

# Contoso Manufacturing

|                      |                 |                   |           |                     |
|----------------------|-----------------|-------------------|-----------|---------------------|
| INSTANCE             | VERSION         | EDITION           | DATABASES | COLLECTED           |
| SAMPLE01             | 13.0.5026.0 SP2 | Standard (64-bit) | 5 user    | 2026-09-01 09:30:12 |
| ASSESSED BY          |                 |                   |           |                     |
| GRD13 Consulting LLC |                 |                   |           |                     |

97/100

SEVERE RISK

This assessment found 5 critical issues and 10 high-severity issues. The critical items describe conditions where data loss or unauthorised access is possible under circumstances that are plausible today, not hypothetically.

|            |         |           |       |                 |
|------------|---------|-----------|-------|-----------------|
| 5 Critical | 10 High | 11 Medium | 2 Low | 1 Informational |
|------------|---------|-----------|-------|-----------------|

## WHAT THIS REPORT IS

A read-only collection script was run against the instance named above. It read configuration metadata, backup history, SQL Agent job history, and server-level dynamic management views. It read no rows from any of your tables and changed nothing.

Findings are ordered by severity. Each one states what was observed, why it matters in business terms, and what fixing it involves. Where a finding maps to a question that commonly appears on cyber-insurance applications or compliance audits, the relevant control is tagged.

## FINDINGS AT A GLANCE

| ID      | FINDING                                   | SEVERITY | CATEGORY       | EFFORT |
|---------|-------------------------------------------|----------|----------------|--------|
| REC-001 | 2 databases have no backup history at all | Critical | Recoverability | Low    |

| ID      | FINDING                                                    | SEVERITY | CATEGORY       | EFFORT |
|---------|------------------------------------------------------------|----------|----------------|--------|
| REC-002 | 2 databases have no recent full backup                     | Critical | Recoverability | Low    |
| REC-003 | Databases in FULL recovery with no transaction log backups | Critical | Recoverability | Low    |
| SEC-001 | 2 SQL logins with a blank or trivially guessable password  | Critical | Security       | Low    |
| SUP-001 | SQL Server 2016 is past end of support                     | Critical | Supportability | High   |
| CFG-001 | AUTO_SHRINK is enabled                                     | High     | Configuration  | Low    |
| CFG-003 | Page verification is not set to CHECKSUM                   | High     | Configuration  | Low    |
| CFG-004 | Max server memory is unlimited                             | High     | Configuration  | Low    |
| OPS-001 | 2 SQL Agent jobs are failing                               | High     | Operations     | Medium |
| OPS-002 | Backup or maintenance jobs are disabled                    | High     | Operations     | Low    |
| OPS-003 | No scheduled integrity check could be identified           | High     | Operations     | Medium |
| REC-004 | Transaction log backups have stopped running               | High     | Recoverability | Low    |
| REC-005 | Backups are written to a drive-letter path, not a UNC path | High     | Recoverability | Medium |
| SEC-005 | xp_cmdshell is enabled                                     | High     | Security       | Low    |
| SEC-008 | TRUSTWORTHY is enabled on user databases                   | High     | Security       | Medium |
| CFG-002 | AUTO_CLOSE is enabled                                      | Medium   | Configuration  | Low    |

| ID      | FINDING                                                     | SEVERITY      | CATEGORY       | EFFORT |
|---------|-------------------------------------------------------------|---------------|----------------|--------|
| CFG-005 | MAXDOP is unconfigured on a 16-core server                  | Medium        | Configuration  | Low    |
| CFG-008 | Large files are set to grow by percentage                   | Medium        | Configuration  | Low    |
| CFG-009 | Large files are set to grow 1 MB at a time                  | Medium        | Configuration  | Low    |
| OPS-006 | The instance has not been restarted in 668 days             | Medium        | Operations     | Medium |
| PRF-001 | Page life expectancy is 141 seconds                         | Medium        | Performance    | Medium |
| SEC-002 | 7 named accounts hold sysadmin                              | Medium        | Security       | Medium |
| SEC-003 | The 'sa' account is enabled under its default name          | Medium        | Security       | Low    |
| SEC-004 | 3 active SQL logins with password policy disabled           | Medium        | Security       | Medium |
| SEC-006 | OLE Automation Procedures are enabled                       | Medium        | Security       | Low    |
| SUP-004 | 3 databases running an old compatibility level              | Medium        | Supportability | Medium |
| CFG-006 | Cost threshold for parallelism is still at the 1995 default | Low           | Configuration  | Low    |
| CFG-007 | Configuration changes are waiting on a restart              | Low           | Configuration  | Low    |
| PRF-002 | PAGEIOLATCH_SH accounts for 41% of server wait time         | Informational | Performance    | Medium |

