

Supplier Business Continuity Planning Guide

Practical guidance and self-assessment for chemical and packaging suppliers

Summary: A solid Business Continuity Plan (BCP) should establish a common, practical resilience baseline and be proportionate to the supplier's criticality, supplied products/services, supplying sites and key dependencies.

Suppliers can use the following areas as a practical reference to build and document a robust BCP

- BCM governance and plan ownership, including policy and objectives, accountability, activation authority, resources, escalation and document control;
- A structured Business Impact Analysis (BIA) covering critical products, services and supporting activities, impact over time, recovery priorities and critical dependencies;
- A risk assessment that identifies disruptive events, threats, vulnerabilities, existing controls, residual risk, action priorities and risks outside tolerance, including direct site events and failures in critical dependencies;
- Climate resilience and natural hazards assessment by location and across the supply network, including physical climate hazards, utility scarcity, critical thresholds, lead time, current controls, autonomy and adaptation actions;
- Business continuity strategies and solutions that are safe, legally compliant, technically feasible, funded, documented and tested across products and inventory, raw materials/components, manufacturing, utilities and facilities, quality/regulatory, logistics, workforce, IT/OT/data and finance/suppliers.
- Customer and Solenis communication management, including notification triggers, initial notification, , communication log, secure channels and coordination with legal, EHS, quality, cybersecurity and regulatory teams.

The BCP should be operational through training, awareness, exercises and competence, with records of tabletop exercises, functional/technical tests, alternate site or supplier tests, lessons learned and corrective actions.

It should also be kept current through BCP maintenance, review and continuous improvement, including review frequency, event-driven update triggers, management review, revision history, evidence of action closure and management approval.

ISO 22301 certification is not a mandatory requirement; however, suppliers are expected to demonstrate that the plan can be activated under pressure and can protect people, the environment, operations, customers and continuity of supply.

This guide walks through each area in more detail, offering practical guidance to help you build, review and continuously improve your BCP. **TOGETHER we can build a more resilient and sustainable supply chain.**

As part of the Solenis Supplier Risk Program and supply chain resilience assessment, Solenis may, where required and proportionate to the supplier's risk profile, request supporting BCP evidence through a due diligence process managed via the Coupa Risk module. If you haven't received any request, but you want to share proactively your BCP with us, you can email out to supplierrisk@solenis.com .

Solenis Supplier Risk Team

More information about Solenis Supplier risk program are available here [Supplier Risk Program](#)

Purpose Help suppliers understand, build, test and maintain a proportionate Business Continuity Plan (BCP) that protects people, the environment, operations, customers and continuity of supply. This guide uses ISO 22301 principles; it does not require ISO 22301 certification.

Table of Contents

The guide follows a simple cycle: understand what is critical, identify disruption risks, select workable continuity strategies, prepare the response, exercise the plan and improve it.

1. INTRODUCTION: WHY SOLENIS PREPARED THIS GUIDE	3
2. BCM GOVERNANCE AND PLAN OWNERSHIP	4
3. BUSINESS IMPACT ANALYSIS (BIA)	5
4. RISK ASSESSMENT	6
5. CLIMATE RESILIENCE AND NATURAL HAZARDS	7
6. BUSINESS CONTINUITY STRATEGIES AND SOLUTIONS	8
8. CUSTOMER AND SOLENIS COMMUNICATION	10
10. BCP MAINTENANCE, REVIEW AND CONTINUOUS IMPROVEMENT	12
11. SUPPLIER SELF-ASSESSMENT	13
12. CORRECTIVE ACTION PLAN, EVIDENCE AND APPROVAL	14
DOCUMENT REVISION HISTORY	14
APPENDIX A — ONE-PAGE BCP MINIMUM CONTENT CHECKLIST	15
APPENDIX B — SCENARIO EXERCISE PROMPTS	15
APPENDIX C — GLOSSARY	15
APPENDIX D — REFERENCE FRAMEWORK AND NOTES	16
IMPORTANT INTERPRETATION NOTES	16

Recommended participants BCP owner, site/operations, EHS, supply chain/procurement, quality/regulatory, engineering/maintenance, IT/OT/cybersecurity, HR, customer service/sales, logistics and senior management. Include relevant contractors and alternate-site representatives.

1. Introduction: Why Solenis prepared this guide

Solenis depends on a global network of suppliers to maintain safe, compliant and reliable supply to customers. A disruption at a supplier can move quickly across the value chain through unavailable materials, missed production, constrained transport, quality deviations or delayed information.

1.1 Objectives

- Establish a common, practical resilience baseline for chemical and packaging suppliers.
- Help suppliers protect their own people, assets, revenue, obligations and customer relationships.
- Improve early warning, transparency and coordinated mitigation when supply is threatened.
- Encourage risk-based planning that includes cyber, utilities, upstream dependencies, climate and natural hazards.
- Support continuous improvement without making ISO 22301 certification a condition of using this guide.

