



What is BCDR? Business continuity and disaster recovery guide

March 2023

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

Downtime can do serious damage to an organization's bottom line and reputation. Business continuity and disaster recovery -- two closely related practices -- help keep an organization running even in the wake of disaster. This guide explains how BCDR works, why you need it and how to build a BCDR plan for your organization to protect it today and into the future.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

What is BCDR? Business continuity and disaster recovery guide

JOHN MOORE, INDUSTRY EDITOR

Business continuity (BC) and disaster recovery (DR) are closely related practices that support an organization's ability to remain operational after an adverse event.

Resiliency has become the watchword for organizations facing an array of threats, from natural disasters to the latest round of cyber attacks.

In this climate, [business continuity](#) and [disaster recovery](#) (BCDR) has a higher profile than ever before. Every organization, from small operations to the largest enterprises, is increasingly dependent on digital technologies to generate revenue, provide services and support customers who always expect applications and data to be available.

"Mission-critical data has no time for downtime," said Christophe Bertrand, practice director of data management and analytics at Enterprise Strategy Group (ESG), a division of TechTarget. "Even for noncritical data, people have very little tolerance."

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

More than two-thirds of respondents to Uptime Institute's 2021 Global Data Center Survey had some sort of outage in the past three years. And disruption isn't just an inconvenience for customers.

"[W]hen an outage occurs, about a fifth are classified as severe or serious, meaning there were big financial, reputational and other consequences," according to Uptime Institute, a Seattle-based data center standards organization.

WHY IS BCDR IMPORTANT?

The role of BCDR is to minimize the effects of outages and disruptions on business operations. BCDR practices enable an organization to get back on its feet after problems occur, reduce the risk of data loss and reputational harm, and improve operations while decreasing the chance of emergencies.

Some businesses might have a head start on BCDR. DR is an established function in many IT departments with respect to individual systems. However, BCDR is broader than IT, encompassing a range of considerations -- including crisis management, employee safety and alternative work locations.

A holistic BCDR approach requires thorough planning and preparation. BCDR professionals can help an organization create a strategy for achieving resiliency. Developing such a

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

strategy is a complex process that involves conducting a [business impact analysis](#) (BIA) and risk analysis as well as developing BCDR plans, tests, exercises and training.

Planning documents -- the cornerstone of an effective BCDR strategy -- also help with resource management, providing information such as employee contact lists, emergency contact lists, vendor lists, instructions for performing tests, equipment lists, and technical diagrams of systems and networks.

BCDR expert and consultant Paul Kirvan noted several other reasons for the importance of BCDR planning:

- Results of the BIA identify opportunities for process improvement and ways the organization can use technology better.
- Information in the plan serves as an alternate source of documentation.
- The plan provides a single source of key contact information.
- The plan serves as a reference document for use in product planning and design, service design and delivery, and other activities.

An organization should strive for continual improvement, driven by the BCDR process.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)



In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

WHAT IS BUSINESS CONTINUITY AND DISASTER RECOVERY?

An organization's ability to remain operational after an incident relies on both BC and DR procedures. The goal of BCDR is to limit risk and get an organization running as close to normal as possible after an unexpected interruption. These practices also reduce the risk of data loss and decrease the chance of emergencies, which helps maintain and even improve the organization's reputation.

The trend of combining business continuity and disaster recovery into a single term, BCDR, is the result of a growing recognition that business and technology executives need to collaborate closely when planning for incident responses instead of developing schemes in isolation.

WHAT'S THE DIFFERENCE BETWEEN BUSINESS CONTINUITY AND DISASTER RECOVERY?

BC is more proactive and generally refers to the processes and procedures an organization must implement to ensure that mission-critical functions can continue during and after a disaster. This area involves more comprehensive planning geared toward long-term challenges to an organization's success.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

DR is more reactive and comprises specific steps an organization must take to resume operations following an incident. Disaster recovery actions take place after the incident, and response times can range from seconds to days.

BC typically focuses on the organization, whereas DR zeroes in on the technology infrastructure. Disaster recovery is a piece of business continuity planning and concentrates on accessing data easily following a disaster. BC includes this element but also considers risk management and any other planning an organization needs to stay afloat during an event.