REC-001

Critical

## 2 databases have no backup history at all

### WHAT WAS OBSERVED

```
No successful full backup appears in msdb history for: WebPortal, Reporting.
```

### WHY IT MATTERS

If the storage holding these databases fails right now, the data is gone. There is no recovery path. This is the single highest-consequence finding any assessment can produce, and it is more common than people expect -- usually because a database was added after the backup routine was written and nobody updated the routine.

### WHAT FIXING IT INVOLVES

Take a full backup today, before anything else on this list. Then add these databases to the scheduled backup routine and change the routine so it enumerates databases dynamically instead of naming them.

Maps to: [SOC 2 A1.2](#) [ISO 27001 A.8.13](#) [Cyber insurance questionnaire](#)

REC-002

Critical

## 2 databases have no recent full backup

### WHAT WAS OBSERVED

```
Days since last successful full backup: ERP_Archive (75d), CRM (23d).
```

### WHY IT MATTERS

Your worst-case data loss on these databases is at least 75 days. Whatever recovery objective the business believes it has, this is the number that is actually true today.

### WHAT FIXING IT INVOLVES

Find out whether the backup job is failing silently or was never scheduled. Fix the schedule, then add alerting so a failed backup raises a notification rather than waiting to be discovered.

Maps to: [SOC 2 A1.2](#) [Cyber insurance questionnaire](#)

REC-003

Critical

## Databases in FULL recovery with no transaction log backups

### WHAT WAS OBSERVED

These databases use the FULL or BULK\_LOGGED recovery model but have no log backup history: model, ERP\_Prod, WebPortal.

### WHY IT MATTERS

Two problems at once. First, the transaction log will grow until it fills the drive, because nothing is truncating it -- this is the most common cause of an unplanned outage on an otherwise healthy SQL Server. Second, the FULL recovery model exists specifically to allow point-in-time recovery, and without log backups you do not have it. You are paying the cost of FULL recovery and receiving the recovery capability of SIMPLE.

### WHAT FIXING IT INVOLVES

Decide which the business actually needs. If point-in-time recovery matters, schedule log backups every 15 minutes. If it does not, switch the database to SIMPLE recovery and the log stops growing.

Maps to: [SOC 2 A1.2](#) [ISO 27001 A.8.13](#)

SEC-001

Critical

## 2 SQL logins with a blank or trivially guessable password

### WHAT WAS OBSERVED

```
reportuser -- password matches login name; test_login -- blank password
```

### WHY IT MATTERS

These logins can be used by anyone who can reach the instance on the network. If any of them holds elevated rights, this is a complete compromise of the database and every credential stored in it. Password guessing against SQL Server is fully automated and constant.

### WHAT FIXING IT INVOLVES

Change or disable each login today. Where a login belongs to an application, coordinate the change with the application owner, then enable CHECK\_POLICY so it cannot recur.

Maps to: [PCI DSS 8.3.6](#) [SOC 2 CC6.1](#) [ISO 27001 A.5.17](#)

SUP-001

Critical

## SQL Server 2016 is past end of support

### WHAT WAS OBSERVED

Instance reports version 13.0.5026.0 (SQL Server 2016, build level SP2). Extended support ended 14 July 2026 -- 49 days ago.

### WHY IT MATTERS

Microsoft no longer issues security patches for this version. Any vulnerability discovered from that date forward stays open permanently unless you buy Extended Security Updates. Most cyber insurance applications and every major compliance framework ask directly whether your systems are vendor-supported; the honest answer here is no.

### WHAT FIXING IT INVOLVES

Upgrade in place to a supported version, migrate to a new instance, or move to Azure SQL. Where none of those fit the timeline, price Extended Security Updates as a bridge -- year one is commonly quoted at around 75% of the original license cost, but confirm current pricing with Microsoft or your reseller before budgeting. Note that ESU is included at no extra charge for instances running in Azure, which changes the arithmetic on a migration.

