Critical SQL Server and database-related alerts that are typically configured by SQL DBAs for **proactive monitoring**, with notifications sent to a DBA distribution list (e.g., *SQLDBATeam@…*) on **hourly, daily, and weekly basis**.

The list is organized by **alert category**, with **severity**, **what to monitor**, and **recommended notification frequency**. This aligns with enterprise DBA runbooks and ITIL-based monitoring practices.

1. Availability & Instance Health (Critical)

1.1 SQL Server Service Status

- SQL Server Engine service stopped/unresponsive
- SQL Server Agent service stopped
- SSIS / SSAS / SSRS service stopped (if applicable)

  Frequency: Real-time / Hourly

  Severity: Critical

1.2 Server Connectivity

- Unable to connect to SQL instance
- Login timeout errors
- Listener (AG) unreachable

  Frequency: Real-time / Hourly

  Severity: Critical

1.3 Failover & High Availability

- Always On Availability Group failover
- AG replica not synchronizing
- Replica suspended
- Quorum loss (WSFC)
- Failover cluster node down

  Frequency: Real-time / Hourly

  Severity: Critical

2. Database Availability & Integrity (Critical)

2.1 Database State Issues

- Database offline
- Database in suspect / recovery pending / emergency mode
- Read-only database when not expected

  Frequency: Hourly

  Severity: Critical

2.2 Database Corruption

- DBCC CHECKDB failures
- Allocation or consistency errors
- Torn page / checksum failures

  Frequency: Daily (Immediate alert on detection)

  Severity: Critical

2.3 System Database Health

- Master / MSDB / Model / TempDB offline or inaccessible

  Frequency: Hourly

  Severity: Critical

3. Backup & Recovery (Critical)

3.1 Backup Failures

- Full backup failure
- Differential backup failure
- Transaction log backup failure

  Frequency: Hourly

  Severity: Critical

3.2 Missing Backups

- No full backup in last X hours
- No log backup in last X minutes (FULL/BULK recovery)

  Frequency: Daily

  Severity: Critical

3.3 Restore Validation

- Restore verification failure
- Backup file corruption

  Frequency: Weekly

  Severity: High

4. Storage & Capacity (Critical)

4.1 Disk Space

- Data drive space below threshold (e.g., <15%, <10%, <5%)
- Log drive space below threshold
- Backup drive space exhausted

  Frequency: Hourly

  Severity: Critical

4.2 File Growth Issues

- Data or log file unable to grow
- Autogrowth disabled or set too small
- Excessive autogrowth events

  Frequency: Hourly / Daily

  Severity: Critical

4.3 TempDB Space Issues

- TempDB full or nearing capacity
- TempDB data file imbalance

  Frequency: Hourly

  Severity: Critical

5. Performance & Resource Utilization (Critical)

5.1 CPU

- Sustained high CPU usage (e.g., >85%)
- SQL Server consuming abnormal CPU
- Scheduler queue length high

  Frequency: Hourly

  Severity: High / Critical

5.2 Memory

- Memory pressure (PLE below threshold)
- SQL Server memory trimmed by OS
- Insufficient max server memory configuration

  Frequency: Hourly / Daily

  Severity: High

5.3 IO Performance

- High disk latency (Data / Log / TempDB)
- IO stalls
- Read/write latency exceeding SLA

  Frequency: Hourly

  Severity: High

6. Blocking, Deadlocks & Concurrency (Critical)

6.1 Blocking

- Long-running blocking chains
- Head blocker sessions

  Frequency: Hourly

  Severity: High

6.2 Deadlocks

- Deadlock detected
- Repeated deadlocks on same objects

  Frequency: Immediate / Hourly summary

  Severity: High

7. Job & Automation Failures (Critical)

7.1 SQL Agent Jobs

- Job failure (backup, maintenance, ETL, monitoring)
- Job disabled unexpectedly
- Job running longer than expected

  Frequency: Hourly

  Severity: Critical

7.2 Maintenance Plans

- Index maintenance failure
- Statistics update failure
- Cleanup job failure

  Frequency: Daily

  Severity: High

8. Security & Access (Critical)

8.1 Authentication & Authorization

- Repeated login failures
- Locked or disabled critical SQL logins

- Orphaned users
  Frequency: Hourly / Daily
  Severity: High

8.2 Permission Changes

- sysadmin role changes
- Elevated permission grants
- Unauthorized schema changes
  Frequency: Daily / Weekly
  Severity: High