There are similarities between business continuity and disaster recovery. They both consider various unplanned events, from cyber attacks to human error to a natural disaster. They also have the goal of getting the business running as close to normal as possible, especially concerning mission-critical applications. In many cases, the same team is involved with both BC and DR.

WHAT'S THE DIFFERENCE BETWEEN BUSINESS RESILIENCE AND BUSINESS CONTINUITY?

[*Business resilience*](#) and *resiliency* began appearing in the BCDR vocabulary in the early 2000s. Resilience, at times, has been used interchangeably with business continuity, but the [terms have different shades of meaning](#).

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

Kirvan said a resilient business can return to its previous operational state following an event that shut it down. Business continuity management, technology disaster recovery and incident response are among the disciplines that fuel an organization's resiliency.

Resilience focuses on building a business to be impervious to potential disruptions of various kinds, according to Jeff Ton, strategic IT advisor at InterVision Systems, an IT service provider with regional headquarters in San Jose, Calif., and Chesterfield, Mo. Business continuity, in contrast, involves resuming operations from an outage once it has occurred, Ton noted.

Resiliency "is more about being able to resist and withstand issues, and business continuity is about being able to continue business after something has disrupted your business," Ton said.

Using a rubber band analogy, Ton said an event might stretch an organization; but, if resiliency has been achieved, it resists and reassumes its shape. Business continuity kicks in when the rubber band snaps and the organization takes steps to address the breakage, he added.

ESG's Bertrand said business continuity revolves around the ability to fail over and maintain systems at a high level of availability, while resilience is the ability to resist disruption and prevent problems from happening in the first place.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

WHAT'S THE DIFFERENCE BETWEEN ORGANIZATIONAL RESILIENCE AND OPERATIONAL RESILIENCE?

The idea of resilience and its role in business continuance has also diversified into the concepts of organizational and operational resilience.

[Organizational resilience](#) (OR) is the ability of the entire organization to guard against disruptive events. The entire organization includes all personnel in every department or business unit; the applications, infrastructure and other technologies across the enterprise; facilities, including buildings and workspaces; and the processes and policies involved in running the organization.

In order for OR to be fully realized, every element of the organization must be protected from adverse events and demonstrate the capability to change and adapt -- even just temporarily -- to continue running the business until the disruption is alleviated and normal operations are restored.

[Operational resilience](#) (OpR) is generally regarded as a close subset of organizational resilience, but OpR focuses on the people, processes and infrastructure of the business to respond and adapt to changing patterns. It's worth noting that this description isn't solely about BCDR but can apply to any issues or situations that affect business conditions.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

Where OR takes a more holistic view of resilience, OpR slants the view in favor of resilience issues involved in running the business day to day. There are several standards that relate to OpR, including international standard ISO 22316:2017 and British standard BS 65000:2014.

OR and OpR require careful attention to prediction and planning so potential disruptions are identified and prepared for in advance. Disruptions that aren't considered or planned for can overcome an organization's resilience posture and cause major, long-lasting business impacts.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

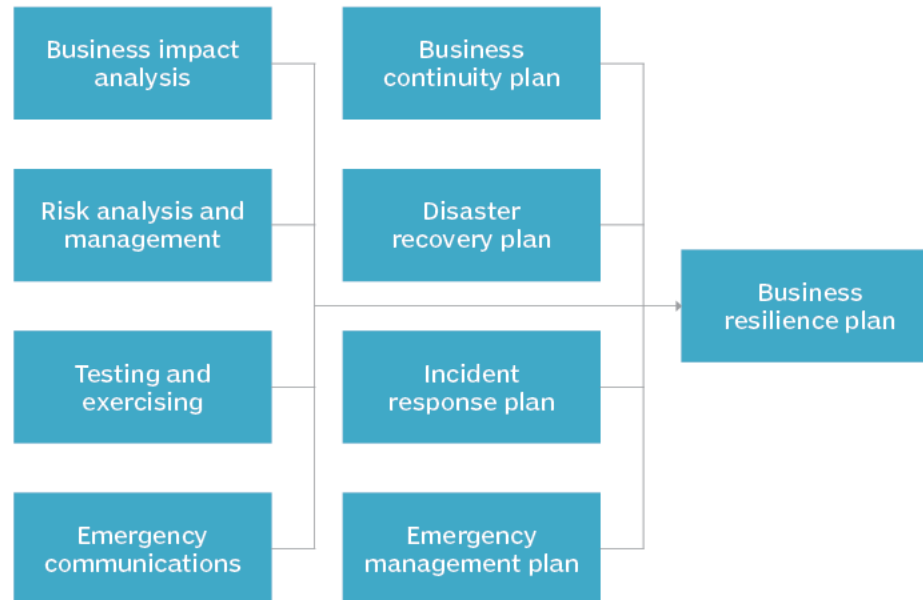
[Standards, templates, software and services](#)


