dynatrace

How to build a future-ready **log management strategy for financial services**

This checklist outlines the essential steps for moving from legacy, fragmented log tools to a unified observability approach tailored to the needs of financial institutions. By modernizing your log management strategy, you can reduce operational risk, improve resiliency, control costs, and strengthen regulatory compliance—all while enabling faster, data-driven decision-making.

The result: fewer tools to manage, more predictable costs, and the ability to turn logs telemetry from a maintenance overhead into a strategic asset that accelerates innovation and resilience.

PHASE ONE

Strategic assessment

This phase helps financial institutions establish a clear understanding of their current environment and define modernization outcomes aligned with operational risk, compliance, **cost control**, and customer-experience priorities.

- **Identify log sources and volume:** Catalog all critical log sources across core banking systems, trading platforms, digital channels, payment systems, cloud workloads, and third-party integrations. Estimate daily ingest volume and growth patterns to ensure capacity planning aligns with regulatory requirements and future growth.
- **Classify log types and usage:** Differentiate between log types—such as application, audit, transaction, fraud, network, and security logs—and map each category to its stakeholders (e.g., risk teams, SOC analysts, compliance officers, application owners). Clarify how each log type supports activities like incident investigation, fraud monitoring, regulatory reporting, or operational performance tracking.
- **Define retention requirements:** Determine retention periods based on FFIEC, FINRA, PCI DSS, SEC, and internal governance obligations. Ensure you understand which logs must be immutable, how long they must remain "always accessible," and which business units rely on them for audits or investigations.
- **Evaluate current costs and value:** Analyze licensing fees, storage overhead, infrastructure dependencies, and the operational effort required to manage legacy log tools. Identify areas with excessive ingest costs, duplicate tooling, manual correlation overhead, or limited analytical value: common challenges in risk and compliance environments.
- **Set modernization goals:** Define specific objectives tied to key financial-services KPIs, such as reducing MTTR for critical customer journeys, optimizing log spend without limiting retention, enhancing fraud detection accuracy, or improving audit readiness with faster, more complete log access.

PHASE TWO

Implementation and optimization

This phase focuses on deploying a modern, AI-powered log management platform designed for highly regulated environments and addressing whether data flows are optimized to deliver maximum operational and financial value.

- **Unify observability telemetry:** Consolidate logs, metrics, traces, and events into a single, unified platform. This eliminates fragmented tooling across operations, security, and compliance teams while providing full context for incident response and regulatory investigations.
- **Structure your telemetry with buckets:** Organize log telemetry into dedicated buckets based on use case (e.g., fraud, payments, customer-facing applications, regulatory audit logs), team access, retention period and team structure. This reduces dad scanned per query, improving performance and lowering costs.
- **Filter and route logs on ingest:** Use ingestion pipelines to filter irrelevant logs, extract metrics or business events, and route telemetry to the appropriate buckets. This optimizes costs while ensuring teams—especially those responsible for fraud, risk, and compliance—retain access to required historical logs, for up to 10 years.
- **Configure retention policies:** Optimize storage costs by setting specific retention periods for each bucket to meet regulatory, legal, and operational mandates. For auditability and rapid investigations, a modern platform should enable long-term access aligned to your defined requirements.
- **Implement access controls:** Use IAM policies and policy boundaries to enforce least privilege access. Ensure each team—Security, Risk, Operations, Compliance—can only query the logs required for their function, reducing unnecessary data exposure and controlling costs.

PHASE THREE

Proactive operations and automation

This phase centers on using your modern log management platform to shift from reactive issue resolution to proactive prevention, leveraging automation and real-time insights critical for managing operational risk and maintaining always-on customer experiences.

- **Leverage AI-powered analysis:** Use AI capabilities, such as Dynatrace Intelligence to analyze logs in context with other telemetry, identify root causes and reduce manual troubleshooting. This significantly reduces investigation time during outages, fraud events, and performance degradation impacting digital banking or trading systems.
- **Create log-based metrics and events:** Convert high-volume log telemetry such as payment failures, authentication attempts, or trading latency signals—into cost-effective monitoring and alerting on dashboards. Create events from logs to trigger automated workflows that accelerate incident response and support operational resilience mandates.
- **Enable contextual troubleshooting:** Use AI-powered context to analyze logs in context of specific entities (e.g., a customer session, ATM device, mobile banking microservice, or trading engine). This dramatically reduces the time required to identify the source of issues affecting transaction throughput or customer experience.
- **Shift to proactive issue prevention:** Leverage predictive analytics provided by Dynatrace Intelligence to forecast patterns that could lead to service degradation, fraud anomalies, or compliance risks. Automatically trigger remediation actions to prevent incidents before users are impacted, supporting operational resilience and SLA commitments.
- **Track usage and adoption:** Monitor ready-made dashboards that provide insights into ingest volume, query patterns, and costs. Use these insights to optimize routing rules, reduce unnecessary scanning, and demonstrate measurable efficiency gains to technology leaders, risk officers, and finance teams.

Your logs are already shaping outcomes

Make sure they're driving the right ones

See how leading financial institutions are strengthening operational resilience, reducing compliance risk, and improving customer experience with modern log management in our free eBook:

"From operational overhead to strategic value: Driving outcomes with modern log management."

Download now

ABOUT DYNATRACE

Dynatrace is advancing observability for today's digital businesses, helping to transform the complexity of modern digital ecosystems into powerful business assets. By leveraging AI-powered insights, Dynatrace enables organizations to analyze, automate, and innovate faster to drive their business forward. Learn more at www.dynatrace.com.

dynatrace

dynatrace.com/blog @dynatrace linkedin.com/company/dynatrace instagram.com/dynatrace

05.08.26 BAE25341_WP_USLet_cs