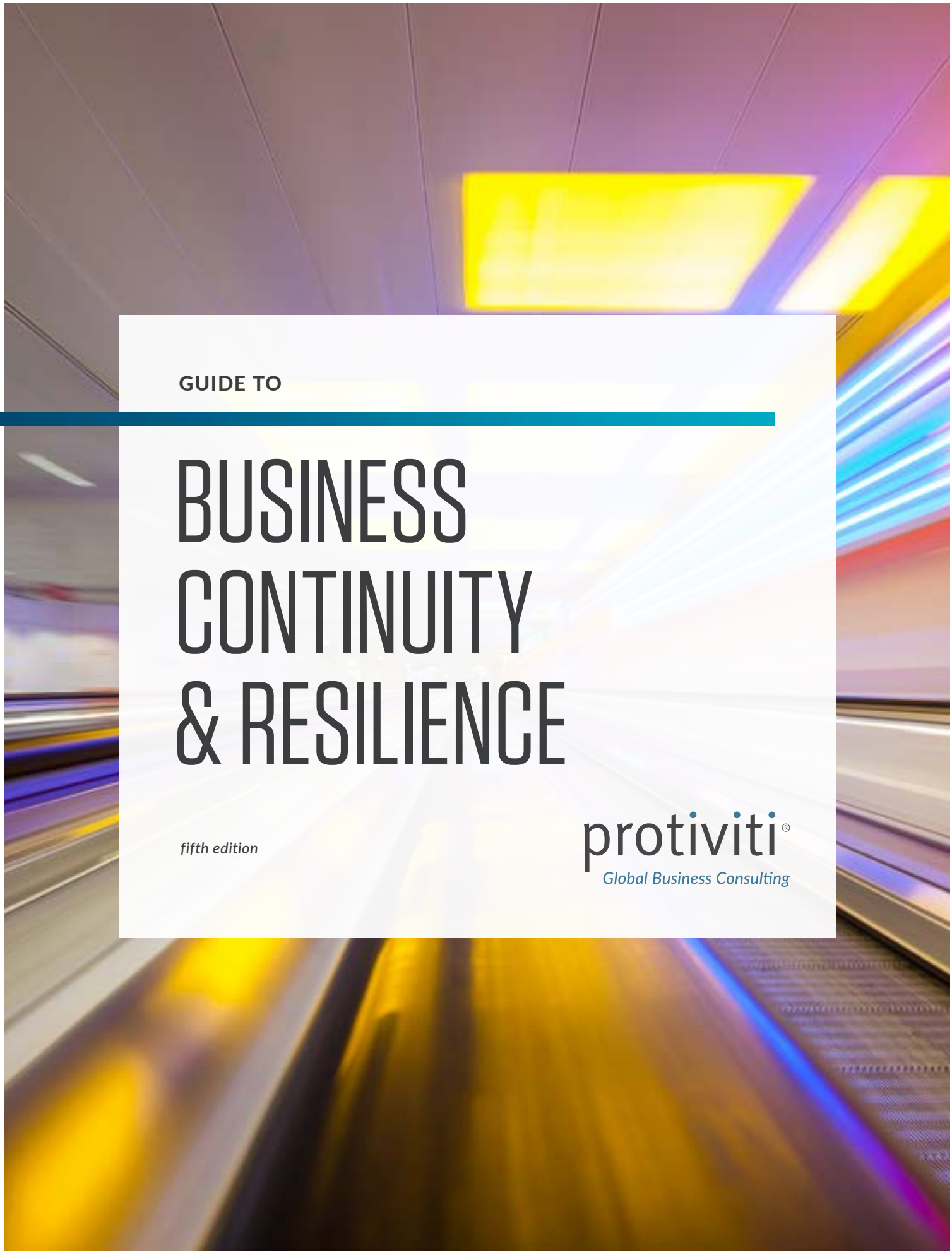


GUIDE TO

BUSINESS CONTINUITY & RESILIENCE

fifth edition

protiviti®

Global Business Consulting

INTRODUCTION

Calamities and setbacks continue to be a part of today's environment. Twenty-four-hour news coverage full of headlines of disasters and catastrophes around the world — severe weather, oppressive heat, earthquakes, mass shootings, geopolitical events, health concerns (e.g., mpox, COVID-19 variants), data breaches, and terrorist attacks — have become increasingly less shocking. Oftentimes, we are tempted to change the channel, or turn down the volume or scroll past the headline.

However, as business and process owners, team leaders, and business continuity practitioners, we do and must pay attention. We worry daily about all things impacting business continuity — the newly formed hurricane and how it may impact next week's shipments, the cloud outage that disrupted e-commerce overnight, new regulations that may create additional operating bottlenecks, or the market's possible reaction to missing a reporting deadline. Business continuity demands contemplating all disruption scenarios and potential responses, regardless of the event's cause and whether it was within our control.

In the current environment, in which businesses of all sizes and types are being tested in unprecedented ways by disruption scenarios, business continuity and resilience has become a critical discussion in boardrooms and C-suites around the world. The current landscape has forced organisations to revisit business continuity planning (BCP) and how to embed BCP practices in day-to-day operations. Operational resilience has taken on new urgency, as the expectations of business leaders to lead resilience efforts, not by assumptions, but with meaningful and substantiated data, intensifies.

As we consider the ongoing landscape changes brought on by the pandemic, it's important to remember that other business risks continue to threaten business continuity. Natural and man-made disasters, as well as technology risks, abound. How can organisations stay prepared for these events? How can they develop a business continuity management (BCM) program that responds to all crisis types and scenarios? Who is the right person in the organisation to own and manage the BCM program? And, what are the critical elements of a business continuity policy?

In Protiviti's *Guide to Business Continuity & Resilience*, we answer these critical questions along with many other pressing questions about BCM and related practices. The complete fifth edition covers many areas, including:

- COVID-19 and large-scale disasters
- Business continuity management basics
- Ownership and governance
- Program and plan development
- IT disaster recovery and other technology considerations
- Third-party risk management and BCM
- Regulations, standards and guidance
- Testing, training and maintenance

Also in this edition is an appendix that includes a glossary of key BCM terms and definitions, links to regulatory information sources, and BCM program testing options. No one can predict when the next disaster or business disruption will strike; the only certainty is that something unplanned and disruptive will happen. Staying informed is the first step toward becoming prepared and building resilience for the unknown. Our goal is to help companies keep ahead of risks by building sustainable business continuity and resilience programs.

Protiviti
September 2022

CONTENTS

THIRD-PARTY RISK MANAGEMENT AND BCM

REGULATIONS, STANDARDS & GUIDANCE

TESTING, TRAINING & MAINTENANCE

INDUSTRY-SPECIFIC CONSIDERATIONS: FINANCIAL SERVICES

INDUSTRY-SPECIFIC CONSIDERATIONS: HEALTHCARE

INDUSTRY-SPECIFIC CONSIDERATIONS: TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

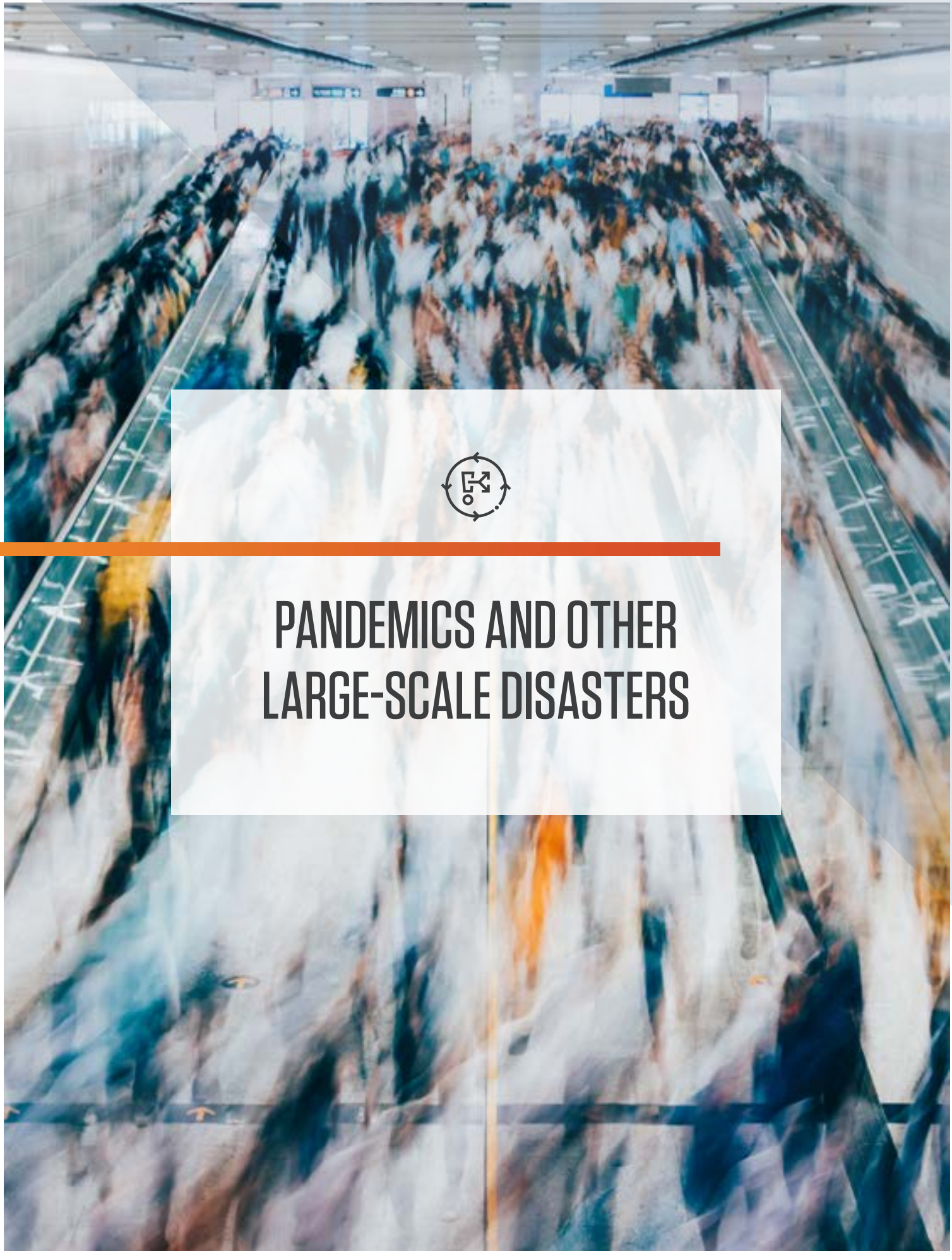
INDUSTRY-SPECIFIC CONSIDERATIONS: CONSUMER PACKAGED GOODS/RETAIL

INDUSTRY-SPECIFIC CONSIDERATIONS: ENERGY/UTILITIES

INDUSTRY-SPECIFIC CONSIDERATIONS: MANUFACTURING

INDUSTRY-SPECIFIC CONSIDERATIONS: GOVERNMENT

APPPENDIX



PANDEMICS AND OTHER LARGE-SCALE DISASTERS

Q1 Considering the continuing implications of the COVID-19 pandemic, what role should business continuity management (BCM) programs play in pandemic planning and response?

As we have seen, pandemic preparedness presents unique challenges for businesses, given a pandemic's far-reaching geographic impact and difficulty with predicting its scale and duration. The wide range of impacts on businesses (e.g., worker displacement, technology constraints, decreased production and challenges with third-party capabilities) are now in the forefront. Below we list a few of the critical roles BCM can play in pandemic planning and response:

- During a pandemic response, BCM should ensure the crisis management function remains engaged, particularly as it relates to following a defined protocol and crisis communications. Following a defined protocol that also can be flexible to the fluidity of any disruptive situation is key to a successful response. Since a pandemic can cause the workforce to be dispersed, which can lead to feelings of isolation and disconnectedness among employees, teams and even third parties, crisis communications can and should include strategies for both internal and external audiences.
- The business continuity program provides critical information that can be utilised as key inputs to the pandemic response plan. Similar to other plans (e.g., business resumption and IT disaster recovery plans), the contents of a pandemic response plan should be informed by foundational activities such as the business impact analysis (BIA) and continuity risk assessment. Outputs of these efforts should include elements such as the criticality of business processes, expected impact to the business caused by a disruption, and maximum tolerable downtime. This information can be used to shape or inform a company's response.
- Another important data element that can be useful to pandemic response is the identification of critical third parties essential for each business process to function. These critical third parties can be identified during the BIA, along with the resulting impact if they are disrupted or unable to provide products and services. This information will serve as a guide to develop subsequent strategies and planning discussions.
- Business continuity planning often requires developing playbooks that contemplate a variety of events or disasters that can impact the business, and then outlining how organisations should respond during and/or after those events or disasters. These playbooks can take the form of checklists or detailed step-by-step procedures and plans, and are typically scenario agnostic (i.e., an all-hazards approach). The most effective way to manage the impact of a pandemic, or any other crisis or disaster, is to implement playbooks that have been developed as part of a mature business continuity program.

Q2 What are some key business continuity considerations or priorities when developing a pandemic response, and what lessons have we learned so far from COVID-19 that would inform future business continuity planning?

The health and safety of personnel, the welfare of customers, and concerns about other human life should be the priority. Continued operation of the business, or maintaining or preserving business assets, must be secondary to preserving human life, health and safety. Once this is addressed, attention can shift to a more traditional risk management process, which focuses on the key people, processes and technology driving the business. Following are some key considerations when developing a pandemic response:

- It is important to understand the key business objectives and which pandemic-related risks could impact your ability to meet those objectives. Having a firm understanding of your business objectives allows you to focus your time, resources and attention on mitigating those risks to an acceptable level.

- For a protracted event such as a pandemic, it is essential to have an ongoing and evolving process for identifying, tracking and managing risks. As new risks emerge or existing risks evolve, companies should continue to monitor those changes and adjust their responses accordingly.
- Organisations should revisit the results of any previous BIA to determine whether the perceived impact pre-pandemic was accurate, particularly as it relates to process dependencies, key personnel risks, key third parties and critical applications.
- Comparing the previously established impact tolerance to the actual impact experienced during a disruption, and using that comparison to recalibrate the organisation's true impact tolerance, can help the organisation enhance its strategies and plans going forward.

One of the positive aspects about business continuity planning is that the discipline is ever evolving. Most organisations have already launched after-action activities — even though the COVID-19 crisis is not over yet — to understand what happened, what was learned from it and what should change about their response so they can be more effective if it ever happens again.

Q 3 How should your BCM program provide support for returning to normalcy post-pandemic?

The core building blocks of any good BCM program are business resumption, crisis management and IT disaster recovery. Each plays an important role in a business continuity lifecycle, which extends beyond the duration of an event. It also addresses how organisations return to normalcy after the event. As an example, the crisis management team formed during a crisis to make critical business decisions in a timely manner that will direct and guide the response is the same team that will guide activities to restore normal operations.

Simultaneously, the group of IT professionals who executed an IT disaster recovery program that allows, for example, an entire workforce to go remote all at the same time, along with all of the bandwidth and infrastructure implications necessary to make that a possibility, are also responsible for helping that same workforce return to normalcy.

Q 4 What are some of the common lessons learned from large-scale natural disasters that organisations should be aware of when developing their own BCM programs?

Regardless of what causes a disruptive event, the "signature" of that event is unique unto itself. The same is true for outages caused by environmental or natural events, such as hurricanes, pandemics, etc. As such, the detail of lessons learned will be specific to each company based on the products or services they provide, geography in which they operate, locations that may have been impacted, and nature of the disruption and its impacts. There are general lessons learned from these events that can apply to most every organisation.

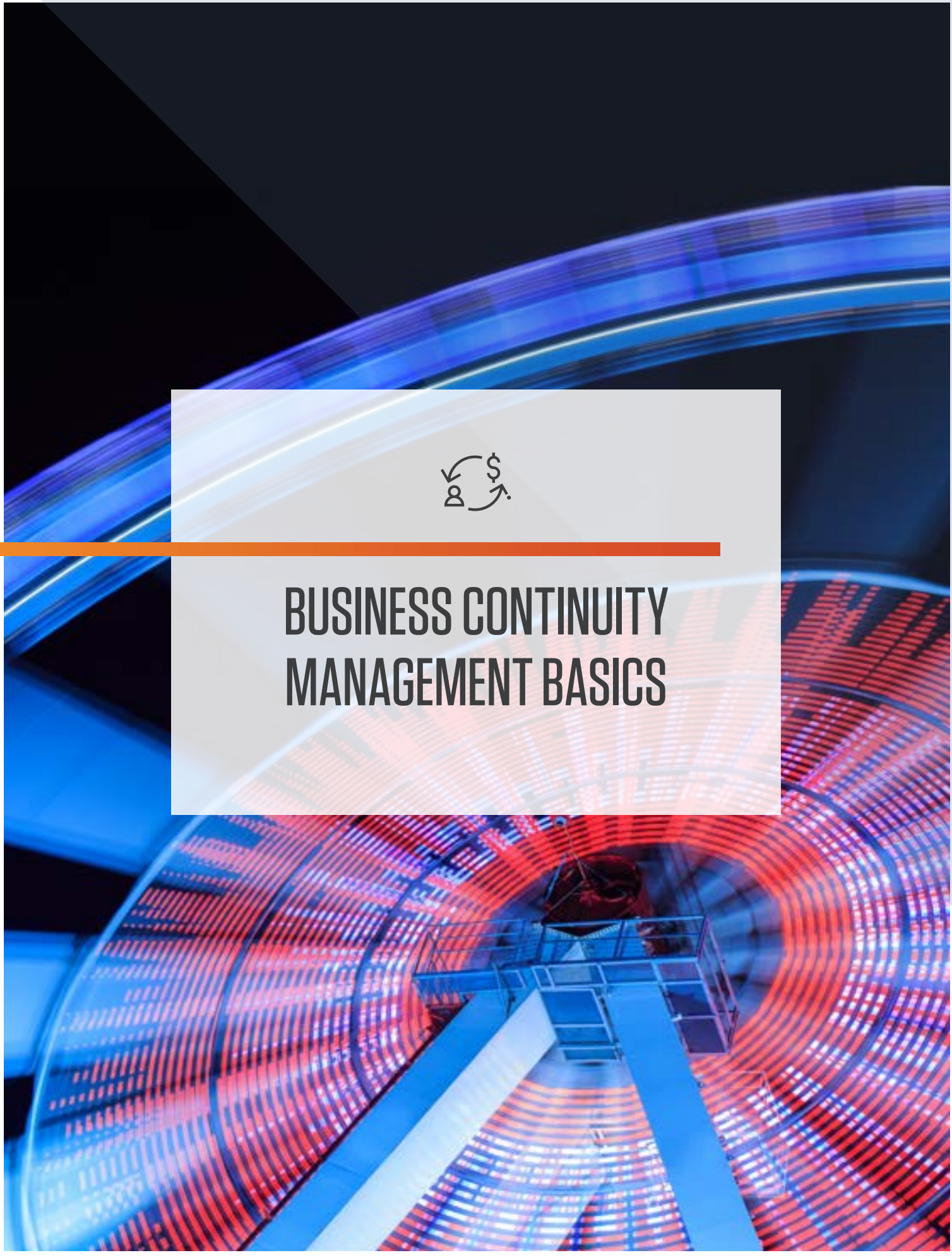
- **Communications —** At the top of most lessons learned from an event is the need to ensure appropriate communication to employees, executives, key internal stakeholders and third parties. Communication mechanisms must be well-vetted and familiar before an event occurs for communication to be effective during and after an event. While email seems ubiquitous, especially when hosted in a cloud environment, other communication mechanisms may be necessary. Many organisations are utilising Emergency Mass Notification Systems, or EMNS (e.g., AlertMedia, Everbridge, OnSolve), to utilise personal and business-related email, text messaging, and phones to contact employees and obtain immediate confirmation of their well-being. This is especially important when people are forced to disperse and life-safety considerations are critical. Developing communication teams for internal and external audiences, rehearsing roles and responsibilities, and testing-related systems are all valuable exercises that provide a baseline for senior management to use as it makes decisions following an event.

- **Availability of employees —** Most business continuity planning assumes employees will return to work to support business recovery; however, employees without a strong economic incentive who are forced to evacuate an area for an extended period are less likely to return. Ensuring employees can work remotely and connect to necessary systems is essential and practically a necessity for most organisations. If employees are simply not available, basic cross-training of critical processes should be performed to ensure there are no single points of failure related to critical personnel.
- **Employee assistance plans —** Since employees' first concern naturally will be for their families and their homes, developing and communicating an assistance plan for a disaster is both compassionate and pragmatic. Companies that provide material assistance for affected employees will find that their workers are able to return to their jobs substantially earlier than if they had not received assistance. These plans will likely need to be tailored to fit the event and the specific issues facing their employees.
- **Proactive evacuation —** It is not uncommon for people to spend 24 hours or more trying to leave a pending disaster area. When a hurricane or other disaster is imminent, businesses may want to encourage their employees to err on the side of caution and relocate early. This increases the likelihood that workers will be able to obtain hotel rooms or other accommodations near the business recovery site and that they may retrieve all necessary materials and equipment before they evacuate.
- **Supporting infrastructure services —** Basic services such as utilities, trash collection and publicly accessible healthcare can be interrupted for an extended period. Frequently, following regional disasters, some organisations recover their own operations only to find the supporting infrastructure, sanitation, utilities, mass transit, telecommunications, hotels, restaurants, etc., are not as well-prepared. Organisations should determine in advance how they will compensate for the absence of such services, including contracting with third-party vendors in the private sector to provide these basic services to employees until supporting infrastructure services resume.
- **Decentralised critical processes —** Companies located in disaster-prone regions whose critical processes (e.g., information systems, call centres, distribution centres, manufacturing) are concentrated in the region may find that they have lost — and therefore have to recover — everything. Companies that have decentralised their processes may find that while one area is affected, other critical processes remain operational and can support customers and sites affected by the disaster.
- **Testing and exercising —** Many organisations with plans to relocate people and resources have never tested them in preparation for a disaster of regional scope. Some plans fail to consider the competition for everyday resources (e.g., rental cars/trucks, hotel rooms, shipping providers) which occurs after a massive event, or they fail to consider the difficulty in obtaining custom or highly specialised equipment, such as in the manufacturing industry. Others identify in general terms the types of people, vital records, and equipment they would like to relocate, but do not have a system to quickly identify, gather and transport these resources. Businesses also must anticipate and plan for secondary damage (e.g., flooding, fires, theft). This includes obtaining the appropriate insurance to assist with recovery.
- **Actionable plans —** When disaster strikes, it is not uncommon for businesses to ignore their plans. This is because plans might be too general, overloaded with detail, or unfamiliar to the personnel intended to use them during the crisis. Companies should critically evaluate the information contained in their plans and ensure the information is complete, accurate, comprehensive and actionable. This will help ensure the plan reflects the current state of the business and can serve as a useful guide during a disaster and its aftermath.
- **Emergency funds —** Disaster events prove that the adage, "cash is king," is still correct. In the absence of infrastructure to process credit cards or other forms of electronic payment, cash is still the most effective way to acquire resources — especially those in short supply and high demand. Companies should consider how cash will be made available in a secure fashion to meet the needs of the business continuity effort.