Maps to: [PCI DSS 12.3.4](#) [SOC 2 CC7.1](#) [Cyber insurance questionnaire](#) [ISO 27001 A.8.8](#)

CFG-001

High

## AUTO\_SHRINK is enabled

### WHAT WAS OBSERVED

AUTO\_SHRINK ON: ERP\_Archive

### WHY IT MATTERS

Auto shrink repeatedly releases and re-allocates file space. It comprehensively fragments every index in the database, consumes CPU and IO at unpredictable times, and the space it frees is immediately re-consumed by normal growth. There is no workload for which this setting is the right answer, which is why it has been on every SQL Server bad-practice list for twenty years.

### WHAT FIXING IT INVOLVES

Set AUTO\_SHRINK OFF, then rebuild indexes once to undo the fragmentation.

CFG-003

High

## Page verification is not set to CHECKSUM

### WHAT WAS OBSERVED

```
PAGE_VERIFY setting: ERP_Prod (TORN_PAGE_DETECTION), Reporting (NONE)
```

### WHY IT MATTERS

CHECKSUM is how SQL Server notices that storage silently corrupted a page. Without it, corruption is discovered when a user reads the bad row -- often months later, by which time every backup you hold contains the same corruption and there is nothing clean to restore.

### WHAT FIXING IT INVOLVES

Set PAGE\_VERIFY CHECKSUM on each database, then run DBCC CHECKDB to establish that the current state is clean.

Maps to: [SOC 2 PI1.4](#)

CFG-004

High

## Max server memory is unlimited

### WHAT WAS OBSERVED

```
max server memory is at its default of 2147483647 MB on a host with 65,536 MB of RAM.
```

### WHY IT MATTERS

SQL Server will take essentially all memory on the machine and give it back only under pressure. Windows, the backup agent, and monitoring tools end up competing with the database for RAM, and the symptom is server-wide sluggishness that looks like a hardware problem.

### WHAT FIXING IT INVOLVES

Set max server memory to roughly 52,428 MB on this host, leaving headroom for the OS and any other services. The setting is dynamic and needs no restart.

OPS-001

High

## 2 SQL Agent jobs are failing

### WHAT WAS OBSERVED

```
Last run outcome was Failed for: Index Maintenance - Weekly (2026-08-30 01:00:00.000),  
ETL - Load Warehouse (2026-09-01 04:00:00.000)
```

### WHY IT MATTERS

Something scheduled is not happening. When the failing job is a backup, index maintenance, or an integrity check, the consequence compounds quietly for as long as nobody looks.

### WHAT FIXING IT INVOLVES

Work through the job history for each. Then configure Database Mail and set a failure notification on every job, so the next failure announces itself.

Maps to: **SOC 2 CC7.2**

OPS-002

High

## Backup or maintenance jobs are disabled

### WHAT WAS OBSERVED

```
Disabled: Backup - Log - Every 15 min
```

### WHY IT MATTERS

A disabled job produces no failure alert, no error, and no output. It is the quietest possible way for a backup routine to stop existing.

### WHAT FIXING IT INVOLVES

Determine why each was disabled. Re-enable it, or delete it so the next person does not assume it is running.

Maps to: **SOC 2 A1.2**

OPS-003

High

## No scheduled integrity check could be identified

### WHAT WAS OBSERVED

Across 4 SQL Agent job(s) and 5 user database(s), no job name suggests it runs DBCC CHECKDB. This check reads job names only, not job steps -- if integrity checks run under a job whose name does not indicate it, or outside SQL Agent entirely, say so and this finding can be withdrawn.

### WHY IT MATTERS

Storage corruption is silent until something reads the damaged page. Without a scheduled integrity check, the discovery event is a user error message, and by then the corruption is present in every backup you still hold. Backup retention is only protective if you know the date corruption began.

### WHAT FIXING IT INVOLVES

Schedule DBCC CHECKDB weekly against every database, with failure alerting. On large databases, spread it across the week or run it against a restored copy.

Maps to: [SOC 2 PI1.4](#) [ISO 27001 A.8.13](#)

REC-004

High

## Transaction log backups have stopped running

### WHAT WAS OBSERVED

Hours since last log backup: CRM (528h).

