VIVIFY SOFT TECH

Smart Factory Readiness Checklist

Find the gaps that could delay ROI before you invest in sensors, software, or automation.

A practical self-assessment for manufacturing leaders

72 questions | 9 readiness areas | Action-planning worksheets

Plant / company: _____

Assessment date: _____

Completed by / role: _____

Use this guide with operations, maintenance, IT/OT, quality, and finance. Assess one defined line, plant, or use case at a time.

Design note: This guide uses a neutral layout. No logo or unverified brand colors have been applied because approved brand assets were not supplied.

How to use this guide

1. Define the scope: a line, plant, asset group, or first use case.
2. Review the questions with the teams that own the work.
3. Mark one answer per question. Record evidence and gaps.
4. Assign actions to the highest-risk gaps before scaling.

Answer	Meaning
Yes	Documented, evidenced, and working consistently within scope.
Partial	Exists, but is incomplete, inconsistent, or not yet validated.
No	Missing, unclear, or not demonstrated.

Keep the assessment honest

Mark unknown answers as No until evidence is available. If an item appears irrelevant, record why and review it with the relevant owner. Use the count as a discussion aid, not as a certification or investment approval.

Important limitations

This is an editorial self-assessment, not a validated maturity model, safety audit, cybersecurity audit, or compliance certification. A high total cannot override a critical safety, security, data, or ownership gap. No score guarantees ROI.

Reference basis

NIST describes factory readiness assessment and manufacturing cybersecurity resources. These references inform the assessment themes; they do not endorse this checklist or its scoring. [1][2]

[1] NIST: Smart Manufacturing Systems Readiness Level (SMSRL) Tool
Read the NIST readiness resource

[2] NIST: Manufacturing Sector cybersecurity resources
Read the NIST manufacturing security resource

1. Business value and ROI

Start with a measurable production problem, not a technology purchase.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
1.1	Have we identified our top three production problems affecting output, cost, quality, or delivery?	[ ]	[ ]	[ ]
1.2	Do we know the financial impact of downtime, defects, rework, delivery delays, and lost capacity?	[ ]	[ ]	[ ]
1.3	Have we selected two or three priority use cases instead of trying to digitize everything?	[ ]	[ ]	[ ]
1.4	Do we have agreed baselines for the KPIs relevant to those use cases?	[ ]	[ ]	[ ]
1.5	Have we set a measurable target improvement for each use case?	[ ]	[ ]	[ ]
1.6	Have we assigned an accountable business owner to each use case?	[ ]	[ ]	[ ]
1.7	Have we defined implementation costs, running costs, expected benefits, and how ROI will be measured?	[ ]	[ ]	[ ]
1.8	Do operations, finance, IT, and maintenance have an agreed review schedule?	[ ]	[ ]	[ ]

Priority warning

If a use case has no baseline, target, or accountable owner, complete the business case before approving a large rollout.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

2. Process and operations

Understand how work happens before deciding what to automate.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
2.1	Can we map the production flow from raw material to finished goods?	[ ]	[ ]	[ ]
2.2	Do we know our bottleneck machines, lines, and processes?	[ ]	[ ]	[ ]
2.3	Are downtime reason codes standardized across shifts and departments?	[ ]	[ ]	[ ]
2.4	Do operators record downtime, quality issues, and production counts consistently?	[ ]	[ ]	[ ]
2.5	Do supervisors review shift performance and assign corrective actions?	[ ]	[ ]	[ ]
2.6	Are current operating procedures available for critical production and maintenance activities?	[ ]	[ ]	[ ]
2.7	Do we investigate root causes of recurring stoppages, defects, and delays?	[ ]	[ ]	[ ]
2.8	Have we identified where manual data entry creates delays or errors?	[ ]	[ ]	[ ]

Priority warning

Inconsistent downtime codes create misleading comparisons, even when machine signals are collected automatically.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

3. Machine and data

Check whether the required data is available, understandable, and trusted.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
3.1	Do we have an up-to-date inventory of priority machines, PLCs, HMIs, sensors, and controllers?	[ ]	[ ]	[ ]
3.2	Do we know which machines expose production, downtime, cycle-time, alarm, or quality data?	[ ]	[ ]	[ ]
3.3	Have we identified legacy equipment that needs gateways, retrofits, or manual capture?	[ ]	[ ]	[ ]
3.4	Are required data points, units, sampling rates, and timestamps defined?	[ ]	[ ]	[ ]
3.5	Is data available at the speed needed for the chosen use case?	[ ]	[ ]	[ ]
3.6	Is there an agreed source of truth for production, downtime, quality, and maintenance records?	[ ]	[ ]	[ ]
3.7	Have we assigned ownership for each system and data type?	[ ]	[ ]	[ ]
3.8	Do we validate completeness, accuracy, timestamps, and context before using data for reporting or AI?	[ ]	[ ]	[ ]