Q 5 How should firms integrate climate resilience into their business continuity management program and address regulatory requirements?

Building climate change resilience is now a top business priority for various industries, but specifically the financial services industry. On November 8, 2021, the Office of the Comptroller of the Currency (OCC) set climate response as a banking priority, as regulator interest amplifies. In response to this current challenge, building resilience in the face of emerging risks such as climate change requires a broader view than traditional BCM. Improving climate resilience involves assessing how climate change will create new, or alter current, climate-related risks, and taking steps to better cope with these risks. The climate resilience crisis is deeply embedded in business continuity management but challenges firms to go a step further as organisations aim to understand and address the risks and pronounced effects of climate change.

- **Program considerations —** Implement or enhance programs to proactively address climate control risks (e.g., enterprise risk management, third-party risk management, agility).
- **Risk assessments —** The first step is that boards should seek to balance "top-down" and "bottom-up" approaches to assessing their firm's exposures to climate change. Understanding the potential effect of extreme weather on the continuity of critical operations is an important part of effective climate risk management. Organisations should be conducting risk assessments that include climate-related risks for all of their various locations.
- **Resiliency planning —** Location strategy and work area recovery alternate location analysis can help to reduce the risk of potential impacts associated with weather and site unavailability. A full view of alternate recovery strategies is required, including the identification of improvement opportunities or gaps in recovery time objectives (RTO) and/or recovery point objectives (RPO) in connection with critical business activities.
- **Testing/exercising and training —** Firms should engage in scenario testing that challenges their teams and capabilities. Think about the "what if" scenarios in connection with climate change risk and develop the frameworks to challenge what currently is in place so the organisation can effectively manage the risks from climate change.



BUSINESS CONTINUITY MANAGEMENT BASICS

Q6 What is business continuity management?

Business continuity management (BCM) is the design, development, implementation and maintenance of strategies, teams, plans and actions that provide protection over, or alternative modes of operation for, those activities or business processes which, if they were to be interrupted, might bring about seriously damaging or potentially significant loss to an enterprise. As BCM has evolved, the threat landscape has grown considerably to include both internal and external events, as well as extreme-but-plausible incidents.

BCM consists of three core disciplines:

- **Crisis management and communications —** This discipline enables an effective and cohesive response to an event. Crisis management processes focus on stabilising the situation and supporting the business if alternate modes of operation are needed, using effective planning, leadership and communication protocols.
- **Business resumption planning or business recovery planning —** This discipline focuses on the resiliency of business functions and processes that relate to or support the delivery of core operations (i.e., products or services) to a customer. The objective of business resumption planning is to mitigate potential impacts from disruptions, regardless of the cause, by developing plans that guide personnel through operations with diminished capabilities and toward business as usual. Business resumption processes typically consider dependencies of the function or process such as the people, processes, technology and other resources vital to supporting operations.
- **IT disaster recovery (ITDR) —** This discipline encompasses technology resilience and addresses restoration of critical IT assets, including systems, applications, databases, data storage and network assets. An ITDR strategy also should encompass all technology service provider (TSP) relationships (e.g., cloud service providers, SaaS partners, co-located data centre providers) to ensure that all technical stakeholders remain aligned.

In addition to the traditional BCM disciplines listed above, many organisations manage other closely related programs as part of their overall BCM program. These programs include:

- **Incident management (or incident response) —** This term commonly refers to identifying, analysing and managing the response to a disruptive event. Regardless of nomenclature, incident management programs typically include emergency response measures such as evacuation of facilities, first-aid response and first-responder interactions.
- **Cybersecurity incident response —** This is specific to the planning for, response to and recovery from a cybersecurity incident such as a data breach, ransomware attack, phishing attempt or distributed denial of service (DDoS) attack.

Finally, due to the nature of business continuity, it is common for several functions to be integrated at various phases of business continuity planning. For example, facilities or physical security teams may engage in emergency management activities. Environmental, health and safety teams may have input in developing recovery strategies. Integration of these enterprise-impacting functions, depending on the organisation or industry, can be confusing and should be considered when developing a BCM program.

Q7 What is the value to an organisation in designing and deploying BCM programs?

The value of BCM lies in risk mitigation — minimising the risks associated with any disruption to business as usual. In the wake of recent catastrophic natural disasters, geopolitical uncertainty and the COVID-19 pandemic, business leaders are more mindful than ever of the need to plan for and respond to business disruptions.

The business environment is fraught with risks that can impact businesses' ability to not only continue operations, but also protect their people and brand, earn revenue, maintain relevance and remain compliant with regulations. Companies need to stay ahead of these risks by understanding priorities, planning for disruptions, employing good business practices and exercising forethought to increase their ability to course-correct quickly when things go wrong.

Organisations realise value when they proactively design and deploy business continuity solutions to manage a specific risk or multiple risks. For example, understanding and developing contingency plans for the loss of a key supplier can help a business mitigate potential financial, operational and reputational impacts.

Financial risk — This is the most evident and quantitative area of risk. Companies can minimise financial loss and maintain market share by focusing on several factors, including:

- Responding to customer demands and maintaining a viable supply chain
- Understanding officer liability or potential revenue impacts from business disruptions
- Inventorying potential replacement loss (i.e., the cost of replacing damaged assets)

To protect the supply chain and ensure that supply keeps up with customer demand, a company may hold its suppliers accountable for disruptions to the supply chain that impact its operations. For example, a company can use contract provisions to hold a supplier accountable for timeliness in delivery of products or services, as well as for quality of products or services delivered.

A company can implement BCM solutions to minimise the potential for huge unexpected costs stemming from single points of failure and critical external dependencies. For example, if a company depends on a single critical supplier that suddenly is unable to provide core products or services, a well-designed BCM solution would provide contingencies to mitigate the financial loss.

Operational risk — This area of risk stems from the inability of companies to produce core products and services as expected. This can include risks associated with equipment or technology obsolescence, a failure in internal functions, and unexpected changes to a leadership team. Other operational risks directly impacting business as usual include:

- Loss due to failed single points of failure and critical external dependencies
- Productivity loss (employees unable to perform their jobs for any period)
- Response loss (cost of time/materials required to respond to the disruption)

A company should implement BCM solutions to minimise operational gaps and ensure that the delivery of products and services continues, even during unusual circumstances. Comprehensive implementation of a BCM program will lower risks associated with readiness, planning and response, which can decrease overall operational risk.

Regulatory risk — Regulatory bodies are increasingly holding companies accountable for maintaining validated capabilities, teams and plans, and can issue fines to those that operate without a BCM program. Depending on the regulator, a repeated and unmitigated issue at a regulated entity could result in a reportable item, which could impact the company's creditworthiness or reputation. Generally, companies that violate regulations or compliance requirements face:

- Fines, penalties and judgments
- A Matter Requiring Attention (MRA) or similar rebuke from a regulatory body, which could invite an additional level of scrutiny or a higher expectation of performance
- In some extreme cases, a temporary shutdown of operations

Reputational risk — Bad press can cause a decline in revenue, unwanted social media attention, lower market capitalisation and, in the long term, a negative opinion of an organisation in the eyes of the discerning public. In today's 24-hour news cycle and social media-driven world, a measured, empathetic, rapid and relevant response to any event is crucial to maintaining a positive reputation. A mature BCM program drives value by protecting a company's brand and adeptly managing the ever-changing business landscape in the face of growing competition.

Q 8 BCM incorporates many different terms that appear to be very similar. What are the similarities and differences with some of the common terms?

One of the more confusing aspects of BCM is its terminology. The confusion is mostly due to differences in how regulators and industry groups use and define terms in the BCM lexicon. Below are a few examples grouped according to the core discipline to which they are most aligned.

Crisis Management and Communications

- **Continuity of operations plan (COOP) —** Federal government agencies and entities typically use this term to establish policies and guidance for essential functions related to a broad range of events and disasters.
- **Emergency management and operations —** This phrase is commonly used in the healthcare field, particularly in the clinical (i.e., patient-facing) side of contingency planning. It is sometimes used interchangeably with "crisis management" in other industries, but typically as a reference to the initial response aspects immediately following an event.
- **Emergency response —** This term refers to the immediate actions taken to preserve life and safeguard property and assets, often a subset of a broader crisis management program. A building evacuation plan is an example of an emergency response component.
- **Incident management and response —** This is often used interchangeably with "crisis management." It is also commonly used to refer to responses to any number of events impacting a particular entity or location, such as a hurricane on the Gulf Coast, an earthquake in California or a supply chain disruption for a logistics provider. Recently, firms have been developing incident response plans as part of their crisis management programs to leverage the shared, high-level protocols associated with escalating and reporting an event. This strategy enables companies to quickly and efficiently put into action predefined plans designed for scenarios that may impact a function or facility.
- **Major incident management (MIM) —** This term refers to a response program for serious interruptions of business activities. It is frequently used interchangeably with "crisis management."
- **Resilience —** This is an evolving concept that refers to the ability of companies to withstand and quickly adapt to disruptions while attempting to maintain continuous operations. Resilience focuses on preserving business services and relies on regular maintenance to ensure that the entire business operation, or process or function, maintains its ability to remain flexible in all circumstances. Recently, this term has been used to describe a focus, such as technology resilience, business resilience and cyber resilience.

Business Resumption Planning

- **Business recovery planning —** This term refers to various steps taken for an individual process or business line as it relates to the planning of inputs/outputs, personnel resources, information technology and physical work locations in the aftermath of a disruption. This term is often used interchangeably with "business resumption," "contingency planning" or "business continuity planning."
- **Business continuity planning (BCP) —** This term is used to denote the planning aspects of business continuity management (BCM). BCM usually refers to the comprehensive program, while BCP is the predefined set of steps taken to recover a business process in the event of a disruption. This term is often used interchangeably with "business resumption," "contingency planning" or "business recovery planning."
- **Business resumption planning —** This process focuses on recovery of business functions. The term is often used interchangeably with "business recovery," "contingency planning" or "business continuity planning."
- **Contingency planning —** This phrase refers to the set of tactical steps a team or function may take to resume a disrupted process. Often the term is used interchangeably with "business recovery," "business resumption planning" or "business continuity planning."

IT disaster recovery (ITDR)

- **Disaster recovery —** This is a term reserved for recovery and resumption of critical technology assets in the event of a broad and unplanned outage. Disaster recovery can include tasks such as resuming individual systems or recovering all critical aspects of the IT environment. Disaster recovery is a component of an overall BCM program.

(**Note:** The above list is not comprehensive. The practices within a specific industry or regulatory landscape may influence how BCM terminology is used.)

Q 9 Is there a best practice approach to business continuity planning?

Although vague, this frequently asked question is a valid one. BCM approaches and scopes vary widely; one size does not fit all. The primary driver of a BCM program should always be the recovery requirements of the business. However, several recommended attributes or program characteristics should be integrated into every BCM program. The process of embedding each of these into the program may vary:

- **BCM program governance —** This involves identification and formalisation of the BCM steering committee and executive-level risk management oversight to determine BCM program requirements.
- **BCM program and implementation design —** This includes definition of policies, standards and tools to support business continuity efforts. An effective BCM program should also define the operating model, which includes who is accountable and responsible for each key discipline of the program (e.g., crisis management, business resumption and IT disaster recovery), technology tools used to monitor and manage the program tasks, and any defined key risk indicators (KRIs) and key performance indicators (KPIs).
- **Business impact analysis (BIA) —** The BIA, a type of risk assessment that serves as the foundation of a BCM program, enables organisations to capture and effectively measure the potential business impacts of a disruption (i.e., operational, reputational, financial, regulatory or compliance impacts). The objective of the BIA is to establish recovery priorities for business processes and the resources (i.e., technology, workspace, equipment, personnel and third parties) on which each of those processes rely.
- **Risk assessment —** In BCM parlance, this may be referred to as the continuity risk assessment (CRA), which includes identification and prioritisation of threats and failure scenarios to which the organisation may be vulnerable. The CRA is not an enterprise risk assessment (ERA). Rather, the scope of the CRA encompasses those scenarios that pose a direct risk to operations (e.g., a supply chain disruption, a technology outage, a data breach, or severe weather in a densely populated area where operations reside).
- **Strategy design and implementation —** Identification and implementation of continuity strategies that best meet the organisation's needs, based on a cost-benefit analysis and operational risk tolerance, is crucial. The results of the CRA and the BIA should inform the design of the recovery strategies.
- **Plan documentation —** Following the design of a viable recovery strategy for a particular risk, the response, recovery and restoration procedures should be documented to enable effective business continuity operations. Each discipline employed (i.e., crisis management, business resumption and IT disaster recovery) should have a documented strategy and plan.
- **Testing —** A BCM program that is not tested regularly cannot be confidently relied on. Testing and continuously improving the validity of business continuity strategies and corresponding teams and plans are critical. Rigorous testing of each key discipline's teams and plans, both separately and in tandem, should be conducted to ensure confidence in the BCM program.
- **Training and awareness —** An organisation is better prepared operationally if its employees are knowledgeable about their respective roles and responsibilities regarding business continuity activities. Training should be provided to all employees, including those directly responsible for response/recovery team efforts, as well as to those not directly engaged on a recovery team.
- **Compliance monitoring and audit —** Conducting regular, objective reviews of the BCM program contributes to the continual refinement of the effectiveness, completeness and rigour of the program overall. When executed under the oversight of the organisation's internal audit or compliance function, it creates an opportunity for a broader communication with leadership regarding the strengths and weaknesses of the current program and generates support, both organisational and financial, to address unmitigated program risks.

Q 10 What is the connection between operational resilience and business continuity management?

Regulators around the world remain resolute in their expectations aimed at strengthening the operational resilience of the financial services sector, an effort that has been spearheaded by supervisory authorities in the United Kingdom. Operational resilience defines the ability of an organisation to withstand adverse changes in its operating environment and continue the delivery of business services and economic functions. Below are the various approaches by which an operational resilience program can enhance and extend traditional BCM practices and concepts.

- **Identifying important business services —** These include most critical product suites or lines of business that may directly impact end consumers any time there is a disruption (e.g., ATM accessibility interruption or degraded payment processing).
- **Setting impact tolerance —** Under traditional BCM programs, risk appetites are not easily quantifiable, and most risk appetite statements lack forward-looking metrics or documented thresholds for triggering actions (e.g., containment options) in a crisis. Under operational resilience, institutions are expected to develop quantitative impact tolerances for each important business service.
- **Testing —** Testing various aspects of a BCM program and capabilities is typically discrete and segmented within the IT, operations or crisis management teams. In most cases, these tests are not scoped or facilitated in a manner that validates all aspects of the function or line of business being tested. Under operational resilience, institutions are expected to test extreme-but-plausible scenarios to better understand realistic recovery times versus established impact tolerance. Additionally, full scenario testing is key to helping institutions identify areas of failure or vulnerability, as well as concentration risks that could result in a business disruption. Testing will also indicate where investment in technology or processes is needed to stay within established tolerances.
- **Mapping —** Front-to-back process mapping and more comprehensive and integrated testing activities are essential elements of an effective operational resilience program. Though process mapping has been recommended for years, accuracy and completeness are not regularly enforced. Under operational resilience, front-to-back mapping is expected to help institutions better understand what constitutes an important business service. Institutions can use mapping to:
  - Identify people, skill sets, processes, technology, data, third parties, operations, reporting requirements and legal entities, along with clearly defined cross-functional/business dependencies and handoffs.
  - Identify important business services and rank them in order of priority or criticality.
- **Understanding economic impact across stakeholders —** Beyond identifying their own important business services and setting impact tolerance, organisations are expected to demonstrate a firm understanding of the impact of an adverse event on the financial sector and the broader economy. For example, banks must look at all upstream and downstream impacts, employ a systemic look at potential service degradation scenarios and how they may need to prioritise clients and channels, and consider the effects of prolonged disruptions or outages. Under most traditional BCM programs, there are no formal or consistent definitions of important business services, testing or severity levels.

OWNERSHIP AND GOVERNANCE

Q 11 Where should the BCM program be placed in the organisation?

As organisations begin to develop their BCM program capabilities and plans, they are confronted with a common question and dilemma: Where should the overall program sit and/or who should own it? A successful BCM program requires various levels of accountability and responsibility within an organisation. While some organisations may ultimately decide to create a separate business function or unit to own the program, many choose to utilise existing resources and/or personnel.

Organisations typically provide leadership to the BCM program through one of three roles: sponsors, owners or custodians. Sponsors provide and ensure organisational and financial support. Given that consistent visibility to the board and senior leadership is essential, sponsors should be executives. Owners have direct accountability or are responsible for ensuring support and overall program execution. BCM owners are department leads with an understanding of strategy and direct working relationships with those implementing the annual plan and managing day-to-day tasks. Finally, custodians have the primary responsibility for coordinating BCM tasks executed throughout the organisation. Custodians understand the various roles needed for each aspect of a comprehensive program and are empowered to escalate a concern in a timely and coherent manner.

It is not uncommon for these oversight roles to be aligned to the respective BCM discipline. For example, the CTO, CIO or CISO may own the IT disaster recovery program, and the head of marketing may own crisis management. It is common for organisations to have a BCM steering committee or other similar decision-making and governance group providing oversight.

There is no single recommended structure for a BCM program and no "best-fit" placement functionally. The nuances of a company's industry, risk profile, culture and operations can influence the decision about where the BCM should reside. Sometimes the biggest hurdle to adoption is a perception that BCM is strictly an IT or business problem. Placement in one group or another may lend credence to that perception, whether warranted or not. Some examples include:

- **Finance —** The CFO's function or vertical.
- **Executive council —** A subset of the senior management team, which may include the general counsel and the directors of human resources or corporate communications.
- **Operations —** The COO's function or vertical.
- **Risk management —** The CRO's function or vertical; this is most common, as a designated and qualified business continuity practitioner would align most directly within an operational risk program and provide "second-line" effective challenge to owners of crisis, business resilience, and technology resilience strategies and plans.
- **Information technology —** The CTO's, CIO's or CISO's organisation or vertical.

As a matter of practice, it is recommended that BCM program ownership be maintained at an executive level within the organisation so that it remains visible to decision-makers and influences enterprise adoption while supporting all aspects of a mature program.

Q 12 How do you structure an internal business continuity function or planning team?

The size and composition of an organisation's business continuity function depends on various characteristics of the enterprise, including:

- Total employee headcount
- Amount and geographic dispersion of company locations
- Similarity of operations between business departments, subsidiaries and organisational units
- Degree to which management oversight and leadership are centralised versus decentralised
- Risk profile of the organisation (e.g., highly regulated, governed by external oversight bodies)

While it is common for companies to have a few individuals responsible for the organisation's overall business continuity efforts, many businesses have realised

that maintaining an effective BCM program truly takes a village. Nobody knows the intricacies of a particular department or underlying business processes like the respective leaders and their supporting team members who are the "boots on the ground." BCM leaders and their teams bring domain expertise and serve as risk, impact and mitigation advisers to business and technology personnel. This collaborative assessment of "what ifs" ensures that a BIA and the resumption plan for a department reflect current risks and are actionable based on agreed impact criteria and prioritisation.

Similarly, a BCM lead must act as a conduit for relaying important recovery priorities to the IT organisation and for ensuring that relevant IT disaster recovery plans and supporting technologies are in alignment with the recovery needs of the business. In industries like manufacturing or energy and utilities, where operational technology is not managed in the same manner as the enterprise or corporate aspects of an IT organisation, specialised knowledge may not be readily available. These organisations or industries may have critical resiliency and recovery requirements that a BCM lead can help identify and prioritise. Further, the BCM lead can influence how subsequent recovery planning documentation addresses those priorities.

BCM leads must have clearly defined roles and responsibilities, as well as the support and sponsorship of the executive management team. Further, in many organisations, it is not uncommon for some BCM responsibilities to be delegated to several levels of personnel. If this occurs, executive sponsors should be engaged to ensure that all stakeholders remain aligned and that the needs of the organisation are the focus when the time comes to manage all aspects of the program.

From an operation model standpoint, BCM programs can be organised into one of three primary models: centralised, divisional and federated.

- **Centralised —** Under this model, a central continuity office serves all business units and/or geographies by providing policy, guidance, tools, templates, metrics and maintenance as well as program execution.
- **Divisional —** Multiple continuity offices serve the different region and business lines, aligned to unique needs.
- **Federated —** A central continuity office, linked to various regional/business line centres of excellence, provides dedicated services to different regions and business lines.

Q 13 How do you convince executive management to fully support the organisation's business continuity efforts?

When not a compliance requirement, BCM is often viewed as discretionary, since the value of time and resources spent planning, training, documenting, testing and validating all aspects of a program cannot be realised until something truly goes wrong. In the absence of regulatory requirements, audit findings or specific customer demands, the most effective way to convince executive management to fully support BCM efforts is to conduct and share results from an exercise that highlights risk (e.g., tests or validations of a plan, the business continuity risk assessment, or the BIA). Results from the exercise, which typically include recovery priorities, corresponding recommendations and industry benchmarking data, should provide executive management a complete view of the organisation's business continuity needs.

Communicating the value of business continuity efforts to executive management can also be accomplished through a cost-benefit analysis. The cost analysis addresses the funding and resources necessary to add resiliency and recoverability to key areas of the existing business and technology environment, while the benefit analysis relates to avoiding the potential impacts of a disruptive event (e.g., revenue loss, downtime, property damage and reputation degradation). To aid this cost-benefit analysis, the FAIR (Factor Analysis for Information Risk) methodology, commonly used for analysing cybersecurity risk, is an emerging method for quantifying potential disruption loss.

Another data point that can be shared with executive management is business interruption premium savings

from the organisation's insurance provider as the result of implementing a tested BCM program. Program implementation can also help firms realise savings in the cost of procuring directors and officers (D&O) liability insurance. From a fiduciary perspective, if the directors and officers understand that they can be held personally liable for the organisation's response to a business interruption, they are more likely to support implementation of robust BCM programs.

