INFINITECH

Infinitech Regulated Data Platform: technical brief

Infinitech LLC · Technical brief · November 2026

IRDP is a data platform for regulated data that Infinitech deploys in a customer's own AWS accounts. Sources land in an S3 lake encrypted with customer-managed keys. A pipeline curates, loads, and checks the data every 10 minutes, a warehouse serves it to people who sign in by role, and a second region holds a recovery copy. Policy rules check every change before it is applied.

This brief is for the architects, security reviewers, and data leads who will check that claim. The numbers in it come from 15 demo cycles run from 25 October to 4 November 2026 in Infinitech's commercial AWS demo account, each torn down afterward. They are demo measurements, not service levels or a measure of your workload.

WHO IT FITS

IRDP's defaults are set for four requirements:

1. **Every module is built to move to AWS GovCloud** by switching its region profile; the open items under Government status are what remains.
2. **Recovery meets the buyer's targets at a separate site**, by default a second region of the same provider. The analytics procurements Infinitech has read ask for a recovery time of 4 to 24 hours and a recovery point of 15 minutes to 8 hours; none asks for a second cloud provider.
3. **Each pipeline run finishes inside half its schedule interval**: 300 seconds of the default 10 minutes, so one retry of the slowest step still fits and runs don't overlap.
4. **People see only what their role allows**: dashboards and tables open by IAM Identity Center group.

DEFAULTS AND OPTIONS

Layer	Default	Options	Why the default
Ingest	Amazon Data Firehose for message sources; files written straight to the S3 landing bucket for file sources	Amazon MSK for sources that already publish to Kafka; AWS Transfer Family (not built yet) for sources that can only push SFTP	Firehose batches events into files and retries delivery when S3 is unavailable. Priced for the typical customer at about $34 a month, against about $477 for MSK, whose brokers bill every hour. Files to S3 cost under $1 a month
Pipeline	AWS Step Functions running Curate, Load, and Verify as Fargate tasks	Airflow 3.2.2 on EKS, with a queue-depth autoscaler, Microsoft Entra sign-in, and Prometheus and Grafana	Nothing to patch and no idle cost: about $60 a month for the typical customer, against about $360 for Airflow on EKS. Provisioned Amazon MWAA isn't offered in GovCloud, so a buyer who needs Airflow there gets Airflow on EKS
Warehouse	Amazon Redshift Serverless	Snowflake Business Critical over PrivateLink, as a replacement. A deployment runs one warehouse	One AWS bill and IAM model, no government price premium, and no vendor-created account. Priced at about $3,500 a month for the typical customer, against about $9,000 for Snowflake ($12,700 in government regions)

Layer	Default	Options	Why the default
Recovery	Snapshots copied to a second AWS region	Warm standby in the second region; cross-cloud recovery to Azure, on request	Copied snapshots carry the whole database and cost the least. Both second-region paths work with Redshift only. Details below
Monitoring	CloudWatch dashboards and alarms, opened by role	Prometheus and Grafana, with the Airflow option	Step Functions, Firehose, and Redshift publish their metrics at no charge, and the dashboards and alarms fit the free tier in commercial regions (about $6 a month in GovCloud)

The "typical customer" is a cost model, not a customer: a mid-market buyer built from published figures, with about 2,200 warehouse hours a month and an assumed 10 TB stored. Prices are US list prices read in late October 2026.

Snowflake fits when recovery has to cross to Azure Government, because it runs on both clouds and replicates between them. IRDP doesn't build that replication yet, so a deployment that runs Snowflake has no standby.

GOVERNMENT STATUS

IRDP is a reference implementation, not an authorization to operate. An ATO needs a third-party assessment and an agency sponsor, which are outside Infinitech's offering.