1.2 What “aligned with ISO 22301 principles” means

ISO 22301 describes a management-system approach to business continuity: leadership and governance; understanding the organization; planning; resources and competence; operational analysis and solutions; response arrangements; evaluation; and improvement. This guide translates those principles into supplier actions and evidence. It is not a clause-by-clause certification checklist and does not reproduce the standard.

1.3 What Solenis expects from suppliers

The assessment should cover every site, process and dependency that can materially affect products or services supplied to Solenis. Where a corporate BCP exists, the supplier should show how it is applied locally and how site-specific hazards, contacts, utilities, permits, transport routes and recovery capabilities are addressed.

Proportionality A smaller supplier may use a concise plan, but the plan must still identify critical supply, recovery priorities, responsible people, practical workarounds, communication and testing. Complexity should match the risk—not the size of the document.

2. BCM governance and plan ownership

Governance makes continuity repeatable. It prevents confusion over who can activate the plan, commit resources, stop unsafe operations, contact customers and authorize recovery.

2.1 Recommended governance content

Element	What good practice looks like	Typical evidence
Policy and objectives	Management statement covering safety, legal obligations, priority products/customers, recovery and improvement.	Approved policy; objectives; scope.
Accountability	Executive sponsor, BCP owner, deputy and process/site owners.	Named roles; job titles; deputies; 24/7 contact method.
Activation authority	Who may classify an incident and activate/deactivate the BCP.	Activation criteria; decision log; escalation matrix.
Resources	Budget, people, contracts, emergency purchases, alternate sites, equipment and training.	Approved resources; emergency procurement authority.
Document control	Version, owner, approver, distribution, secure access and offline availability.	Controlled copy; revision history; accessible emergency copy.

2.2 Crisis/continuity team

Define a cross-functional core team. Roles should be assigned by function so the arrangement survives personnel changes. For multi-site supply, identify corporate, site and alternate-site interfaces.

Role	Core responsibility	Primary / deputy / 24-hour contact
Incident leader	Overall command, classification, priorities and external commitments	
EHS / emergency lead	Life safety, hazardous materials, environment and authority liaison	
Operations / engineering	Damage assessment, safe shutdown, restart and capacity	
Supply chain / logistics	Materials, suppliers, inventory, carriers and routes	
IT/OT / cyber	System isolation, recovery, backups and OT safety	
Quality / regulatory	Specifications, release, change control, permits and notifications	
Customer communication	Solenis/customer notices, updates and action tracking	
HR / workforce	Accountability, welfare, staffing and labor arrangements	

3. Business Impact Analysis (BIA)

A BIA is a structured analysis of how disruption affects the organization over time. It identifies which products, services and supporting activities are most time-sensitive, what resources they need and how quickly they must be restored. The BIA sets recovery priorities; it is not the same as a risk assessment.

Why the BIA comes first Without a BIA, a supplier may protect the most visible asset rather than the activity that must recover first. The BIA links customer impact to processes, people, equipment, utilities, data, materials, permits and logistics, providing a defensible basis for investment and recovery decisions.

3.1 Key terms

Term	Practical meaning
Maximum Tolerable Period of Disruption (MTPD)	Point after which impacts become unacceptable to the organization and its obligations.
Recovery Time Objective (RTO)	Target time to resume an activity at an agreed minimum level after disruption. RTO should be shorter than the MTPD.
Minimum Business Continuity Objective (MBCO)	Minimum acceptable capacity or service level during recovery, e.g., 40% of normal output for priority SKUs.
Recovery Point Objective (RPO)	Maximum tolerable data loss measured in time, mainly for IT/OT information and transactions.
Work Recovery Time	Time needed after systems/assets return to clear backlog, validate quality and stabilize service.

3.2 How to perform the BIA

Step	Supplier activity
1. Define scope	List Solenis-supplied products/services, supplying sites, lanes and relevant customer commitments.
2. Map delivery chain	From incoming raw material through processing, quality release, storage, order processing and transport.
3. Assess impact over time	Consider safety/environment, customer, legal/regulatory, quality, financial, reputation and contractual impacts at realistic time intervals.
4. Set priorities	Determine MTPD, RTO, MBCO and backlog recovery needs; validate assumptions with customers/contracts where appropriate.
5. Identify dependencies	People/skills, equipment/tooling, utilities, IT/OT, data, raw materials, packaging components, laboratories, permits, warehouses, carriers, ports and contractors.
6. Validate capability	Compare required recovery time with actual recovery capability. Record gaps and actions.

