

End-to-End Supply Chain Readiness Card

Score your supply chain end to end, from plan, source and make through deliver and return, in ten minutes.

By John Foley, former Air Force Lt Col

HOW TO SCORE

Rate each statement: 0 not in place · 1 ad hoc · 2 in place, not consistent · 3 in place, measured and owned. Add each domain (0–12), then your total (0–96).

Questions, scale and bands are FSA's own scoring, not an industry standard. Domain labels show alignment, not certification.

Domains cover the whole chain using all seven SCOR Digital Standard processes: Orchestrate, Plan, Order, Source, Transform, Fulfill, Return¹ (Deliver = Order + Fulfill), plus visibility and cyber^{3,4}.

WHY IT MATTERS

95%

see supplier risk at tier one²

42%

see it at tier two or beyond²

Plan

SCOR: Plan¹

- 1 One demand plan is agreed by sales, operations, finance and procurement each month. (0) (1) (2) (3)
- 2 We measure forecast accuracy and act on the error, by product family. (0) (1) (2) (3)
- 3 Supply plans check supplier and plant capacity, not just our own demand. (0) (1) (2) (3)
- 4 We can re-run the plan within a week when a major input changes (demand, lane, supplier). (0) (1) (2) (3)

Domain score ____ / 12

Source & Procurement

SCOR: Source¹

- 5 Spend is categorized and each top category has a written sourcing strategy. (0) (1) (2) (3)
- 6 Critical single-source parts have a qualified second source or a documented exception. (0) (1) (2) (3)
- 7 Supplier scorecards (cost, quality, delivery, risk) are reviewed with suppliers on a set cadence. (0) (1) (2) (3)
- 8 Contracts spell out how input-cost and price changes are shared. (0) (1) (2) (3)

Domain score ____ / 12

Make

SCOR: Transform¹

- 9 Production schedules are built from the current demand plan, not last month's. (0) (1) (2) (3)
- 10 We know our constraint operations and protect their capacity. (0) (1) (2) (3)
- 11 Quality escapes are traced to root cause and closed with the supplier or line. (0) (1) (2) (3)
- 12 Maintenance on critical assets is planned, not run-to-failure. (0) (1) (2) (3)

Domain score ____ / 12

Deliver

SCOR: Order + Fulfill¹

- 13 We track on-time, in-full delivery to customers every week. (0) (1) (2) (3)
- 14 Each major freight lane has a backup carrier or mode. (0) (1) (2) (3)
- 15 Inventory targets are set by item and reviewed against service and cash goals. (0) (1) (2) (3)
- 16 Customers get proactive notice when an order will be late. (0) (1) (2) (3)

Domain score ____ / 12

Return

SCOR: Return ¹

- 17

Returns are logged with a reason code and reviewed for root cause.

0

1

2

3
- 18

Returned goods are dispositioned (restock, repair, recycle, scrap) within a set time.

0

1

2

3
- 19

Supplier-caused returns are charged back or recovered.

0

1

2

3
- 20

Return volumes feed back into the demand and quality plans.

0

1

2

3

Domain score ____ / 12

Risk & Resilience

SCOR: Orchestrate, risk mitigation ¹

- 21

We have mapped which suppliers, sites and lanes could stop revenue, and by how much.

0

1

2

3
- 22

Revenue exposure is quantified by critical part, supplier and site.

0

1

2

3
- 23

There is a tested playbook for a top-supplier or top-lane outage.

0

1

2

3
- 24

A named executive owns supply chain risk and reports it to leadership.

0

1

2

3

Domain score ____ / 12

Visibility & Data

Multi-tier visibility ²

- 25

We can see risk at our tier-one suppliers.

0

1

2

3
- 26

We have mapped our tier-two suppliers for critical parts and are in direct contact with them.

0

1

2

3
- 27

Inventory, orders and shipments are visible in one place, not in separate spreadsheets.

0

1

2

3
- 28

Master data (items, suppliers, lead times) is owned and kept current.

0

1

2

3

Domain score ____ / 12

Cyber

NIST SP 800-161r1 ³; CSF 2.0 GV.SC ⁴

- 29

Suppliers with system or data access are risk-tiered before onboarding.

0

1

2

3
- 30

Contracts require suppliers to report cyber incidents to us within a set time.

0

1

2

3
- 31

We know which supplier outages would stop our ordering, production or shipping systems.

0

1

2

3
- 32

Supplier access is reviewed and removed when no longer needed.

0

1

2

3

Domain score ____ / 12

Total score ____ / 96

What your score means

0-24

Exposed

Gaps across most domains. A single disruption likely reaches customers. Start with Risk & Resilience and Visibility.

25-48

Reactive

Basics exist but depend on people, not process. Fix the two lowest domains first.

49-72

Managed

Repeatable processes in most domains. Close remaining gaps, especially deep-tier visibility and cyber.

73-96

Resilient

Integrated, tested and owned end to end. Keep testing playbooks and widen supplier visibility.

Bands are Foley Strategic Advisory's rubric, not an industry benchmark. Any single domain scoring 0-5 is your weakest link, whatever your total.

Want a second set of eyes on your score?

Book a 30-minute call →

Sources. 1. ASCM, SCOR Digital Standard, "SCOR Processes," scor.ascm.org/processes (read Oct 16, 2026). 2. McKinsey, "Supply chain risk pulse 2025," Dec 2, 2025 (n=100), mckinsey.com. 3. NIST SP 800-161 Rev. 1, May 2022, csrc.nist.gov. 4. NIST Cybersecurity Framework 2.0, GV.SC, nist.gov.
John Foley, former Air Force Lt Col · Foley Strategic Advisory