onboarding and security review of Atlassian and of every Marketplace vendor whose app carries your data. Under DORA, a cloud arrangement supporting a critical or important function needs a pre-contract risk assessment, and your competent authority may need to be informed of the planned arrangement in a timely manner — before signature, not after cutover. Then the migration itself must pass a change board, land in agreed change windows, and leave an audit trail. Each of those steps has its own queue.

Stack them up and the honest conclusion is this: an estate that must be fully off Data Center by early 2029, with app renewals ending in early 2028, needs its assessment done and its plan approved now. The real decision point is not 2029. It has, for practical purposes, already arrived. There is also a reason to move early rather than merely on time: Atlassian's migration incentives — covered in section 7 — are richest for those who commit before the crowd, and one of them expires in mid-2027.

02

What actually moves — and what does not

The Jira Cloud Migration Assistant (JCMA) is Atlassian's recommended tool for moving Jira Server and Data Center data to Cloud. It is bundled with Jira 8.14 and later, supports Jira Core, Jira Software, Jira Service Management and Advanced Roadmaps plans, and offers app assessment, user and email checks, pre-migration checks with error reports, and the choice between migrating everything at once or building a selective migration plan. A pre-migration report shows exactly what a run will include, and Atlassian retains migration data for just 14 days after a migration plan is created — a detail your data-protection team will want in writing.

Used within its scope, JCMA is genuinely capable. At project level it moves project details, issue types and schemes, workflows and workflow schemes, permission, notification and issue security schemes, field configurations, screens and standard custom fields. At issue level it moves the things auditors care about: comments (including security-restricted ones), attachments, work logs, issue history, links and issue key

history, plus watchers, votes, sprints, versions and epics. For Jira Service Management it carries request types, queues, SLAs, approvals, customer organisations and portal settings, and it can migrate unlicensed portal customers as a distinct step.

Now the other column — because a bank plans around what a tool does not do, not around its brochure.

JCMA does not migrate dashboards or filter subscriptions; they are rebuilt in Cloud. It does not migrate cross-project boards, cross-project filters, boards owned by inactive users, or Kanban sub-filters.

Webhooks, custom events, user-defined notification events and custom issue-type icons stay behind.

Users arrive without avatars or passwords — expect a reset unless SSO is in place — and deleted Server users surface as "Former user". Advanced Roadmaps plans migrate, but only after their issue sources have moved, and classic plans, scenarios, saved views and programmes do not come across at all.

Two behaviours deserve particular attention in a regulated environment. First, accounts are keyed on unique email address: if an address already exists on the destination site, migrated data is linked to that existing account. Clean directories are therefore a precondition, not a nicety. Second, groups are linked by name, and on re-migration JCMA only ever adds members — it never removes them. A user removed from an admin group on the source can remain in the matching privileged Cloud group. Atlassian documents this as a permission-escalation risk; your access-recertification process should treat post-migration group review as mandatory.

And then the largest gap of all: app data. Custom fields provided by Marketplace apps, and app data generally, do not migrate unless the app's vendor has built a migration path. That single sentence drives more migration effort in real estates than everything above combined — which is why it gets its own section.

03

The app estate: triage before trust

JCMA's "Assess your apps" screen inventories every installed Marketplace app, showing Cloud availability, a migration path, usage, and a decision column. Atlassian's own triage is three-way — "Needed in cloud", "Not needed in cloud", "Choose alternative". In practice we run a four-way triage: **keep** (Cloud version, adequate parity, workable data path), **replace** (a better Cloud-native or alternative app), **rebuild** (re-implement the capability on Jira's native Automation or on Forge), and **retire** (usage data says nobody will miss it). The fourth option is used more often than app vendors would like.

Read the assessment columns sceptically, because they encode two traps.

"Cloud version exists" does not mean your data moves. Migration paths range from "Automated" — where Atlassian further grades apps into Stage 2 (demonstrated high success rates) and Stage 1 (unknown or low success rates) — through "Install-only" (the app's data lives inside core Jira data and moves with it), to "Contact vendor", which usually means a Cloud app exists but no data path does. If a Stage 1 migration fails, your support route is the vendor, not Atlassian.

