MANUFACTURING MSP EVALUATION SCORECARD

30 QUESTIONS · UPTIME, CYBERSECURITY & OPERATIONAL FIT

The Manufacturing MSP Evaluation Scorecard.

Thirty questions to compare managed IT providers by uptime, cybersecurity, and operational fit. Built for manufacturing CIOs, IT leaders, operations leaders, and owners. Ask each provider the same questions, request evidence, and score every answer from 0 to 3.

— HOW TO SCORE

0 **No evidence or unacceptable risk.** Cannot answer or demonstrate the capability, or has a material deficiency.

1 **Partial capability or important gap.** Partial solution, unclear ownership, or an undocumented process.

2 **Meets the requirement.** A credible, documented approach for the evaluated environment.

3 **Strong, manufacturing-specific capability.** Documented evidence, relevant experience, references, or a mature process.

Weighted score, out of 100. 85–100 = strong fit; 70–84 = potential fit, clarify gaps; 55–69 = material concerns; below 55 = high risk. Cybersecurity and IT/OT risk carries the most weight. A score of 0 in a critical area — identity, endpoint, segmentation, monitoring, incident response, RTO/RPO, or backups — can disqualify a provider even if the total looks acceptable.

01 Manufacturing and operational fit

20% OF SCORE · 6 QUESTIONS

#	EVALUATION QUESTION & EVIDENCE TO REQUEST	CUR	A	B
1	How many active manufacturing, warehouse, logistics, or industrial environments does the provider support, and can it provide relevant references? **Evidence:** Industry references, anonymized use cases, client mix, case studies	☐	☐	☐
2	Does the provider understand how IT incidents can affect production, shipping, receiving, inventory, quality, warehouse workflows, and customer service? **Evidence:** Incident-priority model, manufacturing examples, escalation documentation	☐	☐	☐
3	Has the provider supported the infrastructure around your ERP, MES, warehouse-management, labeling, or production-planning systems? **Evidence:** Relevant platform experience, vendor-coordination process, infrastructure examples	☐	☐	☐
4	Can the provider clearly define the boundary between IT responsibilities and OT responsibilities? **Evidence:** Responsibility matrix, change-control process, examples of IT/OT coordination	☐	☐	☐
5	Does the provider have a documented approach for working with plant engineering teams, OEMs, ERP vendors, carriers, and other third parties? **Evidence:** Vendor-coordination workflow, RACI, escalation process	☐	☐	☐
6	Can the provider support multi-site operations, remote facilities, warehouses, and operational wireless requirements? **Evidence:** Network architecture examples, field-support model, monitoring approach	☐	☐	☐

02 Cybersecurity and IT/OT risk

35% OF SCORE · 9 QUESTIONS

#	EVALUATION QUESTION & EVIDENCE TO REQUEST	CUR	A	B
7	Does the provider enforce MFA for remote access, cloud services, privileged accounts, and other high-risk workflows? CRITICAL **Evidence:** MFA policy, identity architecture, conditional-access examples	☐	☐	☐
8	Does the provider use modern endpoint security with monitoring, alerting, investigation, and response processes? CRITICAL **Evidence:** Security-stack description, endpoint coverage reporting, response workflow	☐	☐	☐
9	Does the provider provide layered email security and practical phishing-awareness training? **Evidence:** Email-security architecture, training cadence, reporting example	☐	☐	☐
10	Does the provider maintain a vulnerability-management process that prioritizes exposure, exploitability, business impact, and operational safety? **Evidence:** Vulnerability workflow, remediation report, exception process	☐	☐	☐
11	Can the provider design and manage segmentation using VLANs, firewall rules, access controls, separate IT/OT zones, and industrial DMZ concepts where appropriate? CRITICAL **Evidence:** Network diagram, segmentation methodology, firewall-change process	☐	☐	☐
12	Does the provider secure vendor remote access through MFA, least privilege, time-limited access, approval workflows, logging, and defined network paths? **Evidence:** Remote-access standard, vendor-access workflow, logging example	☐	☐	☐
13	Does the provider provide 24/7 monitoring and defined alert-response or escalation procedures? CRITICAL **Evidence:** Monitoring scope, escalation matrix, after-hours coverage description	☐	☐	☐
14	Does the provider have a documented incident-response plan that includes communication, containment, evidence preservation, recovery coordination, and production-impact escalation? CRITICAL **Evidence:** Incident-response plan, tabletop-exercise evidence, sample communications	☐	☐	☐
15	Does the provider maintain or support asset inventory, lifecycle tracking, and risk treatment for legacy or unsupported systems? **Evidence:** Asset-inventory report, lifecycle plan, risk-register example	☐	☐	☐