Additionally, it is becoming more common for customers to require (as part of the contract) that their suppliers and business partners have a robust business continuity plan in place, inclusive of business and technology service delivery as well as supplier-customer coordination. A company may hold its suppliers accountable to maintain continuity plans and protect its supply chain. It is now common practice for customers to have a vendor management department that will review a partner's or supplier's business continuity program, through either the completion of a standardised information-gathering questionnaire or requesting third-party service provider audit reports. They may also require active participation by both parties in mutual exercises.

Finally, lessons learned by peer companies in past events or their experiences related to increased focus by regulators in a particular industry carry a lot of weight with leaders. Business continuity actions taken by other organisations (of a like size or in the same industry) often drive action or increase maturity in others. This is particularly the case if an organisation successfully recovered from a perceived catastrophic failure (although the opposite also can be true). Regulatory areas of focus by an examiner at one financial services institution tend to become themes at their next stop, and leaders will discuss their experiences with their counterparts in industry groups.

Q 14 What are the critical elements of a business continuity policy?

A growing number of organisations are developing formal, documented business continuity policies to support their BCM programs. Typically, the content and format of the policies differ based on existing standards and the culture of the organisation. Below are the critical elements of a business continuity policy:

- **Accountability —** Identifies the executive or executives accountable for BCM program planning and execution, as well as those responsible for resourcing and strategy decision-making.
- **Roles and responsibilities —** Establishes roles and responsibilities for all employees regarding planning and activities before, during and after a disaster.
- **Program scope —** Defines program tenets and recovery priorities via the continuity risk assessments and a BIA. Further, this foundational effort establishes the criteria for the type and scale of incidents to be addressed in the BCM program. Importantly, this also documents any exclusions, known gaps in capabilities, and planned/in-flight initiatives which could impact the program.
- **Recovery strategy development —** Identifies specific actions necessary to develop relevant and right-sized strategies to enable preparation for, response to and recovery from impactful events. Recovery strategies should be developed to mitigate impacts from the loss of key personnel, key processes and technology, or primary workspace and facilities. Cost and time to design and implement recovery strategies should be commensurate with the loss potential and impact tolerances determined in the business assessment lifecycle phase.
- **Plan development and maintenance —** Defines the standards for putting recovery strategies into action via playbooks to be executed by business and technology personnel, and considers disruptions to one or more of people, processes, technologies and suppliers/service providers.
- **Testing (exercising) —** Defines the various types, frequency and required participants (e.g., internal employees and external business partners or third-party service providers) of testing activities. Planning of each discrete exercise (e.g., defining scope, objectives and success criteria) and capturing test results should also

be enforced by policy. As organisations adopt aspects of operational resilience, policy should also direct planners and participants to focus on exercise scenarios with similar "extreme but plausible events." Additionally, business end users should participate in BCP exercises (in conjunction with technology, operations and BCM teams) for a more comprehensive simulation of actual events and to enhance readiness across the organisation.

- **Training and awareness —** Establishes standards for role-based training of personnel named in the response and recovery plans, as well as general awareness for employees affected by the business continuity strategies.
- **Legal, regulatory and contractual alignment —** If applicable, captures the organisation's understanding of legislation, regulation and industry standards, as well as customer contractual requirements impacting business continuity requirements.
- **Internal audit participation —** Defines the role of internal audit in the planning process and/or the review of compliance with the requirements set forth in the BCM policy.
- **Reference —** Provides linkage to a glossary, industry source, standards, guidelines, regulations and policies that the BCM program relies on within the organisation.

These key elements of a business continuity policy will assist an organisation's planning team with gathering the necessary support and resources to manage the BCM program effectively.

Q 15 What is the role for internal audit in the BCM process?

Due to their perspective, exposure to all areas of the organisation, and associated influence, internal audit departments are well-positioned to add considerable value in terms of BCM. Here are several ways the third line of defense can make an impact:

- **Act as an internal salesperson —** Support the business case for business continuity through participation in the risk assessment and BIA processes (tasks that internal audit may address through the development of annual audit plans).
- **Ensure creation and maintenance of business continuity policies —** Because of its familiarity with policies, controls and the key components associated with BCM processes, internal audit can assist with the development of initial policies and standards (in line with reasonable maturity levels and business objectives).
- **Maintain project management standards —** Similar to the development of business continuity policies, internal audit is typically familiar with project management standards and project risk management programs.
- **Understand the fluid landscape —** In addition to encouraging the development of a comprehensive program (i.e., governance, business and technology), internal audit can assist in the necessary maintenance efforts of all program components, as opposed to a sole focus on plan documentation. Specific attention should be paid to the planning and execution of business continuity tests and exercises as teams, plans and recovery strategies evolve. Internal audit should observe such tests and follow up on action items captured in observation/gap logs. Internal audit can also play a role in event after-action reporting, playing a similar role to simulated exercises.
- **Encourage continuous improvement —** Based on familiarity with internal and industry standards/requirements, internal audit is positioned to regularly review the planning process and strategies to ensure compliance. Internal audit also can remain engaged through the development of recommendations to address opportunities for improvement.
- **Communicate to management —** Internal audit can formally communicate program status and capability to the board and management to ensure expectations are met and that the BCM program continually matures over time.

Because BCM is a management-owned process, internal audit can be an active participant and adviser to the organisation's business continuity executive sponsor and steering committee, suggest key performance indicators and program health metrics, and then evaluate actual results over time.

Q 16 How often should the business continuity program be audited?

The answer is organisation-specific, based on internal standards, regulatory requirements and changes to the business. In most cases, an audit should be conducted every 12 to 24 months to ensure compliance with internal policies and procedures, with emphasis on the execution of testing, training and maintenance activities. In a growing number of firms, internal audit is an observer of all major testing activities, as opposed to a reviewer of test summary documentation. As such, the frequency of audit-related activities increases.

The Institute of Internal Auditors (IIA) published Global Technology Audit Guide (GTAG) 10: Business Continuity Management (most recently updated in 2014), which states that BCM-related audit activity should take place "on a regular basis" and can include:

- Playing a role in the organisation's planning, to include the risk assessment. (It is typical for internal audit to help with an assessment of an organisation's internal and external environment.)
- Evaluating the business continuity and disaster recovery plans during the planning and development phases. (Internal auditors have a thorough understanding of the business and the individual functions and interdependent relationships and can contribute to the BCP process.)
- Reviewing the proposed business continuity and disaster recovery plans for design, completeness and overall reasonableness/viability.

PROGRAM AND PLAN DEVELOPMENT

Q 17 How has the Business Impact Analysis (BIA) process evolved?

The BIA is used to identify and prioritise an organisation's business processes and supporting dependencies, as well as how long each business process can operate in a degraded state before intolerable harm is caused. The BIA process is constantly evolving, but how each process is measured should include an assessment of the collective impacts from operational, financial, customer, reputational, technological, regulatory, legal and compliance standpoints.

A primary metric gathered as part of the BIA is the Recovery Time Objective (RTO), expressed in time and captured for each process and associated technology dependency. The use of metrics like the RTO has been a part of the BIA for years. As operations and technology continue to become more integrated, critical processes rely on technology, thereby causing that technology to also be critical. These dependencies highlight complexities requiring analysis and the need for a tailored and flexible approach particular to the operational environment.

In the past, practitioners used BIAs to explore a range of threats to an organisation. However, more recently, the BIA has adopted an event-agnostic approach, meaning it is more common to focus on possible impacts of a disruption on each business process. The collective impacts on the organisation become the driver, rather than the triggering event, for the development of recovery strategies and planning. Further, current best practice is for process owners, information technology teams and the executive team to agree on the resultant RTOs for each critical process and supporting technology.

A facilitated BIA with interviews and discussions is recommended. Ideally, the person or team responsible for business continuity management leads all BIA discussions. Questionnaires without facilitation can introduce bias or cause confusion if respondents are unclear about terminology used in the printed questions. The quality of data gathered from questionnaires also suffers when participation is low or when the number of responses from a particular group is disproportionate.

It is important to note that the BIA is a point-in-time discovery exercise and should be revalidated and updated regularly for, at least, the areas of the business most sensitive to downtime (i.e., those with low RTOs). Further, BIA results should not be viewed as "set in stone" for a long period of time and should be discussed among the stakeholder groups as the process(es) or technology dependencies evolve.

The quality of the BCM program, which is significantly influenced by the BIA, can benefit from having objective experts trained in program development best practices. BCM experts with facilitation experience can guide process owners to develop meaningful and realistic RTOs. They can then apply BCM and industry best practices (e.g., supporting organisations with data collection, validating analyses, and documenting and reporting mechanisms) to strengthen their preparedness and response capabilities.

Lastly, an effective BIA process relies on appropriate planning and scoping. The BIA or similar information-gathering exercise would help improve understanding of all factors impacting how to plan and respond to a disruptive event.

Q 18 What are the most common approaches to executing a continuity risk assessment?

The fundamentals of a continuity risk assessment do not differ from most other risk assessments. Continuity risk should be evaluated from the standpoints of likelihood, impact, and mitigating and compensating controls, just like any other type of risk. From a probability standpoint, organisations should:

- Consider their unique risk profile. For instance, organisations located in an earthquake zone will devote more planning to the response and recovery from a possible earthquake event.
- Conduct research to determine the likelihood of a threat and focus the assessment on threats most significant to the business. Most organisations have cybersecurity

risk and aspects of geographical hazards such as earthquakes, hurricanes and tornadoes. Additional risks may be specific to the organisation's industry, such as supply chain, seasonality and compliance. Continuity risk assessments should consider several factors, as types of events may evolve over time.

When assessing impact, organisations should:

- Determine the type of impacts that may arise from any event. The collective impact from an event should be considered carefully. Impacts can take multiple forms, such as operational, financial, customer, reputational and technological, as well as legal, regulatory and compliance related.
- Categorise the risks (or events) that have similar attributes. Events that cause broad operational, reputational and compliance risk would warrant more attention than events that are localised or isolated and unlikely to cause detrimental impacts.

Business continuity planners should consider available controls as countermeasures or mitigation techniques for the most probable and impactful of the risks. These techniques may include enhancing environmental or physical security controls or documenting a scenario-specific incident response plan for that specific risk (e.g., a hurricane preparedness plan for the Gulf Coast or an earthquake response plan for the West Coast).

Q 19 What are some alternatives to performing an exhaustive BIA and risk assessment?

When planning for near-term events with business continuity implications, organisations are increasingly implementing creative processes to streamline the rigorous and detailed analysis effort required to complete a formal BIA and risk assessment, which can span many months. Organisations often do not have the time to complete an exhaustive analysis of all environmental, manufactured, business process, supply chain and IT continuity risks.

One option to identify risks and prioritise recovery needs is to perform an abbreviated BIA and/or risk assessment through an executive work session. A facilitator leads a high-level cross-functional team to define impacts (at an organisational level, as opposed to a business-function or technology level), which in turn will be used to assist with establishing business-process and technology priority levels, recovery objectives, and an order of recovery. This process is designed to reach preliminary conclusions in days, as opposed to many weeks, using the input of business leaders throughout the organisation.

Regarding an alternative for the comprehensive continuity risk assessment, a business continuity steering committee and/or project team can define a realistic worst-case scenario to inform an abbreviated scoping and planning process. The scenario, which should impact the entire organisation, can provide a framework to assist planners with developing response and recovery strategies. The value in this approach is found in the streamlined manner of identifying the numerous impacts of a disruption without dissecting each type of triggering event. Many organisations have found that using a worst-case scenario can help them plan for less-impactful events.

While substituting a risk assessment and BIA process with an abbreviated approach will not result in a thorough understanding of all risks and impacts to the organisation, the examples noted provide a way to jump-start the planning process, particularly when the organisation faces a distinct deadline or management has not formally endorsed the BCM process. Going forward, the abbreviated processes should be refreshed with more thorough analyses that consider information and perspectives from multiple levels within the organisation.

Q 20 Are there ways to make the BCM planning process more efficient and effective?

The focus of any continuity planning effort should address the most relevant threats identified during the continuity risk assessment and consider impacts identified through the BIA. Not every area of the business needs to be prepared for every type of event or have the same level of rigour applied to continuity planning. Companies should consider being more thorough on their most critical business lines and apply a lighter touch (e.g., less frequent, or less rigorous maintenance or testing) for less critical areas of the business. Ensuring alignment of the recovery priorities and subsequent plans will enable a more efficient response and effective recovery. The business continuity plan should address the facilities and resources necessary to enable effective business continuity operations.

A common approach for recovery planning is focusing on extreme but plausible (i.e., worst-case) scenarios. Plans based on extreme but plausible events should also allow for flexibility in their implementation to allow for use during less-impactful situations. Alternatively, organisations may choose to mitigate likely scenarios by implementing a scenario-specific incident response plan (IRP) that aligns with risks associated with events that may be highly likely and highly impactful. Examples of these events include hurricanes along the Gulf Coast, earthquakes along the West Coast, or tornados in Tornado Alley. In these instances, the existence of plans that were developed for a likely event improves awareness of what to do, can lessen the risk of harm or severe injury, and can be worth any upfront cost associated with planning or training.

Consideration may also be given to using checklists and flowcharts to summarise response and recovery procedures, as opposed to more robust narratives. If the necessary steps are clear, the likelihood that those steps will be followed is higher. The use of checklists and flowcharts may also shorten any review and revision cycles needed as part of program management, as the amount of editing and formatting will be reduced.

Lastly, it is recommended that tests (or exercises) of the teams are used as opportunities to "break the plan." A focus on continuous improvement should allow the program to progress as areas for improvement are captured. Companies should consider a thorough approach for critical business lines and processes that include end-to-end testing and apply a less rigorous testing approach to those business lines or processes that are considered less critical or nonessential.

Q 21 What is the difference between crisis management and crisis communications?

Crisis management is an entity's overall effort to stabilise and prevent further damage after an unplanned event. Crisis management takes place at all organisational levels, beginning with executive management. It includes initial efforts from all departments, such as communications and public relations; regulatory affairs; environment, health and safety (EHS); human resources; legal; corporate security; and all business units.

Crisis communications is a crucial component of crisis management. It encompasses all communications before, during and after an event, including targeted communications to employees, customers, community, regulatory agencies, shareholders, the board of directors and all others who may be affected by the situation. These communications can be deployed during any type of event that may be deemed a crisis, from a product recall to a data centre fire. The trend in crisis communications is to have multidisciplinary teams for internal and external communications working together on messaging. Public relations, sales and marketing, communications, legal, human resources and investor relations may collaborate to develop and deliver internally and externally directed messages.

This example illustrates how crisis management and crisis communications can work together:

After a manufacturing director is confirmed to have been infected with a severe and highly communicable disease, EHS notifies the crisis management team that the director's temperature was on the rise throughout the week but there was no concern about the virus until additional symptoms surfaced. The director oversees two manufacturing plants and is consistently in the corporate office for meetings. EHS informs the crisis management team that the director was on-site at all three locations throughout the week. The crisis management core team makes the following decisions:

- The CEO decides to close both factories and the corporate office until further notice.
- General counsel advises the CEO to require testing for all employees before reopening the facilities.
- The CFO determines that the organisation should pay employees regardless of the shutdown.
- The CRO notes the various regulatory implications that could result from the outbreak.

The crisis communications team takes the next step to communicate all decisions internally to employees and to release a statement to external stakeholders (customers, shareholders and regulatory bodies).

As shown in this example, crisis communications processes are dependent on decisions made by the crisis management team, which acts as a liaison between the business and internal and external stakeholders.

Q 22 How do you integrate social media into the crisis communication strategy?

If an organisation uses social media channels to communicate with its customers, clients and other key stakeholders during normal business activities, those channels should be integrated into its crisis communications strategy. If an organisation does not use social media during normal operations, a crisis event is the wrong time to start.

While it can be a very valuable tool, the use of social media involves considerable risks. Certain information should not be shared on social media due to the potential for sensitivity and compliance risks. When engaging with the public over any social media platform, there are reputational risks that also need to be considered.

In a crisis, effective social media communication requires a higher level of care and management than during normal operations. Organisations should have a set of instructions prepared in advance for how social media will be managed during a crisis, with consideration given to publishing approvals and content authorisations, compliance matters, and reputation management. Those instructions should include using a more rigorous social media control structure for the duration of the crisis. The control structure should include employee guidance and reminders on how individuals should use social media during crises. Social media policies should state clearly — during a crisis and at any other time — which individuals and, by extension, shared accounts are authorised to speak for the business.

Among its advantages, social media offers employees an opportunity to connect and network as part of various subgroups, a dynamic that can promote ad hoc connections, especially during a crisis. Employees can also assist each other, using social media, in recovery of a business or even to recover personally from an event. While only semi-sponsored from a business standpoint, these channels can be well-received and efficiently "tagged" by the company's official social media accounts to raise awareness and share information to a wider audience.

> "Technology is a primary tool for enhancing organisational resilience. Software as a service (SaaS). Remote desktops. Public cloud providers. Internet of things (IoT). These technologies have had a significant impact on the ability of an organisation to withstand adverse events by, among other things, enabling the decoupling from a desktop, decreasing concentration risk, and providing enhancements in the storage and availability of data."
>
> — Kim Bozzella, Managing Director, Global Leader of Technology Consulting, Protiviti

Q 23 Do you need a business continuity management software/system (BCMS) to develop an effective BCM program?

Not necessarily. For organisations that are building an enterprise BCM program from scratch, buying BCM software is not the recommended first step. A software's structured nature can force users into providing generic responses to crucial discovery questions and important planning phases where some level of variance can be valuable. Another hazard with BCM software is the false sense of security it may provide teams that rely solely on it.

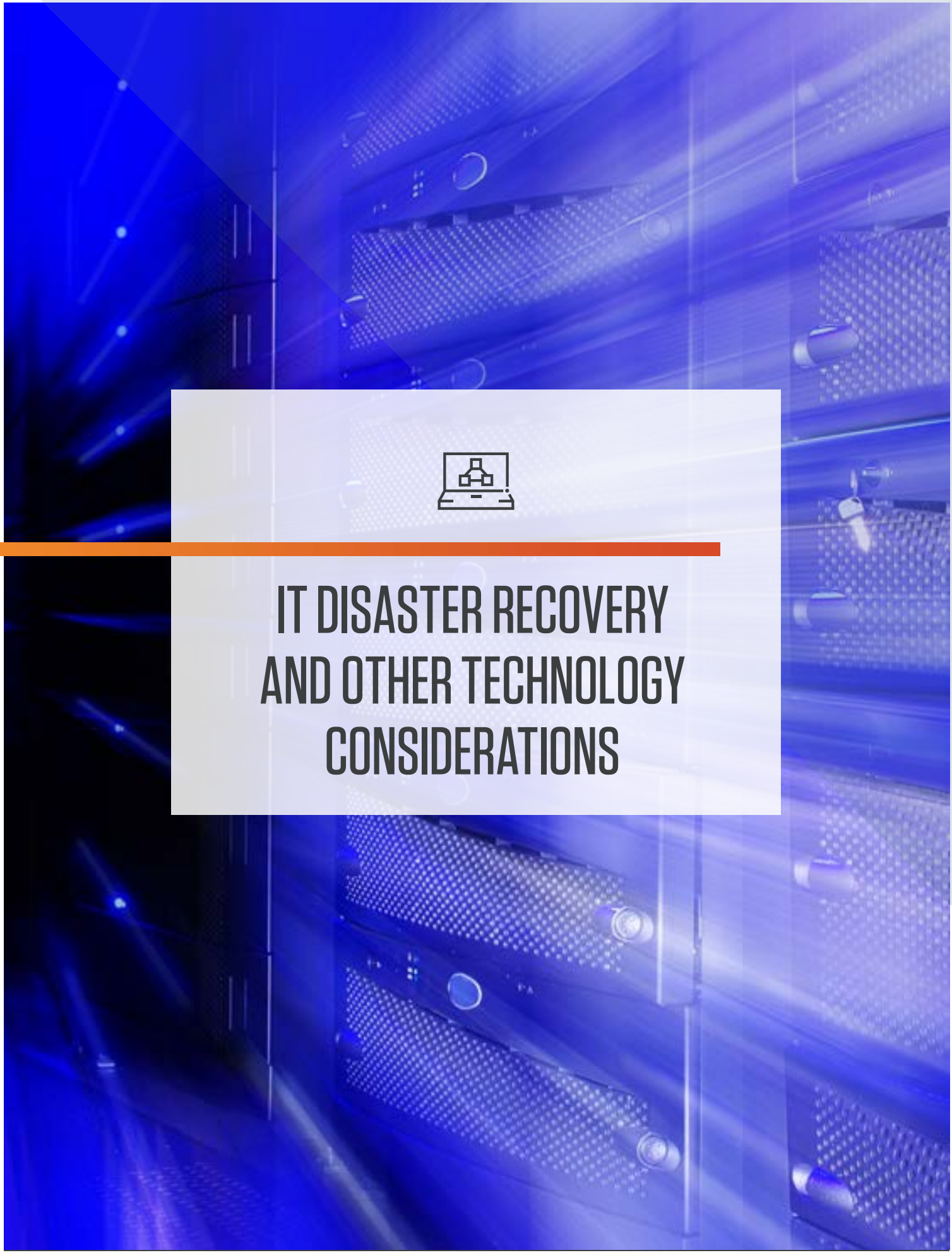
Organisations that do not have concerns related to regulation or complexity can run an effective BCM program with office productivity software paired with a knowledge management application that may already be in place and familiar to the employee base. However, BCM software can be valuable for:

- Highly regulated businesses like financial services or insurance providers. There, a centralised BCM application and plan repository may simplify adherence to compliance obligations.
- Enterprises that have multiple processes, many international locations, varying jurisdictions, or diverse geographical threats. Such organisations will likely benefit from using centralised BCM software to manage the complexity of their BCM programs.

For organisations that use BCM software, it is important to remember the application is a means to an end. BCM software does not guarantee an effective BCM program or a cohesive and effective response. Organisations might also consider leveraging a managed services model, in which a trusted third-party partner handles business continuity and resilience management and solutions.

Lastly, businesses should treat the BCM software acquisition as they would any other application: analyse business requirements to guide a diligent application selection process, include the system in the company's third-party risk management (or vendor management) process, and budget for additional headcount to support and maintain the system and data post-implementation.