3.3 Supplier-specific prompts

Chemical supplier examples	Packaging supplier examples
Batch reactors, blending, distillation, bulk storage, nitrogen/steam/cooling water, effluent treatment, hazardous-area controls, laboratory release, feedstock compatibility and transport of dangerous goods.	Extrusion, molding, forming, printing, coating, laminating, converting, tooling/molds, resin/paper/metal/glass, inks/adhesives, compressed air, color/print approval and food/contact compliance where applicable.
Assess safe shutdown/restart, contamination, reaction stability, tank capacity, permit constraints and off-site emergency dependencies.	Assess mold portability, machine compatibility, tooling ownership, artwork/cylinder availability, dimensional tolerances and alternate material qualification.

3.4 Example of BIA worksheet

Critical product / activity	Site / process	Impact if unavailable	MTPD	RTO	MBCO	Critical dependencies

4. Risk assessment

The risk assessment identifies disruptive events, vulnerabilities and control gaps that could prevent the organization from meeting the recovery requirements set by the BIA. It should examine both direct site events and failures in critical dependencies.

4.1 Practical method

1. Describe the scenario and affected asset, process, site or route.
2. Identify causes, warning indicators and existing preventive/response controls.
3. Score likelihood and impact using defined criteria. Impact should consider the BIA and time to loss of supply.
4. Assess residual risk after current controls.
5. Assign additional mitigation with an owner, due date and target residual risk.
6. Escalate risks outside tolerance to management; integrate accepted risks into exercises and monitoring.

4.2 Simple 5 × 5 scoring

Rating	Likelihood guide	Impact guide
1 – Rare / Insignificant	Exceptional; limited credible history/exposure.	No material interruption; handled within routine operations.
2 – Unlikely / Minor	Possible but not expected.	Short disruption; no missed critical commitment.
3 – Possible / Moderate	Credible under current conditions.	Customer impact or constrained supply requiring management coordination.
4 – Likely / Major	Has occurred or exposure is significant.	Extended outage, major customer/regulatory/EHS consequence.
5 – Almost certain / Severe	Expected repeatedly or indicators are present.	Threat to life/environment, prolonged loss of critical supply or major legal impact.

Risk score = likelihood × impact. Suggested action bands: 1–4 Low (monitor); 5–9 Moderate (improve where proportionate); 10–16 High (formal mitigation and management oversight); 17–25 Critical (urgent treatment and continuity strategy). Suppliers may use their own method if criteria and acceptance are documented.

4.3 Typical risk potentially affecting Chemical and Packaging suppliers

Category	Example scenarios to evaluate
Common manufacturing	Fire/explosion, equipment or tooling failure, utility outage, building loss, quality contamination, warehouse loss, labor shortage, strike, pandemic, key-person dependency.
Chemical-specific	Loss of feedstock; runaway reaction; spill/release; hazardous storage or transfer incident; waste/effluent treatment failure; cooling, steam, nitrogen or water loss; permit restriction; dangerous-goods transport constraint.
Packaging-specific	Resin/paper/metal/glass shortage; mold/die/cylinder damage; extrusion or molding outage; ink/adhesive shortage; print/artwork data loss; product-contact compliance change; compressed-air or curing-system failure.
Supply chain/logistics	Single/sole source; sub-tier insolvency; port/terminal closure; carrier or container shortage; customs/sanctions/export restriction; bridge/road/rail disruption; temperature-control failure; warehouse capacity loss.
Digital and cyber	Ransomware; ERP/MES/WMS/QMS outage; OT compromise; telecommunications loss; corrupted backup; third-party cloud/EDI outage; loss of recipes, specifications, artwork or certificates.
External / geopolitical	Civil unrest, conflict, border closure, trade restriction, sudden regulation, critical infrastructure disruption, fuel shortage and security threat.

4.4 Example of Risk register worksheet

Scenario	Critical activity / dependency	Existing controls	L	I	Score	Additional action / owner / due

5. Climate resilience and natural hazards

Climate and natural hazards must be assessed by location and across the supply network. Evaluate chronic stresses, such as water scarcity or rising heat, as well as acute events, such as floods, storms and wildfires. Consider combined events and knock-on failures of electricity, water, telecommunications, transport and workforce access.

5.1 Assessment questions

- Which supplying sites, sub-tier sources, warehouses, ports and transport corridors are exposed?
- What credible event intensity and duration should be planned for, using recognized local hazard information and engineering assessments?
- Which utilities or infrastructure fail first, and how long can the site operate safely without them?
- Can employees safely reach the site, and can emergency services access it?
- Could protective actions, safe shutdown or restart create chemical, environmental or quality risk?
- Do alternate sites and suppliers share the same hazard zone, grid, watershed, port or feedstock source?
- Are insurance, emergency authority, landlord and community interfaces defined?

