APTO SOLUTIONS

Building Your Observability Strategy

A Practical Framework from Assessment to Operate

aptosolutions.co.uk
March 2026

Assessed. Architected. Operated.

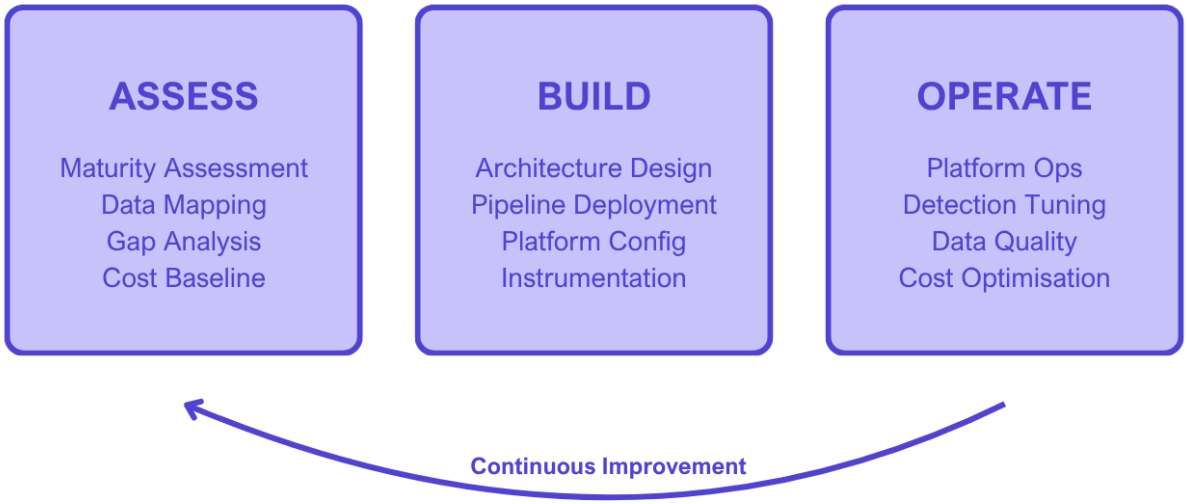
Introduction

Most organisations that invest in observability make the same mistake: they start with the platform. They evaluate vendors, run proof-of-concepts, negotiate licences, and deploy a tool. Six months later, they have an expensive platform that ingests a fraction of their telemetry, dashboards that nobody trusts, alerts that nobody responds to, and a growing sense that observability was oversold.

The platform is not the strategy. Observability success requires a structured approach that begins with understanding your current state, defines clear business outcomes, designs a data architecture that serves those outcomes, and plans for the ongoing operations that make it all work. The platform is simply the tool that executes the strategy.

This guide provides a practical, field-tested framework for building an observability strategy that delivers measurable value. It follows the same Assess, Build, Operate lifecycle that underpins all Apto Solutions engagements, because this phased approach consistently delivers better outcomes than “big bang” platform deployments.

The Assess, Build and Operate Lifecycle



> *This framework is drawn from real customer engagements where Apto Solutions has designed and delivered observability strategies for organisations across financial services, healthcare, critical national infrastructure, and technology sectors.*

Phase 1: Assess

The assessment phase answers the fundamental question: where are you today, and where do you need to be? It provides the evidence base for every subsequent decision — platform selection, architecture design, budget justification, and roadmap planning.

Observability Maturity Assessment

A structured maturity assessment evaluates your current capabilities across five dimensions:

1. Telemetry Coverage

What telemetry are you currently collecting, and from where? Map your existing data sources against your critical services and infrastructure. Identify gaps — services with no instrumentation, infrastructure with basic metrics but no logs, application tiers with logs but no traces. The goal is a comprehensive view of what you can currently see and what remains invisible.

- Inventory all current monitoring and logging tools and agents
- Map telemetry coverage against your service catalogue
- Identify critical services with insufficient or no observability
- Assess the quality and structure of existing telemetry (structured vs unstructured, consistent tagging vs ad hoc)

2. Data Architecture

How does your telemetry data flow from source to destination? Assess your current data architecture for efficiency, cost-effectiveness, and resilience. Common problems include: no central pipeline (data flows directly from agents to backends), duplicate collection (multiple agents on the same hosts collecting overlapping data), no data tiering (all data treated equally regardless of value), and no retention strategy (everything kept forever at full cost, or nothing kept long enough for compliance).

- Document all data flows from collection to storage
- Calculate current ingestion volumes by source and destination
- Identify duplicate or overlapping data collection
- Assess data retention policies against compliance requirements

3. Tooling and Platforms

What platforms and tools are currently in use? Evaluate whether your existing tooling is fit for purpose, whether there is unnecessary overlap, and whether the organisation is getting full value from its current investments. Many organisations are using less than 30% of the capabilities of the platforms they already own.