> One way an organisation can improve its continuity impact assessment process is by taking a scenario-agnostic approach and focusing on the disruption-event impact on critical business processes, key personnel and supporting technology. Establishing a repeatable process that focuses on the impact vs. the cause of the disruption will help you identify, track and manage these risks on an ongoing basis, and will serve as the foundation for well-constructed response plans.
>
> — Matthew Watson, Managing Director, Protiviti



IT DISASTER RECOVERY AND OTHER TECHNOLOGY CONSIDERATIONS

Q 24 What are some of the key considerations when developing Information Technology Disaster Recovery (ITDR) strategies?

The first consideration when developing a comprehensive set of ITDR strategies is to ensure they are aligned with the organisation's business continuity requirements. It is not uncommon for IT teams to drive priorities while inadvertently being misaligned with the business needs.

The impact on customers when systems fail is also paramount. For instance, depending on the organisation, customers may tolerate disruption to, or unavailability of, services for some time. In other cases, customers may take their business to competitors without notice. Teams should consider the cost of a lost sale and how committed the customer is to the relationship (e.g., airline customers can easily take their business to a competitor, but a financial services client would face a more onerous task of switching).

Organisations should consider their respective industry regulations (e.g., HIPAA, FFIEC guidance, etc.) and ensure the ITDR plan is in compliance. It is not unusual for one instance of noncompliance to intensify the scrutiny of regulators overall. Any instance of noncompliance puts a brand's reputation at risk.

Another consideration is cost versus benefit. ITDR strategies should always weigh the degree of resilience against the cost to achieve it. A complete, immediately available backup of every system is ideal but might not be feasible from a cost perspective. Too often, failure to proactively invest in adequate ITDR capabilities before a disaster event winds up being a costly miscalculation after the event has occurred and the full cost is realised.

The role of third parties, especially SaaS and cloud providers, in the organisation's supply chain and their own technology resilience are important parts of an integrated operational ecosystem. Teams should understand what recovery capabilities are stipulated in formal agreements and confirm that vendors can keep those commitments.

Additionally, teams need to consider the volume, latency and sensitivity of data consumed and processed by each system. These factors guide decisions about the location of technical recovery capabilities and how current the data needs to be when it is recovered. If the ITDR strategy includes co-location facilities, it is prudent to consider data volume versus available bandwidth and the speed with which data must be restored.

The baseline hardware requirements of each system are important. One common mistake is to use decommissioned equipment for backup. Often, as systems are updated and their usage and data sets grow, these older platforms become inadequate.

Lastly, consider the skill sets of the technologists designated to support recovery operations, focusing on whether they can actually be made available and are sufficiently equipped to resume operations as rapidly as the business needs.

Q 25 What should disaster recovery planners consider when choosing primary and alternate sites?

In the past, BCM practitioners had a rule of thumb to have primary and alternate sites at least 30 miles apart (i.e., out of region). These days, decisions about siting are more likely to depend on an organisation's risks and the nature of its systems and data. Given the current low cost of bandwidth and the availability of multiple viable options, organisations have more latitude in selecting primary and alternate sites. Still, the following factors should be considered when making siting decisions:

- A system's function should drive requirements for backup location. For trading systems, for instance, the transaction speed and data volume would require high-performance network connectivity between sites. Other systems may be less demanding.
- Businesses should be prepared to move systems to alternate sites if the primary location is exposed to disasters such as a flood, earthquake or hurricane. A single event could impact a wide geographic area of potentially

hundreds of miles. If this is likely or an unacceptable risk, then the alternate site should be outside the risk area. Likewise, risks such as terrorism, geopolitical instability and unstable infrastructure in a particular region could have a significant impact on a data centre.

- Regulators may specify requirements for siting data centres, disaster recovery sites, alternate offices and business resumption centres. Some requirements may be relaxed if regulators can be assured that the business has comprehensively assessed and documented its own risks and demonstrated diligence by refreshing its plans and assessments regularly.
- Location of staff has historically been a major consideration in siting primary and alternate data centres, but it is less important more recently. The COVID-19 pandemic has shown that businesses may not need staff located near alternate sites. The staff's ability to access facilities in extreme weather is constrained if co-location is part of the disaster recovery strategy.

If a business's systems interact with the public via the internet, alternate sites need bandwidth equivalent to the primary site, so failover is transparent to the user. Bandwidth is an even more significant factor when backups are not updated in real time; recovery in these situations involves transferring large volumes of data swiftly.

Cloud computing provides an attractive alternative to owned and operated data centres, or even hosted data centres. Cloud providers often concentrate multiple data centres within a region, enabling them to respond effectively to localised issues. These concentrations may be repeated in other regions to create an exceptionally resilient network that is responsive to failures at any single location.

Data replication strategies can also impact the desired distance between primary and alternate sites. Synchronous replication might be safe for an application's most critical data, while less critical data could be replicated asynchronously.

Q 26 How is advancement of technology changing disaster recovery planning considerations?

The availability of robust, secure cloud solutions for disaster recovery represents a fundamental shift in disaster recovery planning and an opportunity to increase operational resilience. Cloud solutions can be more secure and provide better failover capabilities than businesses can accommodate with their on-premises environments.

For organisations that employ cloud technology for their production environments, resiliency and recovery are intrinsic to the platform, and disaster recovery (DR) capabilities are easily added. It is essential for these organisations to possess the expertise to govern and manage cloud implementations, keeping requirements of business process owners in the forefront. When businesses attend to these concerns, configuration of DR features in the cloud is reasonably straightforward.

There are businesses that cannot consider cloud solutions for disaster recovery. Disaster Recovery as a Service (DRaaS) is another way for such businesses to offload risks associated with hosting and operating their own data centres, and they can usually do so at a lower cost.

Whether a business pursues an on-premises or cloud-based DR solution, testing the chosen platform is critical to demonstrating that failover and related processes are designed, documented and executed as expected. Organisations taking advantage of DevOps practices already benefit from an automated approach to developing, building, testing, and configuring and deploying software. DevOps also provides a high degree of confidence that systems will run effectively in any environment to which they are deployed. Businesses that do not follow DevOps practices will want to pay greater attention and carefully manage risk related to design, development and deployment of systems that grow organically or ad hoc, or that are deployed via manual processes.

It is also worth noting that edge technology is growing in popularity in the context of DR planning. Where high availability is important, organisations push systems and content to providers all around the world. This approach limits the risk of overloading a central data centre. Data can be stored and processes run at these remote points, providing an extra level of resilience for highly available systems and services.

Q 27 What are some key considerations for pursuing Disaster Recovery as a Service (DRaaS) or other disaster recovery vendor solutions?

There are many solutions for setting up internally owned and managed disaster recovery capabilities or engaging with third parties at varying levels — from specific services/parts of the solution to an entirely out-of-the-box managed services model provided by an outside firm.

Disaster Recovery as a Service (DRaaS) provides a way for businesses to enhance their technology resilience by offloading risks associated with hosting and operating their own data centres, usually at a lower cost.

Well-documented, clear requirements are essential to managing DRaaS costs. Detailed requirements should correspond to line items comprising the overall price, which may build in an added level of rigour and discipline to DR planning for some organisations.

DRaaS works most effectively for common technologies that vendors can easily operate and manage. When systems are customised or tightly integrated with other elements in the technical environment, they are more challenging for the vendor to support. DR teams should also consider whether the production environment is using old, unusual or highly specialised equipment, and should integrate the appropriate level of due diligence when finding vendors who have that same equipment available. For cases like these, businesses still have the option to engage providers who address data recovery, while retaining responsibility for infrastructure recovery in-house. However, infrastructure recovery can also be supported by vendors. Here, the challenge is to ensure that the system runs as well on the vendor's platform as it does in the business's production environment.

When choosing DRaaS, data recovery and infrastructure recovery solutions, a business needs to examine its requirements in the context of cost versus time to recover. Traditional cold sites have equipment standing ready to be configured and updated when they are needed. Warm sites have servers ready for installation of production environments. Hot sites are set up for immediate use, with up-to-date systems and data ready for failover.

With the variety of offerings for ITDR support in the market now, businesses have more options than ever. The key to success is knowing requirements, documenting them in a detailed way, and seeking the managed technology services providers or other vendors whose capabilities best match the needs of the business.

Q 28 How can organisations leverage cloud services as a viable disaster recovery solution?

Cloud-based solution providers offer a wide array of options, so businesses can allow their own disaster recovery (DR) strategies to drive their selections. Start with an assessment of the business's own capabilities versus the resilience it needs. Consider size, budget and maturity level of the organisation, as well as DR requirements particular to the business.

For organisations whose DR strategy is already sound, implementation of cloud-based solutions can be straightforward and rapid. Among the multitude of options, cloud-based DR solutions fall into two fundamental categories:

- High availability and hot-hot resilient services, where a business's servers and data are replicated from the primary to the secondary data centre with the shortest possible recovery time. This approach takes advantage of cloud-native features and offers configuration options so businesses can establish their own resilience parameters. To duplicate these capabilities without cloud-based services, a business would need three or more instances of its production infrastructure, located in various regions, each with staff on site. In these terms, the value of cloud-native architecture for DR is clear.
- Data recovery and backup, whereby businesses can back up their data to the cloud over an Internet or direct network connection. This solution relieves businesses of the responsibility for managing various forms of media as well as the data backup and recovery

storage infrastructure, but they'll remain responsible for restoring the backed-up data to infrastructure in the event of an outage. Therefore, cloud-based data backup only partially meets DR requirements for most businesses. Cloud providers who only offer data recovery and backup are beginning to lose ground against competing cloud providers who offer more robust, high-availability solutions, raising questions about the long-term viability of a data-only approach.

Q 29 How does switching to a cloud-based disaster recovery solution affect risk in the organisation?

While a cloud-based disaster recovery (DR) solution introduces risk associated with storing data outside the organisation, that risk is offset by the resilience gained by adopting a cloud-based approach to DR. Cloud providers invest significant resources into security measures, both in the latest security technologies and in the skills of their personnel. Adopting a cloud-based approach to DR could increase an organisation's risk tolerance from a variety of perspectives. Organisations that adopt cloud-based DR can benefit in the following ways:

- The cost of DR testing in the cloud is usually lower than it is for organisations with owned or hosted data centres, increasing the organisation's appetite for more frequent tests. More frequent tests result in more resilient environments.
- Cloud-based DR environments can be set up on demand, so the organisation is freed from hardware procurement processes (including selection, negotiation, ordering, installation, configuration and provisioning), as well as procurement costs and delays. This vastly increases the flexibility of DR environments, facilitating nimbler modification of systems.
- Cloud-based DR environments provide resilience faster and at a lower cost, so organisations can launch new products without compromising the DR strategies. This enables businesses to meet regulation-driven resiliency requirements with little additional overhead.

Ultimately, organisations incur the risk of storing data outside the organisation in exchange for superior resilience, greater flexibility and lower overall risk. Organisations are unique in their security needs and regulatory requirements and should evaluate cloud-based DR's advantages from the perspective of these factors.

Q 30 What approaches are available when leveraging a cloud solution for disaster recovery?

The approach any organisation takes to leveraging a cloud-based disaster recovery (DR) solution will depend on the organisation's rate of adoption of the cloud strategy. Organisations that already host applications on cloud platforms will want to take advantage of the built-in features their cloud providers offer.

Organisations not yet in the cloud may want to offload responsibility for operating their own disaster recovery data centres and instead turn to cloud providers that specialise in services like these, with approaches varying from full-scale to point solutions. It is not uncommon for organisations to embrace the cloud version of the application, as resilience is often a benefit associated with a move away from an on-premises strategy. If a vendor offers a cloud-based service for their application, it is possible to run the system with the cloud version of the application as a backup.

Approaches to adopting cloud-based DR vary by degree of reliance on integration with cloud technology. In other words, solution options vary by the degree to which an organisation chooses to take advantage of cloud technology's intrinsic benefits. To take greatest advantage of these features requires fundamental changes to the organisation's system architecture.

Approaches can be broadly considered by increasing degrees of cloud integration:

- Cloud-based DR as an additional data centre requires configuring a cloud environment to emulate the on-premises data centre. This approach replicates servers, processes and all other components of the physical environment to enable swift and smooth transition when needed. Organisations can specify that the cloud environment be set up in advance. This approach of treating the cloud as another data centre and preconfiguring it is more sophisticated and complex than many organisations require, but it can represent dramatic cost savings for some applications and some use cases.
- Cloud-based DR takes advantage of cloud-native offerings, including snapshots, data replication and other services. Cloud-native applications are built with a high degree of automation and resilience in mind. Cloud-native applications are designed to be more resilient, as failover can be instant and transparent for the best-available resilience of systems. In comparison, applications designed for DR in a traditional data centre are typically reliant on manual monitoring and recovery activities.

Q 31 What are some key considerations for selecting and/or negotiating hosted solutions or disaster recovery support?

Selection of a disaster recovery (DR) solution depends primarily on an organisation's specific technical recovery needs. Cloud-based DR providers offer superior capabilities and security, but it is unusual for a cloud provider to negotiate anything at variance with their standard service level agreements (SLAs). In many cases, organisations that use unusual or older infrastructure may find cloud providers do not offer customised solutions that allow for a company's architectures or nuances. In these instances, these companies must rely on traditional DR providers that are constrained by the physical hardware in their data centres. Organisations can also engage a third party, such as a managed services firm, to oversee their cloud-based DR, placing the third party between themselves and the provider to bolster the SLA with additional services. When selecting cloud-based DR providers, companies should ensure the provider can scale to accommodate the organisation's needs and, if so, understand how, and how quickly, that scaling is accomplished.

Whether they choose cloud-based or traditional DR providers, companies should ask the following:

- How long can the organisation run in DR mode? Standard contracts may specify a week or two. Organisations should consider whether that duration is enough and must understand the implications if that timeline is exceeded.
- Can the provider assist with failback (i.e., restoring data saved or modified in DR mode back to the primary environment)?
- How is DR testing conducted, and how does the provider support those tests?
- How is the provider's technology and physical space used when the organisation does not need it? Do the provider's facilities function as primary for one customer and secondary for another, for example?
- How does the provider handle events that require simultaneous recovery of multiple systems? If the provider has several clients in a DR situation at the same time, how are they prepared to address that circumstance? To what extent can the provider abide by the SLA in extreme circumstances or when the organisation may be competing with the provider's other customers for the same resources after a large-scale or regional disaster?
- Is the hot site also used as a primary site for other clients, thereby calling into question whether it is always available? Sites used only for DR — and thus unused for periods of time — may not function as planned when needed.

- Can the provider (or the organisation's own team) configure infrastructure remotely? In the absence of this capability, DR infrastructure can "drift," causing a misalignment with the production environment.
- Does the provider stay current with new versions of hardware, operating systems, middleware and other infrastructure components?
- What are the costs related to testing and other processes to exercise the infrastructure from time to time? These are sometimes overlooked in negotiations, but they do require time and resources on the part of both providers and their customers.

Ultimately, when choosing cloud-based or traditional DR providers, it is important to be clear and detailed about delineating responsibilities.

Q 32 What other requirements and recommendations should organisations consider as part of their IT governance practices?

There are numerous BCM-related resources that may offer guidance, requirements and/or recommendations which apply to most companies. For instance, most of the well-known cybersecurity standards (e.g., NIST CSF, ISO 27001, CIS CSC) focus not only on the confidentiality and integrity of data but also its availability. Additionally, the increased focus on privacy with the introduction of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) has heightened the focus on not only how to maintain continuous access to data subject information but also how to ensure privacy protections regardless of how or where the data is stored.

The expectations on IT leadership of both public and private sector organisations for improved preparedness are higher than ever before. Additional government and industry bodies and/or requirements and control standards for technology components of business continuity and crisis management are listed in the regulatory sources in the Appendix.

> A BCM best practice is enabling the chief operations officer to engage board members and discuss the potential shocks to business processes and systems throughout the enterprise. Gaining additional perspectives provides all constituents with a more thorough understanding of the crucial importance for establishing BCM plans and simulating situational impacts. Conversations about how the organisation manages cybersecurity risks or responds to a ransomware attack are just a couple of examples of why broad executive perspectives are necessary.
>
> — Terry Jost, Managing Director, Protiviti

THIRD-PARTY RISK MANAGEMENT AND BCM

Q 33 How do sourcing, outsourcing and procurement strategies impact business continuity and operational resilience?

An organisation's approach to sourcing, outsourcing and procurement has a direct impact on its ability to maintain business continuity. If the sourcing and procurement strategy focuses exclusively on driving down costs, organisations may find themselves sourcing from fewer providers to leverage spend and increase buying power. Relying on fewer vendors increases the risk, however, should any one vendor be unable to support their customers due to a disruption and an inability to recover promptly. Organisations should consider all aspects of a vendor's capabilities and total cost of ownership, including business continuity, and not consider cost alone when selecting vendors. They should also evaluate "fourth-party" vendors, vendors/suppliers of the organisation's key vendors, where feasible. Examples of fourth-party vendors are prevalent in the technology space and could include Amazon Web Services or Microsoft, which may host critical SaaS products.

Organisations in heavily regulated industries must understand specific requirements and obligations as they pertain to third-party management, including requirements for business continuity management and disaster recovery capabilities and plans. These considerations, including risk assessment, due diligence, contracting requirements and ongoing monitoring, must be addressed as part of the sourcing and vendor selection process. In addition, regulators increasingly are focusing on fourth-party risk, as noted above.

Outsourcing is especially impactful on an organisation's business continuity capabilities. Executives sometimes develop blind spots when they assume that outsourced providers are managing their own business continuity effectively and when estimating the impact that out-sourced provider operations and processes can have on their own internal processes. As a result, organisations do not typically apply the same level of rigour and over-sight to outsourced functions as they would to internal functions. The inclination to assume outsourced vendors are managing business continuity effectively grows more hazardous as organisations increasingly rely on outsourcing. It is prudent for organisations to understand contingencies that may need to be employed as they relate to any third party deemed critical.

Q 34 How should organisations identify and prioritise vendors to manage business continuity effectively?

Ideally, all new and prospective vendors go through a risk assessment process that addresses the inherent risks across applicable risk domains (including business continuity) associated with the service or category of spend being addressed. The results of the initial risk assessment, combined with vendor criticality — as identified through the BIA — should dictate the level of due diligence required, with results of the due diligence culminating in segmentation and tiering. The vendor segmentation should then drive contract considerations and specific requirements, as well as frequency of ongoing monitoring. Segmentation and tiering will dictate whether, and how often, the organisation reviews and tests vendors' business continuity plans. The riskiest or most critical vendors might be reviewed every quarter, where the least risky or least critical vendors may be reviewed only every year or two.

When considering management of vendor relationships, organisations can prioritise based on the difference between transactional dealings with vendors of commodity goods and services that can be readily replaced, versus more strategic relationships, where the cost, time frame and complexity of switching providers is more severe. These more strategic vendors should be prioritised and more actively managed as part of an organisation's overall business continuity posture. Organisations should assess if their strategic vendors' business continuity plans are aligned with the

organisation's own strategy and should evaluate how these vendors manage their plans in terms of oversight, testing and other factors.

For vendors that supply goods — particularly goods that contribute to an organisation's finished product — businesses should assess the revenue generated from the finished product to determine the criticality of the vendor's goods to production and prioritise accordingly.

For information technology vendors, considerations should include whether the vendor will access the organisation's network or share data, what software is used to perform tasks on the network, how many business users rely on the vendor-provided service, and what business process the service supports. The vendor's responses may trigger more questions to understand the vendor's systems and protocols better. How is the application developed and hosted? Do they test the application regularly? Does the vendor have practices in place to recover systems quickly enough? Does the vendor rely on other key vendors/suppliers (fourth parties) to deliver the service to the organisation?

Q 35 Why is it important for organisations to understand and assess their vendors' business continuity plans and capabilities?

Organisations can enhance their in-house recovery strategies if they have a better understanding of their vendor's contingency plans. Having a high level of comfort in a vendor's plans and how those plans are validated and tested means the company may not need to put as much time and resources into a particular element of planning. Also, knowing how those critical vendors will respond to a disruption can influence the organisation's recovery activities.

The criticality of any good or service, and the probability and impact of vendor outages and disruptions, are likely considered as part of the organisation's BIA, where each vendor is assigned a level of criticality and, perhaps, a recovery time objective (RTO).

Business continuity procedures should include documenting whether a vendor possesses or will gain the capabilities to ensure they can provide goods and services within agreed-to SLAs. Additionally, as vendors are onboarded, they may be segmented and tiered according to the inherent risks to govern the depth and extent to which any vendor's business continuity capabilities will be overseen and reviewed.

All of these actions can be reinforced by having frequent, open communication between the organisation and the vendor. The first step is requiring all critical vendors to have defined relationship owners on both sides. These relationship owners can communicate expectations, assist in monitoring performance against agreed-upon measures and contract terms, and actively participate in plan development, exercising and gap resolution.

Q 36 How should a business continuity program consider the impacts of disruption to vendor or supply chain partner operations?

An organisation's business continuity plan should document its vendors' or trading partners' abilities to identify, respond to and recover from potential business interruptions. The process starts with identifying what potential risks could lead to an interruption of services delivered to consumers or disruption of the entire supply chain. The process must consider all components and contributors to the consumer service or to the supply chain.

Business continuity planning typically assesses the probability and impact of any threat. It is important, however, to consider unlikely threats as well. These are sometimes called black swan events — unexpected outlier events with severe consequences that are extremely difficult to predict. Those organisations adopting operational resilience practices should already be planning and exercising for "extreme but plausible events." Defining and testing risk response strategies in anticipation of both likely and unlikely events protects organisations from undue struggle and chaos when a crisis is underway; they would only need to execute on the plans already developed.

Q 37 Should vendors' business continuity plans and capabilities be tested? If so, how often?

When an organisation tests its business continuity plan, either as a tabletop exercise or a thorough dry run, the vendors supplying critical goods and services should participate. Vendors with roles in the organisation's disaster recovery strategy should collaborate on periodic cutover testing. Organisations should also seek opportunities to participate in their vendors' testing where and when appropriate.

Assessments of vendors should include evidence that they have sound business continuity programs and that those programs include rigorous testing, followed by a review of test results to demonstrate that the vendor can meet the organisation's recovery time objectives.

Where a vendor's outage could have a high impact on the organisation, such tests might occur as frequently as annually. Where vendor relationships carry less risk, testing might be conducted in alternate years. Relationship owners on both sides should work together to determine the frequency and depth of testing and how they will participate.