### WHY IT MATTERS

Point-in-time recovery is unavailable for the last 528 hours, and the transaction log is growing the entire time.

### WHAT FIXING IT INVOLVES

Investigate the log backup job history and restore the schedule.

Maps to: [SOC 2 A1.2](#)

## Backups are written to a drive-letter path, not a UNC path

### WHAT WAS OBSERVED

The most recent full backup went to a drive-letter path for: ERP\_Prod -> E:\SQLBackup\ERP\_Prod.bak, CRM -> E:\SQLBackup\CRM.bak. A drive letter may be local storage, a mapped network drive, or a SAN or iSCSI volume -- the backup history does not distinguish them. Confirm which before treating this as settled.

### WHY IT MATTERS

If these paths are local storage, the backups protect against exactly one failure mode: someone dropping a table. They do not protect against server loss, storage failure, fire, or ransomware -- and ransomware is the scenario insurers now ask about by name, because modern strains deliberately encrypt local backup files first. If the paths are on separate storage, the remaining question is whether the database service account can delete them, which is the control insurers actually want.

### WHAT FIXING IT INVOLVES

Copy backups to a separate system with different credentials, and keep at least one copy that the database service account cannot write to or delete. Immutable or write-once storage is the current expectation on insurance questionnaires.

Maps to: [Cyber insurance questionnaire](#) [ISO 27001 A.8.13](#) [SOC 2 A1.2](#)

SEC-005

High

## xp\_cmdshell is enabled

### WHAT WAS OBSERVED

```
sys.configurations reports xp_cmdshell running value = 1.
```

### WHY IT MATTERS

xp\_cmdshell runs operating system commands under the SQL Server service account. Combined with any SQL injection flaw in any application touching this instance, it turns a database vulnerability into control of the Windows host. It is the single most requested feature in published SQL Server attack tooling.

### WHAT FIXING IT INVOLVES

Disable it. Where a job genuinely needs to run OS commands, move that work into a SQL Agent CmdExec step with a dedicated proxy account scoped to just that task.

Maps to: **PCI DSS 2.2.4** **SOC 2 CC6.6** **ISO 27001 A.8.9**

SEC-008

High

## TRUSTWORTHY is enabled on user databases

### WHAT WAS OBSERVED

```
TRUSTWORTHY ON: CRM
```

### WHY IT MATTERS

A db\_owner in one of these databases can escalate to sysadmin on the whole instance. This is a well-documented privilege escalation path and it is almost always switched on by accident during a restore or a CLR deployment.

### WHAT FIXING IT INVOLVES

Set TRUSTWORTHY OFF. If a CLR assembly or cross-database call depends on it, replace it with certificate signing.

Maps to: **PCI DSS 7.2** **SOC 2 CC6.3**

CFG-002

Medium

## AUTO\_CLOSE is enabled

### WHAT WAS OBSERVED

```
AUTO_CLOSE ON: ERP_Prod
```

### WHY IT MATTERS

The database shuts down when the last user disconnects and must fully restart on the next connection. Users experience this as random multi-second hangs on the first query of the morning, and the cause is almost never found because it does not reproduce under load.

### WHAT FIXING IT INVOLVES

Set AUTO\_CLOSE OFF.

CFG-005

Medium

## MAXDOP is unconfigured on a 16-core server

### WHAT WAS OBSERVED

```
max degree of parallelism = 0 with 16 logical processors.
```

### WHY IT MATTERS

A single large query can commandeer every core on the box. Under concurrency this produces CXPACKET waits and wildly inconsistent response times -- the same report taking two seconds one minute and ninety the next.

### WHAT FIXING IT INVOLVES

Set MAXDOP to 8 as a starting point for this core count, and raise cost threshold for parallelism at the same time.

CFG-008

Medium

## Large files are set to grow by percentage

### WHAT WAS OBSERVED

```
Percentage autogrowth on large files: ERP_Prod.ERP_Prod_Data (371 GB, +10%),  
ERP_Prod.ERP_Prod_Log (31 GB, +10%)
```

### WHY IT MATTERS

Percentage growth compounds. A 100 GB file growing at 10% asks for 10 GB in a single allocation, and the database stops responding for the duration. The bigger the file gets, the longer the freeze.

