NETWORK BUILDERS IT
INDUSTRY REPORT | APRIL 2026

Industry 4.0 in Food & Beverage Manufacturing

A practical guide to connectivity, data, OT/IT integration, cybersecurity, regulatory readiness, and the path to Industry 5.0.

Executive Summary

Most food and beverage manufacturers are in the middle of Industry 4.0, not beyond it. Sensors have been installed. ERPs have been upgraded. Some machines report to dashboards. But the connective tissue between those investments is frequently incomplete, untested, or absent entirely: the network architecture, the data infrastructure, the security controls, the compliance documentation.

That gap is no longer just an operational inconvenience. It is a business risk. Retailers are tightening supplier qualification criteria. FDA traceability requirements are now in effect. Cyber insurance underwriters are demanding documented evidence of controls that many mid-market manufacturers cannot produce. The financial cost of a ransomware incident or a failed audit, measured in production downtime, remediation spend, and damaged customer relationships, has never been higher.

This report is a practical guide to Industry 4.0 for food and beverage manufacturers: what it actually requires, where the gaps typically are, how the regulatory environment intersects with technology decisions, and what a credible adoption roadmap looks like. The final section introduces Industry 5.0 as the logical destination for organizations that build the 4.0 foundation correctly.

A self-assessment checklist and glossary are included at the back. Use the checklist to place your organization on the maturity roadmap and identify the gaps that matter most.

CENTRAL ARGUMENT

The manufacturers who get the most from Industry 4.0 are not the ones who buy the most technology. They are the ones who build the infrastructure that makes their technology investments actually work: network, identity, data, security, and compliance. That foundation is where competitive advantage is built, and it is available to any mid-market F&B operation willing to approach it systematically.

01 THE COST OF STANDING STILL

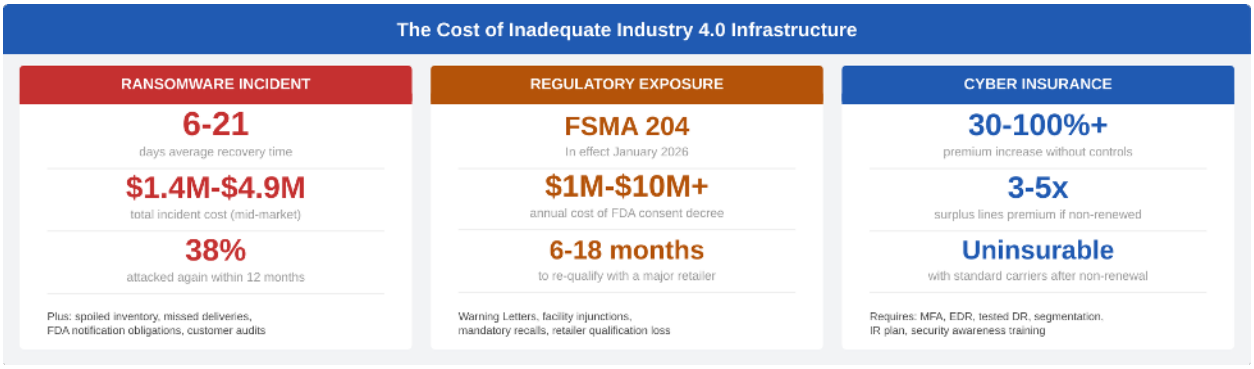
The Cost of Standing Still

The operational and financial consequences of inadequate 4.0 infrastructure are well documented. In food and beverage manufacturing, where production continuity and regulatory standing are

existential, those consequences are more severe than in most sectors. Before examining what Industry 4.0 requires, it is worth putting specific numbers on what it costs to delay.

Ransomware: The Manufacturing Sector Reality

Manufacturing has been the most frequently targeted sector for ransomware attacks for three consecutive years, according to IBM's annual X-Force Threat Intelligence Index. The targeting is rational: production downtime is immediately costly, pressure to restore systems is high, and OT security maturity is typically low. Mid-market manufacturers offer attackers high disruption potential with limited defensive capability.



Impact Category	Documented Range	F&B-Specific Aggravating Factor
Average ransomware recovery time (manufacturing)	6 to 21 days (IBM X-Force; Coveware quarterly reports)	Perishable inventory does not wait for recovery. A six-day production shutdown can mean complete ingredient write-off and missed retailer delivery windows with contractual penalties.
Average total cost of a ransomware incident (mid-market)	$1.4M to $4.9M total impact including downtime, remediation, and recovery (Sophos State of Ransomware 2024)	This figure excludes food safety consequences from the inability to maintain CCP monitoring during the outage, and regulatory exposure from incomplete production records during the incident period.
Cyber insurance premium increases since 2021	30% to 100%+ for organizations unable to demonstrate baseline controls (Marsh McLennan; Coalition 2024 Cyber Claims Report)	F&B manufacturers with OT environments and no documented network segmentation are now in the highest-risk underwriting tier.

Impact Category	Documented Range	F&B-Specific Aggravating Factor
Probability of repeat ransomware attack within 12 months	38% of organizations that paid ransom were attacked again within the year (Cybereason 2022 Ransomware Report)	Paying ransom without remediating the underlying access path is not recovery. It is a temporary settlement with the same adversary.

Regulatory and Qualification Costs

The cost of inadequate 4.0 infrastructure also accumulates through regulatory exposure and lost business qualification. These consequences build more slowly than a ransomware incident, but the financial impact is comparable.

FSMA 204

The FDA Food Traceability Rule went into effect January 2026. Manufacturers of covered foods who cannot produce KDE/CTE lot-level data within 24 hours of an FDA request are operating out of compliance today. Enforcement consequences include Warning Letters, consent decrees, facility injunctions, and mandatory recalls where public health risk exists. A consent decree typically costs $1M to $10M or more in annual compliance and oversight expenses.

RETAILER QUALIFICATION

Losing a major retailer qualification (Walmart SQF, Kroger supplier approval, Costco food safety certification) is not quickly reversible. Re-qualification processes take 6 to 18 months. A mid-market F&B manufacturer with $8M in annual revenue and 40% attributable to one major retailer faces a $3.2M annual revenue gap during that window, with no guarantee of reinstatement.

CYBER INSURANCE NON-RENEWAL

An organization that loses cyber insurance coverage, whether through non-renewal after a claim or failure to demonstrate required controls, does not simply pay more. It may be uninsurable with standard carriers. Surplus lines coverage, where available, typically carries premiums 3x to 5x the standard market rate with materially lower limits and higher retentions.

