

Halcyon Instruments: maturity profile

A mid-size manufacturer of laboratory equipment, about 3,000 employees, running Jira Software, Jira Service Management and Confluence on Atlassian Cloud Premium since a 2023 migration. Sponsor: Director of Engineering Operations. Two people in IT administer the platform part-time.

PREPARED FOR HALCYON INSTRUMENTS (FICTIONAL) · PREPARED BY VERAXENT · READOUT V1.0

SCOPE AGREED

One Jira Cloud site (Software and JSM) and its Confluence site. Bitbucket and a second regional Jira site excluded.

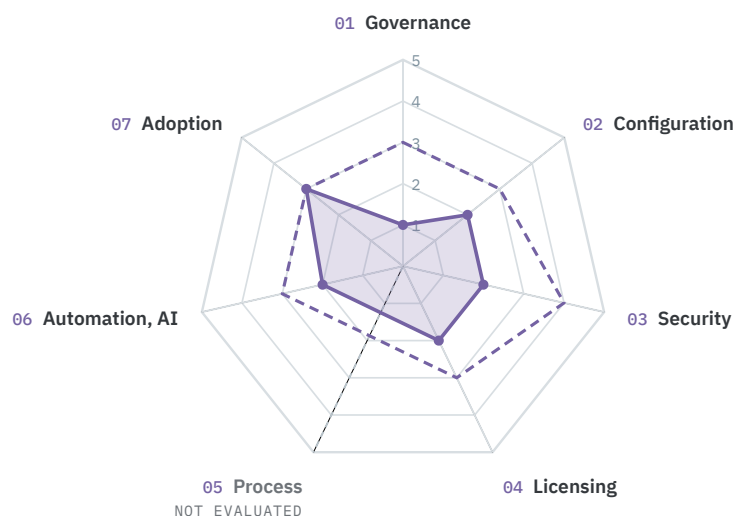
ENVIRONMENT

2,400 licensed Jira users (2,251-2,500 tier), 500 JSM agents, 118 spaces, 642 automation rules, 38 Marketplace apps, 1,140 custom fields.

EVIDENCE BASE

Three discovery sessions; product and organization admin access for 12 days; configuration, user, audit-log and automation exports.

MATURITY PROFILE



Current (measured)

----- Target if findings 1-5 are acted on. A projection, not a measurement.

FIVE-LEVEL SCALE

- Ad hoc.** No defined ownership or practice; outcomes depend on individuals.
- Reactive.** Practices exist but are inconsistent; problems are handled after they surface.
- Defined.** Documented standards and owners; applied unevenly.
- Managed.** Standards enforced and measured; exceptions are deliberate.
- Optimized.** Continuous improvement driven by data and business outcomes.

SUMMARY

Halcyon's platform works day to day, and SSO and MFA are in place. The gaps are in ownership and control: four platform owners are named on paper, but none has authority over the 29 admins, and 71 team-managed spaces run with no shared standard. Spend runs ahead of use, with 520 inactive Jira users, 387 JSM agent seats without recent agent work, and JSU licensed at the full tier for 17 workflow entities. Over-permissioned content is easy to find, through dashboards and filters shared with Anyone and visible without logging in and through Rovo search. All five findings can be started by the internal team; none requires a large engagement.

WHAT THIS ASSESSMENT DID NOT COVER

Out of scope by agreement. Bitbucket, the second regional Jira site, and the HR team's Confluence spaces.

Not done by design. Field-by-field and space-by-space review, rule-by-rule review of all 642 automations, pen testing, ROI study.

Within scope but not reached. JSM queue and SLA configuration, which is why dimension 07 carries low confidence. Depth was also reduced in dimensions 05 and 07 to stay within the effort cap.