[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

What encompasses a business resilience plan?



©2020 TECHTARGET. ALL RIGHTS RESERVED 

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

THE ROLE OF RISK ANALYSIS, BIA AND BCDR STRATEGIES

Risk analysis and BIA are critical tools for organizations facing the question of how to build a BCDR strategy.

[Determining internal and external risks](#) is important to the BCDR process. The risk analysis identifies risks and the likelihood they will occur. This risk assessment works in tandem with the BIA, which helps quantify the potential effects of disruption. Financial analysis is one aspect of a BIA, but this exercise also considers the non-financial costs of unplanned outages. In addition, the [BIA identifies the mission-critical functions](#) an organization must maintain or restore following an incident, and the resources needed to support those functions.

It's important to gain management support when pursuing a BIA, given the intensity of the process. The BIA provides a way for an organization to learn about itself and details opportunities for improvement.

An organization uses risk analysis and BIA data to determine business continuity and disaster recovery strategies and the appropriate responses. Each strategy is turned into a series of actions that will help achieve operational recovery, such as data replication, [failing over to a cloud-based service](#), activating alternate network routes and working remotely.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

WHY SHOULD YOU USE BCDR, AND WHEN SHOULD IT BE ACTIVATED?

Motivations for an organization developing a BCDR strategy might include protecting the lives and safety of employees, ensuring the availability of services to customers and protecting revenue streams. Competitive positioning and reputational management are factors that often underlie other motivators: A business perceived as unable to protect employees or deliver services will struggle to attract workers and customers.

The regulatory and compliance environment also influences organizations in their pursuit of BCDR. The HIPAA Security Rule, for example, [requires](#) covered entities such as hospitals to provide an emergency mode operation plan, which includes "procedures to enable continuation of critical business processes for protection of the security of electronic protected health information."

The Financial Industry Regulatory Authority (FINRA), an organization that oversees broker-dealers, requires firms to "create and maintain written business continuity plans" that address emergencies or disruptions to the business. FINRA spells out its required business continuity measures in its emergency preparedness rule.

U.S. federal agencies, meanwhile, are also required to develop BCDR strategies, which in government terminology are called *continuity of operations plans*. The aim is to "ensure that essential government services are available in emergencies -- such as terrorist attacks,

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

severe weather, or building-level emergencies," according to the Government Accountability Office.

Customers might also put pressure on businesses to develop adequate BCDR plans. An assessment of an organization's BCDR stance might be part of a prospective client's vetting process. Federal regulators, such as the Office of the Comptroller of the Currency, encourage banks to include resilience as part of the vendor due diligence process. Specifically, OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," [states](#) that banks should "determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data."

The "why" of BCDR potentially has many answers, and the "when" of business continuity and disaster recovery is similarly nuanced. Organizations must weigh several factors before declaring a disaster and triggering the BCDR plan. Chief among those are the expected duration of the outage, the outage's effects on the organization, the financial cost of activating the BCDR plan and the BCDR plan's potential for causing disruption. Paradoxically, the process of failing over from an organization's primary place of business to a backup facility -- and then failing back after an event -- might significantly interrupt operations, noted Paul Thomann, regional principal for cloud and data center transformation at Insight Enterprises Inc., an IT services provider based in Tempe, Ariz.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

Accordingly, an organization's leadership must carefully size up when to enact the BCDR plan. Migrating to a backup facility, Thomann said, "comes with an impact to the budget." An organization, for instance, might deem a six-hour outage not significant enough to make the disaster call.