The Compounding Effect

These cost categories do not occur in isolation. A ransomware incident that takes production offline for 10 days triggers ingredient spoilage, missed delivery penalties, emergency remediation spend, a cyber insurance claim that affects next-year premiums, an FDA or FSIS notification obligation if CCP monitoring was interrupted, and a customer security audit triggered by the disclosure. The

total financial exposure from a single incident in a mid-market F&B operation routinely reaches $2M to $8M when all categories are counted.

Building the 4.0 security and compliance foundation that prevents most of this exposure typically costs $150K to $400K over 18 months for a mid-market operation moving from Level 1 to Level 3, including MSP support, tooling, and infrastructure upgrades. The cost-benefit comparison is straightforward.

THE REAL COMPARISON

The question is not whether the 4.0 infrastructure investment is affordable. The question is whether the cost of the incident it prevents is acceptable. For most mid-market F&B manufacturers, one avoided ransomware event pays for three to five years of managed IT and security investment.

02 WHAT IS INDUSTRY 4.0

What Is Industry 4.0

The Core Concept

Industry 4.0 is the integration of digital technology into manufacturing operations. It connects machines, people, data, and business systems in ways that were not previously practical, enabling manufacturers to monitor production in real time, automate repetitive decisions, catch problems before they become failures, and operate with visibility that paper-based systems cannot provide.

The term originated in Germany around 2011 as a government-industry initiative to modernize manufacturing through four enabling technologies: industrial IoT (connected sensors and devices on the production floor), cloud computing, advanced data analytics, and cyber-physical systems (machines that operate based on real-time data inputs). It has since become the standard framework for describing the digital transformation of manufacturing operations globally.

For a food and beverage manufacturer, Industry 4.0 in practice looks like this: a temperature sensor on a pasteurizer logs readings continuously to a cloud platform and triggers an alert when a critical limit is approached. A production scheduling system pulls real-time inventory data from the WMS and adjusts run sequences to minimize allergen changeovers. An ERP receives yield data directly from production equipment rather than relying on manual entry at shift end. A maintenance technician receives a predictive work order on a tablet based on vibration anomaly data from a conveyor motor.

None of these capabilities require cutting-edge technology. They require connected technology, properly implemented on a foundation of solid network architecture, identity management, and data infrastructure.

Why F&B Manufacturers Are Still in the Middle of It

Industry 4.0 adoption in food and beverage manufacturing lags behind other industrial sectors for well-understood reasons. Production environments are hostile to standard IT hardware. Legacy OT equipment was designed before network connectivity was a consideration and frequently cannot be patched, updated, or integrated with modern systems. Regulatory obligations can still be met manually, which reduces urgency. Mid-market operations rarely have the internal IT depth to drive a transformation program alongside day-to-day support.

The result is a characteristic adoption pattern: point solutions deployed without a unifying architecture. Sensors that report to isolated dashboards. ERPs that contain production data only because someone manually entered it. Cloud storage used for backup rather than analytics. Security controls applied to office systems but not to production networks.

This is a normal middle stage of a multi-year transformation. The question is not whether you have started. The question is whether your current state is stable enough to build on, or whether the gaps in the foundation are creating risk that will surface before the transformation is complete.

HONEST ASSESSMENT

Most mid-market F&B manufacturers are at partial Industry 4.0 adoption: meaningful technology investment, incomplete integration. The value gap between what has been spent and what is being realized typically comes down to three things: network architecture that does not support what the technology requires, security controls that were never extended to OT systems, and data that exists in systems but cannot be accessed because nothing connects it.

03 WHY F&B MANUFACTURING IS DIFFERENT

Why F&B Manufacturing Is Different

Industry 4.0 principles apply across all manufacturing sectors, but the specific pressures, constraints, and requirements of food and beverage create a distinct implementation context. Understanding those differences is the starting point for any credible 4.0 strategy in this sector.

F&B Characteristic	How It Shapes Industry 4.0 Implementation
Consumer Safety Liability	A production failure in F&B is a potential public health event, not a warranty claim. The ability to reconstruct the complete production record of any affected batch, trace it to every ingredient and supplier, and identify every customer who received it is a legal requirement under FSMA. That capability depends entirely on the quality of data captured during production.
Perishable Inventory	Production schedules are constrained by ingredient shelf life, cold chain requirements, and retailer delivery windows. System downtime during a production run has direct, unrecoverable costs. Real-time visibility into production status, yield, and equipment health directly determines whether a run completes on schedule or results in spoiled inventory.
Sanitation Environments	Technology deployed in production areas must survive washdown cycles, high humidity, temperature extremes, and cleaning chemicals. Standard IT hardware is not rated for these environments. Endpoint selection, network infrastructure placement, and cable management all require specifications that general IT procurement does not address.
Regulatory Depth	F&B manufacturers operate under FDA, USDA, and food safety certification requirements that generate ongoing documentation obligations. Every CCP monitoring record, corrective action, and traceability event must be captured, retained, and producible on demand. Technology that does not integrate with these requirements adds compliance burden rather than reducing it.
Retailer Qualification Requirements	Major retailers (Walmart, Kroger, Target, Costco) have supplier qualification programs covering cybersecurity posture, traceability data, sustainability reporting, and EDI integration. These are active qualification criteria today. Suppliers who cannot satisfy them lose placement.

The OT/IT Divide

Every F&B manufacturer operates two distinct technology environments. The IT environment covers business systems, email, ERP, Microsoft 365, and cloud platforms, managed through standard IT practices. The OT environment covers PLCs, SCADA systems, HMIs, temperature controllers, and packaging line automation, which was historically isolated and managed by operations or engineering rather than IT.

Industry 4.0 requires connecting these environments. That integration is where nearly all of the value 4.0 promises comes from, and where nearly all of the risk it introduces originates. Manufacturers who handle this well treat OT/IT integration as a deliberate architecture decision: what connects to what, under what access controls, monitored by whom. Manufacturers who

struggle treat it as a series of one-off projects, each of which adds connectivity without adding oversight.

