SUPPLY CHAIN RISK SELF-ASSESSMENT QUESTIONNAIRE

Category	#	Question	Yes	No
1 Governance	1	Is there a C-level position responsible for managing supply chain management?		
	2	Is there a Chief Risk Officer or similar position responsible for managing risk?		
	3	Is your staff trained in predictive analytics?		
2 Strategy	4	Does your business plan address contract, operating, and environmental risk?		
	5	Is your company certified in ISO 31000 or an alternative risk management standard?		
3 Measurement	6	Do you track the cost of supply chain disruptions?		
	7	Do you have a standard methodology for measuring supply chain cost?		
	8	Do you quantify your company's dependence on certain suppliers?		
	9	Do you know which parts or components would cause a stockout of your end-product if unavailable for two weeks?		
	10	Does your sustainability reports include Scope 1, 2, and 3 carbon footprint?		
4 Visibility	11	Do you know who your sub-suppliers are?		
	12	Can you track products in your supply chain in real time?		
	13	Do you have regular visibility to inventory at Tier 3 suppliers?		
	14	Do you have a supply chain control tower or dashboard?		
	15	Do you use AI in demand planning and procurement?		
	16	Do you conduct scenarios of supply chain disruption?		
5 Contracting	17	Do you have a policy on single and dual sourcing?		
	18	Do you hold Tier 1 and 2 suppliers accountable for safe risk management practices?		
	19	Do procurement procedures assure that contracts are profitable for suppliers?		
	20	Do you base procurement decisions on the Total Cost of Ownership?		
	21	Do you audit supplier compliance to contract terms?		
6 Quality	22	Do you measure the Cost of Quality, including internal and external failure costs?		
	23	Do you use Cause and Effect Tools?		
	24	Do you use Failure Modes and Effects Analysis (FMEA) tools?		
	25	Do your company assess suppliers' conformance to environmental protocols?		
7 Cybersecurity	26	Is there a policy that governs and limits development in adversarial environments?		
	27	Do you assure supplier compliance to Denied Persons, Disapproved Vendors, and Related lists and orders?		
	28	Do you use standard contract language about cybersecurity and provenance?		
	29	Do you require vendors to validate the authenticity and origins of third-party hardware and software?		
	30	Are you aware of current threats to mitigate active supply chain cybersecurity risks?		

Evaluation: >25: Top of the Heap, 20-25: Congratulations! You are methodically closing off sources of supply chain risk. 15-20: You are vulnerable in some areas. <15: You are exposed on multiple fronts.