FIRN
Analytics ▪ Knowledge ▪ Insight

From Proliferation to Control:

Managing ‘Agent Sprawl’ in the Enterprise AI Era

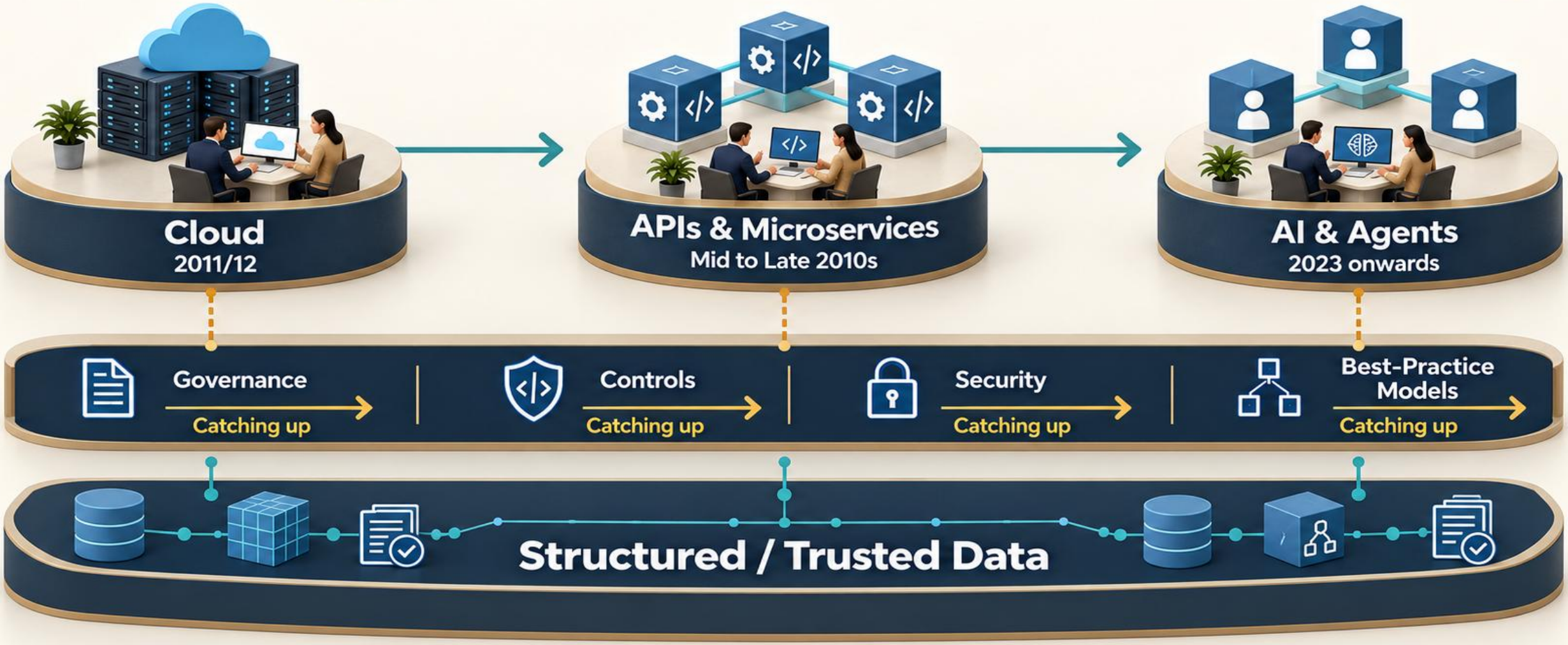
A consulting perspective.
Observations noted across the NZ Market.

Paul Sadler | Client Director
FIRN Analytics



FIRN
Analytics · Knowledge · Insight

Technology Moves First. Governance Catches Up.



New technology. The same need for ownership, discipline and trusted data.

FIRN
Analytics · Knowledge · Insight

MARKET AI GOVERNANCE MATURITY

The AI Governance Maturity Curve



STAGE 1
Unaware
2023/24
No systematic understanding of what AI is running.

STAGE 2
Visible
2024/25
Discovery has happened. There is an inventory. But controls are thin beyond the approved stack. The gap is real.

STAGE 3
Controlled
2026
Policy is operational across the full inventory. Enforcement is real time. Audit trails exist. Ungoverned AI gets pulled into the governance framework automatically.