"Cloud-compatible" does not mean feature parity. Atlassian points customers at vendor-maintained "View differences" pages for a reason: Cloud editions of the same app routinely have altered or missing features. Every kept app gets checked feature by feature against how your teams actually use it — parity claimed is not parity delivered.

Two facts matter specifically to your third-party-risk function. Atlassian states plainly that the migration assistant performs no security assessment of app data migration; that due diligence is yours. And in automated app migrations, it is the Marketplace vendor — not Atlassian — that performs the data

migration, under a vendor agreement you must accept so the vendor can access your data. Each such app is a distinct processing relationship for your DORA register and your DPO. Favourable signals to look for: SOC-style evidence on the listing's Privacy & Security tab, Cloud Fortified status, and the "Runs on Atlassian" badge, which marks Forge apps that stay entirely on Atlassian-hosted compute and storage, inherit data residency, and let admins control or block external data egress.

The hardest single item in most banking estates is scripted automation — typically ScriptRunner. Be under no illusion: this is a rewrite, not a migration. On Data Center, scripts run synchronously inside Jira's JVM against the Java API and can veto events. On Cloud, ScriptRunner runs as a separate, asynchronous service against public REST APIs; nothing runs in Jira's JVM and events cannot be vetoed. Atlassian's own guidance says Java API calls must be replaced with REST calls and scripts manually rewritten. The vendor's migration tooling automates part of the transfer — some saved filters and listeners come across, with migrated scripts arriving commented out pending rewrite — while behaviours, fragments and built-in configurations are recreated by hand; and per the vendor's own Cloud documentation, hard constraints apply, such as 240-second script timeouts and hourly minimum scheduling.

The pragmatic sequence: rebuild simple listener and post-function logic on Jira Cloud's native Automation first (noting plan-based run limits — effectively unconstrained only on Premium and Enterprise tiers), reach for the UI Modifications API and Jira expressions for behaviour-like logic, keep ScriptRunner Cloud for what genuinely needs scripting, and put bespoke in-house plugins onto Forge, whose tenancy isolation and egress restrictions are designed for exactly your security team's questions. Budget the scripting workstream separately and early — it is the one most likely to move your cutover date.

04

Clean up before you move: migrate less, migrate better

Every year a Jira instance runs, it accumulates weight: projects nobody has touched since a reorg, duplicate custom fields, near-identical workflows, inactive users, orphaned groups. Migrating that weight costs time in the cutover window, money in Cloud subscriptions, and credibility with users who arrive in a new platform carrying old clutter.

Atlassian's guidance is unambiguous: before migrating, remove unneeded projects, delete unused and duplicate custom fields, standardise workflows, and clear out inactive users, underused groups and unused apps. Two fixes are mandatory rather than advisory: duplicate email addresses, which Jira Cloud does not support and cannot migrate, and group-name conflicts between source and destination, since same-named groups are merged in Cloud — with the access consequences that implies. Sync external directories (LDAP, Crowd, your IdP) before migrating so what moves reflects reality.

Cleanup is also where Cloud's hard limits get handled ahead of time instead of as pre-flight failures: descriptions and comments over 32,767 characters are rejected, embedded HTML in field descriptions must go, and duplicate names across shared configurations should be renamed. If you run Assets in Jira Service Management, check object volumes against Cloud tier limits and the per-object-type attribute cap now, not in the cutover window.

A practical rule of thumb: sort projects by last update, archive what has been dormant for years, and migrate archived material separately from the active estate — or, for some of it, accept an export-and-retain answer instead of a migration. The best migration is the one with less in it. Fewer objects means shorter windows, fewer pre-flight errors, and a Cloud site your admins can actually govern from day one.

05

The regulated layer

This is the part generic migration guides skip, and the part your second line will read first.

