

## Section 2: Framework Overview

This Framework is structured around seven key dimensions. Each dimension contains specific variables, SLA targets, measurement methods, and practical evaluation guidance. This section defines the architecture and monitoring cadence of the framework.

### 2.1 Framework Architecture

#	Dimension	Focus Area	Key Stakeholders
1	<b>System Performance &amp; Reliability</b>	Technical infrastructure stability	IT, Operations
2	<b>Functional Performance</b>	Core scheduling capabilities	Operations, Planning
3	<b>Vendor Service Delivery</b>	Support quality and SLA compliance	IT, Management
4	<b>Business Value Realization</b>	ROI and benefit achievement	Finance, Management
5	<b>User Experience &amp; Adoption</b>	User satisfaction and utilization	All Users, Training
6	<b>Integration &amp; Data Quality</b>	System connectivity and data accuracy	IT, Data Teams
7	<b>Financial Performance</b>	Cost management and value	Finance, Procurement

### 2.2 Review Frequency

Different variables require different monitoring frequencies. Real-time monitoring is non-negotiable for system availability and response time for these are the metrics that directly affect operational continuity. Business value and financial metrics require quarterly analysis with sufficient data to produce statistically meaningful trend readings.

Review Frequency	Variables Covered
<b>Real-time / Daily</b>	System availability, response times, error rates, integration health alerts.
<b>Weekly</b>	Support ticket resolution, user issues, data sync status, open defects.
<b>Monthly</b>	Functional accuracy, integration health summary, user satisfaction pulse, invoice audit.
<b>Quarterly</b>	Business value metrics, ROI tracking, strategic alignment, documentation audit, contract compliance.

 **How to Use This Framework**

Section 3 defines each performance dimension and its variables. For each variable, a metric card provides the definition, SLA target, formula, and a practical evaluation tip. Use these cards directly in monthly and quarterly review meetings. Appendix A provides a consolidated variable matrix for quick reference. Appendix B provides the monthly SLA compliance checklist for use in vendor review meetings.

## Section 3: Performance Review Dimensions

Each dimension contains specific variables that are measured, tracked, and reported against established baselines and SLA targets. For each variable, the framework provides a definition, measurement formula, SLA target, and a practical evaluation tip drawn from airline implementation experience.

Dimension owners are responsible for data collection, monthly reporting, and escalation when SLA thresholds are breached. All dimension scorecards are consolidated into the quarterly vendor scorecard reviewed at the Quarterly Business Review.

<b>1 System Performance &amp; Reliability</b>	Focus: Technical infrastructure stability	Stakeholders: IT, Operations
---	---	------------------------------

This dimension tracks the technical health and stability of the scheduling system infrastructure. These metrics are the operational foundation of the framework, without system availability and acceptable response times, no other dimension can deliver value. System performance metrics must be monitored continuously, not reviewed retrospectively.

### SLA Targets & Measurement

Metric	SLA Target	Calculation	Monitoring Tool
<b>System Availability (Uptime)</b>	≥ 99.5% (24/7 for global carriers)	$(\text{Total Hours} - \text{Downtime}) / \text{Total Hours} \times 100$	Datadog, New Relic, Nagios
<b>Response Time — Schedule Search</b>	< 2 seconds average	95th percentile tracked via APM tools	Application Performance Monitoring
<b>Response Time — Flight Creation</b>	< 5 seconds	Server-side timestamp logging	APM + server logs
<b>Response Time — Optimization Run</b>	< 30 seconds (100 flights)	Elapsed time from trigger to results	System event log
<b>Response Time — Report Generation</b>	< 10 seconds	User-facing timer	APM tools
<b>Error Rate</b>	< 0.5%; zero critical crashes/month	$(\text{Failed Transactions} / \text{Total}) \times 100$	Error tracking + help desk log
<b>Backup Success Rate</b>	100% of scheduled backups	$(\text{Successful} / \text{Scheduled Backups}) \times 100$	Backup management console
<b>RTO (Recovery Time Objective)</b>	< 4 hours	Quarterly DR test — elapsed recovery time	DR test log
<b>RPO (Recovery Point Objective)</b>	< 15 minutes data loss	Quarterly DR test — data gap at recovery	DR test log

### Additional Metrics

Metric	Description	Target	Owner
<b>API Success Rate</b>	Percentage of successful data exchanges with MRO, HR, and Finance systems.	99.95%	IT Operations
<b>Data Latency</b>	Time delay for schedule updates to reflect in downstream systems (e.g., GDS).	< 5 seconds	IT Integration
<b>Security Compliance</b>	Adherence to data protection standards (GDPR, PCI-DSS).	100%	IT Security

**📄 Worked Example: System Availability — January 2026**

Total service hours: 744 (31 days × 24 hours). Planned maintenance: 4 hours (excluded from SLA calculation per contract). Unplanned downtime: 2.5 hours.

**Calculation:  $(744 - 4 - 2.5) / (744 - 4) \times 100 = 99.66\%$  → SLA MET (target: 99.5%)**

Action: Continue monitoring. Root-cause analysis for the 2.5-hour outage must be completed and documented within 5 business days, regardless of SLA compliance status.

**📄 Worked Example: Response Time Breach — Week of 15 January 2026**

Schedule Query Response Times: Average 1.8s | 95th percentile 3.2s | Peak-time average 2.4s.

**Assessment: 95th percentile exceeds the 2-second target by 60% - SLA MISSED.**

**Root cause: database query optimization needed; peak load 08:00-10:00 UTC causing delays.**

Corrective action: Vendor to optimize database indexes within 2 weeks. Load balancing enhancement to be assessed. Response times re-tested post-fix. If not resolved within 2 weeks, escalate to PMB.

**📄 Worked Example: Error Rate & Backup Compliance — January 2026**

Error rate: 180 failed / 45,000 total transactions = 0.4% — within 0.5% target. However: 2 critical system crashes recorded (target: 0) → SLA BREACHED.

Root cause: memory leak in optimization module.

Patch deployed Jan 28.

Vendor credit applied: 5% of monthly fee.

Backup audit (Q4 2025): 91/92 successful backups (98.9%).

DR test result: RTO 2hr 45min ✓ (target < 4hr). RPO: 8 minutes data loss ✓ (target < 15min). The single failed backup was a monitoring alert error - backup actually succeeded.

Monitoring process improved.