- Catalogue all monitoring, observability, and SIEM platforms

- Assess licence utilisation and feature adoption
- Identify tool sprawl and consolidation opportunities
- Evaluate platform suitability for your architecture (cloud-native, hybrid, on-premises)

4. People and Processes

Do you have the skills and processes to operate an observability platform effectively? This is the dimension most organisations underinvest in. A world-class platform operated by a team without the skills, processes, or capacity to maintain it will underperform a more modest platform with dedicated, skilled operators.

- Assess team skills against platform requirements
- Evaluate incident response processes and MTTR metrics
- Review on-call and escalation procedures
- Identify the Operator gap: who runs the platform day-to-day?

5. Business Alignment

Is your current observability investment aligned with business priorities? A frequent misalignment is that development and staging are monitored under exactly the same rules as production — same retention, same resolution, same label policy — with no separate budget and no separate governance. Non-production often should be instrumented comprehensively, because it is where a problem is cheapest to find; what it should not do is inherit production's cost profile by default. Another common pattern is extensive infrastructure monitoring with little application-level observability for the services that customers actually interact with.

- Map current observability coverage against revenue-critical services
- Assess whether SLOs and SLIs are defined and measured for key services
- Evaluate whether observability data informs business decisions

> *Apto's Observability Maturity Assessment is a structured engagement that covers all five dimensions. The deliverable is a scored assessment with clear recommendations and a prioritised roadmap, providing the evidence base needed to justify investment and align stakeholders.*

Data Mapping and Discovery

Alongside the maturity assessment, a detailed data mapping exercise provides the quantitative foundation for your architecture and cost planning.

- Identify every telemetry source (applications, infrastructure, security tools, cloud services, third-party SaaS)
- Measure current data volumes by source (GB/day)
- Classify data by value (high-value signals vs noise)
- Estimate future volume growth based on planned infrastructure changes
- Calculate current cost per GB across all platforms
- Measure active series count by source and environment wherever a platform prices on cardinality rather than volume

This data map becomes the input for pipeline design (what to filter, aggregate, and route) and platform sizing (what capacity and licence tier you actually need).

Phase 2: Build

The build phase translates your assessment findings and strategic objectives into a concrete architecture. It covers platform selection, pipeline design, instrumentation, and the initial deployment.

Defining Business Outcomes

Before any technology decisions, define measurable outcomes that align with business priorities:

- **Operational resilience:** Reduce MTTR for Severity 1 incidents from 4 hours to 30 minutes within 6 months.
- **Cost efficiency:** Reduce total observability and SIEM platform costs by 30–60% within 12 months through pipeline optimisation and data tiering.
- **Security posture:** Achieve full telemetry coverage for all internet-facing services within 3 months, enabling detection of the OWASP Top 10.
- **Developer productivity:** Provide self-service observability dashboards for the top 20 microservices within 6 months, enabling developers to diagnose issues without escalating to the operations team.

These outcomes drive your architecture decisions, your implementation priorities, and your success metrics. They also provide the business case needed to secure budget and stakeholder support.

Architecture Design: The Pipeline-First Approach

We advocate a pipeline-first architecture for every observability strategy. This means designing the data pipeline before selecting or configuring the analytics platform. The pipeline determines what data you collect, how it is processed, where it is routed, and what it costs. The analytics platform consumes the output. Cost accrues on two axes here, not one: volume ingested, and active series retained. Platforms priced on cardinality respond to the second, so an architecture optimised only for gigabytes can reduce volume and increase spend at the same time.

The core architecture follows the two-tier model described in our Telemetry Pipeline Playbook:

1. Edge collection: Lightweight agents (OpenTelemetry Collector, Cribl Edge, or vendor agents) on every host and container
2. Central pipeline: Cribl Stream or OTel Collector gateways for filtering, enrichment, aggregation, routing, and cardinality control through label allow-lists and series budgets
3. Primary analytics: Your chosen SIEM and/or observability platform, receiving only high-value, processed data

4. Data lake: Cheap object storage receiving 100% raw data for compliance and retroactive analysis

Platform Selection

With your data architecture defined, platform selection becomes a more focused decision. Your assessment data tells you:

- What data volumes the platform needs to handle (after pipeline optimisation, not raw)
- What query and analytics capabilities are required for your specific use cases
- What integration points matter (your existing security tools, cloud platforms, CI/CD pipelines)
- What your team can realistically operate (or what a managed service partner needs to provide)

This evidence-based approach avoids the common trap of selecting a platform based on a flashy demo, only to discover it does not fit your data architecture or your team's operational capacity.