04 THE FOUR TECHNOLOGY DOMAINS OF INDUSTRY 4.0

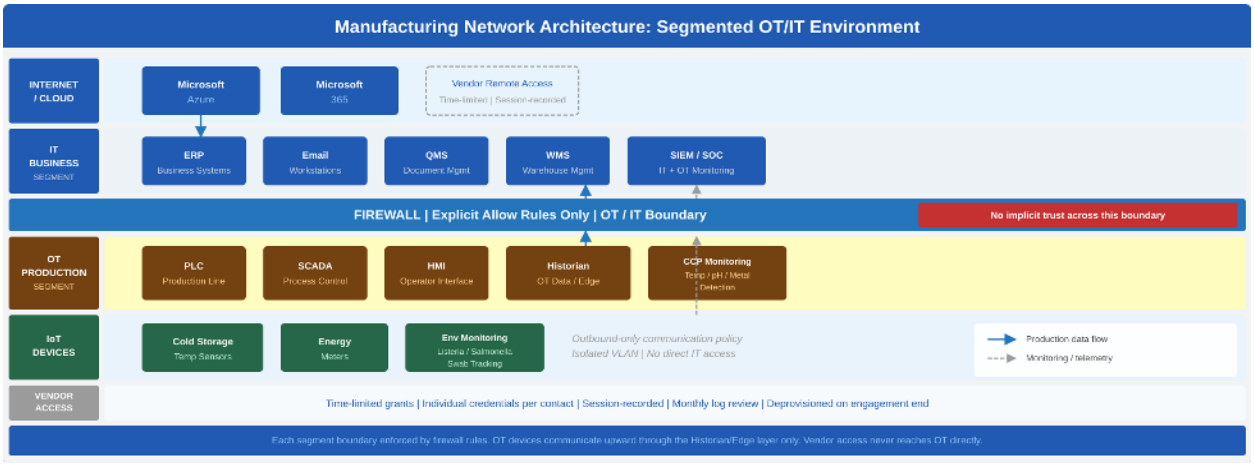
The Four Technology Domains of Industry 4.0

Industry 4.0 readiness in a food and beverage operation depends on maturity across four interconnected technology domains. Progress in any one of them is limited by gaps in the others, which is why point-solution approaches consistently underperform. Each domain is described below with its requirements, common gaps, and what a well-functioning Level 3 operation looks like in practice.

Domain 1: Network Architecture

The network is the foundation everything else runs on. Most mid-market F&B manufacturers are running flat or minimally segmented networks designed for office connectivity, not for the converged OT/IT environments that Industry 4.0 requires.

A properly designed manufacturing network connects OT systems, IT systems, and cloud platforms while maintaining appropriate segmentation between them. Segmentation is a practical operational control: it contains a failure to the segment where it originates rather than allowing it to spread. In a flat network, ransomware that enters through a business email account has a direct path to production control systems.



- Production and business networks segmented at the firewall with explicit allow rules, not implicit trust.
- Industrial IoT devices in a dedicated VLAN with outbound-only communication policies where operationally feasible.
- Vendor and remote access using time-limited, monitored sessions rather than standing VPN credentials.
- Wireless infrastructure on the production floor meeting the latency and reliability requirements of real-time control systems.
- Network monitoring providing visibility across all segments, not just the office LAN.

COMMON GAP	*The most frequent network architecture problem in mid-market F&B is partial segmentation that has never been tested. A VLAN exists on paper, the firewall rules have exceptions that effectively collapse it, and nobody has verified that an OT device cannot reach the business network. Untested architecture is not the same as working architecture.*

WHAT GOOD LOOKS LIKE	A Level 3 F&B operation has a documented network diagram showing distinct segments for business systems, production control, IoT devices, and vendor access. Firewall rules are reviewed quarterly. A penetration test or segmentation validation has been completed within the past 18 months and findings have been remediated. Vendor remote access sessions are logged, time-limited, and reviewed monthly. The network team can identify every device on every segment within 30 minutes.

Domain 2: Connected Equipment and IoT

The core value of Industry 4.0 in manufacturing comes from data collected directly from equipment: production rates, temperatures, pressures, yields, energy consumption, and equipment health indicators. That data enables real-time visibility, exception-based management, predictive maintenance, and the digital production records that regulatory compliance requires.

Getting data from equipment is rarely as simple as installing a sensor. Legacy OT equipment communicates over industrial protocols (Modbus, OPC-UA, PROFINET) that standard IT systems do not understand natively. Historian platforms or edge computing devices typically sit between the OT layer and the IT/cloud layer, translating and buffering data. A poorly designed data pipeline produces unreliable data, which is worse than no data because it erodes trust in every system downstream of it.

- **Start with the highest-value data first.** CCP monitoring (temperatures, pH, metal detection) for regulatory compliance, then yield and downtime for operational performance, then energy and sustainability metrics.
- **Validate data integrity before building workflows on it.** A temperature sensor that drifts 2 degrees and is never calibrated produces records that look compliant and are not.
- **Document the data lineage.** For FDA and audit purposes, you must be able to show that records accurately reflect what happened in production. That requires knowing where the data originated, how it was processed, and where it is stored.

WHAT GOOD LOOKS LIKE

A Level 3 F&B operation has all CCP monitoring points connected to an electronic monitoring system with automated alerting on limit deviations. Data flows from production equipment directly to the ERP or quality management system without manual re-entry. Calibration records for all monitoring instruments are maintained electronically and linked to the associated data records. Equipment downtime is captured automatically and integrated with the maintenance work order system.

Domain 3: Data Infrastructure and Integration

Connected equipment generates data. Data infrastructure is what makes that data usable: stored reliably, accessible to the systems that need it, retained for the periods compliance requires, and presented in formats that support both operational decisions and regulatory reporting.

For mid-market F&B manufacturers, Microsoft Azure is the most practical cloud platform for this layer. Its integration with Microsoft 365, its compliance certifications, and its native support for hybrid environments align with how most mid-market operations are structured. Core capabilities required:

- Structured storage for time-series production data, with retention periods that satisfy FSMA, SQF, and 21 CFR Part 11 requirements.
- ERP integration with production and warehouse systems for real-time operational visibility and lot-level traceability.
- Identity integration between on-premises Active Directory and Entra ID for consistent access governance across IT and OT-adjacent systems.
- Tested backup and disaster recovery with documented RTO and RPO defined separately for business systems and production systems.

The integration between ERP and production systems deserves specific attention because it is where the most valuable 4.0 capabilities live and where the most implementation failures occur. ERP systems that receive production data manually (through shift-end entry or spreadsheet upload) introduce latency, transcription errors, and gaps that undermine traceability, scheduling accuracy, and financial reporting. The 4.0 standard is direct, automated data flow from production to ERP, with human review rather than human data entry.

WHAT GOOD LOOKS LIKE

A Level 3 F&B operation has production data flowing automatically into the ERP with no shift-end manual entry. Lot traceability covers the full chain from receiving through transformation through shipping, queryable in under 10 minutes. Backup and DR has been tested within the past 12 months with documented restore results. Cloud storage retention policies are configured by record type to match regulatory requirements rather than set to a single default retention period.

Domain 4: Identity and Endpoint Management

The range of connected endpoints in a 4.0 manufacturing environment is wide: workstations, tablets, kiosks, handheld scanners, PLCs, HMIs, IoT gateways, and building management systems. Each endpoint is a potential entry point, and in most mid-market environments, the management discipline applied to office devices has not been extended to production-floor endpoints.