### WHAT FIXING IT INVOLVES

Switch to a fixed growth increment sized for the workload, commonly 512 MB to 1 GB.

CFG-009

Medium

## Large files are set to grow 1 MB at a time

### WHAT WAS OBSERVED

```
1 MB autogrowth on: CRM.CRM_Data (+1 MB)
```

### WHY IT MATTERS

Every megabyte of growth is a separate allocation event, each one pausing writes. It also fragments the file badly at the filesystem level, which slows every sequential read for the life of the database.

### WHAT FIXING IT INVOLVES

Set a fixed growth increment of 512 MB or 1 GB.

OPS-006

Medium

## The instance has not been restarted in 668 days

### WHAT WAS OBSERVED

```
SQL Server start time: 2024-11-02 03:14:55.000.
```

### WHY IT MATTERS

More than a year of uptime means more than a year without an operating system or SQL Server patch. It also means the failover and startup path has not been exercised in that time -- nobody knows whether this server comes back up cleanly.

### WHAT FIXING IT INVOLVES

Establish a patching window. Use the first one to confirm the instance restarts cleanly and every application reconnects.

Maps to: [PCI DSS 6.3.3](#) [Cyber insurance questionnaire](#)

PRF-001

Medium

## Page life expectancy is 141 seconds

### WHAT WAS OBSERVED

```
Page life expectancy counter reads 141.
```

### WHY IT MATTERS

Data pages are surviving in memory for well under five minutes before being evicted, so the same data is being read from disk repeatedly. This is either a memory shortage or a query reading far more data than it needs -- usually the second.

### WHAT FIXING IT INVOLVES

Check max server memory first, then look at the highest-read queries. A single missing index is a common cause.

SEC-002

Medium

## 7 named accounts hold sysadmin

### WHAT WAS OBSERVED

Members of the sysadmin server role, excluding 0 built-in service principal(s): sa, CONTOSO\Domain Admins, CONTOSO\jsmith, CONTOSO\mdavis, erp\_app, reportuser, vendor\_support. Note that Windows group membership is not expanded here, so anyone who is sysadmin by virtue of belonging to a group listed above is additional to this count.

### WHY IT MATTERS

Every sysadmin can read every row in every database, disable auditing, and delete backups. Auditors treat a large sysadmin population as a failure of least privilege, and it is one of the few findings that is trivially easy for them to check. Where one of the members is a Windows group such as Domain Admins, the effective population is everyone in that group.

### WHAT FIXING IT INVOLVES

Review each member. Application service accounts almost never need sysadmin -- db\_owner on their own database is usually sufficient. Remove the ones that cannot be justified in writing.

Maps to: [PCI DSS 7.2](#) [SOC 2 CC6.3](#) [ISO 27001 A.8.2](#)

SEC-003

Medium

## The 'sa' account is enabled under its default name

### WHAT WAS OBSERVED

Login 'sa' exists, is enabled, and has not been renamed.

### WHY IT MATTERS

'sa' is the first login every automated attack tries, because it is the one account guaranteed to exist and guaranteed to be sysadmin. Leaving it enabled and named 'sa' gives an attacker a free half of the credential.

### WHAT FIXING IT INVOLVES

Disable 'sa' if nothing uses it -- which is usually the case. If something does use it, rename the login and set a long random password, then fix the thing that uses it.

Maps to: [PCI DSS 2.2.2](#) [SOC 2 CC6.1](#)

SEC-004

Medium

## 3 active SQL logins with password policy disabled

### WHAT WAS OBSERVED

```
CHECK_POLICY is OFF for: erp_app, reportuser, vendor_support
```

### WHY IT MATTERS

These logins are exempt from Windows password complexity, expiry, and lockout rules. Password guessing against them is unlimited -- there is no lockout to stop an attacker trying indefinitely.

### WHAT FIXING IT INVOLVES

Enable CHECK\_POLICY on each login. Expect to reset the password at the same time, and coordinate with application owners.

Maps to: [PCI DSS 8.3.6](#) [ISO 27001 A.5.17](#)

SEC-006

Medium

## OLE Automation Procedures are enabled

### WHAT WAS OBSERVED

```
sys.configurations reports Ole Automation Procedures running value = 1.
```

### WHY IT MATTERS

Another documented path from SQL injection to code execution on the host. It is rarely used by modern applications and is usually left on from a one-off task somebody ran years ago.

