BUSINESS CONTINGENCY PLANNING — A SEVEN-STEP GUIDE.

Every business faces risks from different types of natural and man-made perils or loss exposures. It's important to have action plans in place for disruptions that could negatively impact your business.

Use this guide to help make business contingency plans to address potential risks that could impact your business.

Business contingency planning overview

A contingency plan includes a set of predefined tactics or actions to employ after events which result in a disruption of your business operations. The individual contingency plans for specific events which make up the program help serve as a guide to minimize the impact of an interruption and to expedite recovery and resumption of your key business activities. Having such plans allows you to better make timely and effective decisions during times of loss or crisis.

Successful business contingency planning components

Involve and consult with key employees who have a solid understanding of your business operations to participate and help make your business contingency planning successful. Your contingency plan should focus on your business structure and operations, revenue streams, internal and external dependencies, key resource requirements (personnel, inputs, facilities, equipment, technology, support utilities), and customer/market conditions.

The key components of successful business contingency planning include:

- Determine the key business operations and dependencies
- Define acceptable time and operational limitations in the event of disruption
- Document the key minimum resources required
- Conduct a risk assessment of the key operations
- Consider and select strategies to address vulnerabilities from the risk assessment
- Develop individual specific business contingency plans based on selected strategies
- Communicate and train the responsible employees

NOTE: ISO 22301 – Business Continuity Management Systems (BCMS) and ISO 31000 - Risk Management Principles & Guidelines are two international standards that provide guidance on the subject of business continuity management and risk management. This business contingency planning guide includes many of the concepts and steps outlined in those standards, and can be useful for future development of programs in accordance with those standards. However, completing the steps outlined here should not be confused with development of a comprehensive BCMS program, which includes many more elements and requirements, and is beyond the intended scope of this particular guide.

Nationwide®
is on your side

A contingency plan is preparation.

Imagine you own a dairy milking parlor and it's struck by lightning. Your contingency plan that's already in place has helped you prepare for this event. You decided to mitigate this potential loss by having a back-up generator on-site. This means you don't have to wait three or four days for a repair, your milk production is not interrupted and your income is not affected. Contingency planning pays off.

Items each specific business contingency plan should address

A specific contingency plan should identify the disruptive event, management and employee assignments, what actions will be taken, and the assets and other resources needed to initiate and expedite recovery or resumption of the business activity. It should also refer to other company emergency preparedness and response programs and procedures, maintaining the safety of employees and others at all times. Finally, any overall contingency planning should address steps for notifying your insurance carrier and the general duties and responsibilities in the event of a loss.

STEP 1 : Identify the key operations, processes and dependencies

The first step in contingency planning is to take some time and thoroughly review your operations to identify which activities and processes can be prioritized as key business activities. Any activity or process that provides a vital product or service, or that is responsible for generating significant revenue, should be considered as key. Consider your particular organization in order to further define which aspects of the operation are considered a priority.

It can often be helpful to use a flowchart to document the product and process workflow of operations, while listing the supporting activities (sales, finance, human resources, maintenance, logistics, health and safety, etc.) as having a dotted-line relationship to operations. Also, consider any dependencies of the organization as it relates to key business activities or processes. Examples might include suppliers, vendors, contractors, inspectors, or even separate offsite intra-company operations.

Proper assessment of risk and contingency planning are two of the best methods to reduce the effects of a loss and its financial damage to your business. We encourage you to start contingency planning as soon as you can.

STEP 2 : Business impact analysis

Once you have identified the key operations, processes, and any dependencies, put some thought into considering how a disruption of these activities could negatively impact your business and what would be the effects.

Business impacts can be categorized as either quantitative or qualitative. See some examples below:

- **Short-term financial**
  Loss of revenue, negative cash flow, increased costs/additional expenses
- **Long-term financial**
  Loss of key customer(s), loss of market share, lost growth opportunities
- **Operational**
  Impaired production level, degraded customer service level, loss of key suppliers, reduced employee morale, increased employee turnover
- **Regulatory/legal**
  Regulatory non-compliance, loss of license or certification, fines, penalties, breach of contract
- **Capital position**
  Degraded company value, loss of investor confidence, impaired access to funds or working capital, difficulty servicing debt obligations, noncompliance with covenants
- **Reputational**
  Negative publicity, damaged reputation, perception of mismanagement, loss of public or customer confidence, loss of customer goodwill

Select those business impacts that are most relevant or important to your organization. Then, define the criteria for each selected impact that would result in an unacceptable condition in the event of a total disruption Assume no work-arounds or recovery capabilities exist.

Next, while considering the business impacts and criteria that would constitute unacceptable conditions, determine the maximum acceptable outage (MAO) or downtime for your total operation and/or the separate business activities or processes within your operation. Also, determine the associated minimum acceptable level of production/services (often referred to as minimum business continuity objective (MBCO)) required by your business during a disruption. These values will serve as recovery objectives or benchmarks to be used during Step 4.