Data residency. Jira, Jira Service Management and Confluence support data residency on Standard, Premium and Enterprise plans. You can pin in-scope data to the EU (Frankfurt and Dublin), Germany, the UK or Switzerland, among other realms; the default is "Global", with data placed dynamically across Atlassian's AWS regions. In-scope means issues, attachments, comments, board and sprint data, search indexes and project configuration. Out of scope — and this must appear honestly in your assessment — are user account details (name, email, avatar, held in Atlassian's global identity service), product-level app, audit and operational logs (though Atlassian Guard audit log events now support residency pinning), AI-related data, and cached content such as emails and notifications, held for up to 30 days. The sharpest caveat is apps: Marketplace app data is pinned only if the individual vendor supports residency. A Jira site pinned to Frankfurt can still have app data elsewhere. Map this app by app; do not assume the pin covers the estate. Encryption belongs in the same mapping: customer-managed encryption keys are available as an Enterprise add-on, and your assessment should say whether you need them.

The DORA paperwork. Since January 2025, DORA applies to EU financial entities, and a Jira Cloud subscription is an ICT third-party arrangement like any other. Concretely, that means: an entry in your Article 28(3) register of information — including the subcontracting chain, for which Atlassian publishes a sub-processor list and DORA-specific documentation (a contractual-requirements document and an information register) on its Trust Center; an Article 28(4) pre-contract assessment covering criticality, risk and due diligence; and, where you classify the supported function as critical or important, Article 30(3) contract terms (audit and access rights, precise service levels, transition periods) and an Article 28(8) exit strategy that is documented, tested and periodically reviewed. Whether your Jira estate supports a critical or important function is your classification call — make it explicitly and early, because the notification, contract and exit obligations all hang off it.

Two calibration points. There is no such thing as a "DORA certificate" — the regulation creates no certification scheme, so any vendor claiming one is marketing, not compliance. And Atlassian itself frames DORA as shared responsibility: it provides documentation and contractual commitments that map to the regulation's principles, but accountability for the arrangement's compliance stays with you. What Atlassian does bring to your due-diligence file: SOC 2 Type II reports (available under NDA via its Trust Center), ISO/IEC 27001:2022 certification extending to ISO 27018 controls, and — for concentration-risk analysis — the fact that its hosting layer, AWS, is itself a designated critical ICT third-party provider under DORA's oversight framework, while Atlassian is not.

The migration as a regulated change. DORA Article 9 requires documented ICT change management: changes recorded, tested, assessed, approved, implemented and verified in a controlled manner. A platform migration is squarely such a change, so run it as one. The evidence pack is written before the migration, not reconstructed after: the app assessment and decisions, residency mapping, test-migration results with measured durations, the cutover runbook with named owners, the rollback plan (which, for a phased migration, is genuinely available — the source stays intact and read-only until you stand down), and post-migration verification results. Two audit-trail specifics: export the source's records you rely on before decommissioning, and note that the Cloud organisation audit log retains activities for up to 180 days — set up regular export, or SIEM streaming via webhooks, from day one if your retention policy demands more. On Enterprise plans, release tracks let you take most visible product changes as a monthly bundle previewed in sandbox first — which is how you keep change control over a platform that would otherwise update continuously.

The migration itself

We run migrations against Atlassian's canonical six-phase model — Assess, Plan, Prep, Test, Migrate, Launch — with the regulated layer from section 5 threaded through each phase rather than bolted on. If you have read our site, the mapping is simple: Assess and Plan are our Assess; the evidence pack is Evidence, written through every phase; Prep and Test are Rehearse; Migrate and Launch are Cut over.

Assess and Plan. Full inventory (Atlassian's own assessment framework spans migration strategy, apps and customisations, growth, identity, and compliance), the app triage from section 3, method selection, and a cross-functional team with an executive sponsor and security represented from the start. For a bank-sized estate, the method question usually answers itself: Atlassian recommends lift-and-shift only below 10,000 users, assigns a dedicated Cloud Migration Manager once you commit to a migration, and strongly recommends that 1,000-plus-user migrations work with a Solution Partner and contact Atlassian one to three months before the date — depending on which of its documents you read.