> In the financial services industry, financial institutions are more focused than ever on operational resilience, of which business continuity is a key component. The highly interconnected nature of banking environments creates significant concerns about the ability of a contagion to disrupt banking services. Similar concerns are emerging in other industries, underscoring the need for a continuing focus on business continuity and resilience.
>
> — Ali Yasin, Managing Director, Protiviti

REGULATIONS, STANDARDS AND GUIDANCE

Q 38 How should regulations and standards shape the development of a BCM program?

BCM regulatory requirements and standards are increasingly being enhanced in response to a growing focus on corporate governance and risk management and the devastating impacts on the business from technology disruptions and catastrophic events. The enhancements are designed to help organisations develop more effective continuity responses to the evolving threat landscape, including providing enhanced protection for employees and all those who depend on an organisation's services (e.g., customers, clients and patients, third parties).

Regulations and standards are used to drive BCM program development, measure adherence and assess an organisation's resilience maturity. While regulations and standards often provide guidance on required or suggested controls, areas of focus and approaches to BCM, they rarely dictate specific items, formats or levels of detail in planning documentation. The most comprehensive guidelines and standards are geared toward financial services. Using these more rigorous guidelines, it is not uncommon for other industries to apply the relevant controls and strategies as they model their BCM program against best practices.

Q 39 What specific guidance does the Federal Financial Institutions Examination Council (FFIEC) provide regarding BCM?

The FFIEC standard is recognised as one of the most stringent BCM standards in the U.S. marketplace. It places significant emphasis on governance, risk assessment, BIA, planning, recovery, resiliency, testing and maintenance requirements. It also contains a section related to senior management's business continuity responsibilities, which is a helpful reference for any company and an indicator that BCM is no longer something that is just taken care of by back-office technical teams.

Many organisations, including non-financial services entities, model their BCM programs after the FFIEC standard. Originally published in 1996, the standard was significantly expanded in 2003, 2008 and 2015, and most recently refreshed in November 2019. Although still listed in the category of IT examination, the FFIEC standard states that BCM should be based on "enterprisewide, process-oriented approaches that consider technology, business operations, testing and communication strategies critical to the continuity of the entire entity."

Additionally, the 2019 update changed the booklet title from "Business Continuity Planning" to "Business Continuity Management." The update reflects the changes in customer and industry expectations for the resiliency of operations. Further, the booklet emphasises that "business continuity should not be focused only on the planning process to recover operations after an event, but rather it should include the continued maintenance of systems and controls for the resilience of operations. Business continuity should be incorporated into the risk management lifecycle of all systems, applications, services, business processes and operations of an entity."

The points below summarise the FFIEC guidance regarding developing the scope of an effective and efficient BCM program and establishing a repeatable lifecycle:

- Effective BCM governance depends upon the involvement of the board and senior management to set the tone and establish a culture of resilience across the business.
- BCM elements should align with strategic goals and objectives and underpin broader operational resilience objectives of an organisation.
- A thorough BIA and risk assessment should form the foundation of a comprehensive BCM program and identify the maximum tolerable period of disruption where harm would be caused to the customer, firm and market.
- A BCM program should include strategies that meet both recovery and resiliency objectives to remain within impact tolerance.
- The BCM program should be developed on an enterprisewide basis and incorporate incident response, disaster recovery, business resumption, operational resilience and crisis/emergency management.

- A BCM training program should be implemented for personnel and other stakeholders.
- The effectiveness of the BCM program should be validated through annual, or more frequent, testing, capturing lessons learned and opportunities to improve the overarching resilience of an organisation.
- The BCM and test program should be thoroughly documented, evaluated by institution management, independently reviewed by an internal and/or external audit function, and reported to the board.
- The BCM and test program should be updated to reflect and respond to changes in the institution and gaps identified during continuity testing.
- Other financial institution policies, standards and processes should be integrated into the BCM program.

Rather than stipulate a series of "do's and don'ts" with explicit requirements, the FFIEC booklet provides companies with practices to make robust assessments of their needs and reasonable judgments on the composition and content of their BCM programs. For example, following their discussion of institutions serving critical financial markets, the FFIEC suggests that the BCM program and its critical elements be based on an entity's size and complexity and aligned with the financial institution's business strategy and risk appetite.

Q 40 What are ISO 22301 and ISO 22313?

ISO 22301, published by the International Organisation for Standardisation (ISO) in 2012 and updated in October 2019, established an international standard that provides the structure and requirements for implementing and maintaining a BCM program. As with other ISO standards, ISO 22301 applies the Plan-Do-Check-Act (PDCA) model and focuses on the business continuity lifecycle. Organisations seeking ISO certification of their BCM program can do so by engaging an accredited third-party certification group. The ability to certify a BCM program and provide a degree of assurance to third parties (e.g., customers, clients, partners, regulatory bodies) with respect to the integrity of the program is an attractive proposition for a number of organisations.

The introduction of ISO 22301 essentially replaced BS 25999-2, which was developed by the British Standards Institution (BSI). In fact, ISO 22301 is an upgrade because it places greater emphasis on understanding requirements, setting objectives and measuring performance. Ultimately, organisations that have previously aligned their programs with the BSI standard should have a straightforward transition to ISO 22301.

ISO 22301 was designed to be applicable to all types of organisations. The principles are familiar to seasoned BCM professionals, but how the requirements are ultimately applied depends on the risk environment in which the organisation operates and management's goals and objectives.

ISO 22313, published in 2020, clarifies the concepts introduced by ISO 22301 with explanations and examples to assist organisations during implementation. While ISO 22313 does not introduce any new concepts or requirements, it provides a better sense of what an ISO 22301 BCM program looks like and how the standard can be applied.

Q 41 How does NFPA 1600 differ from more familiar BCM guidance?

NFPA 1600 is a standard published by the National Fire Protection Association (NFPA) that focuses on disaster management and business continuity. Headquartered in Massachusetts, NFPA is a standards-making body known for its NFPA 101®: Life Safety Code®, which governs most life-safety issues in commercial buildings across the country. It is common for local and state governments to adopt NFPA standards verbatim into their building and

life safety codes. The standard became especially significant after the federal 9/11 Commission recommended it as the National Preparedness Standard and encouraged entities such as insurance companies and credit rating agencies to include it in their evaluations of customers. The U.S. Department of Homeland Security (DHS) sponsors a resource known as "Ready Business" and has adopted NFPA 1600 as the American National Standard for developing a preparedness program.

Work on the NFPA 1600 standard began in the 1990s, with the first version published in 1995 and most recently updated in 2019. Unlike other standards and regulatory requirements, NFPA 1600 is industry neutral and even applies to the public sector. When it was first published, NFPA 1600 was three pages long and included elements of prevention, preparedness, response and recovery. Today, NFPA 1600 is a complete emergency management and business continuity standard that includes guidance on crisis communications, emergency operations centre (EOC) management and family preparedness.

There is no specific industry or class of organisation that is legally required to adopt NFPA 1600. However, many organisations use it to guide the development of their continuity and emergency response preparations. The standard is sufficiently flexible and can be adopted by all types of organisations (e.g., large, small, public or private), as it is structured on general recovery principles that would be found in an effective emergency management program (e.g., BIAs, crisis management, plan development, testing, training and education). Organisations can tailor the standard to their needs and build procedures specific to their recovery needs. The 2019 edition focuses on crisis management in general and crisis communications in particular, consistent with the distributed nature of the current workforce and the need to effectively communicate with both employees and external groups.

Q 42 How does the COBIT standard address BCM?

Control Objectives for Information and Related Technologies (COBIT) is a generally applicable and accepted standard for sound IT governance and management practices. The standard provides a reference framework for management and users, as well as for information systems (IS) audit and control and security practitioners. COBIT, issued by ISACA and now in its sixth edition (COBIT 2019), provides tools to assess and measure an enterprise's IT capability across one governance and four management domains:

- Domain 1: Evaluate, Direct and Monitor (EDM)
- Domain 2: Align, Plan and Organise (APO)
- Domain 3: Build, Acquire and Implement (BAI)
- Domain 4: Deliver, Service and Support (DSS)
- Domain 5: Monitor, Evaluate and Assess (MEA)

Business continuity activities are addressed primarily in the DSS04 domain/process area. The "manage continuity" process, as described by COBIT, is designed to "establish and maintain a plan to enable the business and IT organisations to respond to incidents and quickly adapt to disruptions." This process enables continued operations of critical business processes and required information and technology services, and helps firms maintain available resources, assets and information at a level that is acceptable to the enterprise.

Although COBIT tends to be IT focused in many process areas, the "manage continuity" process incorporates characteristics that include IT as well as business recovery activities. The DSS04 process is organised into eight practices:

- Define the business continuity policy, objectives and scope
- Maintain business resilience
- Develop and implement a business continuity response
- Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)
- Review, maintain and improve the continuity plans
- Conduct continuity plan training

- Manage backup arrangements
- Conduct post-resumption review

Each practice is supported with suggested activities, example metrics, references (e.g., National Institute of Standards and Technology (NIST) 800-53), typical organisational responsibilities, process inputs/outputs, recommended skills and corresponding policies.

Q 43 Describe the connection (if any) between the Sarbanes-Oxley Act (SOX) and business continuity.

When the Sarbanes-Oxley Act (SOX) was passed in 2002, management and auditors struggled with defining the scope of business continuity as an internal control related to financial reporting. However, as SOX compliance has become more commoditised for public companies, management and external audit firms have been able to come to a middle ground on this topic.

The most common business continuity-related controls in this area focus on system/data backups and periodic restorations of applications/environments deemed in-scope for SOX purposes. In other words, external auditors mainly want to gain comfort that management is backing up their key SOX-related systems and data on a regular basis and has methods of detecting and addressing backup failures should they occur. Further, it is not uncommon for external audit firms to confirm that management can restore systems or critical files from those backups, should the need arise. This can be evidenced by performing and documenting targeted restoration activities and proving that backed-up data is accessible and intact. Most audit firms have determined that specific business continuity or IT disaster recovery plans are not required by SOX regulations.

Regardless of how BCM and IT disaster recovery topics are treated within regulations such as SOX, most executive managers continue to advocate business continuity-related processes because they are viewed as sound business practices that are in the best interests of the companies which implement them. For service-oriented organisations (e.g., payroll services, business process outsourcing, cloud computing), business continuity is a topic that remains very near the top of the list when clients perform their annual vendor audits or issue-related audit questionnaires.

> “Organisations must consider unimaginable disruption scenarios as an essential component of their comprehensive crisis management program. The potential convergence of disaster events will require risk management functions to ask many bold questions. What if there is a regional power outage, with the digital infrastructure failing during a period of work from home with all the corporate offices closed? Do remote workers have the capability to perform their work given that multiple disaster events may be occurring simultaneously? What key infrastructure redundancies should be in place to address aggregate compounding disaster events that will ensure resilient enterprise operations?”
>
> — Damon Owen, Managing Director, Protiviti

TESTING, TRAINING AND MAINTENANCE

Q 44 What are the prevailing practices regarding the storage of business continuity planning documentation?

There is no one-size-fits-all BCM documentation storage approach. Storage practices should be guided by these two important considerations about business continuity plans: They should stay current, and they should be accessible to all personnel when needed.

A library distributed solely in hard copy would be difficult to keep updated and even harder to confirm that all personnel are referencing current versions as needed. For BCM documents, all employees should have access to the most current versions. Further, it is far easier for those tasked with maintaining the documents to keep a primary source updated, instead of multiple versions. Typically, BCP libraries are maintained on an all-company network file share, intranet/SharePoint site, or other employee and/or third-party portals.

While accessibility is key, it is also critical to maintain security over the library of risk assessment, impact analyses, strategies and planning details, and exercise results. These documents often contain proprietary and sensitive data, including names, roles, contact information, IP ranges, procedures and partners, among others. Companies that provide goods or services may also be requested to provide these documents in whole or in part and may or may not desire to share.

Considerations should be made to maintain the classification of these documents and to confirm appropriate controls are put in place to ensure they remain secure.

A library of planning materials should be accessible to personnel based on their role in the organisation, their responsibilities during recovery, or the processes they support. The prevalence of mobile technologies and ubiquitous internet access means most personnel carrying personal or company-issued smartphones and tablets can access these BCM documents through cloud-based document storage and SaaS BCM software solutions as needed.

Storage decisions should be made with the goal of enhancing how quickly employees consume content and can execute on the recovery and resumption procedures. Business resumption plans may be further segmented by end-to-end processes (e.g., periodic financial reporting functions), an entire workstream (procure to pay), or, even further, to the specific responsibilities by role. The goal of this segmentation is to make it as fast and seamless as possible for all personnel to find the parts of the plan that are most pertinent to them, and then to help those people understand the immediate inputs and outputs to their processes.

Q 45 How often should business continuity-related documentation be updated and how can organisations keep the plans current?

In general, business continuity documentation should be reviewed and updated at least annually. However, a more frequent review and update process may be required as changes in the organisation occur. The business continuity team should stay abreast of changes such as mergers, acquisitions, divestitures, entry into new markets, organisational restructuring, or the implementation (or retirement/sunsetting) of technology. Key factors to consider may include:

- Business unit and associated function listing and validation of criticalities as determined in the BIA, including reassessment of maximum tolerable downtime (MTD), recovery time objective (RTO), and recovery point objective (RPO) metrics
- Risks or threats that may impact key business operations
- Business unit/function dependencies/interdependencies (IT and non-IT)
- Adoption of new technologies, including migration to private or public clouds, implementation of new enterprise application solutions, retirement of legacy systems, etc.
- Opening/closure of key office locations or facilities
- Key employee/vendor contact information

- Changes to recovery strategies
- Permanent remote/hybrid work policies
- Resource requirements matrices, including insourcing or outsourcing and offshoring, nearshoring or onshoring of major functions and processes
- Onboarding of new key third-party providers
- Major changes to upstream or downstream supply chains
- Data, intellectual property and documentation storage locations, including cloud-hosted environments
- Changes to regulatory environment/reporting requirements

Given the decentralised nature of most business continuity programs, a cross-functional team should be responsible for maintaining the crisis management and crisis communications plans, as well as updating risk assessments and business impact analyses. Business function and technology owners should be responsible for their individual resumption and IT disaster recovery plans, respectively. These plans tend to focus more on recovery of a distinct process, set of processes, or specific technology stack. While responsibility for making plan updates may lie with various individuals and/or cross-functional teams, the BCM program coordinator should oversee all changes to ensure consistency with organisational policy requirements.

Regardless of the process used, maintenance should be based first on a defined schedule. If an organisational change management process is underway, BCM should be integrated into this program.

Q 46 How often should BCM plans be tested?

BCM plans should be tested as often as possible, but within reason. Management expectations, test objectives, the maturity of the planning process, and system/process criticality are all factors that drive how often to exercise a team and validate strategies and plans. Most organisations test business continuity processes once or twice a year; however, this can be increased due to factors such as:

- Changes in business processes
- Changes in technology, facilities or critical vendors/third parties
- Changes in business continuity or crisis management team membership
- Changes in executive management
- Anticipated or planned events, which may result in a potential business interruption.

Organisations may also choose to conduct more tests or exercises if operations are decentralised across multiple locations. Additionally, some business continuity coordinators may choose to conduct testing in stages, given the dispersion of their personnel, the size of their IT infrastructure, the size of the business, or their relative inexperience with ITDR or BCM testing. Others may decide to rotate as many people as possible through the training experience, via a test or exercise, given the valuable benefits. Regulatory requirements may also influence the number of tests performed annually.

Organisations should also follow up at least annually on the exercises performed by their critical vendors. Many vendor management functions will include this in a periodic review of vendor risk. However, as noted in other questions in this guide related to third-party disruption risk, all critical vendors should have designated relationship owners within the organisation who should also take an active role, as contracts will allow, in validating exercise activity and results. Where possible, joint participation in exercises on both sides of the relationship should occur.

Lastly, IT environments change rapidly. Plan coordinators should ensure IT disaster recovery procedures are updated in tandem with established technology change management procedures. When this occurs, alignment with recovery requirements of the business should be confirmed.

No matter how many tests are conducted each year, planners should schedule them well in advance to ensure maximum participation. Also, planners should develop a progressive, incremental testing schedule that includes a timetable of events.

Q 47 What testing options are available for BCM programs?

Testing options for a BCM program come in all shapes and sizes. (See the Appendix for a detailed list of testing options.) Regardless of the testing option employed, the BCM team should incorporate actual data and simulate real-world conditions whenever possible, and the facilitation team should develop test scenarios based on results from the risk assessment. Additionally, teams should not ignore unlikely events that could occur (e.g., COVID-19). If the organisation is new to BCM testing, it should start small and slowly work up the maturity curve. For example, management could begin by having tabletop discussions regarding various recovery scenarios with the business. From there, management could enhance the test to include a coordinated, sample-based recovery of applications, processes and departments, and graduate to perform a fully simulated test that includes restoring major components of the business and the supporting IT environment simultaneously.

Further, business continuity coordinators should be empowered to be original, to encourage engagement of their recovery teams, and to be creative during the testing.

The following creative measures may be considered:

- Facilitating a test like the Monopoly® board game. The test could then use "Chance Cards" to insert unanticipated variables into the test process.
- Inserting realism into testing exercises by asking key personnel to consider a localised or regional disaster (e.g., tornado or hurricane) that can result in key BCM team members or other personnel being shut out of the communication aspects of the exercise or to "sit out" the entire exercise. This would help evaluate how alternate personnel responds to the situation if key decision-makers are unavailable.
- Organisations should incorporate variability in testing approaches. Conducting the same test twice a year could lead quickly to stagnant outcomes, a lack of perceived value and bored participants.
- Organisations that are adopting operational resilience practices should also consider that their exercises use "extreme but plausible" scenarios and involve cross-functional teams of business, IT and vendor personnel, where appropriate.

Q 48 Should organisations expand testing beyond IT?

Organisations should create a testing strategy and policy that dictates standards and guidelines for both the business and technology teams and functions. All areas of the organisation can experience disruptions unrelated to the loss of technology (e.g., loss of key personnel, facilities, vendors) and need to be prepared.

For non-IT business continuity tests, companies should consider testing all other facets of their programs, such as crisis management and business resumption teams and corresponding plans. Applicable testing methods may include:

- Walk-throughs of existing plans with recovery teams
- Departmental or companywide simulations in which employees must execute crisis management and/or business resumption activities, using their plans as a guide to respond to defined scenarios (scheduled or unplanned)
- Cooperative exercises with key external partners and customers
- Industrywide exercises administered by local industry organisations, trade associations or service bureaus
- Local response procedures to a regional crisis

Furthermore, business users should contemplate and test their preparedness against scenarios in which key systems or data are unavailable for a prolonged period, which may be the case during a complex data centre failover or during the response to a security incident (e.g., denial of service, malware). These black-swan events may be described as "extreme but plausible." Under these circumstances, business teams may need to enact manual workarounds to continue operations and should therefore be rehearsed in their procedures and on a regular cadence.

End users can also participate in the IT team's IT disaster recovery testing by performing validation when data is restored from backups, availability and performance testing when applications are restored, and load testing if there is any concern about making systems unavailable due to a high volume of users. These steps not only validate application and database servers, but also can validate connectivity during periods of high load, assess throughput and performance of the network, and test interfaces with third parties (e.g., cloud service providers, or CSPs).

Organisations should also follow up at least annually on the exercises performed by their critical vendors. Many vendor management functions will include this in a periodic review of vendor risk. Where possible, joint participation in exercises on both sides of the relationship should occur.

Broader participation in testing can help organisations better determine their level of preparedness for dealing with disruptions. This is because various types of disruptions, including any loss or unavailability of systems and data, will require employees to perform alternative procedures. Therefore, it is imperative that representatives from across the organisation participate in business continuity testing. While IT may be responsible for the recovery of systems and data, it is business users who must resume operations and delivery of services and should therefore be familiar with and rehearsed in any communications and workarounds that may be needed.

Q 49 What are some successful business continuity training approaches?

A common approach to business continuity training is to review formal roles and responsibilities and ensure that what is documented meets business requirements. In many cases, roles and responsibilities are boilerplate and may not be cohesive within the organisational structure or culture. After ensuring roles and responsibilities are well-defined and assigned appropriately, training materials should be reviewed to ensure all roles and responsibilities are covered.

For example, as a member of the company's crisis management team, a vice president of IT may wear multiple hats, including being responsible for initiating an IT disaster recovery response and serving as a building evacuation leader. In this example, any training regimen should address both responsibilities and ensure all components of the business continuity program remain relevant and actionable. Additionally, as part of any role-based training, alternate and tertiary personnel to a given role should be trained as well. Training a primary resource without training others who may assume that role during an actual event introduces considerable risk.

Content can be delivered in numerous ways, but it is critical that any multi-site organisation provide the same quality and cadence of training anywhere a defined role is represented. In an actual event, senior management needs to know that local decisions will be made consistently, and that each person in a specific role knows the responsibilities and defined course of action.

For most organisations, some level of customised training is necessary, depending on their individual priorities. Many larger organisations have found a matrix training system to be a highly effective complement to facility-based training. In these approaches, crisis management, business resumption and IT disaster recovery personnel at each site are trained together. This approach improves standardisation and dissemination of best practices without compromising the specificity required in plans covering a call centre, manufacturing plant or other facility.

Q 50 How does BCM awareness differ from BCM training?

Awareness is an inherent part of training; however, training is not necessarily part of awareness. These terms are often used interchangeably, but they represent different levels of involvement as they relate to business continuity.

Awareness implies that one possesses knowledge of the BCM program or related activities. For example, the company may distribute an email communication pointing employees to an internal repository that houses business continuity plan documents and asking that they familiarise themselves with the materials. However, awareness does not necessarily imply that one has knowledge of how to execute the business continuity plan.

Role-based training, on the other hand, is a stricter regimen that pertains to receiving specific instruction on how to execute business continuity plan activities and solidifying that instruction with recorded proficiency exercises. This instruction may be provided through classroom, computer-based, test-based, and/or instructional guides and templates.

Q 51 What certification options are available for BCM practitioners?

There is no shortage of certifications in the business continuity space. Nonetheless, rather than selecting the first certification option that appears through a Google search, people seeking BCM certification must first decide why they are getting the certification in the first place. Do you own a BCM program at your company? Are you in a professional services role and looking to offer consultative advice about BCM to your clients? Are you an internal audit practitioner seeking to broaden your knowledge on auditing your company's BCM program? These questions will offer guidance on which certification option would be the most appropriate for you and your respective circumstance.