Halcyon Instruments: evidence by dimension

SEVEN DIMENSIONS WE LOOKED AT: RATING AND EVIDENCE

DIMENSION	RATING	CONFIDENCE	EVIDENCE BEHIND THE RATING
01 Governance and administration	 1 Ad hoc	High	29 admins with global Jira or organization rights against four named owners who have no authority over the other admins. 71 of 118 spaces are team-managed, each configured by its own admin with no shared standards. No change log for global configuration. F2 · F5
02 Configuration and maintainability	 2 Reactive	High	1,140 custom fields, 690 unused for 12 months. 24 separate global fields named "Category". 71 team-managed spaces with their own field sets. F5
03 Security and access controls	 2 Reactive	Medium	SSO and MFA enforced through the identity provider. Offset by 11 stale admins, two shared admin accounts, and one permission scheme, applied to 14 spaces, that grants space administration to all logged-in users. After the 2023 Cloud migration, 47 dashboards and 112 saved filters are shared with Anyone, meaning they are visible without logging in: their names, the JQL behind them, space keys and user names are readable by anyone on the internet even where the underlying work items are not. Multiple third-party users (non-company email domains) have not logged in for 90+ days but retain access. F2
04 Licensing and commercial efficiency	 2 Reactive	Medium	520 of 2,400 Jira users (22%) inactive 90+ days. Of 500 JSM agents, 113 were assigned or transitioned a work item in the past 180 days. JSU installed at the 2,251-2,500 tier with 12 post functions and 5 validators in active workflows. F3
05 Process and platform alignment	 NOT EVALUATED	-	Two representative workflows were reviewed in configuration only. The owning team leads were unavailable during the access window, so how work actually runs could not be confirmed. A two-hour follow-up would close this gap.
06 Automation, AI and consumption	 2 Reactive	High	642 rules; 19 drove 78% of 1.9 million executions in 30 days, seven with recurring failures. Rovo on for all users with no indexing owner and no consumption review. F1 · F4
07 Adoption and business value	 3 Defined	Low	Active use in 92 of 118 Jira spaces; leadership dashboards in use in two of six business units. JSM queue and SLA configuration not reached within the cap.

Every rating is tied to evidence observed directly in the environment or confirmed in discovery; F-numbers refer to the findings on pages 3 and 4. Confidence reflects how much of the dimension that evidence covered within the agreed scope and the 16-hour cap. Ratings are directional, not audit results. Where a dimension could not be judged, it is marked not evaluated rather than estimated.

Halcyon Instruments: top 5 findings

HOW THESE ARE RANKED

Evidence is interpreted and ranked by a senior consultant. Order is set by operational risk first, then avoidable cost, with effort to act breaking ties. Figures come from the environment itself; dollar impact is stated only where billing data supports it; the one figure here (finding 3) is illustrative. The governance target of 3 rests on findings 2 and 5, which both address it directly. The security target of 4 rests on finding 2.

RISK, COST AND EFFORT ● High ● Medium ● Low Red is unfavorable on all three: high risk, high avoidable cost, high effort to act.