Industry 4.0 requires knowing what is on the network, who is accessing what, and that access is governed by least-privilege principles:

- A current, accurate asset inventory covering OT devices and vendor-managed equipment, not just office systems.
- MFA enforced universally: remote access, email, administrative accounts, and OT remote access without exception.
- Role-based access controls that reflect actual job functions. Shared accounts and generic kiosk logins are access control failures, not acceptable operational workarounds.
- Mobile device management for any endpoint that accesses business or production data.

COMMON GAP

Many F&B facilities have equipment vendor accounts with standing administrative access to production systems, created for a commissioning visit years ago and never deprovisioned. These accounts cannot be tied to a specific individual, cannot be audited, and cannot be revoked quickly in an incident. They are persistent, unmonitored access paths directly into production systems.

WHAT GOOD LOOKS LIKE	A Level 3 F&B operation maintains a complete asset inventory reviewed and updated quarterly. MFA is enforced on all accounts without undocumented exceptions. Every vendor with remote access has a named individual contact, a scoped access grant with an expiration date, and a session log reviewed monthly. Privileged access is reviewed semi-annually and accounts are deprovisioned within 24 hours of personnel departure.

05 CYBERSECURITY IN A CONNECTED F&B OPERATION

Cybersecurity in a Connected F&B Operation

Manufacturing is the most frequently targeted sector for ransomware attacks globally. High operational disruption cost, low OT security maturity, and increasing connectivity have made food and beverage producers consistently attractive targets. Ransomware incidents at food manufacturers have resulted in days of production downtime, multi-million dollar remediation costs, and in some cases, food safety consequences from the inability to maintain temperature and process monitoring during system recovery.

How Attacks Enter F&B Environments

Attack Vector	How It Works in F&B	Control Required
Phishing and Business Email Compromise	Credential theft via phishing gives attackers authenticated access to business systems. From there, lateral movement through a flat network reaches production systems. BEC attacks also target wire transfer fraud directly, a consistent high-cost loss for mid-market operations.	MFA on all email and remote access. Email filtering and anti-phishing controls. Security awareness training with documented completion records.
Remote Access Abuse	Vendor VPN credentials that are shared, permanent, and unmonitored provide direct access to production systems. Because credentials are often reused across organizations, a breach	Zero-trust remote access with session recording and time-limited grants. Unique credentials per vendor contact. Access deprovisioned immediately when the engagement ends.

Attack Vector	How It Works in F&B	Control Required
	anywhere those credentials were used can open your OT environment.	
Unpatched OT Devices	PLCs, HMIs, and SCADA systems running firmware with known vulnerabilities have no patch path from their manufacturers and will remain exposed indefinitely. When they share a network segment with business systems, those vulnerabilities are directly reachable.	OT asset inventory to identify what is exposed. Network segmentation to limit blast radius. Compensating controls where patching is not possible.
Flat Network Lateral Movement	The most common path from initial compromise to production impact is not a sophisticated exploit. It is an attacker walking across a flat network because no firewall rules are stopping them. A compromised office workstation reaches a production HMI because nothing separates them.	Network segmentation enforced at the firewall with tested, documented rules. OT-aware network monitoring to detect anomalous lateral movement before it reaches production systems.

NIST Cybersecurity Framework for F&B Manufacturers

The NIST CSF is the most practical security reference for mid-market manufacturers. It provides a common language for assessing current state, identifying gaps, and communicating security posture to customers, insurers, and auditors. NIST CSF 2.0, released in 2024, added a sixth function called GOVERN, which formalizes cybersecurity as an executive risk management responsibility rather than a purely technical function.

NIST CSF Function	What It Requires	F&B-Specific Consideration
IDENTIFY	Asset inventory, risk assessment, governance documentation.	OT asset inventory is frequently absent or incomplete. Every device with network connectivity (PLC, HMI, sensor gateway, BMS) must be included alongside IT assets.
PROTECT	Access controls, training, data security, maintenance.	MFA on all remote access and email without exception. Network segmentation. Patch management programs that address OT devices alongside IT systems.

NIST CSF Function	What It Requires	F&B-Specific Consideration
DETECT	Monitoring, anomaly detection, continuous assessment.	Standard IT monitoring tools do not detect industrial protocol anomalies. OT-aware monitoring is required for full production environment visibility.
RESPOND	Incident response planning, communications, analysis.	IR plans must account for production impact. OT system restart procedures are different from IT recovery and must be documented and tested separately.
RECOVER	Recovery planning, improvements, communications.	RTO and RPO for production systems must be defined and tested independently. Restoring a SCADA system is a different process from restoring a file server.
GOVERN	Executive risk ownership, policy, cybersecurity strategy.	Cybersecurity is a business risk management function. Executives are expected by insurers, customers, and regulators to demonstrate accountability for security posture, not just delegate it to IT.

Cyber Insurance: Baseline Requirements

Cyber insurance underwriting has changed fundamentally since 2021. Carriers that previously issued policies based on short questionnaires now require documented evidence of specific technical controls before issuing or renewing coverage. The controls they require as a baseline:

- MFA on all remote access, email, and privileged accounts, with documented enforcement rather than just a written policy.
- Endpoint detection and response (EDR) deployed on all managed endpoints.
- Tested backup and disaster recovery with documented recovery time objectives and evidence of restore testing within the past 12 months.
- Network segmentation separating OT from IT, verifiable and not just documented on a diagram.
- Incident response plan reviewed and tested within the past 12 months.
- Security awareness training with documented completion records for all employees.

Organizations unable to demonstrate these controls face non-renewal, coverage exclusions, or premium increases of 30 to 100 percent. The alignment between insurance requirements and

sound 4.0 security practice reflects the same underlying reality: both are responses to the same threat environment.

06 REGULATORY FRAMEWORKS AND IT OBLIGATIONS

Regulatory Frameworks and IT Obligations

The regulatory environment for F&B manufacturers is one of the primary drivers of Industry 4.0 adoption in this sector. FSMA, FDA 21 CFR Part 11, HACCP, SQF, and BRC all create data management obligations that manual and paper-based systems cannot satisfy at production scale. Understanding what each framework requires of your IT infrastructure is a technology planning prerequisite, not a compliance afterthought.

FSMA: The Data Management Law Disguised as a Food Safety Law

The Food Safety Modernization Act represents the most significant overhaul of U.S. food safety regulation since 1938. Its shift from responding to contamination events to preventing them created a documentation infrastructure that most mid-market manufacturers are still building out.