Prep. The cleanup of section 4, Atlassian's pre-migration checklist worked item by item — including firewall allowlisting of Atlassian's Cloud domains, admin permissions, instance sizing, and backups of both sides — plus the Cloud site built out with apps, SSO via Atlassian Guard, verified domains and SCIM provisioning. Identity work is a full workstream here, not a checkbox.

Test. The phase that separates migrations that hold their date from migrations that slip. Never migrate only once: the pattern that works is a full test migration into a sandbox (available on Premium and Enterprise plans), validation, fixes, a second test, then production. Validation covers workflows — especially post-functions that depended on apps — permissions, boards, filters, links and app data; UAT deliberately mixes power users with occasional users and records confusion for the training plan. Atlassian publishes project-level estimates and a rough average throughput for JCMA — about five million issues per 24 hours — but no per-run duration formula, and it explicitly declines to estimate downtime; your test run is the only credible benchmark, and its measured timings go straight into the runbook alongside owners and steps. One mechanical note: JCMA does not overwrite existing Cloud data, so repeat test cycles need a site reset or deletion of previously migrated projects.

Migrate. Downtime is engineered, not endured. Users and groups migrate in advance with zero downtime. Attachments — typically the longest part of any migration — pre-migrate weeks ahead, with later runs skipping what has already moved. At cutover the source goes effectively read-only (a browse-only permission scheme plus site-wide banners), the delta migrates inside the agreed change window, and verification runs before anyone is invited in. For large estates we cut over in cohorts — per division, or active projects separately from archived ones — while respecting the hard constraints of phasing: Advanced Roadmaps needs its associated projects together, some apps require all dependent projects in the same phase, and the documented risk of phased migration is configuration drift between waves. A short freeze discipline between phases is the price of a phased approach; plan for it rather than discovering it.

Launch and hypercare. Communications, quick-start guidance, invitations (JCMA does not send them for you), office hours and a visible support channel. Then hypercare until steady state: group memberships reviewed against the escalation risk from section 2, product links re-pointed via Atlassian Administration's link-fixing tools, dashboards and subscriptions rebuilt, integrations re-keyed — entity IDs change in Cloud, and Atlassian provides an API to fetch the server-to-cloud ID mappings for exactly this. The migration is closed when your admins say so, not when the data lands.

A closing word on Confluence: it follows the same playbook through the Confluence Cloud Migration Assistant (CCMA) — spaces, permissions, macros and app dependencies get the same triage, rehearsal and cutover discipline described above. This guide focuses on Jira because in almost every estate we have seen, Jira is the pacing workstream.

Money: what the move can fund

Migration cost conversations usually start too pessimistic, because they ignore what Atlassian is putting on the table under its Ascend initiative — and what licensing optimisation recovers.

On the Atlassian side: Data Center customers qualify for a free Cloud migration trial matching their current user tier for the remaining length of their Data Center subscription, up to 12 months — your test and rehearsal environment, funded. Dual licensing lets larger customers run Cloud and Data Center in parallel during the transition without paying for both; step-up credits offset unused Data Center maintenance so you avoid double-paying; and under the Ascend initiative Atlassian has offered 10 to 20% Cloud Enterprise discounts for commitments made by June 2027 — terms are set deal by deal through Atlassian sales, so confirm with your Account Executive. All of these are arranged through Atlassian sales and eligibility varies — we validate them deal by deal rather than assuming, and so should you. For estates over 1,000 seats, the complimentary FastShift programme adds dedicated Atlassian migration resources.

On the optimisation side, Cloud's per-user billing rewards the cleanup you did in section 4: migrated users without product access do not count towards billing, so directory hygiene converts directly into subscription savings — while careless approval of group-based product access does the opposite, adding every active user in the group to the bill. Edition choice is the other lever. Enterprise brings the financially backed 99.95% uptime SLA, included Atlassian Guard Standard (enforced SSO, SCIM, audit log), multiple sites under one organisation, and the audit and release-track capabilities section 5 leans on; whether every division needs Enterprise, or a mixed-edition structure serves better, is precisely the kind of analysis that pays for itself. In our experience the honest cost picture — incentives netted against migration effort, and Cloud subscription against the true run cost of operating Data Center infrastructure to bank standards — is closer than most first drafts of the business case assume.