Throughout this process continue to ask yourself, "How can I deal with risk effectively?" as the motivation to complete the business contingency plan process.

STEP 3 : Identify critical resources

Now that you have established recovery objectives in terms of maximum downtime and minimum level of production or service to be maintained during a disruption, it is necessary to identify the critical (minimum) resources required.

Start by reviewing the key business activities and/or processes determined from Step 1. Then think about those resources and/or assets that, at a minimum, are required to support the key business activities. In addition, consider whether any of these resources can be characterized as single-points-of-failure. Some example resources include:

- Facility buildings, structures, and operations space(s) — indoors or outdoors
- Machinery and equipment
- Technology and controls equipment
- Operations inputs (feedstocks, ingredients, packaging materials and other supplies)
- Utilities (electrical and power, telecommunications, process water, process steam or other heating, refrigeration or air conditioning, gas/fuels and wastewater treatment)
- Personnel
- Vendors, contractors and outside consultants

In Step 4, you will examine how a loss of these critical resources, and the potential disruption to the associated business activities or processes they support, could impact your business and its ability to maintain operations and meet its objectives.

STEP 4 : Risk assessment

Risk assessment is the process of risk identification, risk analysis, and risk evaluation. In business contingency planning this process seeks to examine an organization's exposure to risk in terms of the loss of key business activities or processes by discovering the intersection between the resources relied upon, the threats facing these resources, and vulnerability to interruption of operations — then deciding what, if anything, to do about it.

There are many different risk assessment techniques or methods that can be employed. In the end, the questions to be answered by completing a risk assessment are the same:

- What can happen to cause a disruption?
- What are the consequences?
- What is the likelihood of occurrence?
- Are there any mitigation measures in place to reduce the probability or the severity of loss if a disruptive event occurs? Are they adequate?
- If the level of risk is not tolerable, what further treatment measure is required?

For simplicity, Nationwide recommends using a combination of brainstorming and what-if methods to conduct a risk assessment.

When identifying risks that could threaten your business, it's important to include all natural and man-made risks.

Risk identification

Risk, in the context of business continuity, is a potential incident that could have a negative impact upon an organization's ability to deliver its key products or services. Business risk typically takes the form of a loss of critical resources due to a potential threat (peril). Because one cannot identify and plan for every threat, it is also helpful to consider business risks from an "all hazards" approach, whereby risk identification is non-specific but considers that loss of critical resources could be from any unidentified threat.

While the following list doesn't capture every type of potential threat (peril), it can help to give you some examples that could be severe enough to lead to a loss of critical resources and result in a disruption.

FACILITY THREATS

- Arson
- Explosion
- Chemical leak or spill
- Collapse–structure/ equipment
- Equipment failure
- Fire
- Heating/cooling system failure
- Mechanical/electrical system failure
- On-site power disruption
- Theft
- Water/sprinkler system failure

NATURAL THREATS

- Earthquake
- Flood
- Hail storm
- Lightning
- Sinkhole
- Volcanic eruption
- Wildfire
- Windstorm/tornado/ hurricane
- Winter weather (ice and snow)

OPERATIONAL THREATS

- Civil disturbance
- Financial loss or breach
- Loss of primary supplier
- Loss of primary customer
- Off-site power disruption
- Plant contamination (food borne illness outbreak)
- Product recall
- Regulatory issue
- Riot
- Site ingress and egress disruption
- Supply chain disruption
- Terrorist attack
- Transportation logistics issue
- Vandalism

PERSONNEL THREATS

- Employee misconduct
- Employee strike
- Epidemics
- Failure to follow procedures/policies
- Loss of key personnel
- Sabotage
- Transportation/ commute problems

SOCIAL THREATS

- Bomb threats
- Domestic terrorism
- Protests
- Sabotage
- Social media protests/ issues
- Workplace violence

TECHNOLOGY THREATS

- Data corruption/loss
- Computer hacking/denial-of-service
- Hardware/software failure
- Network failure
- Phone system failure
- Computer viruses

NOTE: Not all of these threats or perils are necessarily covered by your Nationwide property insurance policy. Be sure to consult with your agent for questions or concerns regarding coverage.

Evaluate each resource analyzed to help highlight where additional risk management measures are required.

Risk analysis

Risk analysis involves estimating or determining the consequences of business risk — loss of critical (minimum) resources — and their likelihood of occurrence, all while taking into account the existence of any administrative or engineering controls, mitigation measures, or existing contingency plans and their estimated effectiveness.

For each critical (minimum) resource identified in Step 3, analyze the risk in terms of the likelihood and consequences of a total loss of each resource due to any threat. In addition, analyze and consider how well each resource is protected from potential disruption due to applicable threats identified above considering existing controls, mitigation measures, or contingency plans. Lastly, for each resource, estimate the maximum recovery time and the minimum level of production and/or service in the event of a disruption given the protection or contingency measures in place.