"Built to move" means four things, each tested in CI: no module hard-codes a partition, region, or endpoint; the region policy accepts us-gov-west-1 and us-gov-east-1 and refuses commercial regions in its government profile; each module's examples pass terraform validate with a GovCloud provider configuration; and every GovCloud difference IRDP depends on is listed with its source. No plan or apply has run in AWS GovCloud or Azure Government.

Known open items for a first GovCloud deployment: no AWS page confirms that Firehose Direct PUT delivers to S3 there; the network module creates no FIPS endpoints yet; and GovCloud accounts must be created from a linked commercial account. IMCLZ's account vending creates that pair as of the IMCLZ commit IRDP pins (`84a1907`), tested against a mocked provider; no pair has been vended live. The first GovCloud deployment is scoped after discovery.

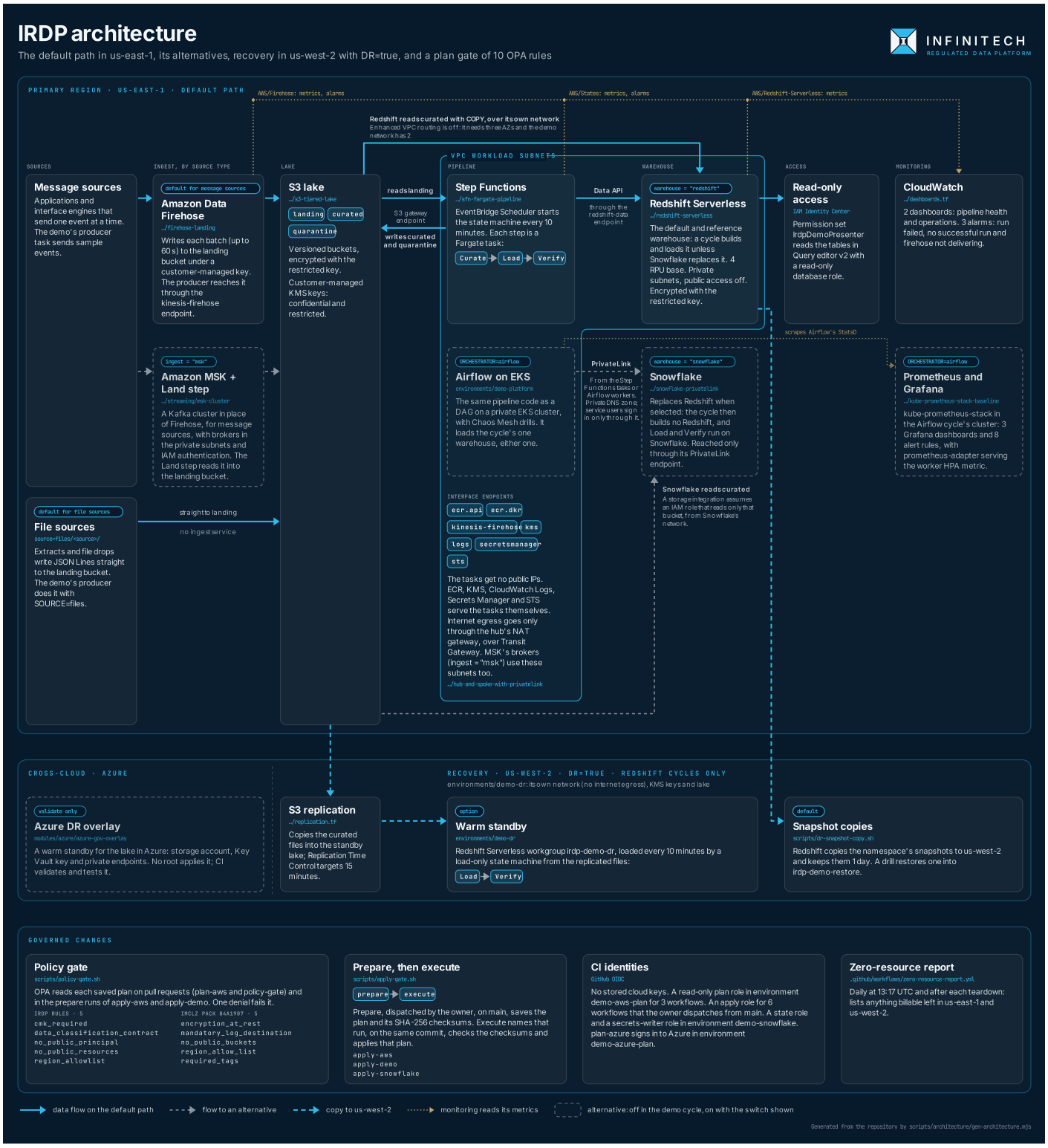
NOT MEASURED YET

- The file-source path (sources writing straight to S3) in a live cycle.
- MSK with Step Functions (it ran under Airflow), and failover to Azure.
- Snowflake in Redshift's place: the setting came after cycle 15, and no cycle has run it.

WHO DELIVERS IT

Michael McKinney, Infinitech's founder, has delivered cloud platform, automation, and DevSecOps work under contract since 2021 and formed Infinitech LLC in 2023. From July 2024 to August 2025 he designed and operated Government Cloud infrastructure aligned to NIST, HITRUST, and FedRAMP requirements for a Fortune 10 healthcare company.

ARCHITECTURE



The diagram is generated from the Terraform, policy rules, and workflows, and CI fails a change that leaves it stale. Dashed cards are options; each names the setting that turns it on.

RECOVERY