That decision, particularly in larger enterprises, is typically made by a committee rather than an individual executive, Thomann said. The committee might consist of the CEO, CFO, CIO and other C-suite executives, he added.

HOW TO BUILD A BCDR PLAN

Organizations can break down a BCDR plan into BC and DR components.

Specifically, according to BCDR consultant Kirvan, a business continuity plan ([BCP](#)) contains contact information, change management procedures, guidelines on how and when to use the plan, step-by-step procedures and a schedule for reviewing, testing and updating. A disaster recovery plan ([DRP](#)) features a summary of key action steps and contact information, the defined responsibilities of the DR team, guidelines for when to use the plan, the DR policy statement, plan goals, incident response and recovery steps, authentication tools, geographical risks and plan history. The DRP should also take staffing into account,

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

ensuring that personnel able to execute the various steps of a DR plan are always available to enact critical recovery tasks.

Good business continuity and disaster recovery plans are clear about the varying levels of risks to the organization; provide well-defined and actionable steps for resilience and recovery; protect the organization's employees, facilities and brand; include a communications plan; and are comprehensive in detailing actions from beginning to end.

A BCDR policy is an important initial step. The policy sets the foundation for the process and typically covers the scope of the business continuity management system, which employees are responsible for it and the activities performed, such as plan development and BIA. A policy might also establish a common set of metrics, such as key performance indicators and key risk indicators. The policy aspect is often overlooked, but it's an important business continuity auditing item.

[Developing the BCP](#) and DRP typically starts by gathering BCDR team members and performing a risk analysis and BIA. The organization identifies the most critical aspects of the business, and how quickly and to what extent they must be running after an incident. After the organization writes the step-by-step procedures, the documents should be consistently tested, reviewed and updated.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

Although certain aspects of the process involve select members of the organization, it's important that everyone understand the plan and is included at some point. The plan should also encompass third parties and the services they provide. A bank, for example, might rely on data that a third-party firm supplies, so the relationship should be documented in the BCDR plan. Such outside entities must be kept in the loop so they understand how the plan is going to work.

Other steps in a [BCDR planning checklist](#) include risk mitigation and an emergency communications plan. The latter details the method, or methods, an organization will use to disseminate information on an emergency to employees.

In summary, the process of building a BCDR plan will typically involve the following activities:

- risk identification
- infrastructure review
- BIA
- plan design
- plan implementation
- testing

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

BCDR TESTING

Testing a business continuity and disaster recovery plan provides assurance that the recovery procedures put in place will work as expected to preserve business operations. The testing phase might also highlight areas for improvement, which the organization can address and incorporate into the next version of the plan.

Tests can range from simple to complex. A discussion-based tabletop exercise brings together participants to walk through the plan steps. This type of test helps employees with BCDR roles become more familiar with the response process, while letting administrators assess the effectiveness of the BCDR plan.

On the other end of the testing spectrum, a full-scale test simulation calls for participants to perform their BCDR functions rather than discussing them in a tabletop exercise. These drills might involve the use of backup systems and recovery sites.

Still, testing requires time, funding, management support and employee participation. The testing process also includes pre-test planning, training test participants and reporting on the test.

The frequency of testing varies by organization. Larger enterprises should conduct tabletop exercises at least quarterly, while smaller organizations can test less often, Insight

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

Enterprises' Thomann said. A full BCDR test, which is more time- and resource-intensive, can be conducted annually, he added.

InterVision's Ton also recommended a quarterly testing schedule, with a DR test conducted twice a year with tabletop exercises in between those tests. Business continuity, as a separate test, can be conducted annually. Ton said he's found it more effective to separate the tests because conducting the DR test on its own is less disruptive to the organization.

Periodic testing, plan maintenance and resilience are interrelated. An organization improves its resilience when it updates its BC and DR plans and then tests them continually.

BCDR COST MANAGEMENT

Changes in the threat landscape or new business ventures might compel an organization to expand its BCDR coverage. That change in scope could call for spending on consulting services or backup and disaster recovery technologies.