STAGE 4
Optimized
AI governance is a competitive advantage. Regulatory reporting is automated. Control and innovation are not in tension.

NZ enterprise perspective

Presenter observation — not a measured benchmark

- Most NZ enterprises are in Stage 2, with leading organisations moving into Stage 3.
- Maturity is uneven: typically one or two business processes are controlled.
- Many other processes still need controls applied.

FIRN
Analytics · Knowledge · Insight

The Risks of AI Agent Sprawl

Excess access



Unmaintained context



Runaway costs or loops



Silent failure



Unauthorised actions



Error propagation



Conflicting decisions



Incorrect outputs acted on



Duplicate work or commitments



Unclear accountability



Combined authority



Supplier data leakage



The Emerging Archetype: 3 Layers, 1 Shared Context Foundation

FIRN
Analytics · Knowledge · Insight

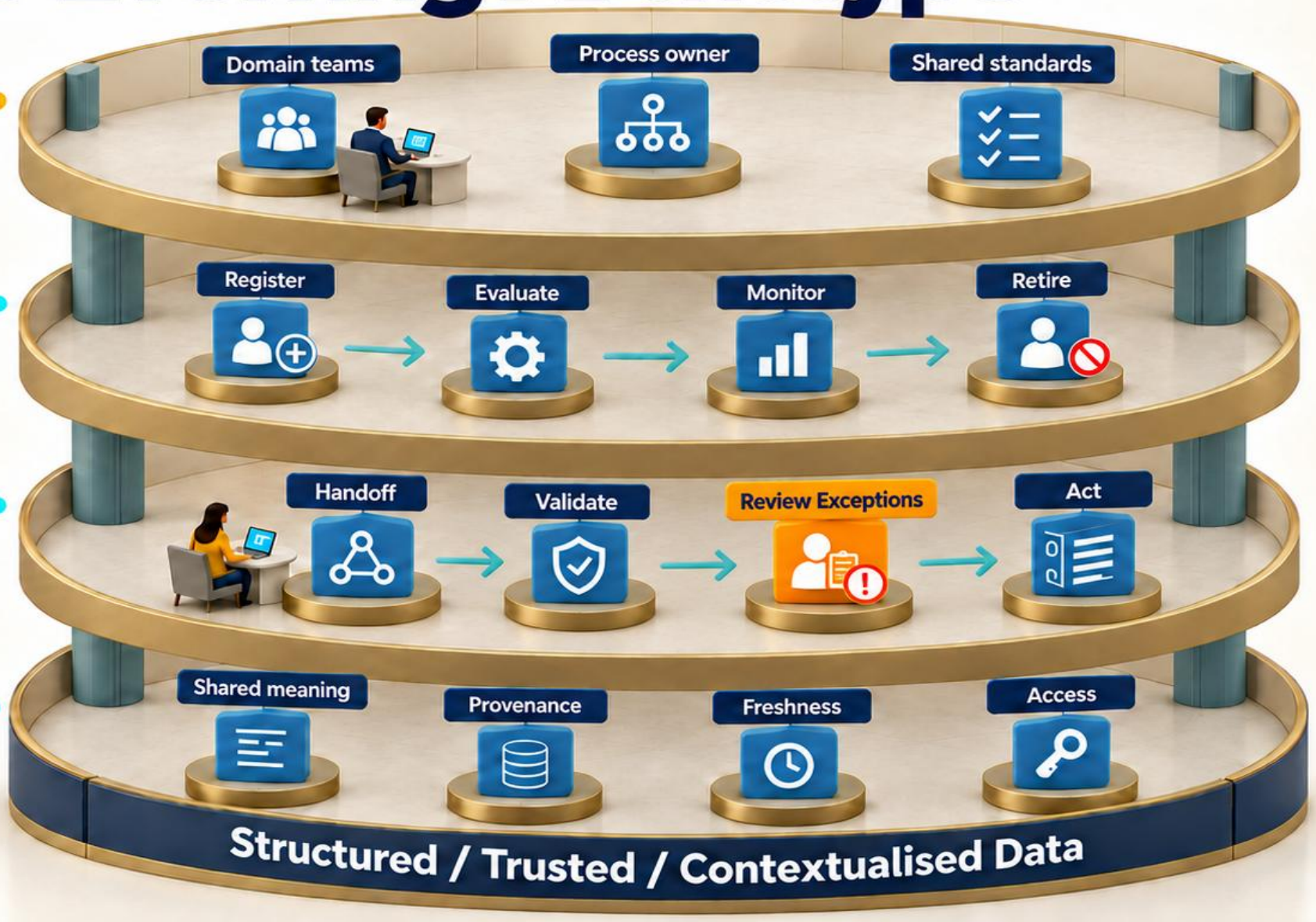
The Evolving Archetype

Organisation
Who owns outcomes and decisions?