Below is a sample of organisations and respective certifications:

- **The Disaster Recovery Institute International**, or DRI International (also known as DRII) — DRII offers several general certifications, including Associate Business Continuity Professional (ABCP), Certified Functional Continuity Professional (CFCP), Certified Business Continuity Professional (CBCP) and Master Business Continuity Professional (MBCP), but they also offer other BCM-related certifications focused on specific areas such as vendor, audit, cyber resilience, healthcare continuity, public sector continuity, and risk management.
- **The Business Continuity Institute (or BCI) —** BCI offers a Certificate of the Business Continuity Institute (CBCI), which is the first step to proving your industry knowledge and joining the BCI's global network of business continuity and resilience professionals.
- **International Organisation for Standardisation (ISO) —** ISO 22301 is an international standard for business continuity management. The ISO organisation offers the Certified ISO 22301 Business Continuity Manager accreditation for practice professionals related to this standard.
- **Business Resilience Certification Consortium International (BRCCI) —** The BRCCI provides business continuity and IT disaster recovery training and certification services. Their mission is to deliver world-class training and certification programs focused on management and planning of business continuity and IT disaster recovery.

It is important to note that senior certifications may require client references and most BCM certifications mandate annual education and CPE requirements to preserve your accreditations.

FINANCIAL SERVICES

Ensuring continuity of operations has long been a foundational consideration for financial institutions when it comes to supporting clients and stakeholders. That focus has only increased over the past several years as organisations transition to new customer-centric services, cloud platforms and other ways of automating their operations. As the industry evolves and risks escalate, maintaining a clear understanding of how to strategically prepare for, respond to, and recover from major disruptive events has never been more critical for financial institutions.

Concerned about the changing risk dynamic, financial regulators are also increasingly focused on continuity of operations. In addition to updating existing guidance and regulations, a number of regulators have proposed rules aimed at strengthening the operational resilience of financial institutions. As explained in the section on business continuity management basics, operational resilience is a logical extension of existing business continuity management elements. Under operational resilience, firms that support important business services that customers (and the broader economy) rely on are expected to demonstrate their ability to respond to "extreme but plausible" scenarios effectively.

Q 52 What regulatory guidance and standards should financial institutions rely on?

Depending on organisational type, U.S. depository institutions may be subject to various regulations and guidance from bodies such as the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). For business continuity specifically, the Federal Financial Institutions Examination Council (FFIEC) maintains a standard Business Continuity Management booklet, which describes principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. The principles in the booklet are designed to guide examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services. Examiners expect financial institutions to apply the guidance and often benchmark against the principles and practices outlined as part of an assessment.

U.S. non-depository financial institutions should look to guidance provided by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Financial Industry Regulatory Authority (FINRA). Sometimes institutions come together to issue joint advisories on business continuity. A good example of this is the interagency business continuity and disaster recovery planning guidance issued by FINRA, the CFTC and the SEC following Hurricane Sandy in October 2012. Websites for each of the agencies also contain agency-specific information on business continuity and pandemic preparedness requirements for supervised firms.

In Europe, the European Banking Authority's Guidelines on Internal Governance (GL44) provides a consolidated view of supervisory expectations on transparency of the corporate structure, the role, tasks and responsibilities of the supervisory function on IT systems as well as business continuity management. Increasingly, the European Commission is focusing on digital operational resilience of the financial sector, particularly in the areas of information and communications technology and security risks. There is also the Basel Committee on Banking Supervision's "High-Level Principles for Business Continuity," outlining key considerations that banks must incorporate regarding business continuity and disaster recovery.

Across the Asia-Pacific region, the Australian Prudential Regulation Authority (APRA), the Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority continue to issue new and updated guidance on business continuity. It is worth noting that many APAC regulators look to international standards, such as the ISO, to shape their respective guidance. As an international organisation, ISO's business continuity management standards, like ISO 22301/22313, blend the requirements from several national standards, including those from the United States, Japan, Singapore, Canada and Australia.

Q 53 How has U.S. regulatory guidance on business continuity changed in recent years?

The most notable recent update to existing BCM guidance came in the form of an updated FFIEC handbook in November 2019. The revised business continuity management booklet offers increased clarity, with detailed examples designed to make it easier for financial institutions to comply with its guidance and to help examiners determine whether management is addressing risks related to the availability of critical financial products and services.

The detailed examples in the latest booklet cover various phases of the BCM lifecycle, from governance to aligning BCM elements with the organisation's strategic goals, developing a BIA, conducting a risk assessment to identify risks, and creating effective strategies for resilience and recovery objectives. It walks through the process of establishing a business continuity plan, disaster recovery plan and crisis management plan, as well as implementing a training program, conducting exercises and tests, updating and improving all programmatic components, and reporting and monitoring.

One of the most significant changes in the new booklet is its emphasis on risk identification and risk assessment, such as the likelihood of impact of different threat categories. For instance, it describes the speed of onset or velocity of a threat, the size of the affected area, and how to assess the likelihood of impact appropriately. Another crucial update is the inclusion of a BIA recovery objective timeline. This is helpful because it describes key concepts such as recovery point objectives, recovery time objectives, maximum tolerable downtime, data loss potential, and critical disruption points. These concepts are more fully defined in the new version than in the previous one.

Q 54 What is operational resilience and how is it relevant to business continuity for financial institutions?

In July 2018, UK supervisory authorities (the Bank of England, the Prudential Regulation Authority and the Financial Conduct Authority) brought the concept of operational resilience into the limelight with the publication of a joint discussion paper, titled *Building the UK Financial Sector's Operational Resilience*. Since then, other regulators have followed suit by issuing proposals on enhancing the resilience of financial institutions. Most recently, the Basel Committee released a consultation paper with proposals intended to strengthen banks' ability to withstand significant operational failures or wide-scale disruptions.

Operational resilience is defined by the UK supervisory authorities as "the ability of firms and financial market infrastructures and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions."

Firms are expected to take ownership of their own operational resilience by following a set of approaches or a framework, which includes identifying their important business services; setting an impact tolerance for each of these services; quantifying the maximum acceptable level of disruption through severe but plausible scenarios; identifying and documenting (also known as mapping) the necessary people, processes, technology, facilities and information required to deliver each of their important business services; and performing a self-assessment of their operational resilience.

Q 55 How should firms consider third-party-related risks as a component of business continuity management?

According to a 2019 survey by the UK Financial Conduct Authority, third parties are the second biggest root cause of operational outages — after change management. Supply chain disruptions can have a significant impact on key business processes and undue concentration of services among shared service providers, such as cloud providers, can also have dire consequences if ignored or left unmanaged. Firms need to understand their third-party relationships well and remember that regulators will hold them responsible for the work (or failures) of third parties. As such, incorporating the third parties into their continuity planning is critical.

Businesses should obtain assurances and verify that their key third parties are maintaining robust controls.

Beyond contractual obligations, firms should take steps to improve their understanding of how vendor outages can impact their own operations. They should proactively understand and address third parties along the critical path of business services, working with them to monitor and respond to events. This includes actively engaging the vendors in testing, exercises and planning activities.

Q 56 Are financial institutions, such as banks, required to recover disrupted operations within a defined time period?

There is currently no regulation or legislation-defined rules mandating specific recovery time objectives for institutions. However, regulators do have a clear expectation that entities will establish their own recovery objectives based on widely used standards such as RTO, RPO, MTD, and impact tolerance, to name a few. Firms are expected to set recovery objectives based on a rational understanding of the potential impacts of an unplanned and undefined disruption. The expectation is that each organisation would apply these standards as outlined in the FFIEC booklet. Recovery time objectives of processes and systems should be established through a BIA. The likelihood of risk and an understanding of cost benefit should be factored into this analysis and as part of the firm's broader risk management program. An examiner would typically assess the work performed and determine whether the conclusions reached around recovery are reasonable.

Q 57 Are business continuity standards for financial institutions set only by the regulatory agencies?

The U.S. Department of Homeland Security (DHS) also offers guidelines to the financial services sector, which it defines as "a vital component" of U.S. critical infrastructure. In 2010, the agency, in partnership with the U.S. Department of the Treasury, published a sector-specific plan that details how the National Infrastructure Protection Plan (NIPP) is implemented within the financial services sector. The NIPP provides a risk management framework designed to enhance the safety of U.S. critical infrastructure. The DHS' Banking and Finance Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan provides a description of the complex nature of the sector and an overview of its products and services. The products and services are:

- Deposit, consumer credit, and payment systems
- Credit and liquidity products
- Investment products
- Risk transfer products (including insurance)

The plan underscores the interconnectedness of the financial services sector to other critical infrastructure sectors, such as communications and IT. These critical infrastructure sectors, if disrupted, would undermine the financial services sector's ability to conduct normal business. The plan also lays out the following vision statement on business continuity: "To continue to improve

the resilience and availability of financial services, the banking and finance sector will work through its public-private partnership to address the evolving nature of threats and the risks posed by the sector's dependency upon other critical sectors." Additionally, these three goals for the financial services sector are outlined:

- Achieve the best possible position in the face of myriad intentional, unintentional, man-made, and natural threats against the sector's physical and cyber infrastructure;
- Address and manage the risks posed by the dependence of the sector on communications, IT, energy and transportation systems sectors; and
- Work with the law enforcement community, financial regulatory authorities, the private sector, and counterparts outside the United States to address threats facing the sector.

Details of the *Banking and Finance Sector-Specific Plan* can be accessed on the DHS website.

Q 58 To what extent are financial institutions responsible for the business continuity of vendor-supported systems?

Regulators expect financial institutions to establish acceptable business continuity plans for all systems required to perform key activities, including systems used for customer-facing, financial reporting and compliance (e.g., AML transaction monitoring and sanctions screening). For vendor-supported systems, a financial institution's due diligence procedures should consider the vendor's business continuity standards and practices, as well as how those standards and practices align with their individual needs. Contracts with vendors should reflect obligations and expectations, and financial institutions should consider participating in vendor business continuity tests or, at minimum, require evidence (such as SOC reports) that the program has been consistently maintained and regularly tested.

Regulators expect financial institutions to establish acceptable business continuity plans for all systems required to perform key activities, including systems used for customer-facing, financial reporting and compliance.

HEALTHCARE

Healthcare organisations are facing multiple challenges in the development and maintenance of emergency preparedness operation and recovery plans. Along with increasing regulatory scrutiny, such as The Joint Commission's reinstatement of the survey process to dealing with simultaneous events and the recent increase in natural disasters, such as the COVID-19 global pandemic, healthcare organisations are being asked to adhere closely to current mandated emergency preparedness standards.

While this guide does not present the many details surrounding each potential variable that healthcare organisations may want to take into account when developing and/or assessing the strength of their emergency management program, all healthcare organisations should at least consider the points highlighted below (in addition to the industry-independent considerations already discussed in this publication).

Q 59 How can healthcare organisations ensure their emergency preparedness plans meet current regulatory requirements?

Both the Centres for Medicare & Medicaid Services (CMS) and The Joint Commission are advising healthcare organisations to ensure their readiness for an all-hazards approach to emergency management is a top priority. With the increased likelihood for simultaneous events, such as a global pandemic occuring at the same time as natural disasters like hurricanes and wildfires, organisations that are not prepared to bring their facilities and systems up to compliance would face significant challenges. Not only will lives depend on organisations being prepared and compliant, but the future of the organisation as a key contributor to the healthcare infrastructure could also be at stake.

Developing an emergency preparedness plan that is consistent with regulatory requirements is no simple task. Healthcare organisations should be continually developing, refining and executing all emergency preparedness plans to not only meet regulatory expectations, but more importantly, to increase their readiness to respond effectively to an emergency situation when it occurs.

To meet all the requirements, at a minimum, healthcare organisations must consider undertaking the following activities:

- Engage in planning activities prior to developing a written emergency operations plan, which is a critical component of the emergency preparedness plan.
- Engage leaders to help develop and maintain a written emergency operations plan that describes the response procedures to follow when emergencies occur. The plan also should include identification of the healthcare organisation's capabilities and response procedures for when the organisation cannot be supported by the local community to provide communications, resources and assets, security and safety, staff, utilities or patient care for at least 96 hours.
- Conduct a hazard vulnerability analysis (HVA) to identify potential events, and rank them based on probability, severity and organisational risk. Through the HVA, organisations can work with community partners to prioritise the potential emergencies identified, communicate needs and vulnerabilities to emergency response agencies, and identify the community's ability to meet its needs.
- Develop a communications plan to help facilitate how the healthcare organisation connects with staff, external authorities, patients and their families, media, suppliers, vendors, and others regarding the emergency; to update local, state and federal authorities; and to connect with identified alternative care sites. The communications plan must include any backup systems and technologies utilised, how resources and assets will be managed during emergencies, how the organisation will obtain and replenish medications and supplies, as well as share resources and assets with other local healthcare organisations; and arrangements for transporting patients, managing security and safety during an emergency, managing hazardous materials and waste, and managing utilities, water and fuel. Memoranda of understanding should be created for all community resource partners.

- Staff must be trained for their assigned emergency roles to determine how the organisation will manage patients during emergencies. For example, develop a plan for keeping patients on the premises or evacuating them if the facility is not safe; determine how the organisation will manage scheduling, triaging, assessing, treating, admitting, transferring and discharging patients; and finally, define how the organisation will manage any increase in demand for services, medications, patients' personal hygiene and sanitation needs, mental health needs, dietary needs, and mortuary services.
- Disaster privileges need to be granted for volunteer licensed independent practitioners during emergencies. Determine how volunteers will be distinguished from regular staff and who will oversee their performance, addressing any state or federal waivers.
- Perform an evaluation of the effectiveness of the healthcare organisation's emergency management planning activities. This should include activating the emergency operations plan twice a year and conducting an annual exercise that includes an influx of simulated patients. In addition, the organisation should conduct an annual exercise that includes participation in a communitywide exercise.
- Recovery strategies and policies need to be developed for mandated after-action reports and business and emergency operation plan modification from lessons learned.
- The creation of business continuity plans (BCPs) for all essential and critical services that address an all-hazards approach are essential components of emergency management recovery. Ensuring that patients continue to receive appropriate care and healthcare providers are able to respond to major events in the community are driving forces behind much of what a healthcare organisation's BCP entails. The clinical implications of having an effective or ineffective BCP are too numerous to be addressed in this document. A BCP must protect the organisation's physical plant, IT systems, supply chain, financial and clinical operations, and other infrastructure from direct disruption or damage so that it can continue to function throughout or shortly after an emergency. BCPs assist healthcare facilities in meeting their business resilience and recovery needs, as well as meeting regulator guidelines for recovery, as the goal of regulators is an effective and efficient return to normalcy or a new standard of normalcy for the provision of community healthcare delivery. A healthcare organisation's geographical reach and the breadth/depth of its strategic initiatives also must be taken into consideration in its BCP efforts.
- An effective business continuity plan must be based on a BIA that takes into account all essential and critical services. It should outline the criticality of mission/business processes through an all-hazards risk analysis. Organisations should identify risk mitigation and recovery strategies based on criticality, identify resource requirements needed to resume mission/business processes and related interdependencies (facilities, personnel, equipment, software, data files, system components, and vital records), as well as identify recovery priorities for sequencing recovery and resources.
- The BIA serves as a starting point for the disaster recovery planning and defines the key parameters such as maximum tolerable downtime (MTD), recovery time objectives (RTO), recovery point objectives (RPO) and resources/materials needed for business continuity. It should also be used to support the development of other continuity plans associated with recovery, including, but not limited to, the incident response plan (IRP) and business continuity plan (BCP)/continuity of operations plan (COOP). The BIA also assists in identifying preventive controls for the functions and resources included in the development of business continuity plans.
- Business continuity plans need to also consider how business processes can continue without key critical technologies and those details should be communicated and training provided for those who may need to enact them. These plans need to consider those key systems that may be cloud based to ensure backup processes can occur should the system be unavailable to ensure a resilient organisational approach.
- Business continuity plans need to be tested. The type and extent of testing requirements will ensure a healthcare organisation's BCP is designed effectively and everyone involved is trained and aware of their responsibilities. Also, testing requirements may vary significantly based on the type of organisation and state of operation.

Q 60 Does the Health Insurance Portability and Accountability Act (HIPAA) include a requirement to implement BCM processes?

Several aspects of BCM are included in the security section of the HIPAA requirements. Specifically, HIPAA (Section 164.308) calls for:

- Risk Analysis (required) — §164.308(a)(1)(ii)(A)
- Contingency Plan — §164.308(a)(7)(i)
  - Data Backup Plan (required) — §164.308(a)(7)(ii)(A)
  - Disaster Recovery Plan (required) — §164.308(a)(7)(ii)(B)
  - Emergency Mode Operation Plan (required) — §164.308(a)(7)(ii)(C)
  - Testing and Revision Processes (addressable) — §164.308(a)(7)(ii)(D)
  - Application and Data Criticality Analysis (addressable) — §164.308(a)(7)(ii)(E)

As noted above, the business continuity-related provisions of HIPAA are designated as either required or addressable. In terms of HIPAA, addressable does not equate to optional. This simply means the organisation must assess whether or not the requirement makes sense in its environment; if not, then a similar provision should be in place to act as a compensating control with the intent of performing the same type of safeguard. According to the U.S. Department of Health and Human Services (HHS), decisions made regarding addressable specifications must be documented.

Additionally, HIPAA Section 164.310 requires contingency plans for facility access and security. Section 164.312 requires procedures to gain access to protected health information (PHI) during an emergency. A common misconception is that the HIPAA requirements are focused exclusively on IT. Although most of the Final HIPAA Security Rule can be perceived to be focused heavily on IT, PHI is found in many forms, and the Emergency Mode Operation plan is not truly an IT issue at all. Rather, this requirement addresses how the provider will continue to protect PHI if normal IT controls are not available or functioning appropriately, which could have a significant impact on the organisation's ability to continue operations in an acceptable manner, if not handled appropriately.

Q 61 Does The Joint Commission require business continuity planning for hospitals?

The Joint Commission requires that healthcare organisations have an integrated emergency management plan, including policies and procedures that address the organisation's identification of its emergency preparedness, and response and recovery activities that are coordinated with an organisation's integrated program, including a hazard vulnerability analysis, acquisition and storage of clinical supplies, staff assignments, emergency protocols, and continuity of operations planning. Business continuity plans assist healthcare facilities in meeting their business resilience and recovery needs, as well as meeting The Joint Commission Emergency Preparedness Program's Healthcare Preparedness Capability and Healthcare System Recovery initiative, the goal of which is an effective and efficient return to normalcy or a new standard of normalcy for the provision of healthcare delivery. Continuity of operations planning ensures the ability to continue essential business operations, patient care services and ancillary support functions across a wide range of potential emergencies. The healthcare organisation's continuity of operations planning may be an annex to the organisation's emergency operations plan and, during a response, should be addressed under the incident command system.

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

Q 62 What are some of the supply chain considerations for technology, media and telecommunications (TMT) organisations?

TMT industry group organisations with hardware manufacturing operations around the world need to take the appropriate steps to guarantee that required supplies and materials are available in each region. Prior to COVID-19, many TMT organisations prioritised efficiency in the supply chain, including just-in-time models. Such approaches are vulnerable to being disrupted. Supply chain strategies focused on just-in-time models and single-source providers may need to be revisited. As became evident during the COVID-19 global pandemic, effective business continuity planning around the supply chain likely involves ensuring that TMT companies have more than one source for key supplies and materials. Diversifying the supply chain is key so that it is not concentrated with one supplier or a small group of suppliers, or within a specific geography.

There are several considerations for ensuring continuity of supply, including postponement, inventory pooling, locating supply and manufacturing closer to customers, and establishing multiple sources of supply, among other options. Post-pandemic, it is likely more TMT organisations will shift their supply chain strategy to ensure resilience in the event of future disruptions.

Q 63 How should TMT organisations address or revamp their research and development programs to ensure business continuity?

TMT organisations can benefit from building redundancy into their research and development (R&D) operations. Unforeseen events and business interruptions such as the COVID-19 global pandemic make it clear that establishing R&D operations in just one location or region results in concentrated risk. TMT organisations should consider how they might diversify R&D efforts in different locations around the world, as it is less likely that all of them would experience the same level of interruption.

More broadly, TMT organisations also might consider how they can transform their R&D operations. The type of precision equipment required and clean-room setup that are part of R&D activities prevent this work from being conducted remotely. While it is not possible in every instance, TMT organisations should take a strategic look at their R&D function to assess how they might reinvent it so that progress can continue amid significant business interruptions.

Consider that for some TMT organisations, R&D activities increased notably during the COVID-19 pandemic, but for others they stopped entirely, as onsite facilities were unavailable. Formulating innovative solutions to these challenges will be key for TMT organisations going forward.

Q 64 What are some other key considerations for TMT organisations to address as part of their business continuity planning?

Resources — both human and physical — are key areas for TMT organisations to address in their business continuity management efforts. During the COVID-19 pandemic, many TMT organisations experienced surges in demand in areas including, but not limited to, product delivery, customer service, online traffic (e.g., streaming content) and network bandwidth. TMT organisations should consider the capabilities within their infrastructures, as well as the infrastructure of third parties (e.g., telecommunications and cable providers), to accommodate growth quickly if events and, more important, customers and clients demand it.

From a people perspective, TMT organisations, like those in any other industry, need to have strong communications

plans to keep their workforce engaged continually during a major business interruption that necessitates employees working remotely for an extended period. For example, the COVID-19 pandemic resulted in interruption of key functions such as accounting, finance, customer service and help desk in many organisations. To ensure improved continuity of service in these and other core functions, TMT organisations might explore utilising managed services or variable labor models that are designed to maintain operations and activities even amid a major business interruption.

TMT organisations also can benefit from conducting deeper and more frequent scenario-planning exercises to consider how to manage through unanticipated events and their effects. What is the response if a large percentage of the customer base seeks to renegotiate contracts or agreements? What if revenue is impacted severely by one or more types of unanticipated events or business interruptions? What is the plan for the organisation to manage through the crisis? This last point is especially relevant for emerging TMT companies that may have just one revenue stream or a small number of them. Effective business continuity management might call for exploring strategies to diversify the business so that it can, at least partially, offset the effects of a major business interruption.

Finally, like companies in many other industries, TMT organisations should consider their overall network and data security posture. The COVID-19 global pandemic forced millions of employees to work remotely, creating new and sometimes fertile ground for cyberattacks and bad actors to flourish. TMT organisations, given their heavy reliance on digital and cloud-based environments, should ensure that their cybersecurity measures are not only up to date but also resourced appropriately to manage the many changes that can occur during any business interruption.