03 Service delivery and incident response

20% OF SCORE · 6 QUESTIONS

#	EVALUATION QUESTION & EVIDENCE TO REQUEST	CUR	A	B
16	Does the provider prioritize and escalate support incidents based on operational and business impact, including potential effects on production, shipping, warehouse operations, and customer service? **Evidence:** Severity matrix, escalation policy, operational-impact examples	☐	☐	☐
17	Is 24/7 remote response available, and are after-hours escalation and communication procedures clearly defined? **Evidence:** Service description, escalation contacts, coverage schedule	☐	☐	☐
18	How does the provider coordinate onsite support for production-impacting incidents in your locations? **Evidence:** Onsite-support coverage map, dispatch process, field-service-partner model	☐	☐	☐
19	Are response, escalation, communication, and onsite-coordination commitments clearly defined in the agreement? **Evidence:** SLA or service-level exhibit, exclusions, reporting process	☐	☐	☐
20	Does the provider maintain current documentation for networks, systems, credentials, vendors, recovery processes, and key dependencies? **Evidence:** Documentation standards, sample network diagram, onboarding deliverables	☐	☐	☐
21	Does the provider conduct regular operational reviews and provide meaningful reporting on incidents, service trends, security, projects, and risk? **Evidence:** Sample QBR, executive report, service review cadence	☐	☐	☐

04 Infrastructure, cloud, and business continuity

15% OF SCORE · 5 QUESTIONS

#	EVALUATION QUESTION & EVIDENCE TO REQUEST	CUR	A	B
22	Can the provider evaluate cloud, hybrid, and on-premise options based on application dependencies, connectivity, latency, security, cost, and operational requirements? **Evidence:** Architecture recommendations, migration methodology, similar-project example	☐	☐	☐
23	Does the provider have demonstrated expertise with Microsoft 365, Microsoft Entra ID, Azure, Intune, Microsoft Defender, and related Microsoft technologies when those platforms are relevant? **Evidence:** Certifications, service descriptions, tenant-security baseline	☐	☐	☐
24	Does the provider manage networks, firewalls, switching, wireless, internet connectivity, and remote-site connectivity with proactive monitoring and documented standards? **Evidence:** Network-management scope, monitoring examples, design standards	☐	☐	☐
25	Does the provider define RTO and RPO targets with business stakeholders and align recovery priorities to production, shipping, identity, ERP, and other critical workflows? CRITICAL **Evidence:** Business-impact analysis, recovery-priority matrix, DR plan	☐	☐	☐
26	Does the provider support protected backup copies, restore testing, disaster-recovery planning, and documented recovery procedures? CRITICAL **Evidence:** Backup architecture, restore-test report, recovery runbook	☐	☐	☐

05 Commercial terms, governance, and transition

10% OF SCORE · 4 QUESTIONS

#	EVALUATION QUESTION & EVIDENCE TO REQUEST	CUR	A	B
27	Is the managed-services scope clear about included services, exclusions, client responsibilities, third-party dependencies, and project work? **Evidence:** Proposal, service catalog, responsibility matrix	☐	☐	☐
28	Does the client retain ownership and access to network documentation, administrative credentials, configuration records, backup data, and other essential operational information? **Evidence:** Contract language, transition clause, documentation policy	☐	☐	☐
29	Are pricing, change-control procedures, project costs, and service-level review processes transparent and understandable? **Evidence:** Pricing schedule, change-order process, service-review template	☐	☐	☐
30	Does the agreement include a practical onboarding, transition, offboarding, and knowledge-transfer process that protects operational continuity? **Evidence:** Onboarding plan, transition checklist, offboarding language	☐	☐	☐

— YOU HAVE THE QUESTIONS. NOW MAKE THE RIGHT DECISION.

A scorecard reveals gaps, but it does not replace a conversation about your environment, facilities, operational risks, internal team, and business goals. Network Builders IT helps manufacturers and logistics organizations assess technology risk, improve cybersecurity, support internal IT teams, and build infrastructure strategy around operations.

Talk with NBIT about your completed scorecard →

Schedule a Discovery Call →

Take the Cybersecurity Self-Assessment →

This scorecard supports a business and technology evaluation. It does not replace legal, audit, certification, insurance, regulatory, engineering, or operational-safety advice. Plant engineering teams and equipment vendors should remain involved in decisions affecting PLCs, SCADA, HMIs, machine controls, and direct operational-technology changes.