Operations and Control
How do agents enter service, remain safe and retire?

Orchestration
How does work pass between people, agents and systems?

Context Foundation
What information and meaning can work rely on?



FIRN
Analytics · Knowledge · Insight

Decentralised domain ownership

Local experimentation

Independent tools and rules



Centralised centre of excellence



FIRN
Analytics ▪ Knowledge ▪ Insight

Federated hub and spoke



End-to-end value-stream ownership



Agent purposed roles are delivering to risk-based shared rules

Agent authority must be proportionate to the action it is taking

- Distinguish observe, advise, act with approval and bounded autonomous action.
- Assess impact, reversibility, detectability and propagation.
- Enforce identity, purpose and scope on consequential actions.
- Put human review where it changes the outcome.

All agent transactions must be governed

- Name the owner of the end-to-end outcome.
- Carry identity, context and a transaction ID across handoffs.
- Validate before a conflicting or irreversible action.
- Prevent duplicate writes and preserve separation of duties.

All Controls need an Operating Rhythm

- Did expected work start and finish on time?
- Were permissions, sources and context appropriate?
- Did handoff checks and escalation work?
- Was the outcome useful, at an acceptable cost?



Business process owner

Own the end-to-end outcome, resolve conflicting decisions and set escalation thresholds.

Agent product owner

Maintain purpose, evaluation, permissions, dependencies, support and retirement.

Enterprise platform / CoE

Provide reusable environments, registry, identity, policy integrations and release paths.

Data / knowledge product owner

Maintain meaning, access, quality, freshness, versions and product funding.

Operations and security

Monitor workflows, triage exceptions, manage incidents and verify intervention capability.

Risk / independent assurance

Challenge material risks, exceptions and evidence of control effectiveness.

FIRN
Analytics • Knowledge • Insight

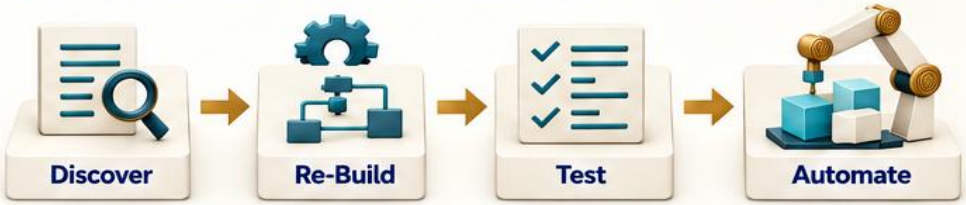
What's Next? What's Emerging?

AI Agent Security



- AI Agent Gateways
- MCP Server Management and Security
- Anti-AI Threats Perimeter Security

Mechanised Business Processes



- Design aim: more explicit, deterministic agents — zero randonmess or ambiguity in governed actions.
- Processes, workflows & pipelines, procedures, business logic, metrics and reporting will continue to be fixed and tested, providing trusted data for agents to act upon.
- Reduced Costs, reduced Token usage

Reduce risks and bottlenecks | **Improve efficiency and cost**

Governance, Governance, Governance!



- From the Executive level to Front-Line Teams — across the entire Enterprise!
- Every team using or relying on agents will feel the effects, understand, and measurably deliver to set Standards.

Redefined Trust Architectures



- Observe behaviour
- Test limits
- Contain actions

Deeper Context Layer



- Improved Agent Business Understanding
- Improved Conversational Analytics

Secure access • Tested processes • Contained systems

FIRN
Analytics • Knowledge • Insight
Where FIRN adds value

Structured / Trusted Data / Shared Context

snowflake | databricks | Microsoft Fabric | DataRobot | alteryx | dbt | coalesce | Fivetran | Airia | sigma



Thank you for being with me today

FIRN

Analytics ▪ Knowledge ▪ Insight

Offerings for attendees

- Current Data Estate/Platform Assessment
- AI Readiness Assessment

AI on Good Data