INOVIQ TECHNOLOGIES

Engineering Intelligent Industry

DIGITAL MANUFACTURING MATURITY — SCORING GUIDE

Evidence-based guidance for consistent self-assessment across manufacturing sectors

How to score

Score	Level	Evidence pattern
0	Not established	No defined process or meaningful capability; information may be unavailable or entirely ad hoc.
1	Initial	Manual/reactive practices; isolated tools or pilots; little repeatability.
2	Developing	Defined practices and some deployed tools; adoption or integration is uneven; outcomes not consistently measured.
3	Advanced	Standardized, routinely used capability; integration where needed; repeatable KPI improvement.
4	Leading	Optimized capability; predictive/prescriptive insights embedded in decisions; value measured and sustained.

Evidence to collect

Use live dashboards, workflows, SOPs, KPI trends, maintenance records, audit evidence, cybersecurity exercises, training records and documented business cases. If capabilities vary by plant or line, score the site under assessment and record the variation.

Overall score interpretation

- 0–8 | Level 1 — Foundational — Establish ownership, baseline KPIs, reliable data capture and core operational controls.
- 9–16 | Level 2 — Emerging — Prioritize high-value use cases, standardize practices and address fragmented data/system foundations.
- 17–24 | Level 3 — Established — Improve interoperability, adoption, governance and measurable performance outcomes.
- 25–32 | Level 4 — Integrated — Scale proven use cases, strengthen advanced analytics and embed cross-functional optimization.
- 33–40 | Level 5 — Intelligent — Sustain benefits, continuously validate models and controls, and expand autonomy only where safe and justified.

Do not rely on the average alone. Cybersecurity, process safety, regulatory compliance, product quality and operational resilience may act as risk gates regardless of total score.

Dimension-by-dimension scoring examples

These are practical anchors, not rigid technology requirements. Judge fit, adoption, evidence and outcomes—not the presence of a particular vendor or product.

1. Digital strategy & leadership

0	1	2	3	4
No digital ownership or roadmap.	Scattered initiatives; business case and ownership are unclear.	Roadmap and sponsors exist; funding, KPIs or governance are inconsistent.	Prioritized roadmap, accountable owners, funding governance and outcome KPIs are routinely reviewed.	Portfolio is dynamically reprioritized using verified value, risk and strategic outcomes; benefits are sustained across sites.

2. Automation & process control

0	1	2	3	4
Little relevant automation or systematic digital monitoring.	Basic control/automation exists but monitoring is limited or reactive.	Automation is deployed in selected areas; standards and performance visibility vary.	Appropriate automation and controls are standardized, monitored and routinely improved.	Control strategies are optimized using advanced control or closed-loop optimization where appropriate, with verified operational gains.

3. Connected operations & systems

0	1	2	3	4
Operational and enterprise information is disconnected or manually reconciled.	Point-to-point links or spreadsheets connect a few processes.	Key systems exchange some data, but gaps and manual workarounds remain.	Relevant plant and enterprise systems share governed data through a maintainable architecture.	Interoperability is scalable and well governed; contextualized information supports end-to-end decisions across functions/sites.

4. Data, analytics & AI

0	1	2	3	4
Data is unavailable, unreliable or rarely used for decisions.	Basic reports or isolated pilots; data quality and ownership are weak.	Dashboards and selected analyses are used, but insights are not consistently embedded in workflows.	Trusted data and analytics routinely inform decisions; use cases and outcomes are measured.	Predictive/prescriptive analytics or AI are governed, monitored and scaled where value and risk justify them.

5. Asset reliability & maintenance

0	1	2	3	4
Maintenance is mostly reactive; asset condition data is not systematically used.	Preventive maintenance and isolated condition monitoring are in place.	CMMS/EAM data and condition insights support selected assets; adoption varies.	Reliability practices use asset criticality, condition and failure analysis; KPIs are reviewed.	Risk-based predictive strategies are continuously optimized and demonstrably improve availability/cost.

6. Quality & traceability

0	1	2	3	4
Quality records are mostly manual; traceability is limited where needed.	Some digital inspection or records exist, but investigations are slow or fragmented.	Quality data is collected digitally in key areas; analytics and traceability are partial.	Digital quality workflows, relevant traceability and root-cause processes are standardized.	Statistical/predictive quality insights prevent defects and deviations; controls are validated and sustained.

7. Planning & supply chain

0	1	2	3	4
Planning relies on manual processes and siloed information.	Some planning systems exist, but updates and reconciliation are manual.	Planning/inventory data is available digitally; cross-functional synchronization	Production and supply planning use connected data, constraints and	Scenario-based or optimized planning improves service, inventory

		is incomplete.	regular performance review.	and responsiveness with measured results.

8. People, skills & adoption

0	1	2	3	4
No structured digital skills or change approach.	Training is ad hoc; adoption depends on a few enthusiasts.	Role-based training and change activities exist, but usage is inconsistent.	Leaders reinforce adoption; competency, usage and frontline feedback are monitored.	Continuous learning and co-design are embedded; workforce capability adapts as technology and roles evolve.

9. Cybersecurity & resilience

0	1	2	3	4
Industrial asset visibility, ownership or basic protections are inadequate.	Basic controls exist, but coverage, recovery or incident procedures are incomplete.	Asset inventory and controls are established for key areas; exercises or remediation have gaps.	Risk-based OT security, access, segmentation, backups and response/recovery are managed and tested.	Security and resilience are continuously improved through monitoring, exercises, remediation and lessons learned.

10. Performance, energy & sustainability

0	1	2	3	4
Relevant operating measures are unavailable or inconsistently defined.	Some KPIs are recorded manually or reviewed reactively.	Digital dashboards cover selected KPIs; definitions, coverage or follow-through vary.	Trusted KPIs are routinely reviewed and linked to improvement actions and accountable owners.	Optimization continuously balances productivity, quality, energy, waste and emissions, with verified benefits.

Radar chart and action planning

Plot scores for dimensions 1–10 on the 0–4 radar chart in the self-assessment. Sharp dips identify potential capability gaps. Do not treat the chart as an industry benchmark unless a validated, comparable dataset is available.

Select two or three priority gaps; define the business problem and baseline; assign an accountable owner; set a measurable target and timeframe; assess dependencies, safety and cybersecurity; validate benefits after implementation.

Industry adaptation: use relevant equivalents such as throughput, yield, process stability, batch consistency, water quality, asset availability or energy intensity.