BCDR managers might need to seek new funding for the expanded BCDR plan and resilience technologies if the dollars aren't available in the current budget.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

An investment proposal should be built on a business case that emphasizes the positive results the new BCDR capabilities will provide for the organization. The bid for funding should also determine whether the revised BCDR plan will affect other areas, such as cybersecurity. Other steps toward obtaining funding include vetting products and services that support the expanded requirements and preparing a procurement request with enough documentation, according to BCDR consultant Kirvan.

Ton said organizations should strike a balance between the level of investment in BCDR approaches and the anticipated financial effects of a given disaster scenario. "You don't want to come up with a solution that costs 200 times more than the disaster would have," he said.

Asking business leaders from various corporate disciplines to estimate the expected costs associated with different types of events can help organizations establish a baseline from which they can make informed BCDR investment decisions.

STANDARDS, TEMPLATES, SOFTWARE AND SERVICES FOR BCDR PLANNING

Organizations embarking on a business continuity and disaster recovery planning process have numerous resources to draw upon. Those include standards, tools ranging from templates to software products, and advisory services.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

"To build a plan, you have many templates that exist and many best practices and many consultants," ESG's Bertrand said. "There's no reason not to have a strong DR plan."

BCDR STANDARDS

Government and private sector standards bodies, including the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), have published BCDR guidelines. The standards, which cover topics from crisis management to risk assessment, provide frameworks on which businesses can build their BCDR plans.

The following is a sampling of standards:

- ISO 22301:2019 Security and resilience -- Business continuity management systems -- Requirements
- ISO 22313:2012 Societal security -- Business continuity management systems -- Guidance
- ISO 22320:2018 Security and resilience -- Emergency management -- Guidelines for incident management
- ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- ISO 31000:2018 Risk management -- Guidelines
- ISO Guide 73:2009 Risk management -- Vocabulary
- IEC 31010:2019 Risk management -- Risk assessment techniques

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

- ISO/TS 22317:2021 Security and resilience -- Business continuity management systems -- Guidelines for business impact analysis
- FINRA Rule 4370. Business Continuity Plans and Emergency Contact Information
- National Fire Protection Association 1600: Standard on Continuity, Emergency, and Crisis Management (new consolidated draft pending)
- NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems
- American National Standards Institute/ASIS ORM.1.201 Security and Resilience in Organizations and Their Supply Chains

BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN TEMPLATES

Templates provide preset forms that organizations can fill out to create BCDR planning documents. Some templates cover the BCDR plan as a whole or address particular aspects of the BCDR planning.

This [general BCP](#), for example, includes provisions for natural disasters, fires, network service provider outages and floods or other water damage. A planning template can also assist SMBs, which could simplify the process, depending on organization's size and complexity.

A BCDR plan might call for a service-level agreement (SLA), which sets standards for the quality of an organization's BCDR recovery program. It can also help ensure services

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

obtained through third parties, such as DR hot sites, perform at acceptable levels. Kirvan created a template that addresses [SLAs for BCDR programs](#).

As noted above, conducting a BIA can help organizations with business continuity planning. This [BIA report template](#) provides a mechanism for documenting parent processes, subprocesses and the financial and operational effects in the event of an interruption.

Organizations can also benefit from [scheduling BCDR activities](#) for the ongoing care and maintenance of business continuity strategy. Activities range from scheduling a BIA to reviewing a technology disaster recovery plan.

BCDR SOFTWARE

Specialized BCDR software provides another tool for organizations ready to build a plan. BCDR products, sometimes referred to as [business continuity software](#) or business continuity management software, aim to help organizations build business continuity and disaster recovery plans. They typically cover a range of planning activities, such as BIA and risk assessment, and offer incident response capabilities.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

BCDR vendors, products and services

Business continuity services	Business continuity firms	Approaches	BCDR software	DR vendors
<ul style="list-style-type: none">Plan developmentBusiness impact analysis preparationAuditingRisk analysisPlan exercise preparationConsultingTechnical and advisory servicesAssessmentsPolicy and procedureDevelopmentInterviewingAdministrative activitiesData gatheringDocumentation	<ul style="list-style-type: none">Big four accounting firmsBoutique consulting firmsAuditing firmsBCDR consultanciesAdvisory firmsSoftware firms	<ul style="list-style-type: none">Different BC services/firms and BCDR toolsBC services partnered with a specific DR managed service provider (MSP)BC planning in-house and cloud services for DRBC MSP and DR as a service	<ul style="list-style-type: none">Data backupSystem backupRemote storage	<ul style="list-style-type: none">On-premises vendorsCloud service providersDR as a serviceHybrid mixMSPsTechnology firms