8.3 Encryption & Certificates

- Expiring certificates (TDE, AG, endpoints)
- Encryption disabled unexpectedly
  Frequency: Weekly
  Severity: High

9. Configuration & Compliance (High)

9.1 Configuration Drift

- Max memory changes
- Cost threshold for parallelism changes
- Trace flags enabled/disabled
  Frequency: Daily / Weekly
  Severity: Medium–High

9.2 Patch & Version

- SQL Server version mismatch in AG
- Missing critical patches
  Frequency: Weekly
  Severity: Medium

10. Replication / Data Movement (If Applicable)

10.1 Replication

- Replication agent failure
- Replication latency threshold exceeded
- Subscriber out of sync
  Frequency: Hourly
  Severity: High

10.2 ETL / Data Sync

- SSIS package failures
- Data load discrepancies
  Frequency: Hourly / Daily
  Severity: High

11. Error Log & Event Monitoring (Critical)

11.1 SQL Error Log

- Severity 16+ errors
- Stack dumps

- Assertion failures
- I/O errors (823, 824, 825)
  Frequency: Hourly
  Severity: Critical

11.2 Windows Event Log

- Disk errors
- Cluster errors
- Service crashes
  Frequency: Hourly
  Severity: Critical

12. Reporting & Summary Notifications

12.1 Hourly Alerts (Immediate Action)

- Service down
- Database offline
- Disk full
- Backup failure
- AG not synchronized

12.2 Daily Health Report

- Backup compliance
- Disk usage trend
- Job success/failure summary
- Performance hotspots

12.3 Weekly DBA Review

- Capacity planning
- Performance trends
- Security changes
- Patch & compliance status

Typical Notification Routing

- **Critical (Immediate):** SQLDBATeam mail + ticket + pager
- **High:** SQLDBATeam mail
- **Daily/Weekly:** Consolidated health report to SQLDBATeam

Critical SQL Server & Database Alerts Every DBA Should Monitor

Title:

Critical SQL Server & DB Alerts – Basic List

(Designed for Operational Monitoring and Rapid Response)

Section 1 — Server Health Alerts (Severity-Based)

Alert Category	Severity	Typical Meaning
Insufficient Resources	17	Server running low on memory/cpu/threads
Nonfatal Internal Errors	18	SQL Server process issues that could escalate
Resource Errors	19	SQL subsystem errors affecting queries
Fatal Error (Current Process)	20	Process crashed but instance survives
Fatal DB Error	21	Database operation failure
Table Integrity Suspect	22	Possible database corruption
Database Integrity Suspect	23	Severe corruption flagged
Hardware Error	24	Underlying hardware fault

Section 2 — Backup & Log Alerts

Critical Alerts to Configure

- **Backup overdue**
  — Last full or log backup older than threshold
- **Transaction log full**
  — Log can't truncate due to no recent backups
- **Backup failure**
  — Job failed or did not complete successfully
- **Restore test failure**
  — Restore verification unsuccessful

(These alerts protect data integrity and recoverability.)

Section 3 — Resource Utilization Alerts

Key Thresholds Typically Monitored

- **CPU > 80% sustained**
- **Memory pressure detected**
- **I/O latency high**
- **TempDB contention / saturation**
- **Worker threads starved**

(Proactive alerts help prevent performance degradation.)

Section 4 — Operation & Process Alerts

Critical Operational Conditions

- **SQL Server Agent stopped**

- **Job failures or hung jobs**
- **Blocking / Deadlocks**
- **Long-running transactions**
- **Failed login attempts**
- **Replication / Mirroring issues**

Section 5 — Integrity & Corruption Alerts

Must Alert On

- **DBCC CHECKDB errors**
- **Corruption detected in pages**
- **Suspect/Offline database**
- **Cluster/Availability group failovers**

Section 6 — Visualization & Alert Actions
Example Thresholds for Monitoring Platforms

Metric	Threshold	Alert Action
CPU avg > 75%	10 min window	Pager / SMS
Disk free < 15%	Immediate	Email + SMS
Backup failure	On every failure	Email + Team alert
Log growth > 1GB/day	Daily	Dashboard alarm
Blocking > 60s	Continuous	Page on call rotation