FSMA Rule	The IT Obligation
Preventive Controls for Human Food (21 CFR Part 117)	Written food safety plan, hazard analysis, preventive controls, monitoring, corrective actions, and verification activities, all requiring documentation with version control, audit trails, and 2-year minimum retention. Paper records create significant audit risk at production scale.
Food Traceability Rule (FSMA 204)	Lot-level traceability data producible to the FDA within 24 hours, covering receiving through transformation through shipping. Effective January 2026 for covered foods. Manufacturers unable to produce this data are out of compliance now. Spreadsheet-based traceability does not meet the requirement.
Sanitary Transportation (21 CFR Part 1, Subpart O)	Temperature control documentation during transport, carrier records, and written procedures. Requires data retention and, for managed cold chain programs, integration with carrier data systems.
Food Defense (Intentional Adulteration Rule)	Vulnerability assessment, mitigation strategies, monitoring documentation, and employee training records. Access control systems

FSMA Rule	The IT Obligation
	and monitoring logs for production areas are the primary IT implementation.

FSMA 204 STATUS	*The FSMA 204 traceability rule went into effect January 20, 2026 for covered foods including fresh produce, shell eggs, nut butters, and ready-to-eat deli salads. The compliance date has passed. Manufacturers who cannot produce KDE/CTE data within 24 hours of an FDA request are operating out of compliance today. Enforcement actions (Warning Letters, consent decrees, facility injunctions) are the operative risk.*

FDA 21 CFR Part 11: Electronic Records Requirements

21 CFR Part 11 governs electronic records and electronic signatures in FDA-regulated environments. For F&B manufacturers using electronic batch records, electronic QMS, or automated CCP monitoring, Part 11 compliance is a legal requirement. The regulation specifies what the systems themselves must implement.

Requirement	What Your Systems Must Do
Audit Trails	Automatically capture the date, time, and user identity for every record creation, modification, or deletion. This must be a system-level control, not a manual log. Audit trail records must be retained for the full record retention period and available for FDA review.
Electronic Signatures	Each signature must be linked to its associated record. Systems must display the signer name, date, time, and the meaning of the signature. Credentials must be unique to one individual. Shared signing credentials are a Part 11 violation.
Access Controls	System-level enforcement that only authorized individuals can access, sign, or modify records. Role-based access controls, not just password protection.
Record Integrity	Records protected from unauthorized alteration. Backup copies maintained at a separate location. Records retrievable throughout the full retention period in a readable format.
System Validation	Documented IQ, OQ, and PQ validation for systems that create or maintain FDA-subject records. Changes to validated systems require change control and may require re-validation.

HACCP, SQF, and BRC: The Certification Stack

HACCP provides the scientific foundation. SQF and BRC are the certification schemes built on top of it that major retailers require for supplier qualification. Together they define the data management infrastructure any F&B manufacturer selling to national retail must maintain.

Standard	Core IT Requirement	Consequence of Gaps
HACCP	CCP monitoring records with timestamps, automated alerts for limit deviations, corrective action records linked to specific deviation events, and verification records with user attribution.	Manual logs that are missed, falsified, or lost cannot trigger alerts. Corrective actions disconnected from monitoring records create direct audit exposure.
SQF Level 2	Electronic monitoring for all CCPs strongly favored; HACCP monitoring records retained and retrievable; corrective action tracking with closure documentation.	Paper-based records at Level 2 pass audits but create significant administrative burden and reliability risk at production scale.
SQF Level 3	Integrated ERP and QMS effectively required. Customer complaint records, product release procedures, and management review documentation at a volume paper systems cannot manage reliably.	Organizations at Level 3 without an integrated QMS spend disproportionate staff time on documentation that should be automated.
BRC Global Standard	Traceability system capable of reconstructing product movement within four hours. Version-controlled document management. Validated computer systems for traceability and quality management.	BRC traceability exercises are timed and unannounced. Four hours is not achievable without integrated lot-level tracking.

07 THE INDUSTRY 4.0 ADOPTION ROADMAP

The Industry 4.0 Adoption Roadmap

Industry 4.0 adoption is a progression through levels of operational and technology maturity, where each level builds on the last. The framework below describes four maturity levels, the business risk at each, and the priority actions required to advance. Use it alongside the self-assessment checklist at the back of this report to place your organization honestly on the map.

Level	Characteristics	Business Risk	Priority to Advance
Level 1 Reactive	IT managed ad hoc. No documented configurations or asset inventory. Backups exist but are untested. OT and IT on the same flat network. Compliance documentation paper-based and unorganized. No formal security program.	Cannot satisfy customer security audits or retailer qualification requirements. Cyber insurance non-renewal risk. Ransomware recovery time unknown and likely measured in weeks. FSMA 204 non-compliance.	Complete asset inventory (IT and OT). Design and implement network segmentation. Deploy and test backup and DR. Enforce MFA on all remote access and email. Establish a document retention policy.
Level 2 Foundational	Core systems under management. Endpoint protection deployed. Basic network segmentation in place. MFA enforced for remote access and email. Backups tested quarterly. No formal IR plan. Compliance documentation partially electronic.	Can pass basic customer security reviews. Moderate cyber insurance risk. Vulnerable to advanced threats without external support. FSMA and certification documentation incomplete.	Develop and test an incident response plan. Complete OT asset inventory. Activate security monitoring across IT and OT. Build a compliance documentation program. Engage a vCIO or formal technology roadmap function.
Level 3 Operational	OT and IT fully segmented with tested controls. Security monitoring active across both environments. Identity governance enforced. IR plan tested annually. FSMA, SQF/BRC, and 21 CFR Part 11 documentation maintained	Low to moderate operational risk. Satisfies most customer security questionnaires. Cyber insurance rates stabilized. Able to respond to FDA audit requests within 24	Build sustainability data infrastructure. Advance to OT-aware threat detection. Integrate supply chain visibility. Implement continuous compliance monitoring. Develop a 3-year technology roadmap

Level	Characteristics	Business Risk	Priority to Advance
	electronically. ERP integrated with production data.	hours. Retailer qualification criteria met.	aligned to business objectives.
Level 4 Strategic	Technology strategy formally aligned to business objectives. vCIO function active. Production data feeds real-time analytics and decision support. Sustainability data captured and reported. Predictive maintenance active. ERP, QMS, and MES integrated.	Minimal technology risk. Preferred supplier qualification capable. Full regulatory audit readiness on demand. ESG reporting capable. Technology is a recognized competitive asset.	Continuous improvement cycle. Emerging technology evaluation (AI-assisted quality inspection, digital twin). Industry 5.0 readiness assessment.