ILLUSTRATION: LA NIKOGAL/ADOBE STOCK, CRYSTAL/GETTY IMAGES

©2020 TECHTARGET. ALL RIGHTS RESERVED 

Vendors in the market include Castellan Solutions, Continuity Logic, Dell Technologies, eBRP Solutions Network, Fusion Risk Management and SAI Global.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

BCDR PLANNING SERVICES

Another option is to outsource the organization's BCDR needs to a third-party firm that can provide risk analysis, plan development and maintenance, and training. It's incumbent upon the business to analyze its needs before selecting a BCDR firm, nailing down such information as what it wants to outsource, what services it expects of the vendor, the risks of an outsourcing agreement and how much it plans to spend.

Potential sources of planning support include accounting firms, which can perform BIAs as part of the business continuity planning process. Accounting firms should typically be able to help clients determine the cost of workload outages, but buyers should ideally select a firm with experience in business continuity or IT resource planning, according to technology writer and former CIO Brien Posey. Consulting firms can also help with BCDR planning, Posey added.

Managed service providers (MSPs) often serve as virtual CIOs for their SMB customers. In that role, MSPs can help with planning. Because their business is to manage a customer's IT assets, they are able to develop a plan for dealing with technology outages.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

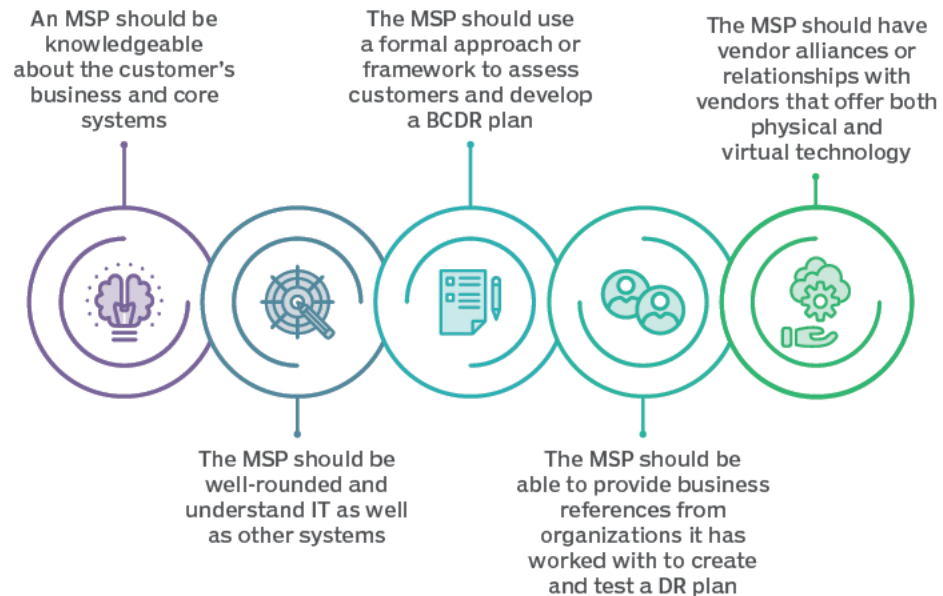
[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

5 considerations for selecting an MSP to create a BCDR plan



ICONS: PRESSURICIA/GETTY IMAGES, ALEXDNDZ/ADOBE STOCK

©2020 TECHTARGET. ALL RIGHTS RESERVED 

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

SUPPORTING TECHNOLOGIES AND STRATEGIES

The technology options for executing the DR portion of a BCDR plan have expanded in recent years due to the advent of cloud computing. Traditionally, organizations built or hired out an off-site facility to handle their disaster recovery needs. Such disaster recovery sites require a duplication of in-house production systems, so they could prove out of the financial reach of many SMBs. However, cloud-based offerings such as [disaster recovery as a service](#) have made DR more accessible for smaller organizations.