5.2 Hazard-to-action guide

Hazard	Potential continuity impact	Practical controls to consider
Flood / storm surge / intense rainfall	Inundation, electrical damage, contaminated stock, road/port closure, wastewater overflow.	Flood maps and site survey; elevate/protect critical electrical and IT/OT assets; barriers/drainage; stock relocation triggers; alternate routes/warehouses; safe shutdown and environmental controls.
Cyclone / hurricane / severe storm	Wind damage, roof loss, prolonged grid/telecom outage, workforce evacuation, port closure.	Pre-season checklist; structural inspection; secure outdoor assets; generator/fuel plan; remote command; inventory positioning; alternate ports/carriers; employee accountability.
Extreme heat	Worker heat stress, cooling failure, reduced line rate, material degradation, fire load, grid curtailment.	Heat thresholds; shift/work-rest controls; HVAC/cooling redundancy; temperature monitoring; storage limits; demand-response plan; critical spares.
Extreme cold / snow / ice	Freeze damage, brittle materials, transport closure, gas/power constraint, sprinkler impairment.	Winterization; freeze protection; alternate fuels; snow/ice access; protected inventory; cold-start and inspection procedure.
Drought / water scarcity	Restricted abstraction, poor water quality, cooling/process/cleaning constraint, wildfire conditions.	Water balance; critical-use priorities; storage/reuse; alternate supply; drought triggers; permit dialogue; low-water operating mode.
Wildfire / smoke	Evacuation, power shutoff, road closure, air-quality risk, ignition exposure.	Defensible space; air filtration; evacuation and shutdown; alternate routes; backup power; remote work; firewater assurance.
Earthquake / tsunami / volcano	Structural/equipment damage, pipeline rupture, hazardous release, port/road closure, ash contamination.	Engineering assessment and anchoring; automatic isolation; emergency supplies; alternate logistics; inspection and safe restart criteria.
Electricity shortage / grid instability	Planned curtailment, voltage/frequency variation, uncontrolled shutdown, IT/OT loss.	Critical-load study; UPS and generator coverage; fuel contracts; black-start/safe-stop tests; production prioritization; energy alerts; alternate site and inventory.
Cascading / concurrent events	Hazard plus cyber incident, utility loss, supplier failure or blocked logistics.	Scenario exercises; independent backups; geographic diversification; longer autonomy assumptions; clear decision thresholds.

Important Backup power does not automatically mean continued production. Validate safe load, starting current, fuel autonomy, emissions/permit conditions, maintenance, connection points, operator competence and routine load testing.

5.3 Example of Climate resilience worksheet

Location / dependency	Hazard and warning source	Critical threshold / lead time	Current control and autonomy	Gap / adaptation action

6. Business continuity strategies and solutions

A continuity strategy is the pre-agreed way to protect, continue or recover a critical activity within its RTO and MBCO. Strategies should be safe, legally compliant, technically feasible, funded, documented and tested—not merely listed as possibilities.

6.1 Strategy selection criteria

- Can the strategy meet the RTO and minimum capacity identified in the BIA?
- Does it introduce unacceptable EHS, quality, regulatory, cybersecurity or customer-approval risk?
- Are capacity, tooling, specifications, permits, contracts, data and competent people actually available?
- Does the alternative rely on the same site, utility, region, sub-tier source, port or IT platform?
- What is the activation lead time, cost, shelf life and ongoing readiness requirement?
- Has Solenis/customer qualification or change-control approval been considered before an emergency?

6.2 Strategy library

Area	Examples to evaluate and document
Products and inventory	Segment critical SKUs; define safety-stock logic and ownership; monitor shelf life; position inventory outside common hazard zones; agree allocation rules.
Raw materials / components	Dual or multi-source; qualify substitutions in advance; reserve capacity; monitor sub-tier risk; hold strategic stock; contract for priority and emergency transport.
Manufacturing	Alternate line/site; portable molds/tooling; toll manufacturer; reciprocal arrangement; prioritized campaign plan; manual workaround; pre-approved recipe/specification transfer.
Utilities and facilities	Generator/UPS; alternate fuel; water storage or tanker connection; redundant compressors/chillers/boilers; critical spares; temporary equipment framework; alternate warehouse/laboratory.
Quality / regulatory	Remote access to specifications and certificates; alternate laboratory; emergency change control; traceability; release authority; customer/regulator approval pathway.
Logistics	Multiple carriers and modes; alternate routes, ports and border crossings; backup 3PL/warehouse; dangerous-goods capability; emergency export/import documentation.
Workforce	Deputies and cross-training; minimum staffing; remote roles; transport/lodging; agency framework; fatigue/welfare controls; succession for licensed or specialist roles.
IT / OT / data	Segmented backup and recovery; offline/immutable copy where appropriate; tested restore; manual order/production/shipping procedures; alternate communications; secure remote access; prioritized system recovery.
Finance / suppliers	Emergency purchasing authority; alternate payment process; business interruption insurance review; supplier financial monitoring; pre-approved emergency spend.