Risk evaluation

Given the level of tolerance for risk of your organization, in conjunction with the results of the risk analysis, determine which (if any) business risks — potential loss of critical resources — require treatment (i.e. new or additional strategies to reduce the risk to an acceptable level).

For each critical (minimum) resource analyzed, evaluate the following two questions:

1. Is the estimated maximum recovery time less than the maximum acceptable outage (MAO) determined in Step 2?
2. Is this estimated minimum level of production and/or service equal to or greater than the minimum business continuity objective (MBCO) determined in Step 2?

The answer to these questions will help to highlight where additional treatment or risk management measures are required. It may be helpful to use a risk assessment spreadsheet or other risk assessment matrix tool to aid in the analysis/evaluation, and to document the results.

Strategy identification, research and selection

Next, it is necessary to consider the various strategies that can be employed for those risks determined during the risk evaluation exercise above to require further treatment.

Treatments or risk management strategies for dealing with risk fall under four categories:

1. **Risk avoidance**
   Stop or discontinue activities that pose a risk
2. **Risk acceptance**
   Retain the risk and take no action
3. **Risk transfer**
   Transfer through purchasing insurance or other contractual means

Invite fellow employees to participate in brainstorming sessions to get ideas that may help reduce losses.

4. Risk control (mitigation):

a. Change the likelihood (loss prevention)

b. Change the consequences (loss reduction/ reduce impact)

c. Separation (different sites), segregation (same site)

d. Duplication and diversification

e. Plans for resumption of activity (contingency measures)

Brainstorm for ideas of potential strategies that might be used to reduce the risk of loss of resources requiring treatment to an acceptable level in the event of a disruption. Then conduct further research and gather information for each potential strategy regarding the options, feasibility, costs, and estimated effectiveness.

Remember the business continuity objectives:

1. Recovery within a time less than the maximum acceptable outage (MAO) and,
2. Achieve a minimum production/service level (minimum business continuity objective - MBCO) while damaged workspace or assets are repaired or replaced and eventually normal operations resume.

Once sufficient information has been gathered, review and make decisions as to the strategies that will be employed. In most cases, the strategies selected will involve either implementing changes, adding administrative or engineering controls, or developing separate formal business contingency plans to address.

STEP 5 : Develop contingency plans

Strategies requiring contingency plans need to be developed and prepared. Recall that contingency plans are the pre-defined tactics or actions to employ after events which result in a disruption of your business operations. It's about the details — these actions need to be developed and documented in writing as a part of each contingency plan. Also, if there are any existing "ad hoc" contingency plans identified during Step 4 which have not been formalized and documented, take this opportunity to do so.

Each specific contingency plan should provide and include information regarding what, when, who, where and how. The overall contingency plan program should also address steps for notifying your insurance carrier and the general duties and responsibilities in the event of a loss.

It is important here to distinguish the difference between business contingency planning, as covered by this guide, and crisis/emergency response. Most every organization should already have separate emergency action plans or emergency response plans in place to deal with the immediate actions required after an incident. Such actions include notification and reporting to authorities, evacuation and routes, procedures for employees who remain behind for critical plant operations, and procedures to be followed by employees performing rescue or medical duties. In addition, these plans should include policies and guidance regarding crisis communications — detecting incidents, alerting employees and emergency responders, dealing with the media (including social media), and communicating with stakeholders (customers, suppliers, shareholders, employee families, etc.). The primary

Developing a contingency plan is just the beginning. To be effective, employees must be notified and trained, and individual plans must be reviewed, updated and tested periodically.

purpose of these plans is to ensure personnel and public safety. The secondary purpose of these plans is to provide immediate protection of property and to limit further property damage.

Once the initial incident has been managed and the danger (if any) has subsided, then further assessment of the damages and the impact may take place, notification of your insurance carrier of any damage can occur to initiate the involvement of claims representatives, and decisions can be made about which business contingency plan(s) should be implemented and when.

STEP 6 : Communicate and train employees

Once contingency plans have been developed and documented, it is important to communicate them to those in your organization who will be required to play a part in implementing the plans. Provide training where required to ensure those responsible to initiate, lead and implement the plans have the necessary knowledge and experience.

Related to this is the need to consider how your contingency plans will be administered and controlled; in particular, protecting the confidentiality while ensuring the integrity and availability of the contingency plans.

STEP 7 : Periodic review, updating, and testing of contingency plans

Because things are constantly changing, it is necessary to periodically review the contingency plans to determine whether they will still achieve objectives, and whether the actions and information contained within the plans is still valid. Update and maintain your contingency plans where required.

Lastly, it is important to test and validate your contingency plans to evaluate the capabilities and to ensure the plans are sound, complete and effective. Be sure to conduct exercises to allow responsible team members an opportunity to practice implementing the contingency plans.

Nationwide®

1-800-260-1356 • NATIONWIDEAGRIBUSINESS.COM