Priority warning

If teams produce conflicting reports, resolve definitions and data quality before adding more dashboards.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

4. IT and OT integration

Plan how business systems and shop-floor systems will share information.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
4.1	Can ERP, MES, SCADA, PLC, CMMS, quality, and IoT systems exchange the data our use cases need?	[ ]	[ ]	[ ]
4.2	Have we agreed which system owns each master record and transaction?	[ ]	[ ]	[ ]
4.3	Have we selected supported integration methods, such as OPC UA, MQTT, Modbus, or APIs?	[ ]	[ ]	[ ]
4.4	Can machine events be linked to work orders, products, batches, and shifts?	[ ]	[ ]	[ ]
4.5	Can maintenance staff access machine history, alarms, work orders, and spare-parts information?	[ ]	[ ]	[ ]
4.6	Can quality results be linked to the relevant batch, machine, shift, and production order?	[ ]	[ ]	[ ]
4.7	Have we documented data flows, error handling, buffering, and recovery after connection loss?	[ ]	[ ]	[ ]
4.8	Can the architecture support additional lines, plants, and use cases without repeated redesign?	[ ]	[ ]	[ ]

Priority warning

If every use case needs a fresh manual export, the integration model is not ready to scale.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

5. OEE and performance management

Turn performance numbers into specific actions and accountable follow-up.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
5.1	Are OEE boundaries, planned production time, ideal cycle time, and good-count rules documented?	[ ]	[ ]	[ ]
5.2	Can we separate availability, performance, and quality losses?	[ ]	[ ]	[ ]
5.3	Can we identify major loss reasons by machine, product, and shift?	[ ]	[ ]	[ ]
5.4	Can we distinguish planned stops, changeovers, minor stops, breakdowns, and defects?	[ ]	[ ]	[ ]
5.5	Do alerts tell supervisors what happened, where, and what response is required?	[ ]	[ ]	[ ]
5.6	Does each major loss category have an accountable team?	[ ]	[ ]	[ ]
5.7	Do teams review losses in daily or weekly operational meetings?	[ ]	[ ]	[ ]
5.8	Do we check whether corrective actions reduce recurring losses?	[ ]	[ ]	[ ]

Priority warning

An OEE percentage alone is not an improvement plan. Agree on the loss, owner, action, and follow-up date.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

6. Maintenance and predictive readiness

Choose maintenance methods according to asset risk and available evidence.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
6.1	Have we classified assets by downtime cost, safety impact, criticality, and available redundancy?	[ ]	[ ]	[ ]
6.2	Have we identified assets where unplanned failure has the highest business impact?	[ ]	[ ]	[ ]
6.3	Do target assets provide usable condition signals such as vibration, temperature, current, or pressure?	[ ]	[ ]	[ ]
6.4	Do we maintain structured maintenance history, failure codes, repair records, and asset IDs?	[ ]	[ ]	[ ]
6.5	Can maintenance teams receive prioritized alerts and act within an agreed response time?	[ ]	[ ]	[ ]
6.6	Are spare-parts availability and procurement aligned with critical assets?	[ ]	[ ]	[ ]
6.7	Have we defined escalation rules and safe responses to high-risk conditions?	[ ]	[ ]	[ ]
6.8	Do we track relevant maintenance metrics, such as MTTR, MTBF, downtime, and planned-work compliance?	[ ]	[ ]	[ ]

Priority warning

Do not assume AI prediction is the first step. Start with asset records, reliable signals, and a workable maintenance response.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

7. Cybersecurity and OT resilience

Review security and recovery before expanding machine connectivity.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
7.1	Do we maintain an inventory of OT devices, gateways, servers, software, and network equipment?	[ ]	[ ]	[ ]
7.2	Are IT and OT networks segmented with controlled, documented connections?	[ ]	[ ]	[ ]
7.3	Is remote access approved, time-limited where practical, role-based, and protected by MFA?	[ ]	[ ]	[ ]
7.4	Do we control changes to PLC programs, SCADA configurations, and network settings?	[ ]	[ ]	[ ]
7.5	Do we monitor unusual access and activity using approaches suitable for the OT environment?	[ ]	[ ]	[ ]
7.6	Do we keep protected backups and test restoration of critical production systems?	[ ]	[ ]	[ ]
7.7	Is there an incident-response plan with clear roles for production, IT, OT, and vendors?	[ ]	[ ]	[ ]
7.8	Have we agreed vendor access, data ownership, security duties, and access removal procedures?	[ ]	[ ]	[ ]

Priority warning

Default passwords, unrestricted remote access, and untested recovery are blockers to wider connectivity. Security controls must suit plant safety and availability.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