6.3 Chemical and packaging validation examples

Chemical supplier	Packaging supplier
Demonstrate that an alternate reactor/blender has compatible materials of construction, process safety review, cleaning controls, permits, recipe/quality controls, raw-material access and waste-treatment capacity.	Demonstrate that alternate lines/sites can accept the mold/die/cylinder, meet dimensional/print/color specifications, access approved resin/paper/ink/adhesive and complete quality/customer qualification.
Validate safe shutdown and restart after loss of agitation, cooling, inerting, steam, power or effluent treatment.	Validate safe stop/restart after power, compressed air, cooling, curing or controls failure; secure artwork and tooling data.

6.4 Strategy record

Critical activity	Selected strategy	Activation trigger and lead time	Owner / resources	Test method / last result

7. Incident response, crisis management and recovery

The response plan converts analysis and strategies into coordinated action. It should be usable under pressure, available when normal systems are unavailable and integrated with emergency, EHS, cyber, disaster-recovery and site security procedures.

7.1 Activation and incident levels

Level	Example	Typical response
1 – Local	Contained event; no expected customer impact.	Local team manages; monitor and document.
2 – Significant	Capacity, delivery or dependency at risk; recovery may approach RTO.	Activate continuity team; assess Solenis impact; prepare/issue notification.
3 – Crisis	Actual or imminent material supply interruption, serious EHS/cyber/regulatory event, or multi-site impact.	Full crisis governance; executive oversight; frequent customer/authority updates; strategic allocation and recovery.

7.2 First actions checklist

- ☐ Protect life and account for people; contact emergency services where required.
- ☐ Stop or stabilize unsafe operations; contain environmental impact.
- ☐ Classify the incident, open an incident log and activate the appropriate team.
- ☐ Confirm facts, affected products/sites/orders, inventory, capacity and likely duration.
- ☐ Preserve evidence and comply with legal, regulatory, insurance and contractual notification duties.
- ☐ Activate continuity strategies and approve emergency resources.
- ☐ Notify Solenis/customer contacts when supply may be affected; establish next update time.
- ☐ Plan safe recovery, quality validation and controlled return to normal.

7.3 Recovery and return to normal

Recovery is not complete when equipment restarts. The supplier should verify EHS integrity, equipment condition, cybersecurity, utilities, raw materials, calibration, cleaning/contamination controls, permits, quality release, traceability, staffing, logistics and backlog. Define who authorizes restart and when temporary controls can be removed.

Recovery gate	Evidence / approval required	Owner / status
People, EHS and facility safe		
Equipment/utilities/IT/OT restored and verified		
Quality, regulatory and customer requirements met		
Capacity and delivery plan confirmed		
Backlog and allocation plan agreed		
Return-to-normal approved; temporary measures retired		

7.4 Incident log minimum fields

Date/time and source • confirmed facts vs assumptions • decisions and approvers • actions/owners/deadlines • affected products/orders/sites • messages issued • next update • resource commitments • risks and safety constraints • recovery forecast changes.

8. Customer and Solenis communication

Early, accurate communication gives Solenis and other customers time to protect operations, prioritize demand, adjust logistics and coordinate alternatives. Silence or unverified optimism can magnify the disruption. Communication should be factual, approved, secure and updated even when there is no material change. Use your Solenis Category Leader contact as primary and eventually copy supplerrisk@solenis.com, so the Supplier Risk Team can remain informed and support follow-up where needed.

8.1 Notification triggers

- Confirmed or reasonably foreseeable delay, allocation, reduced capacity or interruption affecting Solenis products/services.
- Loss of a critical manufacturing site, warehouse, utility, raw material, sub-tier supplier, carrier, route, port or information system.
- EHS, quality, regulatory or cyber incident that may affect product safety, integrity, legality, traceability, confidential information or delivery.
- Natural hazard or geopolitical event affecting a supplying location or critical corridor, even where impact is still being assessed.
- Material change to the previously communicated recovery date, capacity or mitigation plan.

8.2 Recommended timing and cadence

Situation	Recommended communication
Potential impact under assessment	Provide an early warning to the agreed Solenis business contact as soon as credible concern exists; state what is known, unknown and the next update time.
Confirmed material disruption	Target initial notification as soon as practicable and, where feasible, within 4 hours of confirmation. Do not delay solely to obtain complete information.
Active critical incident	Update at the agreed cadence—typically daily or more frequently if decisions are time-sensitive—until supply and recovery are stable.
Significant but stable disruption	Update at least every 48–72 hours, or as agreed, and immediately when forecasts materially change.
Recovery / closure	Confirm restored capacity, order recovery, residual constraints and final lessons/actions relevant to supply.

These timeframes are Solenis guide recommendations, not statements of ISO 22301 requirements. Contractual, legal or regulatory notice obligations may require different timing and take precedence.

