This runbook is triggered when a Service Level Objective (SLO) drops below the defined threshold (e.g., below 99.5% availability in the last 30 days), indicating the service is at risk of violating its SLA.

Preconditions:
- Read-only access to monitoring dashboards (Grafana, Datadog, etc.)
- On-call access to deployment logs and alerting rules
- SLOs are defined and configured in the monitoring system

Steps to Follow:

Step 1: Acknowledge the Alert
- Confirm that the alert is valid and actionable
- Example: PagerDuty alert titled "CRITICAL - API Service SLO below 99.5%"
- Mark the alert as acknowledged (via UI or API)

Step 2: Identify the Breached SLO
- Open the SLO dashboard
- Locate the SLO with the triggered alert
- Note the SLO name, current compliance percentage, error budget remaining, and evaluation window

Step 3: Analyze the Burn Rate
- Calculate how fast the error budget is burning
- A burn rate > 1.0 indicates the SLO is being consumed too quickly
- Determine if the burn is spiky (recent outage) or gradual (ongoing degradation)

Step 4: Correlate With Recent Changes
- Check for any recent deploys in the last 6 to 12 hours
- Look at Git logs, CI/CD pipelines, or deployment dashboards
- Review error logs and performance graphs for increased error rates or latency
- Common causes: 5xx/4xx errors, high latency, backend bottlenecks

Step 5: Roll Back or Mitigate if Needed
- If a recent deploy is identified as the cause, perform a rollback to the last known stable version
- Alternatively, disable any active feature flags that may have introduced the issue
- Coordinate with the owning development team before action if needed

Step 6: Communicate With Stakeholders
- Post a summary in the on-call or incident Slack channel
- If user-facing impact is confirmed, update the public status page
- Include: affected SLO, cause if known, action taken, and estimated time to resolution

Step 7: Monitor Post-Mitigation
- After rollback or fix, monitor the SLO burn rate for signs of recovery
- Ensure the alert clears
- Watch for stabilization in latency and error metrics

Step 8: Create or Update Postmortem

- Record the incident details:
- Alert trigger time
- Impacted SLO