Toltec Systems

IT estate review
Contoso Precision Ltd

Sample report · September 2026

This is a sample. Contoso is the fictional company Microsoft uses in its own documentation. Every name, figure and finding in this report is invented, to show the depth and format of a Toltec estate review.

Prepared by Toltec Systems Ltd · Adamson House, Didsbury, Manchester M20 2YY · www.toltec.io

Summary for the board

Well run day to day, exposed in three places.

Contoso's estate is well looked after: devices are managed, most patching is current and the team knows its systems. The risks sit in three places: an unsupported database platform under the ERP system, a recovery process that has never been timed end to end and cannot yet meet its four-hour target, and administrator access that is wider than it needs to be. None of these needs a new platform to fix, and all three can be substantially addressed within 90 days.

Area	Rating	Area	Rating
Identity and access	Needs attention	Backup and recovery	Urgent
Devices and patching	Adequate	Email and collaboration	Needs attention
Servers and virtualisation	Urgent	Security operations	Needs attention
Network and perimeter	Needs attention	Licensing and cost	Adequate

Five things we recommend first

1. Schedule the upgrade of the ERP database, which has been out of support since July 2026.
2. Time a full recovery of the ERP service and close the gap to the four-hour target.
3. Reduce Global Administrators from six to three and create two emergency access accounts.
4. Enable DKIM, move DMARC to enforcement and block external forwarding.
5. Extend endpoint detection to the servers, and give the alerts a named owner.

The first 90 days need roughly 18 to 24 engineer days, most of it in the database upgrade and the recovery work. We can deliver all of it, or support your team while you do.

Scope and method

What we looked at, and how.

We reviewed Contoso's IT estate between 1 and 12 September 2026, across the head office and both workshop sites. The work included:

- interviews with the finance director, the operations manager and the in-house IT coordinator;
- a read-only review of the Microsoft 365 tenant, Entra ID, Active Directory and Group Policy;
- an authenticated vulnerability scan of every server and a sample of devices;
- a timed restore of one production server from its backups;
- a review of licences, contracts and renewal dates.

Out of scope: application code, physical security, and supplier-hosted systems other than their integration points.

The estate at a glance

86 users	104 laptops and desktops	3 sites
2 Hyper-V hosts	11 virtual servers	4 hours stated recovery time for the ERP system

Key applications	ERP system on SQL Server 2016; CAD file vault; hosted payroll
Microsoft 365	Business Premium, 86 licences assigned, 14 unassigned
Backup	Nightly image backups, one copy on site and one in cloud storage
Connectivity	1 Gbps leased line with 4G failover at head office; broadband at the workshops

Findings

Area by area.

Identity and access

Needs attention

What we found

Conditional Access enforces multi-factor authentication for 81 of 86 accounts. The five exclusions are shared mailboxes with sign-in still enabled and a scanner account. Legacy authentication is blocked. There are six Global Administrators, four of them the everyday accounts of staff who also read email, and no emergency access accounts.

Why it matters

A phished administrator mailbox gives an attacker the whole tenant, and excluded accounts are the first ones attackers look for.

What we recommend

- Block sign-in on the shared mailboxes and move the scanner to a modern send method.
- Give each administrator a separate cloud-only admin account and reduce Global Administrators to three.
- Create two emergency access accounts protected with FIDO2 keys, with an alert on any sign-in.

Effort: 2 to 3 engineer days

Devices and patching

Adequate

What we found

All 104 laptops and desktops are enrolled in Intune and 95 are compliant. Nine have been non-compliant for more than 30 days, mostly workshop machines that rarely leave their docks. Three Windows 10 devices remain in use after support ended in October 2025. Operating system updates are current on 96% of devices, but third-party applications such as PDF readers and CAD viewers are patched by hand. BitLocker is enabled on 101 devices.

Why it matters

Unsupported and non-compliant machines are the easiest way in, and today they can still reach Microsoft 365.

What we recommend

- Replace or upgrade the three Windows 10 devices.
- Require a compliant device for access to Microsoft 365.
- Automate third-party patching and encrypt the remaining three devices.

Effort: 2 engineer days, plus hardware

Servers and virtualisation

Urgent

What we found

Both Hyper-V hosts run Windows Server 2016, whose extended support ends on 12 January 2027. The ERP database runs on SQL Server 2016, which left extended support on 14 July 2026 and no longer receives security updates. Host firmware is two years behind. Capacity is comfortable: peak memory use is 71% and storage 64%.

Why it matters

The system the business depends on most runs on a platform that no longer receives security fixes, on hosts with four months of support left.

What we recommend

- Upgrade the ERP database to SQL Server 2022 or 2025, whichever version the ERP supplier certifies, on Windows Server 2025, in a window agreed with the supplier.
- Bring host firmware up to date, then rebuild the hosts on Windows Server 2025 before January 2027.
- If the supplier needs more time, check whether paid Extended Security Updates can act as a short bridge.

Effort: 6 to 8 engineer days, plus supplier time

Network and perimeter

Needs attention

What we found

Firewall firmware is 14 months out of date. A single flat network carries servers, desktops, printers and the CCTV system. Remote access uses a VPN with multi-factor authentication, and guest Wi-Fi is correctly isolated. Five inbound firewall rules could not be explained, including remote desktop access to the address of a decommissioned server.