FINDING	OBSERVATION	IMPACT	RECOMMENDATION
1 Automation load concentrated in failing rules DIMENSION 06 EVIDENCE: HIGH ● RISK HIGH ● COST MED ● EFFORT LOW	Of 642 automation rules, 19 generated 78% of 1.9 million executions over 30 days. Seven of those showed recurring failures. Eleven of the 19 are owned by deactivated accounts.	Concentrated consumption and repeated failures create reliability risk and exposure to usage-based charges. Failures in unowned rules go unnoticed by the teams that depend on them. Atlassian documents what counts toward automation usage on each plan; consumption monitoring should track that documented unit against the plan's included allowance, not rule counts.	Review the 19 high-volume rules first, resolve the recurring failures, assign owners, and establish consumption monitoring. Then require an owner and description on every rule.
2 Admin and permission drift DIMENSIONS 03 · 01 EVIDENCE: HIGH ● RISK HIGH ● COST LOW ● EFFORT LOW	29 admins with global Jira or organization rights, against four named owners. Eleven are former space leads; two are unowned shared accounts. One permission scheme, applied to 14 spaces, grants space administration to all logged-in users. Since migration, 47 dashboards and 112 saved filters are shared with Anyone and are visible without logging in, exposing names, JQL, space keys and user names. Third-party accounts with no login in 90+ days retain access. Configuration changes are made directly with no work item or record behind them, so nobody can reconstruct why a change was made.	A large admin population makes change control unenforceable and widens the blast radius of an honest mistake. Public sharing exposes structure and people even where the data itself is protected.	Reduce admins to named roles managed through identity-provider groups and replace shared accounts. Correct the shared scheme. Reset dashboard and filter sharing from Anyone to named groups. Review and deprovision third-party accounts by domain. Require a work item for every configuration change, even without a formal approval step, so there is a paper trail. Start a quarterly access review.
3 License and app spend above use DIMENSION 04 EVIDENCE: MEDIUM ● RISK MED ● COST HIGH ● EFFORT MED	(a) 520 of 2,400 Jira users (22%) inactive 90+ days. (b) 500 JSM agent licenses, but only 113 agents were assigned or transitioned a work item in 180 days. Collaborators can view, comment on and follow work items without an agent license, so a large share of the remaining 387 may not need one. (c) JSU licensed at the full user tier for 17 workflow entities (12 post functions, 5 validators).	Marketplace apps are always licensed at the parent product's user tier, so light usage still costs the full tier. The lever is to replace or remove, not re-tier. Renewal is due in five months.	Deprovision the 520 inactive users through the identity provider's leaver process so the renewal in five months lands at least one tier lower; that, not the deprovisioning itself, is where the saving is. Review the 387 against role requirements, convert those who do not need agent capabilities to collaborator access, and reduce the licensed agent count where usage supports it. Rewrite the 17 JSU workflow entities (12 post functions, 5 validators) in JMWE, which is already installed, then unsubscribe from JSU: an illustrative saving of roughly \$10K per year at this tier. Inactive accounts are not confirmed savings until billing impact is verified.

Halcyon Instruments: top 5 findings, continued

RISK, COST AND EFFORT ● High ● Medium ● Low Red is unfavorable on all three: high risk, high avoidable cost, high effort to act.

FINDING	OBSERVATION	IMPACT	RECOMMENDATION
4 Rovo surfacing over-permissioned content DIMENSION 06 EVIDENCE: MEDIUM ● RISK MED ● COST MED ● EFFORT LOW	No owner for Rovo connectors or indexing scope, no permission review before indexing, no monitoring of usage-based consumption. Example: a Jira space created for facilities requests with open access was later reused by HR for sensitive matters. A Rovo search by an engineering manager surfaced an involuntary-termination work item.	Rovo respects existing permissions, so it creates no new access. It turns a latent permission gap into an actual exposure, because discovery no longer depends on knowing where to look.	Name a Rovo owner. Review space permissions before widening indexing, starting with spaces whose use has drifted from their original purpose. Add consumption alerts.
5 Configuration sprawl with no shared standard DIMENSIONS 02 · 01 EVIDENCE: HIGH ● RISK LOW ● COST LOW ● EFFORT MED	1,140 custom fields; 690 (61%) unused for 12 months. 24 separate global fields named "Category", created by different admins over three years; reports that filter on "Category" silently return different results depending on which field was chosen. 71 of 118 spaces are team-managed. Each space admin sets their own fields, workflows and permissions, so there is no shared standard to govern against; this is how spaces drift from their original purpose, including into holding sensitive data (see finding 4).	Reporting across Jira spaces cannot be trusted when one concept lives in 24 fields. Every new space adds to the confusion, and cleanup cost grows each quarter.	Consolidate the 24 Category fields first. Set a policy for when team-managed is allowed. Review permissions on spaces that hold sensitive or cross-team data first; migrate them to company-managed where the governance benefit justifies the effort (there is no in-place conversion). Retire unused fields in batches with 30 days' notice.

Each finding can be acted on by your team directly. If you would rather not tackle them yourselves, we can help either way: a one-time engagement for a deeper dive into workflows, automation, licensing or Rovo governance, or an ongoing part-time retainer, at a low monthly cost, for governance, administration and continuous improvement. Where the evidence justifies neither, the readout says so.

EMAIL	PHONE	WEB
info@veraxent.com	844-VERAXENT	veraxent.com

Veraxent



Gold
Solution Partner