Priority Sequencing: Where to Start

Step 1: Build the Asset Inventory

You cannot protect, manage, or report on what you do not know exists. A complete inventory covers every device with network connectivity, including production floor equipment. For most mid-market F&B manufacturers, this exercise surfaces connected equipment IT did not know about, vendor access paths that were never deprovisioned, and OT devices running firmware that has not been updated in years.

Step 2: Segment the Network

OT/IT network segmentation is the single highest-impact security control available to most mid-market manufacturers. It limits ransomware lateral movement, contains blast radius from any incident, and is the architectural prerequisite for safely connecting OT systems to IT and cloud platforms. It is also what makes OT-aware monitoring possible.

Step 3: Enforce MFA Universally

Credential theft is the most common initial access vector for ransomware and BEC fraud. MFA stops the majority of credential-based attacks. It delivers the highest return on investment of any available security control and should be treated as a hard prerequisite before any other security investment. No exceptions for production-floor systems, remote access, or vendor accounts.

Step 4: Test Backup and Disaster Recovery

Untested backups are not reliable backups. Define RTO and RPO for production systems separately from business systems. The recovery procedures are different and the acceptable downtime thresholds are different. Test restores on a documented schedule and produce evidence

of the test. Cyber insurance underwriters and customer security assessments now request this evidence as a standard item.

Step 5: Close the FSMA 204 Gap

Determine whether your current ERP or WMS captures KDE/CTE data at the lot level and whether it can be produced in the format and timeframe FSMA requires. The compliance deadline has passed. Manufacturers who cannot satisfy this requirement are operating with active enforcement exposure, and remediation should be treated as an immediate priority.

Step 6: Build the Compliance Documentation Program

Centralize FSMA, HACCP, SQF/BRC, and 21 CFR Part 11 records in a document management system with version control, retention policies, and audit trail capabilities. The target state is one where any regulatory audit or customer security questionnaire can be answered with organized documentation rather than a manual search across file shares and email threads.

Step 7: Connect Production Data to Business Systems

Once the security and compliance foundation is stable, the 4.0 value work begins: real-time production visibility, automated ERP data entry, integrated traceability, and the analytics that make operational improvement repeatable. This is where the competitive differentiation lives. Steps 1 through 6 must be stable first, or the data flowing through these integrations will not be reliable enough to act on.

08 WHAT COMES AFTER 4.0: AN INTRODUCTION TO INDUSTRY 5.0

What Comes After 4.0: An Introduction to Industry 5.0

Industry 5.0 is not a replacement for Industry 4.0. It is the next layer, and understanding what it adds helps clarify why the 4.0 foundation being built today matters beyond the immediate operational and compliance pressures.

Industry 5.0 was introduced by the European Commission in 2021 as a framework response to the limitations that became visible as Industry 4.0 matured. Supply chains built for lean efficiency proved brittle under COVID-19 disruption. Connected OT environments turned out to be largely undefended. Workforce displacement created social and political pressure that individual companies could not absorb. And the environmental costs of accelerated industrial output became impossible for regulators, investors, and major customers to ignore.

Industry 5.0 adds three requirements to the 4.0 foundation:

Industry 5.0 Principle	What It Adds to Industry 4.0	Why It Matters for F&B Manufacturers
Human-Centricity	4.0 optimized around machines. 5.0 requires that technology augment human workers rather than simply replace them: collaborative robotics, AI-assisted decision support, AR for maintenance and training.	Enables more flexible production, better worker retention in a tight labor market, and the adaptive decision-making that highly automated lines still require at scale.
Resilience	4.0 optimized for lean efficiency. 5.0 requires operational resilience: the capacity to absorb shocks from cyberattacks, supply disruptions, regulatory changes, and workforce gaps.	Manufacturers who build the 4.0 security, backup, and supply chain visibility infrastructure are building 5.0 resilience in parallel. These are not separate investments.
Sustainability	4.0 measured throughput. 5.0 measures environmental and social impact alongside output: energy consumption, emissions, waste, and supply chain conditions, as verifiable and auditable operational data.	Retailer ESG scorecards, sustainability-linked financing, and customer supply chain requirements are already creating data obligations for F&B manufacturers. The organizations with the data infrastructure to satisfy these requirements have a supplier qualification advantage.

The 4.0 Foundation Enables 5.0

The organizations that reach Level 3 and Level 4 on the Industry 4.0 adoption roadmap will find that they have built most of what Industry 5.0 requires. A properly segmented and monitored OT/IT environment supports resilience. An integrated production data infrastructure supports sustainability reporting. A technology strategy with vCIO oversight and a formal roadmap is the governance structure 5.0 demands.

Industry 5.0 is not a separate initiative requiring a separate budget. It is the direction the Industry 4.0 journey is already heading for manufacturers who execute it with discipline. The 4.0 foundation work is the 5.0 preparation work.

FORWARD LOOK

Industry 5.0 readiness is beginning to appear in supplier qualification criteria, sustainability reporting requirements, and ESG-linked financing covenants. It is not yet

universal, but the direction is clear. Manufacturers who complete the 4.0 foundation work correctly over the next two to three years will be positioned to satisfy 5.0 qualification requirements without the disruption and cost of retrofitting an immature technology environment.

CLOSING PERSPECTIVE

Closing Perspective

The central question for a mid-market food and beverage manufacturer is not whether to pursue Industry 4.0. The investment is already underway. The question is whether the current state of that investment is stable enough to build on, or whether gaps in the foundation are creating risk that will surface before the value is fully realized.

Most mid-market F&B manufacturers are at partial 4.0 adoption: meaningful technology investment, incomplete integration. The gap between what has been spent and what is being realized almost always comes down to the same four things: a network that was never properly segmented, OT devices that have never been inventoried, backups that have never been tested, and production data that exists in systems but cannot be used because nothing connects it.

Closing those gaps does not require a large capital program. It requires a sequenced plan, consistent execution, and the discipline to fix infrastructure before adding more point solutions on top of it. The manufacturers who take that approach will realize the value of their existing investments, satisfy the regulatory and qualification requirements bearing down on the sector, and be in a strong position for what comes after 4.0.

Network Builders IT | nbit.com | Managed IT for Manufacturing

Regulatory requirements evolve. FSMA rules, FDA guidance, SQF edition updates, NIST framework revisions, and cyber insurance criteria change regularly. Verify specific compliance requirements against current FDA, USDA, and standards body publications for your product categories and facility types.

Self-Assessment Checklist

Use this checklist to place your organization on the Industry 4.0 maturity roadmap and identify your highest-priority gaps. Work through each section honestly. Your score is less important than the specific items you cannot check: those are your action list.

HOW TO SCORE

- Check every item that is fully implemented, tested, and documented. Do not check items that are in progress or planned.
- Count checked items per section. Section scores indicate domain-specific maturity.
- Your overall maturity level corresponds to the highest level where you can check all items in that level's sections.

