A FOUR-STEP PLAN FOR BUSINESS CONTINUITY

How to develop and maintain a BC plan to mitigate the risk of business disruption

We live in an era of heightened awareness about the risks that threaten our businesses and our way of life. Extreme weather events and natural disasters dominate the news cycles. Terrorists and cyber criminals create uncertainties that cannot be ignored.

Business leaders are rightly concerned about the risks they face, but few are truly prepared to respond. Some may lack a formal business continuity (BC) plan, while others have one on a shelf that was developed years ago as a "once-and-done" project.

However, BC plans are living documents requiring regular updates to reflect changes in the business and the threat landscape. Even one created today may not stand up to a disruptive event that occurs next month. An out-of-date plan can't be trusted to orchestrate countless details in a time of crisis — when calm, rational action is essential to protect the company and restore its operations.

LEARN FROM THE EXPERIENCE OF OTHERS

How can organizations focus on BC planning and overcome the obstacles to success? Whether your business has an existing plan that needs a refresh or you are starting a plan from scratch, you can learn from the experiences of others who have taken the same journey.

Since Sungard AS has helped companies assess and manage risk for more than 40 years, we've learned a lot from the experiences of our customers and the critical success factors that are essential for a BC program. In this paper, we'll share some of knowledge we've gleaned from those experiences and outline the steps of the BC planning process we use to help our clients.

1 BUSINESS IMPACT ANALYSIS

2 RISK ASSESSMENT

3 BC STRATEGY AND PLANNING

4 EXERCISE PROGRAM

SUNGARD AVAILABILITY SERVICES®

PROGRAM GOVERNANCE

Program governance isn't a step in the BC planning process — it's an overlay that's integral to all steps. It is perhaps the single most important factor in a BC program's success.

The goal of program governance is a lofty one: to establish a commitment to preparedness that's ingrained in the organizational culture. At the center is an assigned team — chartered from the top of the organization — that develops a plan and continually reviews and updates it as the business changes and risks evolve.