8.3 Initial notification template: how you should communicate with Solenis

Required information	Supplier entry
Incident date/time, location and short factual description	
Affected Solenis products, orders, quantities, sites and lanes	
Current supply status, available inventory and capacity	
Known / potential safety, quality, regulatory or cyber impact	
Estimated duration / recovery range and confidence level	
Mitigation activated and support/decision requested from Solenis	
Supplier incident lead and communication contact	
Next update date/time and channel	

8.5 Communication controls

- Maintain current primary and backup Solenis contacts; provide a 24-hour path for critical incidents.
- Use one approved source of truth and a communication log. Separate confirmed facts from assumptions.
- Coordinate customer messages with legal, EHS, quality, cybersecurity and regulatory teams as relevant.
- Avoid disclosing exploit details, personal data or sensitive security information; use secure channels for controlled content.
- Be transparent about uncertainty. Give a range and next decision point rather than an unsupported recovery promise.
- Prepare holding statements and templates in advance; include communication in exercises

9. Training, awareness, exercises and competence

A plan is not operational until people understand their role and the underlying strategies have been tested. Training builds knowledge; exercises test decisions and coordination; technical tests demonstrate that recovery solutions work.

9.1 Recommended program and frequency

Activity	Content / objective	Recommended frequency
All employees – awareness	BCP purpose, alarms, reporting, personal safety, alternate communications and where to find instructions.	At induction and at least annually; refresh after material plan change.
BCP / crisis team	Roles, activation, decision rights, incident logging, customer communication and scenario-specific procedures.	At least annually and when role holders change.
Role-specific operators	Safe shutdown/restart, manual workarounds, generator/utility arrangements, recovery of quality/IT/OT and alternate-site transfer.	Before assignment; periodic refresher based on risk and procedure; after change.
Tabletop exercise	Facilitated scenario requiring decisions and communication without live operational interruption.	At least annually; rotate climate, utility, cyber, supplier and site-loss scenarios.
Functional / technical test	Generator under load, backup restore, alternate communication, manual order process, equipment recovery or alternate supplier activation.	At planned intervals based on criticality and manufacturer/regulatory requirements; at least annually for the most critical capabilities where safe and practicable.
Alternate site / supplier test	Demonstrate capacity, tooling/data transfer, quality and logistics—not only contractual availability.	At least every 1–2 years for critical supply, and after material change.
Full simulation	Multi-function exercise including leadership, operations, EHS, IT/OT, logistics and customer communication.	Risk-based; consider every 2–3 years for high-criticality sites or supply chains.

Frequencies are recommended baselines. Increase frequency after failed tests, major changes, incidents, high staff turnover, new hazards or where law, permits, contracts, insurers or corporate standards require more.

9.2 Exercise design

1. Choose an objective linked to a BIA priority or known risk.
2. Use a credible scenario with escalating injects and incomplete information.
3. Include off-hours activation, unavailable leaders, failed communications and at least one dependency failure.
4. Require a draft Solenis/customer notification and recovery estimate.
5. Use observers and measurable success criteria: activation time, contact success, decision quality, RTO feasibility, safety and message accuracy.
6. Record lessons, assign corrective actions and re-test significant failures.

9.3 Exercise record

Date / scenario	Scope and participants	Objectives / success criteria	Results and gaps	Action owner / due / re-test

10. BCP maintenance, review and continuous improvement

Business continuity information becomes obsolete quickly as products, people, equipment, systems, suppliers and hazards change. Maintenance keeps the plan credible and ensures lessons are converted into stronger capability.

10.1 Recommended review cycle

Item	Recommended minimum	Accountable role
Emergency contacts, call trees and Solenis/customer contacts	Every 6 months and after personnel/contact change	BCP owner / functional owners
Critical supplier, carrier, utility and contractor contacts	Every 6 months	Supply chain / procurement
BIA and recovery objectives	At least annually; after new product/site/process or major demand/customer change	Process owners / BCP owner
Risk assessment, including climate exposure	At least annually and when hazard/exposure information changes	Risk owners / EHS / site leadership
BCP procedures and continuity strategies	At least annually; after material operational or technology change	BCP owner / relevant functions
Training and tabletop exercise	At least annually	BCP owner / HR / crisis leader
Critical technical recovery tests	Risk-based planned schedule; record actual frequency and rationale	Engineering / IT/OT / operations
Management review and approval	At least annually	Executive sponsor / site leader
Post-incident / post-exercise review	Promptly after the event or test, once facts are available	Incident leader / BCP owner
Full controlled reissue	When changes are material; otherwise at least every 1–2 years	Document owner / approver

10.2 Event-driven update triggers: when it's recommended to implement improvements

- New or discontinued Solenis product; significant volume or service change.
- New, moved, closed or materially modified site, line, warehouse or laboratory.
- Change in critical raw material, packaging, process, equipment, tooling, utility, supplier, carrier, port, IT/OT system or contractor.
- Acquisition, restructuring, key-role change or major workforce change.
- New legal, regulatory, permit, customer, quality or cybersecurity requirement.
- Incident, near miss, failed exercise, audit finding or recovery strategy that did not perform as expected.
- Material change in climate/natural-hazard exposure, insurance conditions or public infrastructure reliability.