Instrumentation Strategy

Instrumentation is how your applications and infrastructure generate the telemetry that your observability platform consumes. We recommend an incremental approach:

- **Quick wins (Week 1–2):** Enable infrastructure metrics and log collection for all production environments. Deploy OTel Collectors to collect host-level telemetry.
- **Critical paths (Week 3–6):** Implement distributed tracing for your top 5 revenue-critical transaction paths. Use OpenTelemetry auto-instrumentation for supported frameworks (Java, .NET, Python, Node.js).
- **Broadening coverage (Month 2–3):** Extend tracing to secondary services and dependencies. Add custom instrumentation for business-specific metrics (order value, conversion rate, SLA compliance).
- **Full stack (Month 4–6):** Achieve comprehensive observability across all production services, including frontend real-user monitoring, synthetic monitoring, and database observability.

Phase 3: Operate

This is where most observability initiatives succeed or fail. The build phase delivers a platform; the operate phase makes it useful. Without dedicated, ongoing operations, even the best-designed observability architecture degrades over time.

Platform Operations

Day-to-day platform management includes:

- Monitoring pipeline health, throughput, and error rates
- Managing data volume and cost against budget
- Platform upgrades, patching, and configuration management
- Capacity planning based on growth trends
- User management and access control

These tasks require dedicated attention. When they fall to a team that is also responsible for incident response, application support, and project delivery, they invariably get deprioritised — until the platform breaks.

Detection and Alerting Hygiene

Alerts decay. Over time, thresholds drift, new services are deployed without corresponding alerts, and alert rules accumulate without cleanup. A healthy observability operation includes:

- Regular review of alert rules for relevance and accuracy
- Tuning thresholds based on changing baselines
- Removing or updating alerts that consistently fire without action
- Adding alerts for new services and failure modes as they are discovered
- Tracking alert-to-incident conversion rates to measure signal quality

Data Quality Management

Telemetry data quality degrades silently. Applications change their log formats without notice. New services are deployed without instrumentation. Tagging standards drift as teams adopt their own conventions. Pipeline rules that were once effective become irrelevant as data sources change.

Ongoing data quality management ensures your observability investment continues to deliver value:

- Monitoring data completeness: are all expected sources still reporting?
- Validating data structure: are logs still conforming to expected formats?

- Enforcing tagging standards: are new services adopting required labels and attributes?
- Reviewing pipeline rules: are filters and routing still appropriate?

The Managed Service Model

For many organisations, the most effective approach to the Operate phase is to partner with a managed service provider. This is not about outsourcing — it is about ensuring that your observability platform has dedicated, expert operators whose sole focus is making the platform work effectively for your teams.

Apto's Operate model provides continuous platform management, data pipeline operations, detection engineering, and cost optimisation. Your internal teams focus on using the observability data to improve services and respond to incidents, while Apto ensures the platform itself runs reliably, efficiently, and cost-effectively.

> *The Assess, Build, Operate lifecycle is designed so that each phase delivers standalone value. You can engage Apto for an assessment only, or for a full end-to-end strategy and managed service. The assessment always pays for itself by identifying cost savings and architectural improvements.*

Measuring Success

An observability strategy should be measured by its impact on business outcomes, not by the volume of data ingested or the number of dashboards created. Measure efficiency on both cost axes — cost per gigabyte ingested, and cost per active series where the platform prices on cardinality — because either one alone can show progress while the other deteriorates. Key metrics include:

Metric	What It Measures	Target
Mean Time to Detect (MTTD)	How quickly you identify incidents	Reduce by 50% within 6 months
Mean Time to Resolve (MTTR)	How quickly you resolve incidents	Reduce by 40–60% within 6 months
Alert-to-Incident Ratio	Signal quality of your alerting	Below 5:1 (fewer than 5 alerts per real incident)
Telemetry Coverage	% of critical services with full-stack observability	100% of Tier 1 services within 3 months
Cost per GB Ingested	Efficiency of your data architecture	30–50% reduction through pipeline optimisation
SLO Achievement	Service reliability against defined targets	95%+ of SLOs met consistently
Active Series by Environment	Cardinality load, split prod / staging / dev	Series growth tracking estate growth, not label growth

Next Steps

Ready to take action? Apto Solutions offers a range of entry-point engagements designed to give you clarity before commitment:

- **Free Assessment:** A no-obligation conversation with one of our platform specialists to understand your current state and identify quick wins.
- **SIEM Health Check:** A structured review of your existing SIEM deployment covering architecture, detection coverage, data quality, and operational efficiency.
- **Observability Maturity Assessment:** A framework-driven evaluation of your monitoring and observability capabilities against industry best practice.
- **Data Mapping and Discovery:** An analysis of your telemetry data flows, identifying redundancy, gaps, and optimisation opportunities.

> *Book your free assessment at aptosolutions.co.uk/contact or email enquiries@aptosolutions.co.uk to start the conversation.*

Assessed. Architected. Operated.
aptosolutions.co.uk