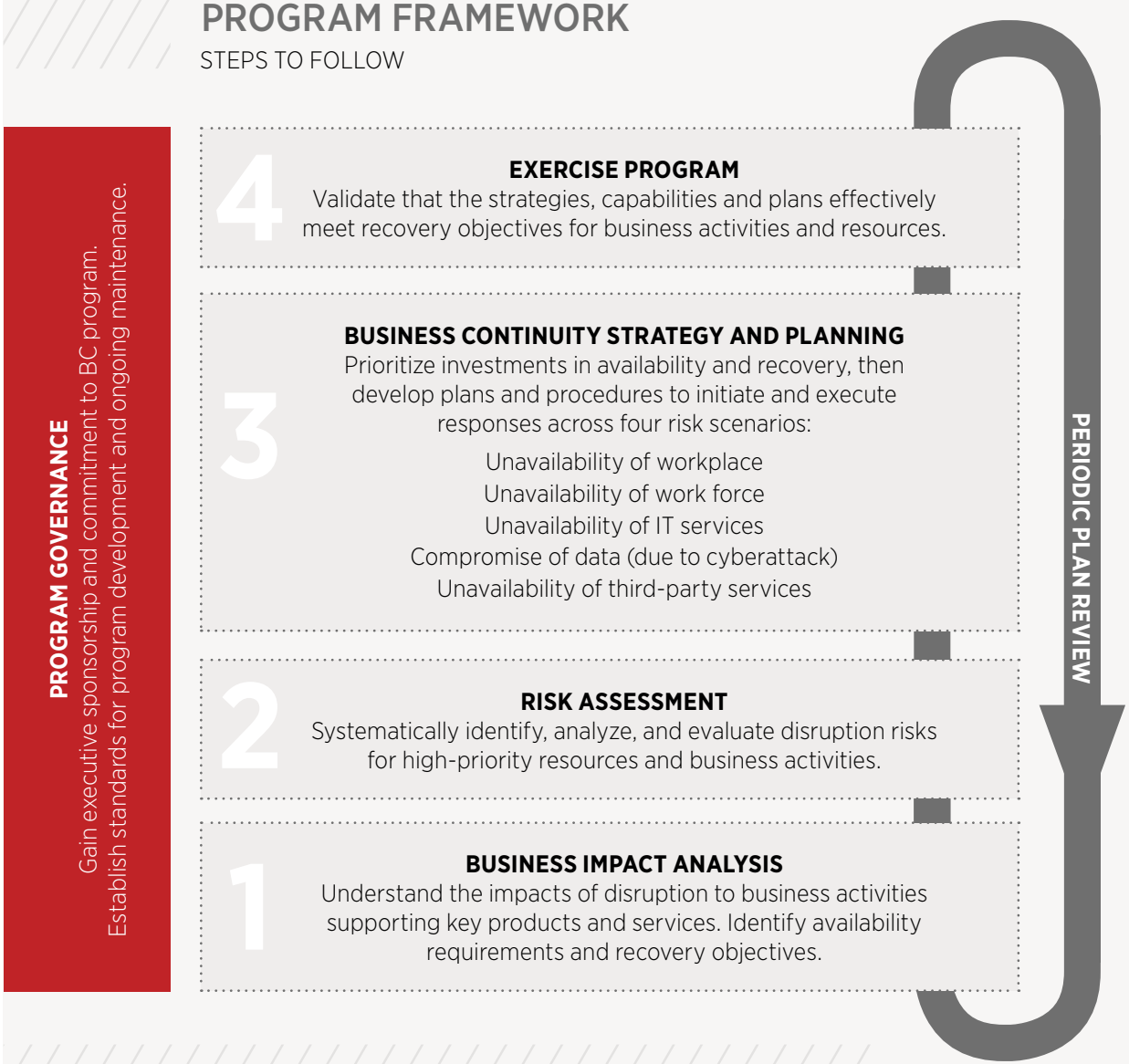
A sustainable BC program needs sponsorship and commitment from top management, guidance from an overarching business continuity strategy, and a committee that sets standards for how the program is developed, maintained and governed over time.

To assure a continued focus on BC, organizations need to assign business continuity responsibilities to a designated owner. In many companies, the responsibility goes to the CIO, given the close association between BC and IT disaster recovery. But the BC responsibility is larger than IT — it spans the entire enterprise. Therefore, the responsibility should ideally be shared with the business side of the organization, as well.

Governance is a critical success factor, because organizations put a lot of effort into developing BC programs and plans, but if they don't have a governance layer in place, the plan collapses and goes dormant over time.

BUSINESS CONTINUITY PROGRAM FRAMEWORK

STEPS TO FOLLOW



STEP 1: BUSINESS IMPACT ANALYSIS

Once governance is established, the team can start its work with a business impact analysis (BIA). The goal is to answer:

- **What are the most-critical business processes in the organization?**
- **What is the business impact if those processes aren't being performed?**

It's important to adhere to a systematic process to determine the potential operational impact of any loss or disruption to critical business functions, identify dependencies, and quantify the financial costs associated with a disaster. This will be the foundation for recovery strategies and priorities and help to determine requirements for resources and time.

STEP 2: RISK ASSESSMENT

What's most at risk? What are the threats that can cause the most harm to the business? The team should look at threats across many categories, including people, property, supply chain, IT, business reputation, and contractual obligations. The assessment will identify points of weakness and look at controls to mitigate those risks. Ultimately, the team will gain a clear picture of the risks that remain once those controls are in place.

The BIA and risk assessment set the stage for all of the detailed strategies and plans that will follow. When organizations understand both the risks and their impacts, they can establish priorities and invest their dollars to protect what's most critical to the business.

STEP 3: BC STRATEGY AND PLANNING

Planning and strategy are the heart of the BC program — developing the BC strategies that are ultimately documented in the BC plans. This is a complex undertaking and is often guided by business continuity management software tools.