The two second-region options work with Redshift only; the second-region stack refuses a deployment whose warehouse is Snowflake.

Option	How it fails over	Writes at risk
Copied snapshots (default)	Restore the newest snapshot copied to the second region into a namespace kept ready there	Everything written after that snapshot. Redshift Serverless takes a recovery point about every 30 minutes, and the copy then has to reach the second region
Warm standby	The second region loads the lake copy into its own warehouse every 10 minutes; failover points readers at it	For the pipeline's tables, the lake copy's lag plus one load: about 25 minutes at worst, an estimate from S3 Replication Time Control's 15-minute SLA. Tables people build by hand in the warehouse aren't on the standby
Cross-cloud to Azure, on request	The lake copies to Azure Government	The Azure overlay validates offline only; this path has never run

Each drill stopped the primary pipeline in us-east-1 and timed recovery in us-west-2. RTO is the time until the warehouse answers queries again; RPO is the window of recent writes at risk, which for the snapshot path is the restored snapshot's age when the primary failed:

Cycle	Events in the warehouse	Copied snapshot (default): RTO, RPO	Warm standby: RTO, RPO	Snapshot copy took
10	4,950	8.1 min, 7.3 min	2.7 min, 0	6.3 min
11	2,475,000	7.3 min, 25.1 min	1.8 min, 0	24.1 min
12 (8 RPU)	990,000	7.3 min, 7.4 min	2.0 min, 0	3.6 min
15	99,000	8.2 min, 20.8 min	2.1 min, 0	18.6 min

Every drill brought back all of the primary's events on both paths. Each drill took its own snapshot, so its age is mostly the copy's trip, for which AWS states no upper bound. In production the newest copy can be older: Redshift takes a recovery point about every 30 minutes, then copies it. Two earlier drills failed and were fixed before these.