	LEVEL 1: Security and Visibility
☐	A complete IT asset inventory exists and was updated within the past 6 months. *Includes all workstations, servers, network devices, and cloud systems.*
☐	A complete OT asset inventory exists and was updated within the past 6 months. *Includes all PLCs, HMIs, SCADA systems, IoT gateways, and production-floor endpoints.*
☐	MFA is enforced on all email accounts without exception.
☐	MFA is enforced on all remote access (VPN, RDP, remote support tools) without exception.
☐	No shared or generic user accounts exist on any system with access to business or production data.
☐	Endpoint protection (antivirus or EDR) is deployed and actively monitored on all managed endpoints.
☐	Backups are performed daily for all critical systems.
☐	A backup restore has been tested within the past 12 months with documented results.
☐	RTO and RPO have been defined for business systems.
☐	A document retention policy exists and is followed for compliance records.
	LEVEL 2A: Network and Access Control
☐	Production/OT systems and business/IT systems are on separate network segments. *Verified by firewall rules, not just VLAN assignment.*
☐	IoT and sensor devices are isolated in a dedicated network segment.

☐	Vendor remote access uses time-limited, individually scoped credentials rather than permanent shared VPN accounts.
☐	All vendor remote access sessions are logged and reviewed monthly.
☐	Role-based access controls are in place on all business systems, reflecting actual job functions.
☐	Privileged access (admin accounts) is reviewed and recertified at least annually.
☐	All employee accounts are deprovisioned within 24 hours of termination.
☐	A written incident response plan exists covering both IT and OT systems.
☐	The incident response plan has been reviewed and tested within the past 12 months.
☐	Security awareness training has been completed by all employees within the past 12 months with documented records.
	LEVEL 2B: Regulatory Documentation
☐	A written FSMA Preventive Controls food safety plan exists and is current.
☐	CCP monitoring records are captured electronically with automatic timestamps.
☐	Automated alerts are configured for CCP limit deviations.
☐	Corrective action records are maintained electronically and linked to specific CCP deviation events.
☐	Electronic records used for FDA compliance meet 21 CFR Part 11 requirements (audit trails, access controls, unique signatures).
☐	Lot-level traceability covers receiving, production transformation, and shipping. *Can you produce a complete forward and backward trace for any lot within 24 hours?*
☐	FSMA 204 KDE/CTE data is captured in your ERP or WMS at the lot level. *Spreadsheet-based traceability does not satisfy this requirement.*
☐	SQF or BRC certification is current and audit findings are tracked to closure.
	LEVEL 3: Data and Integration
☐	Production data flows automatically into the ERP with no manual shift-end entry for yield, downtime, or batch data.
☐	ERP is integrated with the WMS for real-time lot-level inventory visibility.
☐	A full forward and backward lot trace can be produced within 10 minutes from the ERP or WMS.
☐	RTO and RPO have been defined and tested for production systems separately from business systems.
☐	On-premises Active Directory is integrated with Entra ID for consistent identity governance.
☐	Cloud data retention policies are configured by record type to match regulatory requirements.

☐	Security monitoring (SIEM or managed detection) is active across both IT and OT environments.
☐	OT network traffic is monitored for anomalies using OT-aware tools. *Standard IT monitoring tools do not detect industrial protocol anomalies.*
☐	Network segmentation has been validated (penetration test or segmentation verification) within the past 18 months.
	LEVEL 4: Technology Alignment
☐	A formal technology roadmap exists covering a 3-year horizon, reviewed annually.
☐	A vCIO function (internal or external) is actively engaged in technology strategy decisions.
☐	Predictive maintenance is active on at least one critical production asset using sensor data and analytics.
☐	Energy consumption data from production equipment is captured and reportable. *Supports sustainability reporting and ESG-linked requirements.*
☐	The organization can satisfy customer ESG questionnaires with verified production data.
☐	ERP, QMS, and production systems are integrated with automated data flows across all three.
☐	Technology investment decisions are made against a documented business case with defined success metrics.
☐	An Industry 5.0 readiness assessment has been completed or is scheduled.

INTERPRETING YOUR RESULTS

Section Score	What It Means
Level 1: 8-10 checked	Strong foundation. Proceed to Level 2A and 2B priorities.
Level 1: 5-7 checked	Address unchecked Level 1 items before investing in higher-level capabilities. These are your highest-risk gaps.
Level 1: Below 5 checked	Immediate action required. Level 1 gaps represent active cyber insurance, regulatory, and operational risk.
Level 2A: 8-10 checked	Network and access controls are solid. Proceed to Level 2B compliance documentation.
Level 2A: 5-7 checked	Meaningful gaps in access control or segmentation remain. Address before advancing to Level 3.
Level 2A: Below 5 checked	Significant exposure. Prioritize network segmentation and MFA enforcement as immediate actions.

Section Score	What It Means
Level 2B: 6-8 checked	Regulatory posture is foundational. Prioritize FSMA 204 traceability and 21 CFR Part 11 if unchecked.
Level 2B: 3-5 checked	Compliance documentation gaps create audit and enforcement exposure. Treat as a parallel priority alongside Level 2A work.
Level 2B: Below 3 checked	Regulatory risk is high. FSMA 204 non-compliance and certification gaps should be treated as immediate priorities.
Level 3: 7-9 checked	Operational maturity is strong. Ready to invest in Level 4 strategic capabilities.
Level 3: 4-6 checked	Partially operational. Focus on OT monitoring, ERP integration, and tested DR before advancing.
Level 3: Below 4 checked	Foundation work from Levels 1 and 2 may be incomplete. Revisit earlier sections before investing in Level 3 capabilities.
Level 4: 6-8 checked	Strategic alignment achieved. Conduct an Industry 5.0 readiness assessment to define the next horizon.
Level 4: 3-5 checked	Technology strategy is emerging. Prioritize the vCIO function and formal roadmap to drive the remaining gaps to closure.
Level 4: Below 3 checked	Level 4 capabilities are early-stage. Confirm Level 3 is fully complete before significant Level 4 investment.

Glossary

Key terms used throughout this report, written for executive readers and operations leaders who encounter these abbreviations in technology conversations, audit questionnaires, or customer security assessments.