The BC strategy and planning phase addresses the five key risk scenarios that need to be considered in any BC plan:

Unavailability of workplace. What happens and how will the business respond and recover if there's a loss of a workplace where normal day-to-day activities happen? Can the business shift work to an alternate location — or defer certain activities until a new work location is found? Can employees work at home until the original workplace is back in business? There are a number of scenarios that the team will need to work through for the loss of workplace scenario.

Unavailability of technology. What happens if the company's critical business applications aren't available? Even as the IT disaster recovery team addresses the loss of technology and takes care of recovery and restoration, it will take some time before those apps and data are available again. So what does the business area do while that technology is being recovered?

Unavailability of critical third parties and vendors. Many companies have critical relationships to obtain services that are central to the continued operation of the business. What happens if there are outages? Is there an alternate vendor? For manufacturers, is there inventory on hand to continue production lines for a period of time? There's an extensive list of strategies to talk through and procedures to develop to address the loss of critical third-party suppliers.

Absence of critical personnel. Company operations depend on people at all levels of the organization to fulfill the business mission. What if there is a pandemic situation, where a serious flu takes out 30% of the workforce for a prolonged period of time? What does the company do in situations like that? Companies need to document clear strategies to continue critical operations when key personnel are unavailable.

Unavailability of data. Whether data is lost because of equipment failure or human error, or compromised due to a cyberattack, organizations without a data recovery plan that can support the business recovery objectives run the risk of an extended business interruption that can negatively impact future revenues and damage its reputation, especially in the event of a ransomware attack.

STEP 4: EXERCISE PROGRAM

In the BC planning and strategy phase, the team doesn't care so much about the particular incident that causes a disruption. The focus is on impacts and recovery when an incident affects one or all of these four risk scenarios.

The exercise program is the final phase of the process, when companies conduct tests to validate that their BC strategies, plans and capabilities can meet defined objectives for recovery of business activities.

Conducting tests proves that the plans will work, and ensures that every member of the organization knows their roles and responsibilities during a disruptive incident. There are many different types of tests and exercises, from simple call tree notification tests to more elaborate exercises that include relocating personnel to alternate locations.

Plan to Be a Resilient Business

When companies move ahead with a business continuity plan and conduct their first business impact analysis, they often discover that the cost of business interruption is far higher than they expected. That cost becomes a major motivating factor to proceed with BC planning and to maintain the plan with diligence.

In some industries, the impetus for BC planning comes from the government. In financial services and in healthcare, for example, companies must prove to regulators that they have fully documented and tested plans for BC, to ensure that critical institutions can continue to operate following a disruptive event.

Some regulations are based on published international standards, including the ISO 22301 standard and others in that series. Sungard AS uses these standards to guide its BC consulting engagements for clients, to ensure the resulting plans meet compliance requirements and reflect best practices.

Increasingly, potential clients are requesting BC plan details before signing agreements with other companies. For example, manufacturers need assurances that their suppliers of critical components can provide an uninterrupted flow to their production line. Further, all companies want to know that their software-as-a-service cloud suppliers can continue to provide access to critical applications.

Best practices and standards for BC set a base framework for BC programs and plans. These documents are valuable to tell businesses what they should be considering. But they are not prescriptive — they don't explain how to build a program. That's an area where Sungard AS can bring its experience to the table with consulting, software tools, and proven methodologies. Our experts can guide and advise — or they can provide the top-to-bottom BC management services you need to be a resilient business.

GETTING STARTED

Sometimes daily business demands can keep you from building and maintaining a BC program, even when you know how essential it is. Take the opportunity to get your plan started with a **Business Continuity Management Program Assessment** from Sungard AS.

In this brief engagement, our consultants work closely with you to determine your BC readiness and lay out the priorities for moving forward. We tailor the assessment to meet the unique risk tolerance and needs of your organization, applying proven best practices and international standards to assure compliance with industry-specific regulations. **Get started today**.

www.sungardas.com

If you are calling from
North America contact us at:
+1 (866) 714-7209

If you are calling from
EMEA contact us at:
+44 (0) 808 238 8080

About Sungard Availability Services
Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

SUNGARD
AVAILABILITY
SERVICES®