10.3 Management review inputs and outputs

Review inputs	Required outputs
BIA/risk changes; incidents and near misses; exercise/test results; audit findings; action status; supplier/customer feedback; performance against RTO/MBCO; resource adequacy; external changes.	Decisions on scope/objectives; risk acceptance; prioritized investment; approved strategies; assigned actions; training/exercise plan; communication changes; approval of next review date.

Document evidence Keep a revision history, attendance records, exercise reports, technical test results, action closure evidence and management approval. Retain records according to legal, contractual and company requirements.

11. Supplier self-assessment

Evaluate your business continuity readiness by rating each statement honestly and reference evidence. The purpose is to identify capability gaps and implement improvements to secure your production continuity —not to reward lengthy documentation.

11.1 Rating scale

Score	Maturity description
0 – Not in place	No defined approach or evidence.
1 – Initial	Informal or person-dependent; limited coverage; not tested.
2 – Defined	Documented for key areas; some gaps in implementation, evidence or testing.
3 – Implemented	Approved, communicated and operating; roles and evidence are clear.
4 – Assured	Regularly exercised/measured, integrated with change and supplier/customer needs, and improved through lessons.

#	Domain	Assessment statement	0–4	Evidence / gap reference
1	Governance	BCP scope includes sites, products and dependencies serving Solenis; an accountable owner, deputy and management sponsor are named.		
2	Governance	Activation criteria, authority, crisis roles, 24-hour contacts, document control and offline access are defined.		
3	BIA	A current BIA identifies critical products/processes, impacts over time, MTPD, RTO, MBCO and dependencies.		
4	BIA	Required recovery times have been compared with demonstrated capability; gaps are actioned.		
5	Risk	A documented risk assessment covers site, EHS, quality/regulatory, supply chain, utilities, logistics, workforce, cyber and geopolitical scenarios.		
6	Climate	Location-specific flood, storm, heat/cold, drought/water, wildfire, earthquake and electricity risks are assessed for sites and key dependencies.		
7	Strategies	Continuity solutions are selected against RTO/MBCO and validated for capacity, EHS, quality, regulatory, data, people and logistics.		
8	Sourcing	Single/sole sources and common-mode dependencies are identified; alternates, stock or other treatments are documented.		
9	Utilities	Critical loads and autonomy for electricity, water, fuel, steam, cooling, compressed air and telecommunications are understood and tested.		
10	IT/OT	Critical systems/data have prioritized recovery, protected backups, tested restore and manual workarounds.		
11	Response	The incident plan covers safety, classification, activation, logging, assessment, escalation, recovery and return-to-normal approval.		
12	Communication	Solenis/customer triggers, contacts, templates, initial notice and update cadence are defined and exercised.		
13	Training	Employees receive induction and annual awareness; crisis and role-specific personnel are competent and deputies are trained.		
14	Exercises	Contact tests, annual tabletop exercises and risk-based technical/alternate-site tests are completed with measurable objectives.		
15	Improvement	Findings have owners/dates, are tracked to closure and significant failures are re-tested.		
16	Maintenance	Contacts are checked at least semi-annually; BIA, risks, plan and management approval are reviewed at least annually and after triggers.		

11.2 Interpreting the result

Add the scores and divide by the maximum possible score to obtain a percentage. Suggested interpretation: below 40% = foundational gaps; 40–64% = developing; 65–84% = established with targeted improvements; 85–100% = mature/assured. Regardless of total score, treat any critical EHS, legal, sole-source, recovery-time or communication gap as a priority. This maturity scale is a Solenis guide recommendation, not an ISO 22301 certification result.

12. Corrective action plan, evidence and approval

Prioritize actions that reduce the likelihood or duration of interruption, improve safe recovery, or strengthen timely communication. Avoid closing actions based only on a revised document: confirm that the capability has been implemented and, where appropriate, tested.

12.1 Corrective action tracker

Gap / risk	Required action and deliverable	Priority	Owner	Due date	Status	Closure evidence / residual risk

12.2 Suggested evidence pack

Evidence area	Examples
Governance	Approved BCP/policy; scope; roles/deputies; activation matrix; controlled contact list; revision history.
Analysis	BIA; process/dependency map; risk register; climate/site hazard assessment; critical supplier and utility list.
Strategies	Inventory policy; dual-source qualification; alternate-site/tolling evidence; utility autonomy; contracts; IT/OT recovery plan; manual procedures.
Response	Incident checklist; safe shutdown/restart; crisis roster; decision/incident log; customer/Solenis templates; recovery checklist.
Assurance	Training records; call-tree results; exercise reports; generator/backup restore/alternate-site test evidence; action closure; management review.
Controlled sharing	A redacted summary, certification, test result or on-site/virtual evidence review may be used where full documents contain sensitive security information.