PIPELINE AND WAREHOUSE AT VOLUME

- **Run time at the typical customer's volume.** At 8 RPU, GovCloud's smallest Redshift Serverless size, runs that each took a whole 250,000-event batch finished in 248 to 285 seconds (cycle 12, four runs), inside the 300-second limit. At 4 RPU the same runs took 339 to 434 seconds (cycle 11), over it. Four runs is a small sample.
- **Loads.** Cycle 8's benchmark, run on both warehouses to choose the default, loaded a day of the typical customer's events, about 10 GB arriving as 70 MB every 10 minutes. The day's loads cost $3.60 of compute on Redshift at 4 RPU against $11.27 on Snowflake X-Small. Snowflake loaded the 10 GB as one bulk file in 67.0 seconds, Redshift in 297.8.
- **Queries.** Cycle 10, also comparing the two, ran the 22 queries of a TPC-H-derived benchmark at scale factor 100, one at a time: 138.2 to 143.0 seconds and $0.10 a round on Redshift at 4 RPU, against 294.3 to 317.2 seconds and $0.39 to $0.42 on Snowflake X-Small, with all 22 answers matching. These results aren't comparable with published TPC-H results, and queries in several streams at once haven't been measured.

WHAT CYCLE 15 SHOWED

Step	Result
Deploy	The prepare run planned 134 core resources and passed the policy gate; the execute run applied that saved plan after checking its checksums
Ingest and pipeline	Two loads of 50,000 generated events each, 500 of them malformed on purpose. After the first, Redshift held 49,500 events, one row each, and all seven data checks passed after each load
Forced failure	Curate was stopped three times in one run. Step Functions retried twice and failed the run, the run-failed alarm fired 25 seconds later, and a redrive from the failed step succeeded
Read-only access	A presenter signed in through IAM Identity Center: SELECT returned the 49,500 events and DELETE failed with "permission denied"
Teardown	294 resources destroyed across three stacks, each destroy plan read before it ran. The zero-resource report found nothing billable in either region

CONTROLS AND EVIDENCE

- **Keys.** A customer-managed KMS key for each classification stored: internal, confidential, or restricted (the demo stores the last two). Public data has no key.
- **Policy gate.** Five IRDP rules run on every plan beside the five rules of Infinitech's landing zone (IMCLZ): approved regions only; a customer-managed key on confidential and restricted stores; no public endpoints, buckets, or open ingress; no topic, bucket, queue or key policy open to every AWS account; and a classification tag on every data store. A denial from either set fails the change.
- **Changes.** CI signs in through GitHub OIDC with no stored cloud keys; apply uses its own identity, only from the main branch.
- **Deletes.** A subject's delete request reaches the warehouse on every load, in either region, and a lake erasure task removes the records from the lake's objects and old versions (shown in cycle 8).
- **Compliance mapping.** OSCAL component definitions map the components to NIST SP 800-53 controls, emitted and validated in CI.
- **Runbook.** Six procedures, from second-region recovery to the first GovCloud run, checked against the code in CI. Of their scripts, only the second-region recovery's has run live (cycle 16, primary declared lost).

THE ENGAGEMENT

Infinitech adapts IRDP from a repository you own, after a free call on fit and scope. Discovery, USD 4,200, is credited within 60 days; then two phases, USD 37,100 at USD 175/h (launch prices, ±30%; none delivered yet):

- **Phase 1, IRDP Core, USD 29,925 (102–171 h):** discovery, intake, deploy, a source, policy gate, alarms, acceptance, and a handoff that rotates each credential Infinitech could read and removes its access.
- **Phase 2, Recovery & Evidence, USD 7,175 (24–41 h):** the second-region standby and two drills, the failover runbook drilled with you, dashboards, OSCAL; without it, no tested DR.

The base scope is one primary AWS region with snapshot copies to a second, and one standard source: one schema, one Firehose stream or Kafka topic, one merge key, JSON or CSV. The acceptance drill measures recovery; it isn't a recovery-time or recovery-point commitment. A warm standby, Snowflake in Redshift's place, Airflow on EKS, MSK, and more sources are scoped separately. Your accounts need an approved landing zone first, such as an IMCLZ Foundation. Not included: operations after handoff, 24×7 support, cloud and Snowflake bills, and ATO or assessor work. Final scope and fees are set in a signed statement of work.

The evidence repository's measured results name the run behind each cycle 15 figure. Request a discussion at hello@infinitechplatforms.com or infinitechplatforms.com.