Supply Chain Risk Management Plan & Dynamic Risk Register

Acme Widgets Inc. (Made up company)

Author: Quincy Kizekai

Date: July 2, 2025

1. Introduction

Purpose: Establish a formal Supply Chain Risk Management (C-SCRM) program to identify, assess, and mitigate risks among Acme Widgets Inc.'s critical suppliers.

Objectives:

- Define risk appetite and governance.
- Maintain a living risk register with quantitative scoring.
- Map risks to NIST SP 800-53 controls for audit readiness.

2. Scope & Roles

- Scope: Top 5 suppliers supporting Product Lines A & B across North America, Europe, and Asia.
- Risk Appetite: Moderate; acceptable supply delays ≤ 5% of monthly volume.
- Roles & Responsibilities:
  - Supply Manager – Owner of risk register updates.
  - Quality Lead – Executes supplier audits and QC testing.
  - Logistics Manager – Maintains transport contingency plans.
  - IT Security Lead – Oversees ERP software security.
  - Risk Committee – Quarterly oversight and approvals.

3. Policy & Strategy

- All critical suppliers will undergo initial and annual risk assessments.
- Reviewed by Risk Committee quarterly; approved by CFO & CIO annually.
- Policy refresh every 12 months or upon major supply chain events.

4. Risk Assessment Methodology

- Framework: NIST SP 800-30 (Risk Management Guide).
- Rate Likelihood (1–5) and Impact (1–5), then compute Risk Score = Likelihood × Impact.
- Document rationale for each rating (e.g., tariffs driving steel delays).

Rating Scale (1=Low, 3=Medium, 5=High):

1	2	3	4	5
Very Low	Low	Moderate	High	Very High

5. Identified Risks & Risk Register

Risk Register (Numeric Scales 1–5)

ID	Date Raised	Risk Description	Likelihood	Impact	Severity	Owner	Mitigating Action
R001	2025-06-01	Steel supply delay due to new tariffs	5	5	5	Supply Manager	Maintain alternate vendors & buffer inventory; monitor tariff updates monthly and adjust orders proactively.
R002	2025-06-03	Quality defects in circuit boards	3	5	5	Quality Lead	Enforce incoming QC inspections and annual supplier audits; reject batches exceeding defect thresholds.
R003	2025-06-05	Plastic casing contamination	1	3	3	Quality Lead	Require material certificates on every shipment; conduct random batch tests and quarantine suspect lots.
R004	2025-06-07	Transport disruption due to carrier strikes	3	5	5	Logistics Manager	Contract with multiple carriers; subscribe to strike alert feeds and pre book reroute options to avoid delays.
R004	2025-06-09	ERP software data breach	1	5	5	IT Security Lead	Enforce MFA on all accounts; run quarterly pen tests and continuous vulnerability scans; review logs weekly for anomalies.

6. Controls Mapping

Map each risk to NIST SP 800-53 Rev 5 controls:

Control ID	Control Name	Risk IDs Addressed	Evidence/Notes
AC-1	Access Control Policy	R005	Policy Change
SI-2	Flaw Remediation	R002	Issue tracker reports
CM-3	Configuration Change Control	R001	Change logs in CIP
MP-6	Media Protection	R003	Test reports
SC-7	Boundary Protection	R004	Network diagrams

7. Monitoring & Reporting

• Monthly Reviews: Supply Manager updates risk scores and statuses.

• Quarterly Deep Dives: Risk Committee reviews trends and approves new mitigations.

• Dashboard: Bar chart of top 5 risks, table of overdue reviews

8. Maintenance & Continuous Improvement

• Triggers: Supplier performance < 90%, geopolitical or regulatory changes, post-incident.

• Version Control: Document versioned via Git tags; spreadsheets tracked in GitHub.

• Review Cycle: Policy refresh every 12 months or after major events.