Why it matters

On a flat network, one compromised printer or camera can see the ERP server. Unexplained inbound rules are how forgotten services get found.

What we recommend

- Update the firewall and remove the five unexplained rules.
- Separate servers, user devices, printers and CCTV into their own networks, with rules between them.

Effort: 3 to 4 engineer days

Backup and recovery

Urgent

What we found

Nightly image backups succeed and a copy goes off site. Our timed restore of the ERP server took 7 hours 40 minutes against a stated recovery time of 4 hours; most of that went on copying the image back from cloud storage and reconfiguring the database connection. The backup console signs in with domain credentials, and the on-site copies can be deleted by a domain administrator. Microsoft 365 data is covered only by retention policies.

Why it matters

Ransomware that reached the domain could reach the backups too, and even a clean recovery would currently miss its target by almost four hours.

What we recommend

- Make one backup copy immutable and move the backup console to separate credentials with multi-factor authentication.
- Keep a recent copy of the ERP server on site for fast restores, then retest and time the recovery.
- Add a dedicated Microsoft 365 backup.

Effort: 3 to 4 engineer days

Email and collaboration

Needs attention

What we found

SPF is correct, but DKIM is not enabled and DMARC is set to none. Automatic forwarding to external addresses is allowed, and two mailboxes forward to personal accounts. SharePoint allows anyone links with no expiry date.

Why it matters

Without DMARC enforcement, anyone can send email as Contoso. Forwarding and open links can move data out without anyone noticing.

What we recommend

- Enable DKIM, then move DMARC to quarantine and on to reject.
- Block external forwarding, with named exceptions only.
- Make specific people the default link type and expire anyone links after 30 days.

Effort: 1 to 2 engineer days

Security operations

Needs attention

What we found

Microsoft Defender for Endpoint runs on every laptop and desktop but not on the servers. Alerts go to a shared mailbox with no named owner. The unified audit log is on, and Microsoft Secure Score stands at 48%.

Why it matters

The detection works, but nobody is watching, and the servers, where an attacker would do the most damage, are not monitored at all.

What we recommend

- Onboard the servers to endpoint detection and response.
- Route alerts to a named owner with holiday cover.
- Review Secure Score monthly and track the top recommendations.

Effort: 2 engineer days, plus ongoing monitoring

Licensing and cost

Adequate

What we found

There are 14 unassigned Microsoft 365 licences, a legacy antivirus subscription still renewing alongside Defender, and two telephony contracts covering the same numbers.

Why it matters

Around £4,300 a year can be saved without changing a single service.

What we recommend

- Remove the unassigned licences at renewal.
- Cancel the legacy antivirus subscription.
- Consolidate telephony onto one contract.

Effort: Half a day

Risk register

The risks, ranked.

Risk	Likelihood	Impact	Rating	Owner
ERP database on an unsupported SQL Server version	Likely	Severe	Urgent	IT coordinator, with the ERP supplier
Recovery time exceeds its target by nearly four hours	Possible	Severe	Urgent	Finance director
Backups deletable by a compromised domain administrator	Possible	Severe	Needs attention	IT coordinator
Servers without endpoint detection	Possible	Major	Needs attention	IT coordinator
Six Global Administrators and no emergency access	Possible	Major	Needs attention	IT coordinator
Flat network including CCTV and printers	Possible	Major	Needs attention	Operations manager
Email spoofing, and data leaving through forwarding	Likely	Moderate	Needs attention	IT coordinator
Unsupported Windows 10 devices	Likely	Moderate	Adequate	Operations manager

Roadmap

The next twelve months.

Sequenced so the biggest risks close first, and so nothing needs a second visit to the same system.

First 30 days

- Block sign-in on shared mailboxes; reduce Global Administrators; create emergency access accounts.
- Remove the unexplained firewall rules and update firmware.
- Enable DKIM and block external forwarding.
- Onboard servers to endpoint detection and name the alert owner.
- Make one backup copy immutable.

31 to 90 days

- Upgrade the ERP database in an agreed window.
- Retest the recovery, with timings, against the four-hour target.
- Segment the network.
- Move DMARC to reject.
- Replace the Windows 10 devices.
- Add Microsoft 365 backup.

3 to 12 months

- Rebuild the Hyper-V hosts on Windows Server 2025, complete by December 2026.
- Consider Privileged Identity Management at the next licence review.
- Run a full failover test once a year.
- Review administrator and application access every quarter.

Appendix

How to read this report.

Rating	Meaning
Urgent	A realistic risk to the business now. Act within 30 days.
Needs attention	A gap an attacker or an outage could exploit. Plan within the quarter.
Adequate	Working, with improvements worth scheduling.
Strong	Good practice, to keep in place.

Every tool we used was read-only, and no configuration was changed during the review. Evidence for each finding, including screenshots and exports, is held in a separate annex shared securely with the client.

Sample report. Contoso Precision Ltd is fictional, and every name, figure and finding here was invented for illustration. A real review is shaped by your estate, your risks and the questions your board needs answered.