Q 65 What are the best practices for ensuring the availability of critical infrastructure for the communications industry?

Customers have evolved over the years to demand more network availability and performance from communications companies. As a result, these organisations have increasingly focused on the deployment of processes, systems and supporting infrastructure designed to eliminate or minimise the impact of disasters or network outages.

Key areas to consider include, but are not limited to, the following:

- **Topology —** The network topology should be developed to withstand network disruption. It may include redundant paths for transmission networks for critical network elements. Further, the organisation must monitor the transmission capacity for each redundant path. Testing of redundant paths should be included as part of disaster recovery testing.
- **Redundancy —** The critical network infrastructure should be deployed with geo-redundancies. This may include active-active or active-standby configuration.
- **Data centres —** Communications organisations should consider the deployment of data centres in multiple geographic regions. Redundant network elements should be deployed in separate data centres.
- **Preventive maintenance —** The critical network infrastructure elements, especially without redundancy, should include frequent health checks and preventive maintenance activities to minimise unplanned outages.
- **Backup —** The backup strategy and processes should be aligned with recovery point objectives. Organisations should conduct storage and validation of backups in alignment with defined policy.
- **Spare parts —** Communications organisations should have a defined strategy for managing spare parts. Buffer stock should be considered for critical infrastructure at each location. Further, the deployment of a multivendor network infrastructure should include spare parts for each location.
- **People —** Cross-training of employees should be considered to ensure the availability of resources for performing critical tasks in case of network unavailability.

Q 66 What are some key considerations in incident management planning for the communications industry?

The communications industry requires a robust incident management plan due to multipronged threats covering network operations, cybersecurity, and physical infrastructure like buildings and data centres. The following areas must be considered in incident management planning:

- **Functional alignment —** Incident management planning usually covers the network operations centre, security operations centre and physical security. Typically, a separate department deals with each of these areas, leading to multiple incident plans. The organisation must ensure alignment of each incident management plan with the corresponding impact analysis. Further, the organisation should define escalation criteria, including the invocation of a crisis management plan.
- **Crisis management planning —** The crisis management plan should be developed and documented with enough flexibility to address any type of reported incidents. It may include multiple emergency response teams depending on the type and nature of the event. For instance, the response team for network equipment failure would be different from one to address a physical threat to a data centre.

Q 67 What are some vendor-related technology considerations in business continuity planning for communications organisations?

Communications organisations work with numerous technology vendors that provide, for example, telecommunications and IT equipment, as well as security infrastructure. Network operations are sometimes outsourced to vendors as well. Vendor risks are cascaded to the organisation's risks. Therefore, they should be an essential component in business continuity planning.

Vendor-related issues for communications organisations to consider include, but are not limited to, the following:

- **Contractual requirements —** As part of the vendor contract, the organisation should state all expected business continuity requirements, depending on the area of scope. These may include incident and disaster management plans, inventory requirements, information backups, and preventive and health check activities.
- **Disaster recovery plan —** Vendors may be required to submit disaster recovery plans, especially for areas related to network operations. These plans should be aligned with the organisation's requirements and its recovery point and time objectives. Moreover, these plans should be tested in alignment with the organisation's BCM policy.
- **Incident management plan —** The vendor's incident management plan should adhere to the organisation's incident policy. It may include the alignment of escalation and impact criteria, workflow requirements and evidence collection requirements.

Q 68 What are some of the key technology-related challenges faced by communications organisations in maintaining an effective business continuity program?

Communications organisations face unique business continuity planning challenges due to the large number of IT and telecommunications systems they leverage. They should review the following areas on a periodic basis to ensure the alignment of the business continuity program.

- **Network changes —** Due to the size and number of network systems in communications organisations, they are among the top challenges these organisations must address in maintaining their BCM program. Network changes occur due to factors including, but not limited to, new technologies, patch upgrades, network optimisation and network faults. These changes may accumulate over time and alter business continuity requirements significantly. Therefore, the BCM program must continuously monitor network changes.
- **Disaster recovery testing —** The critical infrastructure may limit the ability and type of disaster recovery tests performed by the organisation. These tests should be scheduled to minimise the impact on the business.

Resources — both human and physical — are key areas for TMT organisations to address in their business continuity management efforts. TMT organisations should consider the capabilities within their infrastructures to accommodate growth quickly if events and, more important, customers and clients demand it.

CONSUMER PACKAGED GOODS/RETAIL

The ability of retailers to adapt to changing conditions and recover rapidly from unexpected natural events, accidents or deliberate attacks can be critical to maintaining customer loyalty and brand reputation, as well as their competitive advantage in the market. The COVID-19 global pandemic put a strain on consumer packaged goods and retail companies' resilience and showed that a BCM program set up to respond to this specific crisis scenario has been decisive for an organisation's survival and transition to the "new normal." Companies that were prepared to shift their business operations from their brick-and-mortar stores to e-commerce had more chances to contain losses. Likewise, organisations that did not rely on a centralised distribution strategy were able to reduce their supply chain disruption risks and maintain product availability, thanks to a broader warehousing and distribution facilities network. Retailers that had emergency procedures in place and had properly trained employees at each location were able to limit the rate of infection and ensure the safety of their employees and customers, reducing the operational and reputational risk of such a disruption.

Many retailers and consumer products organisations must revisit the cost-benefit analysis of their business continuity strategies and operational risk tolerance, with greater focus on the impacts of widespread events affecting the entire supply chain — from sourcing, through manufacturing and distribution and up to the point of sales. They also must address and plan for potential events — such as technology outages, critical supplier unavailability or natural disasters in areas where key operations and facilities reside — that can adversely affect business continuity.

Q 69 What is the impact of omnichannel strategies on the business continuity plan?

Consumers are rapidly shifting their behaviour toward e-commerce. For retailers, it's more important than ever to have the ability to shift their customers seamlessly from one channel to the other (e.g., physical stores, e-commerce, social media), not only in the sales processes but also for various communications and customer engagement activities. In this new environment, IT systems availability is critical to maintain and preserve retailers' digital life. Recovery time objectives need to be reviewed in order to reduce downtime in the event of a business interruption and to enable continuous delivery of a seamless and personalised cross-channel customer experience.

Q 70 Do the organisation's business recovery strategies consider stock keeping units (SKU) optimisation?

In the event of a supply chain disruption due to the unavailability of raw materials or finished/semi-finished products, default of suppliers or subcontractors, or events affecting the organisation's main manufacturing, warehousing and distribution facilities, it is good practice to prioritise the production of high-demand/best-seller products, versus products for which there historically is fluctuating demand, to maximise revenues until operations return to normal. This analysis should also consider that unexpected changes in consumer behaviours might occur, increasing the demand for specific products (or SKUs) at the expense of other products in inventory.

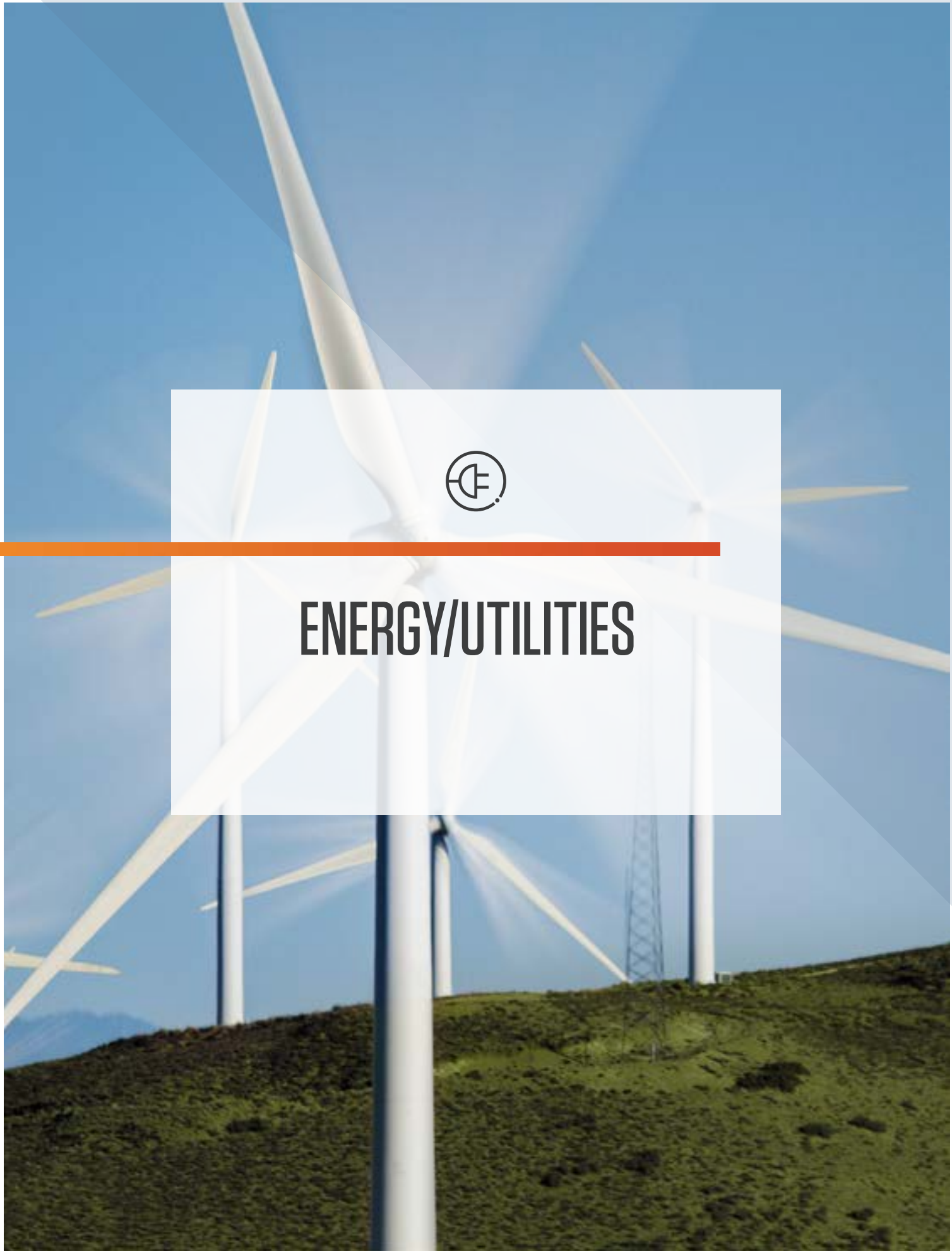
Q 71 How should global trade tensions be considered in the BCM program?

Consumer packaged goods and retail companies should evaluate the risks of a trade war involving emerging markets and significant macroeconomic changes (e.g., Brexit), and evaluate the impact of an import tariff increase or a restriction on imports to their business. This analysis should consider the overall reliance on a foreign country, including manufacturing plants, critical vendors and suppliers, logistics facilities, the likelihood that the country could be involved in a trade war in the future, or the medium- and long-term effects of an existing trade war. In the event of business concentration in high-risk areas, mitigation strategies should be implemented to reduce the impact of a business interruption or slowdown due to a trade war (e.g., reduce imports and differentiate sourcing).

Q 72 Should customer service be included in a business continuity plan?

Customer service typically is not considered to be a critical process for retail operations in the event of a short outage (e.g., a few days). However customer relationship processes become more critical as recovery time becomes longer. In the event of an extended business interruption, customers might need information about deliveries, product availability and online payments, among other areas. A company's failure to communicate with customers and clients during an outage might negatively impact its brand reputation and customer loyalty, especially in an omnichannel/multichannel environment. Business continuity plans should consider resumption solutions for customer service. Contract agreements with external vendors should include business continuity requirements that can adequately support the company's recovery objectives.

In the event of an extended business interruption, customers might need information about deliveries, product availability and online payments, among other areas. A company's failure to communicate with customers and clients during an outage might negatively impact its brand reputation and customer loyalty, especially in an omnichannel/multichannel environment.



ENERGY/UTILITIES

Q 73 Can BCM planning account for complex, international supply chains that can be disrupted by geopolitics?

BCM programs should be developed in a manner that accounts for all levels of risk for the organisation. In the energy and utilities space, this includes well-thought-out considerations of the complexity of their supply chains and should account for multiple contingencies, including geopolitical conflict that can impact these supply chains. Business continuity professionals should engage with all supply chain partners to identify appropriate contingencies to maintain critical operations.

Q 74 Should field sites and operational plants have their own business continuity plans?

This depends on the governance of the organisation. Some have an enterprise continuity plan with flexibility to account for additional contingencies specific to field sites, refineries and plants. Other organisations have separate business continuity plans for operational sites and supporting offices. Either way, it is important that an organisation has appropriate contingencies, with corresponding collaboration and communication strategies outlined for operational facilities so that critical operations can be maintained.

Q 75 Why is having a business continuity program in place especially important for the energy industry?

Having a business continuity program in place is important for a few reasons. First, energy and utility organisations must consider the safety of their employees, visitors, guests, partners, contractors, vendors and other third parties. Next, many organisations may already have environmental, health and safety procedures in place; however, mature crisis management plans and other business continuity plans (depending on the crisis) should run in parallel to ensure there is an organised response and communication from leadership. Further, enterprise risk management is not comprehensive if the BCM posture is not mature. Lastly, energy organisations are highly reliant on IT and other power/utilities and systems to run their operations. A delayed response or recovery time can result in a significant impact to the sector, revenue loss, reduced production, and potential reputational damage due to the increased market and social media attention that likely would result. Having resilience measures and business continuity strategies and plans in place is critical to minimising these impacts.

Q 76 What type of outages should energy and utility organisations plan for?

All energy and utility organisations should perform a continuity risk assessment to identify the highly likely and highly impactful scenarios that could affect them. Based on those identified risks, they should develop recovery strategies and incident response plans. A few examples are:

- Cyber incident response plan
- Hurricane response plan
- Pandemic plan
- IT/power outage plan

MANUFACTURING

Over the past few decades, manufacturers have been consistently trying to eliminate redundancies by streamlining their processes and consolidating their supply chains. In the midst of recent events, such as the COVID-19 pandemic, trade wars and other natural disasters, manufacturers have faced significant disruptions to their business. The challenges facing manufacturers range from supply chain disruptions to potential product defects to IT systems failures. Managing risks that threaten business continuity is even more challenging, often requiring more resources for global manufacturers due to inherently more complex supply chains and dynamic organisational relationships.

In light of recent events, manufacturers must critically analyse their organisations to ensure risks threatening business continuity are appropriately mitigated, including for those events that were considered black swans. Manufacturers should begin by thoroughly reviewing their supply chain, including every supplier that helps support it, to assess risk fully and determine alternatives to replace any essential "cogs" in the machine should they fail. Additionally, manufacturers must consider other factors, such as the use of just-in-time inventory management, co-manufacturers and single-site manufacturing, and their associated risks and benefits, when assessing the organisation's business continuity.

While this guide cannot present the many details surrounding each potential variable that manufacturers may want to take into account when developing and/or assessing the strength of their BCM programs, all manufacturers should at least consider the following questions (in addition to the industry-independent considerations already discussed in this publication).

Q 77 How can pursuing a single-source supply strategy affect my organisation's overall risk of business interruption?

Supply strategies are complex by nature. There are many instances where a single-source supply strategy is the right business decision, even when alternate sources of supply exist. In instances where a company is reliant on a sole-source supplier, finding alternates is more daunting, as it may require changing product specifications or working closely with other key suppliers to develop alternatives. Neither of these approaches is typically fast. Furthermore, moving to an alternate supplier may carry the risk of quality issues and must be managed carefully. Supplier relationships honed over a period of years cannot be replaced overnight with an expectation of comparable performance levels.

As manufacturers streamline their supply chains and rely more heavily on single- and sole-source suppliers, they are discovering new organisational risks they have not measured. Even in cases where companies do measure the financial risks of a certain supplier (e.g., credit risk), they may not have considered business interruption risks stemming from a man-made or natural disaster. The COVID-19 pandemic brought supply chain risk to the forefront as companies, economies and even countries have struggled to appropriately source critical goods, including personal protective equipment. Single- and sole-source vendors should be included in a manufacturer's risk assessment, BIA, continuity strategy and business continuity planning. These critical vendors are key "cogs" in the effective operations of these organisations and should be treated no different from any other internal critical function or process. Additionally, pandemic, political and natural disaster risks, such as COVID-19, trade wars or wildfires, and their impacts on revenue and operations, should be measured; lead times need to be understood; alternate sources for critical supplies should be identified; and strategies to mitigate the impact of business interruptions occurring among key suppliers need to be developed.

Q 78 Has management designed manual backup procedures to carry out manufacturing schedules and order releases?

Most modern manufacturers have switched to automated manufacturing resource planning and enterprise resource planning systems. Therefore, many have not considered manual workarounds to carry out manufacturing schedules and order releases during an outage. If management does not have the confidence in the resumption capabilities of its IT systems, it should consider developing manual backup procedures to facilitate the continued operation of critical manufacturing processes.

It is especially important for manufacturers to think through how these manual workarounds will be executed if their onsite workforce is disrupted.

Alternatively, mothballed systems could be utilised to continue operations in the event of a prolonged disruption. In light of recent global events, these systems may provide manufacturers with a unique alternative to deal with various risks that could impact the company's IT infrastructure.

Q 79 How do companies that rely solely on single-site manufacturing or centralised operations plan for the impact of a long-term outage?

Over the past two decades, globalisation, outsourcing, increased cross-border sourcing, IT and shared services centres have encouraged many organisations to consolidate facilities and streamline processes to eliminate nonessential and redundant activities, as well as to focus and automate remaining activities. The waves of total quality management, process reengineering and Six Sigma process improvements have created a bias for strong supplier relationships and tight coupling with supply chains, with the objective of driving down costs of processes and products while preserving quality standards.

As such, manufacturers may rely solely on a single site for manufacturing of specific products, as opposed to building redundant, or multiple, manufacturing operations to meet total demand for their products. However, considering that the COVID-19 pandemic caused operations to be shuttered in specific cities, states and even countries for extended periods of time, it is important for manufacturers to evaluate the capital cost of retaining multiple sites of operation, with the potential benefit of continued manufacturing during times of crisis. Alternatively, they should consider gaining access to other production facilities that could be retooled in a timely manner to minimise a prolonged disruption.

Q 80 How do companies that utilise just-in-time inventory production methods ensure continuity in operations during disruptions?

In order to reduce the carrying cost of inventory, many manufacturers have continued to decrease inventory levels and adopt just-in-time (JIT) manufacturing and delivery techniques. Having minimal inventory on hand exposes JIT manufacturers to potential disruptive events. Any impacts to the supply chain, especially in the case of sole-source or single-source suppliers, can cause issues for these manufacturers to produce promised goods for their end customers. JIT manufacturers must consider the use of multiple suppliers for key inputs and storing additional inventory to combat possible business continuity risks, while also considering the potential trade-offs in quality, time and cost.

Q 81 How can manufacturers that utilise third-party co-manufacturers ensure minimal disruptions from these organisations?

Whether it be component parts or fully developed products, it is becoming increasingly common for large manufacturers to outsource a portion of their operations to third parties. As with any third-party relationship, it is important to ensure the organisation has included contractual protections, such as service level agreements (SLAs) that guard against shortfalls in performance or disruption. Additionally, defining quick and effective communications protocols between the organisation and the third-party co-manufacturer will allow for timely identification of key issues and bottlenecks and enable agility in handling these problems as they arise.

Q 82 Where does a product recall procedure fit into a BCM program?

Every manufacturer should have a robust and tested product recall procedure as part of its standard operating procedures. The product recall process also should be integrated into the crisis management plan. An effective recall plan should include the following procedures:

- Pull product in the event an issue is discovered due to safety or quality concerns
- Communicate to customers and stakeholders about the issue
- Trace and isolate the product defect's root cause
- Track mechanisms to determine defective product marketplace proliferation and elimination
- Dispose of the product in a financially and environmentally responsible manner

Many industries are regulated to develop and test these plans.

For a manufacturer, a product recall is among the most significant and potentially devastating crises that can occur, because it can affect not only finances and operations but also brand and reputation and people's health and safety. Product recalls should be managed no differently from any other significant crisis event. An interdisciplinary team of business-unit and corporate senior managers should consider all facets of managing the crisis.

In light of recent events, manufacturers must critically analyse their organisations to ensure risks threatening business continuity are appropriately mitigated, including for those events that were considered black swans.

GOVERNMENT

Q 83 Are there any special or unique considerations for government organisations with regard to business continuity planning?

For the most part, no — although circumstances may differ in specific countries. In the United States, most government agencies have adopted business continuity planning as part of contingency planning for their overall risk management program. At the U.S. federal government level, most agencies adhere to guidance set forth in the NIST/U.S. Chamber of Commerce paper, "Contingency Planning Guide for Federal Information Systems."

Of note, some government agencies are moving beyond business continuity planning for many of their systems. They are planning for pandemics and other catastrophic events that not only may bring down data centres, but also eliminate command and control. This is referred to as devolution planning.

Q 84 What are some common challenges or gaps that government organisations may need to consider as part of their business continuity planning?

Among the common gaps, government agencies may not perform sufficient testing and exercises to validate recovery strategies and procedures. Escalation and decision-making often operate differently during an actual event versus what is articulated in plans. A strong testing program is critical to test crisis management and decision-making teams and leaders in different scenarios. Also, continuity planning processes often fail to cover all critical services — instead, they focus on those for which it is easier to demonstrate continuity (e.g., cloud-based systems). Government agencies should consider ways to enhance continuity planning to ensure that all critical business processes are covered by their continuity operations.

Another common business continuity planning challenge in government is siloes, with individual departments in an agency having their own plans that are unknown to other departments. Specifically, there can be challenges with linkages (or lack of effective linkage) to other internal plans and processes, such as incident management frameworks and information communications and technology (ICT) disaster recovery arrangements to support business-critical functions. In addition, an agency's role in the overall government response to an emergency will impact the agency's specific internal business continuity risk management and planning. Across a government agency, there should be a central repository of business continuity plans that management can access immediately in the event of an emergency.

Finally, rotating personnel remains a challenge in government. Individuals designated to be responsible for updating and maintaining government agency business continuity plans will change jobs, and new personnel are not trained to carry out all of their responsibilities regarding continuity planning. This results in less effective preparation for a business interruption or catastrophic event.

Q 85 What actions can government organisations take to remedy these gaps?

