Manufacturing IT Readiness Checklist

Interlink Technology, Inc.
interlinktek.com | Murrieta, CA

Use this checklist to identify gaps in your ERP infrastructure, shop floor connectivity, cybersecurity posture, backup readiness, and lifecycle planning. Each item is labeled Critical, Important, or Recommended.

This checklist is a planning tool, not a formal security audit or compliance certification. Use it to identify areas to review and prioritize.

● CRITICAL
Could stop production, block recovery, affect cyber insurance, or create major business risk

● IMPORTANT
Should be addressed in the next planning cycle

● REC
Improves documentation, consistency, or long-term IT maturity

01 ERP & BUSINESS SYSTEMS

☐	The ERP server operating system is currently supported by the vendor.	CRITICAL
☐	The ERP application is on a supported version with vendor updates available.	CRITICAL
☐	ERP server hardware is within its expected service life and not approaching end-of-life.	CRITICAL
☐	ERP and production-related data is backed up separately from general file backups.	CRITICAL
☐	Users can access the ERP system remotely without using insecure methods.	IMPORTANT
☐	ERP performance issues (slowdowns, timeouts, errors) have been documented and reviewed.	IMPORTANT
☐	Vendor contact information and support agreements for the ERP system are documented.	IMPORTANT
☐	ERP user accounts are reviewed periodically and inactive accounts are disabled.	IMPORTANT
☐	The ERP system has been tested after a server or infrastructure change.	REC
☐	ERP training and onboarding documentation exists for new users.	REC

02 SHOP FLOOR CONNECTIVITY

☐	Shop floor devices (barcode scanners, terminals, production workstations) are on a documented network.	CRITICAL
☐	Production floor devices are on a separate network segment from general office systems.	CRITICAL
☐	Shop floor connectivity failures can be quickly identified, reported, and escalated.	CRITICAL
☐	Wireless coverage has been tested across the full production floor.	IMPORTANT
☐	Shop floor devices are included in the hardware inventory and tracked for lifecycle.	IMPORTANT

☐	Barcode scanners and production terminals are on a supported firmware or OS version.	IMPORTANT
☐	Remote vendor access to shop floor systems is restricted and logged.	IMPORTANT
☐	Known shop floor connectivity issues have been documented and assigned for resolution.	IMPORTANT
☐	Shop floor device replacement planning is included in the annual IT budget.	REC
☐	A floor walk-through has been completed to document all production-connected devices.	REC

03 CYBERSECURITY & CYBER INSURANCE READINESS

☐	Multi-factor authentication (MFA) is enabled on all email accounts.	CRITICAL
☐	MFA is enabled on all remote access methods (VPN, remote desktop, cloud applications).	CRITICAL
☐	Endpoint detection and response (EDR) software is installed on all workstations and servers.	CRITICAL
☐	Office and production networks are segmented, with only required traffic allowed between them.	CRITICAL
☐	The current cyber insurance policy has been reviewed against the carrier's control requirements.	CRITICAL
☐	All cyber insurance renewal questionnaire questions can be answered accurately.	IMPORTANT
☐	Privileged administrator accounts are separate from daily-use accounts.	IMPORTANT
☐	Software and operating system updates are applied on a documented schedule.	IMPORTANT
☐	A documented incident response process exists for ransomware or data breach events.	IMPORTANT
☐	Email security filtering (spam, phishing, attachment scanning) is active.	IMPORTANT
☐	DNS filtering or web content filtering is in place for all users.	REC
☐	Security awareness training has been completed by all staff in the past 12 months.	REC

04 BACKUPS & DISASTER RECOVERY

☐	Backups of the ERP server and production-critical systems run on a documented schedule.	CRITICAL
☐	A backup restore has been tested within the past 90 days and results were documented.	CRITICAL
☐	At least one backup copy is stored offsite or in a cloud location separate from the primary system.	CRITICAL
☐	Recovery time expectations for the ERP server have been defined and documented.	CRITICAL
☐	Backup failure alerts are configured and actively monitored.	CRITICAL
☐	All servers and workstations critical to production are included in the backup schedule.	IMPORTANT
☐	The backup retention period is documented and meets any regulatory or insurance requirements.	IMPORTANT
☐	Backup storage capacity has been reviewed and is not at risk of filling up.	IMPORTANT
☐	A disaster recovery plan exists that covers what to do if the ERP server fails.	IMPORTANT

☐	Backup logs are reviewed at least monthly.	REC

05 SERVER, WORKSTATION & NETWORK LIFECYCLE

☐	A complete hardware inventory exists for all servers, workstations, switches, and access points.	CRITICAL
☐	Any server running an unsupported operating system has been identified and flagged.	CRITICAL
☐	Hardware expected to reach end-of-life in the next 12 months has been identified.	IMPORTANT
☐	Workstation replacement is included in the annual IT budget with defined refresh cycles.	IMPORTANT
☐	Network switches and access points are on supported firmware versions.	IMPORTANT
☐	Any device older than 5 years that is production-critical has been reviewed for replacement.	IMPORTANT
☐	The hardware inventory is updated when new equipment is added or removed.	IMPORTANT
☐	IT capital expenditures for the next 12 to 36 months are documented in a roadmap or budget.	IMPORTANT
☐	Server room or network closet environment (temperature, power, ventilation) is monitored.	REC

06 VENDOR ACCESS & DOCUMENTATION

☐	All external vendor access to internal systems is controlled and requires authentication.	CRITICAL
☐	Vendor access is disabled or revoked when a vendor relationship ends.	CRITICAL
☐	A list of all vendors with system access exists and is reviewed periodically.	IMPORTANT
☐	Vendor access sessions are logged and can be audited if needed.	IMPORTANT
☐	Network and system documentation is current and not stored only on one person's computer.	IMPORTANT
☐	IT contact information, vendor contracts, and support agreements are centrally documented.	IMPORTANT
☐	Passwords and credentials for critical systems are stored in a shared password manager.	IMPORTANT
☐	A documented onboarding process exists for new IT vendors or service providers.	REC
☐	System documentation is reviewed and updated at least annually.	REC

How to Read Your Results

This checklist is a planning tool, not a formal security audit or compliance certification.

● **Critical items marked "No"**	Review first. These represent direct risk to production uptime, ERP availability, backup recovery, or cyber insurance coverage.
● **Important items marked "No"**	Include in your next planning cycle. These gaps create exposure over time even if they do not stop production immediately.

● **Only Recommended items marked "No"**	Your environment may be stable but could benefit from better documentation, lifecycle planning, and process maturity.

If you marked "No" on multiple Critical items, your manufacturing environment may have production, security, or recovery risks that should be reviewed before they become emergencies.

Ready to review your results with an expert?

Book a free manufacturing IT assessment at interlinktek.com