Term	Definition
BEC (Business Email Compromise)	A cyberattack in which an attacker gains access to a business email account, typically through phishing, and uses it to commit fraud, redirect payments, or establish a foothold for ransomware deployment.
BRC / BRCGS	The British Retail Consortium Global Standards for Food Safety. A GFSI-benchmarked food safety certification required by European retailers and increasingly by U.S. retailers with European operations. Requires validated traceability systems and documented quality management.
CCP (Critical Control Point)	A step in the food production process where a control measure can be applied to prevent, eliminate, or reduce a food safety hazard to an acceptable level. CCPs must be monitored and monitoring records must be retained. Examples include pasteurization temperature and metal detection.
CTE / KDE (Critical Tracking Event / Key Data Element)	FSMA 204 terminology. CTEs are the points in the supply chain where traceability data must be captured: receiving, transformation, shipping, and storing. KDEs are the specific data fields required at each CTE, such as lot codes, dates, and supplier information.
Cyber-Physical System	A system in which physical processes are monitored and controlled by computer-based algorithms. Production equipment that adjusts its operating parameters based on real-time sensor data is a cyber-physical system. Central to Industry 4.0.
EDR (Endpoint Detection and Response)	A security tool deployed on endpoints (computers, servers, tablets) that continuously monitors for malicious activity, records endpoint behavior, and enables rapid investigation and response when threats are detected. Required by most cyber insurance underwriters.
Entra ID (formerly Azure Active Directory)	Microsoft's cloud-based identity and access management service. Provides single sign-on, MFA enforcement, and access governance for Microsoft 365 and cloud-connected applications. The identity backbone for Microsoft-centric IT environments.
ERP (Enterprise Resource Planning)	A software platform that integrates core business processes including finance, procurement, production, inventory, and sales. In a 4.0 manufacturing

Term	Definition
	environment, ERP systems should receive production data directly from the floor rather than through manual entry.
FSMA (Food Safety Modernization Act)	U.S. federal law signed in 2011 that shifted the focus of food safety regulation from responding to contamination events to preventing them. Implemented through rules including Preventive Controls, Foreign Supplier Verification, Sanitary Transportation, and the Food Traceability Rule (FSMA 204).
GFSI (Global Food Safety Initiative)	A benchmarking organization that recognizes food safety certification schemes including SQF and BRC/BRCGS. When a retailer or customer requires GFSI-certified suppliers, they are requiring certification under one of the recognized schemes. GFSI itself does not certify; it accredits the schemes that do.
HACCP (Hazard Analysis and Critical Control Points)	A systematic, science-based approach to food safety that identifies biological, chemical, and physical hazards in production and establishes critical control points to prevent them. Required by FDA for certain food categories and forms the foundation of SQF Level 2 and BRC certification.
HMI (Human-Machine Interface)	The interface through which operators monitor and control production equipment, typically a touchscreen panel mounted near the equipment. HMIs are OT devices that are frequently connected to business networks in Industry 4.0 environments and represent a significant security exposure when not properly segmented.
ICS (Industrial Control System)	A broad category of systems used to monitor and control industrial processes, including SCADA systems, distributed control systems (DCS), and PLCs. In food manufacturing, ICS environments cover pasteurization controls, packaging line automation, and cold storage management.
IoT / IIoT (Internet of Things / Industrial Internet of Things)	The network of physical devices embedded with sensors, software, and connectivity that enables them to collect and exchange data. In manufacturing, IIoT refers specifically to connected production equipment, sensors, and monitoring devices on the factory floor.
IR Plan (Incident Response Plan)	A documented set of procedures for detecting, responding to, and recovering from a cybersecurity incident. Must address both IT and OT environments in manufacturing contexts. Required by cyber insurance underwriters and referenced in NIST CSF.
MES (Manufacturing Execution System)	Software that connects, monitors, and controls manufacturing systems and data flows on the production floor. Sits between the ERP (business layer) and the control systems (OT layer), capturing production events, managing work orders, and tracking materials in real time.

Term	Definition
MFA (Multi-Factor Authentication)	An authentication method requiring two or more verification factors, typically a password plus a time-based code or push notification. MFA is the single most effective control against credential-based attacks and is now universally required by cyber insurance underwriters.
NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)	The most widely used cybersecurity framework for U.S. manufacturers. Organizes security activities into six functions: Identify, Protect, Detect, Respond, Recover, and (as of CSF 2.0) Govern. Commonly referenced in customer security questionnaires and cyber insurance applications.
OT (Operational Technology)	Hardware and software that monitors or controls physical processes, devices, and infrastructure. In food manufacturing, OT includes PLCs, SCADA systems, HMIs, temperature controllers, and packaging line automation. Historically isolated from IT and now increasingly connected in Industry 4.0 environments.
PLC (Programmable Logic Controller)	An industrial computer used to control manufacturing processes such as assembly lines, mixing operations, and packaging equipment. PLCs are OT devices that communicate over industrial protocols and are typically not patchable through standard IT patch management processes.
QMS (Quality Management System)	Software used to manage quality-related documentation, processes, and records including customer complaints, corrective actions, product specifications, and audit records. At SQF Level 3 and above, an integrated QMS is effectively required to manage documentation volume.
RTO / RPO (Recovery Time Objective / Recovery Point Objective)	RTO is the maximum acceptable time to restore a system after a failure. RPO is the maximum acceptable data loss measured in time. Both must be defined and tested separately for production systems and business systems in a manufacturing environment.
SCADA (Supervisory Control and Data Acquisition)	A system used to monitor and control industrial processes across large or distributed operations. In food manufacturing, SCADA systems often manage process control across multiple production lines or facilities, making them high-value targets for ransomware actors.
SIEM (Security Information and Event Management)	A platform that aggregates and analyzes log data from across an IT environment to detect security threats and anomalies. Standard SIEMs monitor IT environments. OT-aware SIEMs or specialized OT monitoring tools are required to achieve visibility across production networks.
SQF (Safe Quality Food)	A GFSI-benchmarked food safety and quality management certification developed by the Food Marketing Institute. SQF certification at Levels 1, 2,

Term	Definition
	and 3 is required by major U.S. retailers including Walmart, Kroger, Costco, and Target as a condition of supplier approval.
vCIO (Virtual Chief Information Officer)	An outsourced technology strategy function that provides executive-level IT leadership without the cost of a full-time CIO. A vCIO aligns technology investment to business objectives, owns the technology roadmap, and provides governance oversight, particularly valuable for mid-market organizations scaling through growth phases.
WMS (Warehouse Management System)	Software that manages and optimizes warehouse operations including receiving, put-away, picking, packing, and shipping. In a 4.0 F&B environment, WMS integration with ERP is essential for real-time lot-level inventory visibility and FSMA traceability compliance.
Zero-Trust	A security model based on the principle that no user, device, or network segment should be trusted by default, regardless of whether it is inside or outside the corporate perimeter. Access is granted based on verified identity, device health, and least-privilege principles. In manufacturing, zero-trust remote access replaces standing VPN credentials with session-based, monitored access grants.