Other resilience offerings include emergency notification systems, cybersecurity systems and incident response systems, which might be included in business continuity management products. Organizations might also tap work area recovery vendors that provide alternative work locations for employees.

BCDR MANAGEMENT

The team that builds, manages and -- in the event of a disaster -- executes a BCDR plan should be cross-functional, drawing upon multiple stakeholders and pockets of expertise across the organization.

The team's leadership varies somewhat by organization. In a large enterprise, for example, the risk management officer often chairs the BCDR team with a representative from the IT

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

department as a vice chair, InterVision's Ton said. Smaller organizations lacking a risk management department might appoint the CFO to lead the team, he noted. And, in some cases, the IT department head might direct the BCDR team.

Other members of the team typically include representatives from the organization's key business functions: finance and accounting, facilities, legal -- including in-house and outside counsel -- marketing and public relations, for example.

The task of pulling multiple stakeholders together to develop a BCDR plan -- and conducting the necessary impact and risk analyses -- can prove challenging. Project management thus becomes an important consideration. Organizations should think about appointing a project manager to shepherd the process of building a BCDR plan, Ton noted.

The BCDR team should also take on the task of ongoing business continuity management, making sure plans are up to date. Business initiatives and data center technologies change frequently, so BCDR plans will need regular maintenance to stay on point. As a first step, an organization should assess if the current plan can be updated or whether an entirely new plan is in order, according to George Crump, president of Storage Switzerland, an IT analyst firm. Organizations should conduct BCDR testing to determine the extent to which a plan needs to be overhauled.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

In addition to testing, a BCDR team might also want to consider a [business continuity plan audit](#), which assesses the effectiveness of a plan. The audit should detail the risks that could threaten the plan's success and test the controls currently in place to determine whether those risks are acceptable to the organization. An [IT General Controls audit](#) can also be used to assess risks to the infrastructure and identify areas for improvement, according to BCDR consultant Kirvan.

The various roles and responsibilities of BCDR team members, from planning to testing, can be detailed in an organization's [business continuity policy](#). Such a policy might also encompass external personnel, such as vendors and customers.

Another aspect of BCDR team building is getting individuals up to speed on BCDR best practices. To that end, BCDR team members can avail themselves of business continuity training and certification programs.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

5 things you need for a business continuity plan audit

- 1 Your audit team.** This can be internal staff or an external audit firm. Objectivity and familiarity with the business continuity process among the team members can help ensure accurate results.
- 2 Documentation.** Business impact analyses, risk assessments and established business continuity/disaster recovery/incident response plans provide integral audit information.
- 3 Guidance.** Standards and general industry best practices can guide your audit to ensure that all of your bases are covered and your business continuity plan meets all the requirements for your field.
- 4 Interviews.** Conducting interviews with staff familiar with the business continuity process can add significant insight to an audit.
- 5 Actionable results.** Once your audit is complete, your findings should provide you with the next steps for improving your business continuity plan and getting ready for your next audit.



ILLUSTRATION: MACROVECTOR/ADOBE STOCK

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

The Business Continuity Institute, a global professional organization, offers its Certificate of the Business Continuity Institute, which covers business continuity management process and practices. The institute also offers a Business Continuity Management BCI Diploma for individuals looking for additional insight into business continuity management.

The BCM Institute, meanwhile, offers its Business Continuity Certified Planner (BCCP) accreditation. The BCCP certification aims to recognize a business continuity professional's understanding of core business continuity management concepts.

Other organizations granting [professional business continuity certifications](#) include DRI International, the National Institute for Business Continuity Management and the International Consortium for Organizational Resilience. Such certification bodies usually work with an internal or external training group that prepares students to sit for exams, Kirvan noted.

Conferences also provide an opportunity to educate BCDR team members. Ton cited DRI and *Disaster Recovery Journal* events as helpful for people looking to learn more about business continuity.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

BCDR PITFALLS: MIND THE GAP

Change is perhaps a BCDR plan's key nemesis. As the pace of technology change accelerates, organizations are left updating IT equipment -- from storage and servers to networks and their associated devices. Some IT assets are moving to the cloud. A 5-year-old BCDR plan is unlikely to reflect -- and prove adequate to protect -- the current IT estate.