8. People and adoption

Make the new way of working practical for the people who use it.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
8.1	Have operators, supervisors, maintenance, quality, and planning teams helped define requirements?	[ ]	[ ]	[ ]
8.2	Do users understand which tasks the system will simplify or replace?	[ ]	[ ]	[ ]
8.3	Are workflows usable in the actual plant environment, including devices, language, and connectivity?	[ ]	[ ]	[ ]
8.4	Does training cover everyday tasks and exceptions, not just software features?	[ ]	[ ]	[ ]
8.5	Do supervisors know what actions to take from dashboards and alerts?	[ ]	[ ]	[ ]
8.6	Have we appointed plant-level champions with time and authority to support users?	[ ]	[ ]	[ ]
8.7	Do we track adoption through data completeness, alert response, and work-order closure?	[ ]	[ ]	[ ]
8.8	Is ongoing support available after go-live, including refresher training?	[ ]	[ ]	[ ]

Priority warning

If the system adds duplicate entry without removing old reporting, redesign the workflow with users.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

9. Implementation and scale

Use a controlled pilot to prove value and create a repeatable rollout model.

Tick one box per row: Yes = ready; Partial = incomplete; No = missing.

ID	Readiness question	Yes	Partial	No
9.1	Have we selected a limited first phase with measurable success and stop/go criteria?	[ ]	[ ]	[ ]
9.2	Are scope, timeline, budget, responsibilities, and plant access windows agreed?	[ ]	[ ]	[ ]
9.3	Will we document pilot lessons, configuration, operating procedures, and support needs?	[ ]	[ ]	[ ]
9.4	Can the approach be repeated across suitable machines, lines, or plants?	[ ]	[ ]	[ ]
9.5	Is the rollout sequence based on business impact, readiness, and operational risk?	[ ]	[ ]	[ ]
9.6	Is there governance for changes, data standards, integrations, and new use cases?	[ ]	[ ]	[ ]
9.7	Have we budgeted for support, licenses, connectivity, upgrades, and ongoing improvement?	[ ]	[ ]	[ ]
9.8	Will leadership review verified benefits and remaining risks at every rollout stage?	[ ]	[ ]	[ ]

Priority warning

A technically successful pilot is not enough. Confirm repeatability, support costs, and verified benefits before scaling.

Section totals: Yes ____ Partial ____ No ____

Evidence / top gap: _____

Action owner / due date: _____

Your readiness scorecard

Count the Yes, Partial, and No answers in each section. There are 72 questions in total.

Readiness area	Yes / 8	Partial / 8	No / 8
Business value and ROI			
Process and operations			
Machine and data			
IT and OT integration			
OEE and performance management			
Maintenance and predictive readiness			
Cybersecurity and OT resilience			
People and adoption			
Implementation and scale			
TOTAL / 72			

Use the results to decide what to do next

Do not use fixed numerical bands to approve investment. These questions have different risk levels, and this guide has no validated scoring thresholds. Instead, review the pattern of gaps and the evidence behind each answer.

Proceed to a limited pilot: Value targets, required data, safe access, ownership, and support are demonstrated.
Close gaps first: Critical inputs are partial, inconsistent, or untested.
Pause expansion: Safety, cybersecurity, recovery, data integrity, or accountable ownership remains unresolved.

Critical issues requiring review before expansion: _____

_____

Build your action plan

Prioritize gaps by business impact, safety or security risk, and dependency on other work. Give every action one owner and a due date.

Priority gap / evidence	Business impact	Owner	Due date

A suggested 30-60-90 day sequence

Days 1-30: Define and baseline. Select the first use case, quantify the loss, confirm owners, and review critical security and safety dependencies.

Days 31-60: Connect and validate. Test priority integrations, validate data, train users, and verify recovery and support arrangements.

Days 61-90: Test and review. Run a controlled pilot, compare results with the baseline, investigate exceptions, and make an evidence-based scale decision.

This sequence is illustrative, not a delivery or ROI guarantee. Adjust it to plant complexity, change windows, regulatory duties, and risk.

Track the business case

Agree on these measures with operations and finance before approving a pilot.

Business-case field	Your input
Priority use case	
KPI, definition, baseline period, and target	
Data source and KPI owner	
One-time implementation cost	
Annual operating and support cost	
Expected annual benefit and assumptions	
Pilot review date and stop/go criteria	

Avoid overstating benefits

Separate cash savings from released capacity. Additional capacity becomes revenue only if demand and downstream capacity support it. Avoid double-counting the same improvement across downtime, OEE, output, and labor benefits. Record assumptions and validate realized results with finance.

Turn your gaps into a practical next step

Share your top three readiness gaps with Vivify Soft Tech to discuss a focused assessment or implementation plan for industrial automation, IIoT, machine monitoring, or manufacturing data integration.

Explore Industrial Software & Automation
Explore FactorAI
reach@vivifysoft.com | +91 7305 7305 28

Vivify Soft Tech | Mugappair Road, Padi, Chennai, Tamil Nadu 600058
www.vivifysoft.com