Document revision history

Version	Date	Summary of change	Owner / approver
1.0	September 2026	Guide Creation	Solenis Supplier Risk Management Leader

Appendix A — One-page BCP minimum content checklist

Section	Minimum content
Scope and control	Purpose, scope, sites/products, owner/deputy, approver, version, review date, secure/offline access.
BIA	Critical supply and activities; impacts; MTPD, RTO, MBCO/RPO; dependencies; actual vs required capability.
Risk	Scenario register; likelihood/impact criteria; climate and natural hazards; residual risk; owners/actions.
Strategies	Materials, inventory, manufacturing, alternate site, utilities, logistics, workforce, IT/OT, quality/regulatory and finance.
Response	Activation criteria; roles; 24-hour contacts; first actions; safe shutdown/restart; decision and incident logs.
Communication	Solenis/customer triggers, contacts, initial notification content, update cadence, templates and secure channels.
Recovery	Damage/capacity assessment; priority sequence; quality/regulatory approval; backlog/allocation; return-to-normal authority.
Training/testing	Induction and annual awareness; crisis-team training; contact tests; annual tabletop; risk-based technical and alternate-site tests.
Maintenance	Semi-annual contacts; annual BIA/risk/plan/management review; event-driven updates; lessons and tracked actions.

Appendix B — Scenario exercise prompts

Scenario	Inject
Chemical site	Flash flood closes access and damages substation; grid restoration estimate is uncertain; effluent treatment is constrained; one critical feedstock is delayed at port.
Packaging site	Ransomware disables ERP and artwork records while the primary molding/extrusion line fails; the backup plant has capacity but tooling and approval status are unclear.
Utility shortage	Grid operator announces rotating curtailment during extreme heat; generator covers safety systems but not full production; fuel deliveries are delayed.
Supplier/logistics	Single-source resin/feedstock declares force majeure; alternate source has different specification and long qualification; main port closes after a storm.
Combined event	Wildfire evacuation affects staff and telecommunications; customer demand rises because a competitor is also disrupted; crisis leader is unavailable.

Appendix C — Glossary

Term	Meaning in this guide
BCM	Business Continuity Management: coordinated activities to direct and control continuity capability.
BCP	Business Continuity Plan: documented information guiding response and recovery.
BIA	Business Impact Analysis: analysis of impacts over time and recovery priorities.
MTPD	Maximum Tolerable Period of Disruption.
RTO	Recovery Time Objective.
MBCO	Minimum Business Continuity Objective.
RPO	Recovery Point Objective for data.
IT/OT	Information Technology / Operational Technology.
Residual risk	Risk remaining after existing controls.
Common-mode dependency	An apparent alternative that can fail from the same underlying event or resource.

Appendix D — Reference framework and notes

The guide is a practical tool to help Solenis suppliers to strength business continuity management practices. Suppliers should also comply with applicable law, permits, contracts, corporate policies and local emergency requirements. Where these differ, the stricter or legally controlling requirement applies.

Reference	Use
[1] ISO 22301:2019	Security and resilience — Business continuity management systems — Requirements. International Organization for Standardization.
[2] ISO 22313:2020	Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301.
[3] ISO/TS 22317:2021	Security and resilience — Business continuity management systems — Guidelines for business impact analysis.
[4] ISO 31000:2018	Risk management — Guidelines.
[5] ISO 22301:2019/Amd 1:2024	Climate action changes amendment; organizations should determine whether climate change is a relevant issue and consider relevant interested-party requirements.
[6] Ready.gov / FEMA	Business Continuity Planning resources and business continuity plan guidance.
[7] CISA	Cybersecurity and Infrastructure Security Agency resources on resilience, incident response and cybersecurity performance goals.
[8] UNDRR	United Nations Office for Disaster Risk Reduction guidance and terminology on disaster risk and resilience.
[9] IPCC AR6	Assessment information on climate hazards, exposure, vulnerability and adaptation; use alongside local hazard and engineering information.
[10] Local authorities and utilities	Site-specific flood, storm, wildfire, earthquake, water, energy and emergency-management information.

Important interpretation notes

- ISO standards are copyrighted. This guide summarizes principles and does not replace access to the official standards.
- Recommended frequencies, maturity bands and Solenis communication timeframes in this guide are practical baselines, not ISO 22301 certification requirements.
- Risk controls must be evaluated by competent personnel. This guide does not replace process-safety, engineering, cybersecurity, legal, environmental, quality or regulatory assessment.
- Natural-hazard assumptions should use current, authoritative local data and be updated when exposure, infrastructure or climate information changes.