An organization's change management process can help address this issue. Change management oversees adjustments to systems, networks, infrastructure and documents. It addresses similar situations as BCDR planning and testing, so an organization might decide to include business continuity and disaster recovery in the change management process.

The change management process contains six major activities, according to Kirvan:

1. identify a potential change;
2. analyze the change request;
3. evaluate the change;
4. plan the change;
5. implement the change; and
6. review and close out the change process.

An organization, of course, is also subject to change. Organizations make acquisitions, divest non-core operations and create new lines of business, for example. An effective BCDR plan

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

must be periodically updated to account for those developments. Regularly scheduled BCDR testing can expose gaps in the plan where it has failed to account for technology or business changes.

Perceptual gaps can also undercut BCDR plans. ESG's Bertrand said many organizations adopting SaaS offerings have a false sense of security regarding data protection. A third of the respondents to an ESG survey said SaaS apps, such as Microsoft 365 and Salesforce, don't need to be backed up. Bertrand said that's simply not the case. He cited the example of recovering email an organization's users have sent to the trash bin. He said Office 365, depending on the customer's subscription level, retains deleted email for a limited time.

"SaaS application resilience is being conflated with SaaS data availability," Bertrand said. "SaaS-based applications are not being properly protected today."

Organizations using such cloud-based applications should become acquainted with their vendors' data protection and recovery SLAs and make sure BCDR plans cover SaaS applications and their availability requirements. Bertrand said the percentage of people who are aware of SaaS vendors' SLAs is improving, but not everyone is up to speed. He said 58% of ESG survey respondents said they were familiar with SaaS vendors' data protection and recovery provisions.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

An organization can use a BCDR checklist -- or a series of checklists -- covering plans, policies and recovery strategies to root out potential problems and flag BCDR weak points. BCDR teams should also stay abreast of the changing threat landscape to make sure their plans reflect emerging threats. [Business continuity risks that organizations should monitor](#) range from evolving cybersecurity attacks to active shooter incidents.

THE FUTURE OF BCDR

BCDR planning and execution will continue to evolve with the changing nature of threats. Below are a few developments to consider.

The confluence of cybersecurity and business continuity. The role of cyber attacks, such as ransomware, in disrupting business operations appears set to continue -- if not accelerate. Cybersecurity and business continuity are typically separate and distinct functions in an organization. Kirvan, speaking on the future of business continuity, said he believes those disciplines "ought to be under the same roof."

Going back to the future with tape storage. Backup files might be encrypted in a ransomware attack. Organizations, however, can isolate the files they need for recovery from the corporate network, creating an air gap. That's where time-testing tape storage comes into play. Bertrand said tape storage is reemerging as a way for organizations to

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)

preserve a "gold copy" of their data, offline and off site. "It's coming back," he said of the backup method.

AI's influence on BCDR planning. AI and its cognitive functions might help BCDR teams make decisions on organizing their plans and might also play a role in conducting BIAs and risk assessments, according to Kirvan. AI could also support incident response, recommending actions based on the details of unfolding disaster scenarios.

Service providers play a bigger BCDR role. A large percentage of MSPs are involved in backup and disaster recovery. The MSP sector is likely to emerge as a one-stop shop for business continuity services, particularly for SMBs lacking internal expertise. MSPs, in their trusted advisor role, can advise clients on BCDR planning and make technology recommendations. Some provide their own disaster recovery as a service, while others partner with vendors that provide that tool.

In this guide:

[Why is BCDR important?](#)

[What is BCDR?](#)

[The role of risk analysis, BIA and BCDR strategies](#)

[Why you should use BCDR](#)

[How to build a BCDR plan](#)

[BCDR testing](#)

[BCDR cost management](#)

[Standards, templates, software and services](#)

[BCDR management](#)

[BCDR pitfalls](#)

[The future of BCDR](#)



CONTINUED READING

[Business resilience vs. business continuity: Key differences](#)

[A free business continuity plan template and guide](#)

[Preparing an annual schedule of business continuity activities](#)