Discounts are available on the licensing itself, too. As a Solution Partner managing the license relationship, we can access partner pricing across Cloud editions and Marketplace apps that is not on the public price list — so before you renew anything, Data Center or Cloud, ask what the move can earn you. The worst time to discover a discount is after the invoice.

The one-page checklist

ASSESS

- ☐ Inventory the estate: projects, users, workflows, custom fields, apps, integrations, scripted automation
- ☐ Run JCMA's app assessment; triage every app keep / replace / rebuild / retire
- ☐ Classify whether the Jira estate supports a critical or important function under DORA
- ☐ Map data-residency requirements against in-scope data — and against each app's residency support

PLAN

- ☐ Confirm migration method (phased vs all-at-once) and cohort design
- ☐ Engage Atlassian (support ticket, incentives, FastShift eligibility) one to three months before the target date
- ☐ Complete DORA pre-contract assessment; update the register of information; draft the exit strategy if required
- ☐ Confirm contract terms: residency, audit rights, data return, transition periods
- ☐ Ask about migration discounts and partner pricing before renewing anything

PREP

- ☐ Clean up: archive stale projects, deduplicate fields and workflows, remove inactive users
- ☐ Fix duplicate emails and group-name conflicts; sync external directories
- ☐ Stand up the Cloud site: SSO, SCIM, verified domains, apps installed, audit-log export configured
- ☐ Assemble the evidence pack: runbook, rollback plan, residency mapping, vendor risk records

TEST

- ☐ Run at least two full test migrations; validate data, permissions, workflows, app data
- ☐ Run UAT with power users and occasional users; feed findings into training
- ☐ Measure durations and finalise the runbook with owners and timings

MIGRATE AND LAUNCH

- ☐ Pre-migrate users, groups and attachments; set the source read-only at cutover
- ☐ Verify, then invite users; re-point links and integrations; rebuild dashboards and subscriptions
- ☐ Review group memberships for escalation; run hypercare until admins confirm steady state
- ☐ Close the change with documented verification — and archive the evidence pack

About Dione Technology

Dione Technology is an independent Atlassian Solution Partner with more than a decade of enterprise delivery, including inside BNP Paribas, Société Générale, Barclays and AXA — vendor onboarding, security review and on-site delivery included. We cover the full life cycle: consulting, custom solutions and the licensing that underpins them. You work directly with the people who deliver.

The natural first step: a migration readiness assessment

A fixed-scope engagement, measured in weeks, covering full inventory and app assessment, EU data-residency and DORA mapping, cost and sequencing — including what Atlassian's incentives can fund — and a phased plan with rollback, documented for second-line review. If the right answer for your platform is "not yet", the assessment says so.

Talk to an Atlassian expert: contact@dionetechnology.net · www.dionetechnology.com

Sources

All facts in this guide derive from Atlassian's official documentation and the DORA regulation, as at August 2026. Verify current details before relying on version numbers, prices or dates:

Atlassian — Data Center end of life: atlassian.com/licensing/data-center-end-of-life

Atlassian — Cloud Migration Guide (six phases): atlassian.com/migration/cloud/guide

Atlassian — What gets migrated with JCMA: support.atlassian.com/migration/docs/what-gets-migrated-with-the-jira-cloud-migration-assistant/

Atlassian — Jira pre-migration checklist: support.atlassian.com/migration/docs/jira-pre-migration-checklist/

Atlassian — Assess apps with JCMA: support.atlassian.com/migration/docs/assess-apps-with-the-jira-cloud-migration-assistant/

Atlassian — Understand data residency: support.atlassian.com/security-and-access-policies/docs/understand-data-residency/

Atlassian — DORA compliance resources: atlassian.com/trust/compliance/resources/dora

EUR-Lex — Regulation (EU) 2022/2554 (DORA): eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554