### WHAT FIXING IT INVOLVES

Confirm nothing depends on it, then disable it.

Maps to: [PCI DSS 2.2.4](#)

SUP-004

Medium

## 3 databases running an old compatibility level

### WHAT WAS OBSERVED

```
Instance default is compatibility level 130. These databases are lower: ERP_Prod (level 110), ERP_Archive (level 110), Reporting (level 100).
```

### WHY IT MATTERS

The database is running under an older query optimizer. Performance features shipped in later versions are unavailable, and the gap grows with every upgrade you defer. It also usually means nobody tested the application against the current optimizer -- which turns your next upgrade into a bigger unknown than it should be.

### WHAT FIXING IT INVOLVES

Raise compatibility level one step at a time in a test copy, with Query Store enabled so regressions are visible and reversible.

CFG-006

Low

## Cost threshold for parallelism is still at the 1995 default

### WHAT WAS OBSERVED

```
cost threshold for parallelism = 5.
```

### WHY IT MATTERS

Trivial queries get parallel plans, paying the coordination overhead of going parallel for work that would finish faster on one core.

### WHAT FIXING IT INVOLVES

Raise it to 50 and observe. This is a dynamic setting and is easy to revert.

CFG-007

Low

Configuration changes are waiting on a restart

WHAT WAS OBSERVED

Configured value differs from running value for: optimize for ad hoc workloads

WHY IT MATTERS

Somebody changed these settings and the change never took effect. The server is not running the configuration your team believes it is running.

WHAT FIXING IT INVOLVES

Confirm the intended values, then apply them at the next restart -- or revert the configured value if the change is no longer wanted.

PRF-002

Informational

PAGEIOLATCH\_SH accounts for 41% of server wait time

WHAT WAS OBSERVED

Top wait since last restart: PAGEIOLATCH\_SH, 812,400 seconds (41.2% of total).

WHY IT MATTERS

This is where the server spends its waiting time. reading data pages from disk -- memory pressure or a missing index

WHAT FIXING IT INVOLVES

Treat as the starting point for a performance engagement rather than an item to fix directly.

DATABASE INVENTORY

| DATABASE    | STATE  | RECOVERY | COMPAT | SIZE (MB) | LAST FULL BACKUP    |
|-------------|--------|----------|--------|-----------|---------------------|
| CRM         | ONLINE | FULL     | 130    | 74000     | 2026-08-09 23:20:02 |
| ERP_Archive | ONLINE | SIMPLE   | 110    | 208000    | 2026-06-18 02:00:00 |
| ERP_Prod    | ONLINE | FULL     | 110    | 412000    | 2026-08-31 23:15:41 |

| DATABASE  | STATE  | RECOVERY | COMPAT | SIZE (MB) | LAST FULL BACKUP |
|-----------|--------|----------|--------|-----------|------------------|
| Reporting | ONLINE | SIMPLE   | 100    | 33000     | never            |
| WebPortal | ONLINE | FULL     | 130    | 9600      | never            |

SUGGESTED ORDER OF WORK

| # | DO THIS                                                    | BECAUSE                                                                                          |
|---|------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 1 | 2 databases have no backup history at all                  | If the storage holding these databases fails right now, the data is gone.                        |
| 2 | 2 databases have no recent full backup                     | Your worst-case data loss on these databases is at least 75 days.                                |
| 3 | Databases in FULL recovery with no transaction log backups | Two problems at once.                                                                            |
| 4 | 2 SQL logins with a blank or trivially guessable password  | These logins can be used by anyone who can reach the instance on the network.                    |
| 5 | SQL Server 2016 is past end of support                     | Microsoft no longer issues security patches for this version.                                    |
| 6 | AUTO_SHRINK is enabled                                     | Auto shrink repeatedly releases and re-allocates file space.                                     |
| 7 | Page verification is not set to CHECKSUM                   | CHECKSUM is how SQL Server notices that storage silently corrupted a page.                       |
| 8 | Max server memory is unlimited                             | SQL Server will take essentially all memory on the machine and give it back only under pressure. |