Government entities have compiled a number of best practices in business continuity, including guidelines on training business continuity teams, testing, and exercises to evaluate recovery strategies and ensure the availability of government information systems in the event of a catastrophe. Among the benefits of focusing more on business continuity training, testing and exercises include reinforcing the ability to conduct repeatable procedures, coordinating organisational communications, uncovering weaknesses in procedures, and identifying resource gaps.

Conducting these activities also can happen without adversely impacting government entities. They will help build confidence in the overall operations and maintenance of the government information system, increase the overall strength of the preparedness program, and improve the ability of team members to perform their roles and carry out their responsibilities regardless of adverse circumstances.

APPENDIX

GLOSSARY

Key Term	Definition	Source
BCM program governance	The system of rules, practices and processes by which a business continuity program is overseen, directed and controlled.	Protiviti, based on best practices
Business continuity	The strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.	BCI/DRJ
	The capability of an organisation to continue the delivery of products or services at acceptable predefined levels following a disruption.	ISO 22300:2018
Business continuity management (BCM)	The process for management to oversee and implement resilience, continuity and response capabilities to safeguard employees, customers, and products and services.	FFIEC
	A holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and that provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.	ISO 22300:2018
Business continuity plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organisation's mission/business processes will be sustained during and after a significant disruption.	NIST
	One or more comprehensive written plans to maintain or resume business in the event of a disruption.	FFIEC
	The documentation procedures that guide organisations to respond, recover, resume and restore to a predefined level of operation following disruption.	ISO 22300:2018
Business impact analysis (BIA)	An analysis of an information system's requirements, functions and interdependencies used to characterise system contingency requirements and priorities in the event of a significant disruption.	NIST
	Management's analysis of an entity's requirements, functions and interdependencies used to characterise contingency needs and priorities in the event of a disruption.	FFIEC
	The process of analysing activities and the effect that a business disruption might have on them.	ISO 22300:2018
Business recovery planning	Steps taken to resume the business within an acceptable time frame following a disruption.	BCI/DRJ

Key Term	Definition	Source
Business resumption planning	One of three core disciplines of BCM. Business resumption addresses restoration of disrupted business functions following a disruption. The planning resource is known as the business resumption plan. The audience of these plans is the first-line personnel.	Protiviti, based on best practices
Cloud service provider (CSP)	A company that offers technology platforms, and access to those platforms, for purposes of leveraging cloud-based storage, infrastructure or application services.	Protiviti, based on best practices
Continuity of operations plan (COOP)	Management policy and procedures used to guide an enterprise response to a major loss of enterprise capabilities or damage to its facilities. It defines the activities of individual departments and agencies and their subcomponents to ensure that their essential functions are performed.	BCI/DRJ
Continuity risk assessment (CRA)	The point-in-time process of identifying operational risks to an organisation and defining and implementing relevant controls with a focus on business continuity-related events.	Protiviti, based on best practices
Crisis communications	As part of crisis management, crisis communications is the planning, development and delivery of all messaging utilised as part of a coordinated response to an event. Crisis communications should include audiences both internal and external to the organisation and may include the use of phone, email, websites, social media and mass notification tools.	Protiviti, based on best practices
Crisis management	The process of managing an entity's preparedness, mitigation response, continuity or recovery in the event of an unexpected significant disruption, incident or emergency.	FFIEC BCI/DRJ
Cybersecurity incident response	The reactive security function of an organisation's defense in-depth strategy. If, for any reason, proactive defenses fail, reactive defenses assume the full burden of organisational security. Where mature proactive defenses are characterised by the logical application of resources to risk and functionality, mature incident response and reactive security are characterised by a maximum of flexibility and vigilance. Protiviti's incident response methodology highlights several functions in constant communication. Containment efforts are established and then modified by new discoveries in the investigation. Vigilance efforts protect against new threats or previously unknown threats. Restoration to business function within acceptable risk categories is the goal. Advisory services are directed toward communication of information to organisational leadership and delegation of authority to act during a crisis within acceptable boundaries.	Protiviti, based on best practices
Disaster recovery (DR)	One of three core disciplines of BCM. Also known as IT disaster recovery (ITDR), this set of processes, policies and procedures relates to preparing for recovery or continuation of technology infrastructure, systems and applications vital to an organisation after a disaster or outage. Disaster recovery focuses on information or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning amid disruptive events. Disaster recovery is a subset of business continuity.	BCI/DRJ

Key Term	Definition	Source
Emergency management/ operations	See **Crisis Management.**	FFIEC
	In the healthcare sector, an organisation will use its emergency operations plan to define its response to emergencies and help position itself for recovery after the emergency has passed. Various aspects of a recovery effort could take place during an event or after an event. Recovery strategies and actions are designed to help restore systems critical to providing care, treatment and services in the most expeditious manner possible.	The Joint Commission
Emergency operations centre (EOC)	The facility used by the incident or crisis management team after the first phase of plan invocation. An organisation must have a primary and secondary location for an EOC in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts.	BCI/DRJ
	An EOC is the physical location where an organisation sets up during an emergency to coordinate response, recovery actions and resources, and to make management decisions. These centres are sometimes referred to as crisis command centres, situation rooms, war rooms or crisis management centres. A properly designed EOC should serve as an effective and efficient facility for coordinating emergency response efforts. An EOC can be used for different purposes, including operations tracking, decision-making and training. The EOC can optimise communication and coordination through effective information management and presentation. Due to the difficulty of centralising key decision-makers at a single location, especially during a disaster scenario, organisations should consider making multiple virtual options available (e.g., conference call options, video chat, hard line, and cellular options).	Protiviti, based on best practices
Emergency response	Actions taken in response to a disaster warning or alert to minimise or contain the eventual negative effects, and those taken to save and preserve lives and provide basic services in the immediate aftermath of a disaster, for as long as an emergency situation prevails.	BCI/DRJ
Enterprise risk management (ERM)	Includes methods and processes used by organisations to manage risks and seize opportunities related to achievement of their objectives.	BCI/DRJ
Financial risk	Economic and quantifiable impacts resulting from a disruption to normal business. This may include loss of revenue, unusual incurred expenses, market capitalisation, sanctions or penalties due to legal or compliance concerns, etc.	Protiviti, based on best practices
Incident management	The process of identifying, analysing and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit disruption and restore operations as quickly as possible.	FFIEC
Incident response	The response of an organisation to a disaster or other significant event that may significantly impact the organisation, its people or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment and any other measures necessary to bring an organisation to a more stable status.	BCI/DRJ

Key Term	Definition	Source
IT disaster recovery (ITDR)	See **Disaster Recovery**.	Protiviti, based on best practices
Major incident management (MIM)	See also **Crisis Management**. The method by which an organisation plans for and responds to an event impacting personnel, assets, the brand, property and equipment, etc.	Protiviti, based on best practices
Maximum allowable downtime (MAD)	See **Maximum Tolerable Downtime (MTD)**.	FFIEC
Maximum tolerable downtime (MTD)	The amount of time mission/business processes can be disrupted without causing significant harm to the organisation's mission.	NIST
	The total amount of time the system owner or authorising official is willing to accept for a business process disruption, including all impact considerations.	FFIEC
	The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.	ISO 22300:2018
Mission-critical	Any telecommunications or information system that is defined as a national security system or that processes any information that the loss, misuse, disclosure or unauthorised access to or modification of would have a debilitating impact on the mission of an agency.	NIST
Mobile recovery centre	Mobile recovery centres provide temporary workspace facilities onsite to aid local recovery capabilities. These facilities are typically equipped with power, environmental systems, IT assets (including personal computers) and voice/data communications (delivered through satellite coverage). Most providers of mobile recovery solutions promise delivery within 24 to 72 hours. Mobile recovery solutions are flexible and can be used as data centres, call centres and general office space. Configurations for general office space, ranging from 10 to 1,000 seats, are typically available. Some organisations use mobile recovery solutions as retail space if needed to support an affected customer base (particularly when customer service is needed following a natural disaster).	Protiviti, based on best practices
Operational resilience	The ability of systems to resist, absorb and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction or loss of ability to perform mission-related functions.	NIST
	The ability of an entity's personnel, systems, telecommunications networks, activities or processes to resist, absorb and recover from or adapt to an incident that may cause harm, destruction or loss of ability to perform mission-related functions.	FFIEC
Operational risk	The risk of loss resulting from inadequate or failed procedures and controls. This includes loss from events related to technology and infrastructure failure, business interruptions and staff-related problems, and external events such as regulatory changes.	BCI/DRJ
Pandemic	The worldwide spread of a new disease.	WHO

Key Term	Definition	Source
Public Company Accounting Oversight Board (PCAOB)	A nonprofit corporation established by Congress to oversee the audits of public companies in order to protect investors and the public interest by promoting informative, accurate and independent audit reports.	PCAOB
Recovery point objective (RPO)	The point in time to which data must be recovered after an outage.	NIST
	The point in time to which data used by an activity is restored to enable the resumption of business functions. The RPO is expressed backward in time from the point of disruption and can be specified in increments of time (e.g., minutes, hours or days).	FFIEC
	The point in time to which data is restored and/or systems are recovered after an outage.	BCI/DRJ
Recovery time objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organisation's mission or mission/business processes.	NIST
	The period of time within which systems, applications or functions must be recovered after an outage. RTO includes the time required for assessment, execution and verification.	BCI/DRJ
Regulatory risk	Similar to legislative or statutory risk, but usually comprised of rules imposed by a regulator rather than through direct government legislation.	BCI/DRJ
Reputation risk	A type of risk that relates to unwanted or negative attention resulting from an event or disruption impacting normal business. Reputation risk can be realised due to negative social media activity (e.g., Glassdoor, Facebook or LinkedIn comments) intended to paint the organisation in a negative light toward a broad audience.	Protiviti, based on best practices
Resilience	Ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents.	NIST
	Process and procedures required to maintain or recover critical services such as remote access or end-user support during a business interruption.	BCI/DRJ
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.	ISO Guide 73
	The process of identifying the risks to an organisation, assessing the critical functions necessary for an organisation to continue business operations, defining the controls in place to reduce organisation exposure and evaluating the cost for such controls.	BCI/DRJ

Key Term	Definition	Source
Sarbanes-Oxley Act (SOX)	The Sarbanes-Oxley Act is a series of legislation established in 2002. From a compliance perspective, the most important sections within these are often considered to be 302, 401, 404, 409, 802 and 906. SOX controls regarding IT disaster recovery focus on backup and recovery requirements for all in-scope SOX applications and underlying data.	Protiviti, based on best practices and soxlaw.com
Simulation	One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation.	BCI/DRJ
Third-party (vendor) risk management	See **Vendor (Risk) Management**.	Protiviti, based on best practices
Training and awareness	A formal process for educating employees and raising an understanding for a continuity program.	Protiviti, based on best practices
Vendor (risk) management	The ongoing practice of defining, assessing and monitoring business partners, suppliers or third-party providers to determine risk associated with delivery of necessary products and/or services as part of an established business relationship.	Protiviti, based on best practices
Work from home (WFH)	A recovery strategy and alternative working arrangement where personnel utilise their place of residence, or locale away from the primary office, to complete daily work.	Protiviti, based on best practices

INFORMATION SOURCES

Australian Prudential Regulatory Authority	ISO/IEC 27001, ISO/IEC 27002 and ISO 27031
Basel Accords	ISACA
California Consumer Privacy Act	ITIL
CIS Critical Security Controls (formerly SANS Top 20)	Monetary Authority of Singapore
Commodity Futures Trading Commission	NFPA: High-rise buildings safety
Critical Infrastructure Protection	NASD
DHS — Banking and Finance Sector-Specific Plan	EPA: National Contingency Plan Subpart J
DHS — Financial Services Sector, Sector Overview	NIST Cybersecurity Framework
Dodd-Frank Wall Street Reform and Consumer Protection Act	North American Electric Reliability Corporation (NERC)
Federal Emergency Management Agency (FEMA)	NYDFS Cybersecurity Regulation (23 NYCRR 500)
Federal Energy Regulatory Commission	US DOL: OSHA
Federal preparedness circulars	U.S. Environmental Health and Safety (EHS)
FINRA	The Joint Commission
GDPR.EU	USA PATRIOT Act
Homeland Security Act	U.S. Department of Energy
Hong Kong Monetary Authority	U.S. Food and Drug Administration (FDA)
HHS/HIPAA	World Health Organisation (WHO) — COVID-19 Guidance
ISO 22300:2018	

TESTING OPTIONS

Testing Type	Description/Attributes	Pros	Cons
Tabletop Exercise	A facilitated session with various recovery team members, with a conceptual walk-through of planning materials using test scenarios and a series of predeveloped test scripts for any combination of crisis management, business resumption and IT disaster recovery personnel.	• Easy to coordinate and execute • Low cost and relatively low effort required from participants • Identifies glaring gaps in plans • Safe place for discussion	• Lower value because of limited time and use of verbal discussion only • Requires use of many assumptions that may or may not hold true in a real disaster event
Simulation	Simulation of a disaster event to determine how well the plan responds to the specific event in the operational environment.	• Highest likelihood of identifying gaps in capabilities and the plan (both large and small)	• One of the costlier testing methods and the most impactful to the business if not isolated properly (i.e., could create unintended impact to the business if simulation efforts are unsuccessful)
Procedure Verification Test (Business Function Testing) — also referred to as a "Desktop"	Evaluation of the logic of a specific procedure in determining if a deficiency exists through a combination of desk checks and simulations. Limited in scope to a specific process or business unit.	• Allows for a very focused, deep dive of an area, process or technology to identify a plan and/or configuration flaws	• Narrow in scope and related results
Communication Testing (e.g., Call Tree or Emergency Mass Notification System [EMNS])	Testing the accuracy and completeness of the organisation's employee call tree, customer contact information channels and critical supplier, vendor and business partner contact information. Testing can be done as part of a tabletop exercise or simulation or potentially as a standalone activity. This is a key component of the BCM process.	• Various modes of communication can be assessed (e.g., BCM alert system, email, text message, phone call, recorded message line) • Identifies gaps in coverage for employee and other internal stakeholders	• This testing type often ignores communications with critical third-party vendors, suppliers, regulators and law enforcement
IT Disaster Recovery Testing	An exercise to conduct an announced or unannounced disaster simulation and execute documented system recovery procedures. The primary objective is to verify that critical systems and backup data can be recovered based on a specific timeline and documented application, data and infrastructure interdependencies.	• Can be used to exercise "active-active" and "active-passive" IT continuity models	• Often focuses on specific systems or technologies and utilises scenarios in isolation (e.g., SAN environment outage, VPN concentrator failure) • Failures of IT infrastructure often do not occur in siloes during a true disaster event

Testing Type	Description/Attributes	Pros	Cons
Alternate Site Testing	A test of all restoration/recovery components at an alternate site. This should include a test of the organisation's ability to relocate staff to the alternate site, as well as a validation that recovery processes and IT assets operate.	• Validates if an alternate site is equipped to support failover recovery needs and helps organisations extrapolate how long they could persist in the alternate environment	• Capacity needs, requirements and timing may be hard to replicate in a test, as most companies will choose to perform this testing during the best possible time (versus the worst)
End-to-End Testing	A test of all aspects of alternate facilities, business processes and IT. An end-to-end test differs from an alternate site test in that critical suppliers/business partners and customers — internal or external — are included within the scope.	• This test typically validates connectivity to the business's production site and examines all integration between internal and external stakeholders.	• Very challenging, costly and time consuming to coordinate
Work From Home	Enabling employees to work from home or from a remote location when unable to work from a primary location. As the COVID-19 pandemic of 2020 has shown, having all employees working from home is a real possibility.	• Allows for continued productivity even when employee groups need to be dispersed • Helps to minimise spread of infectious diseases between employees • Identifies what jobs can effectively be performed from outside of the office for a prolonged period	• Increased cost and strain on IT infrastructure supporting remote connectivity • Reduction in team communication and camaraderie unless compensated with technology (e.g., video conference calls)
Pandemic Simulation	A testing scenario focused on the potential disruptions caused by a pandemic and its potential effects on the business (e.g., losing a large portion of the workforce due to illness at the same time)	• Identifies areas where resources are thin and require cross-training • Identifies single points of failure in the system	• Various characteristics about the pandemic (e.g., how long it lasts, length of illness, transmission rate) must all be assumed for the simulation; however, all these things are very hard to predict with real pandemics
Crisis Management Simulation	A testing option focused on convening only the crisis management team to drill on how various types of situations would be handled and the types of decisions that would need to be made, by whom and on what timeline. Often leverages the tabletop approach.	• Frequent exercises like this drive the level of communication and cohesion of the crisis management team • Allows for even the most outlandish scenarios to be contemplated	• Requires many assumptions to be made regarding how things would work "in real life"

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

ABOUT OUR IT CONSULTING SERVICES

In today's rapidly evolving technological environment, a trusted adviser – one who not only provides relevant insights, but delivers a combination of strategic vision, proven expertise and practical experience – can enhance the value of your business with technology. Our global IT Consulting practice has helped CIOs and IT leaders at more than 1,200 companies worldwide design and implement advanced solutions in IT governance, security, data management, applications and compliance. By partnering with us, you ensure that your IT organisation performs with the same focus and excellence with which you manage day-to-day business operations. We will work with you to address IT security and privacy issues and deploy advanced and customised application and data management structures that not only solve problems, but also add value to your business.

CONTACTS

UNITED STATES

Kim Bozzella
Managing Director,
Global Leader of Technology Consulting
+1.212.603.5429
kim.bozzella@protiviti.com

Kevin Khan
Managing Director
+1.212.479.0748
kevin.khan@protiviti.com

Matthew Watson
Managing Director
+1.571.382.9707
matthew.watson@protiviti.com

Damon Owen
Managing Director
+1.212.822.4750
damon.owen@protiviti.com

Dugan Krwawicz
Director
+1.469.374.2439
dugan.krwawicz@protiviti.com

SINGAPORE

Sam Basset
Managing Director
+65.6220.6066
sam.bassett@protiviti.com

INDIA

Sandeep Gupta
Managing Director
+91.22.6626.3333
sandeep.gupta@protivitiglobal.in

AUSTRALIA

Ewen Ferguson
Managing Director
+61.2.8220.9506
ewen.ferguson@protiviti.com.au

ITALY

Enrico Ferretti
Managing Director
+39.06.4204.9801
enrico.ferretti@protiviti.it

UNITED KINGDOM

Thomas Lemon
Managing Director
+44.207.024.7526
thomas.lemon@protiviti.co.uk

JAPAN

Masato Maki
Managing Director
+81.3.5219.6600
masato.maki@protiviti.jp

GERMANY

Kai-Uwe Ruhse
Managing Director
+49.6996.376.8148
kai-uwe.ruhse@protiviti.de

HONG KONG

Michael Pang
Managing Director
+852.2238.0438
michael.pang@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

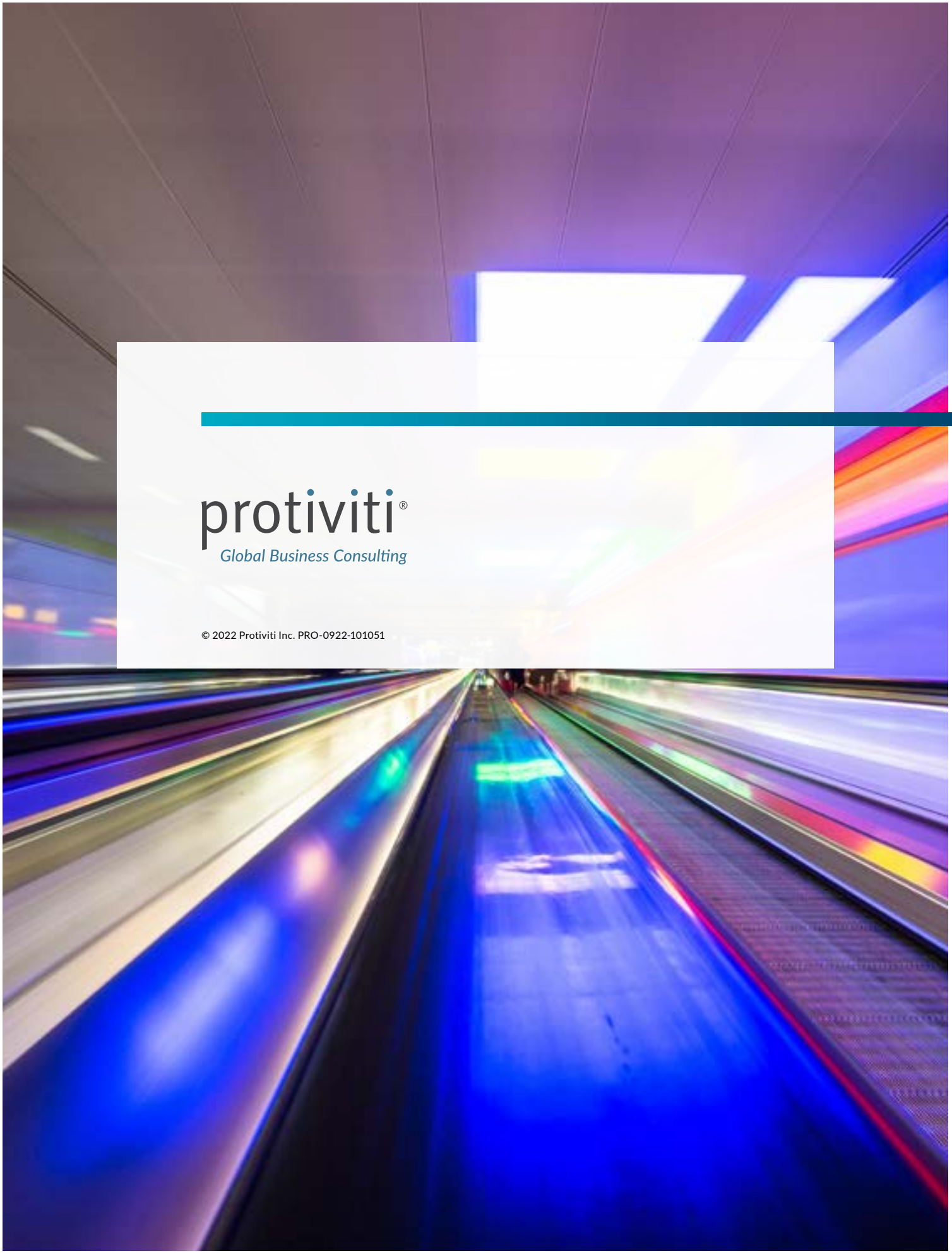
INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®



protiviti®

Global Business Consulting