protiviti®

Face the Future with Confidence

A Guide to Business Continuity Management – Top 15 Frequently Asked Questions

July 2020

Table of Contents

Introduction

Calamities and setbacks are a part of life. Twenty-four-hour news coverage, with screaming headlines of disasters and mishaps around the world — earthquakes, active shootings, severe storms, epidemics, data breaches or terrorist attacks — has become increasingly less shocking to our desensitised senses. 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 means contemplating all scenarios and solutions, 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 the coronavirus (COVID-19) pandemic, business continuity and resilience has become a critical discussion in boardrooms and C-suites across the world. The pandemic's widespread impact has forced organisations to revisit business continuity planning (BCP) and how to embed BCP practices in day-to-day operations. As we consider the changing landscape 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) programme that responds to all crisis types and scenarios? Who is the right person in the organisation to own and manage the BCM programme? And, what are the critical elements of a business continuity policy?

In Protiviti's *Guide to Business Continuity Management: Frequently Asked Questions* (June 2020), we answer these critical questions along with many other pressing questions about BCM and related practices. The complete fourth edition, which is being released in phases, covers many areas including:

- COVID-19 and pandemics
- The Basics of BCM
- Programme development and strategies
- Ownership and governance
- The regulatory environment
- Training and awareness
- Testing and maintenance
- Compliance monitoring and auditing

Also included in this edition is a glossary of key BCM terms and definitions. 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 towards becoming prepared and building resilience for the unknown. Our goal is to help companies keep ahead of risks by building sustainable business continuity programmes.

Protiviti
July 2020

COVID-19 and Pandemics

1. Considering the COVID-19 pandemic, what role should business continuity management (BCM) programmes play in pandemic planning and response?

Pandemic planning or preparedness is an important part of business continuity planning. As COVID-19 has shown, pandemic preparedness presents unique challenges for businesses, given its far-reaching geographic impact and difficulty with predicting its scale and duration. It can also have a wide range of impacts on businesses (e.g., worker displacement, technology constraints, decreased production, and challenges with third-party capabilities). 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 programme 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 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 outline 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 programme.

2. 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 any 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 business impact analysis 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.

The nice thing 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.

3. How should your BCM programme provide support for returning to normalcy post-pandemic?

The core building blocks of any good BCM programme 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 that forms 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 helped execute an IT disaster recovery programme that allows, for example, an entire workforce to go remote all at the same time, and all of the bandwidth and infrastructure implications that go along with making that a possibility, are also responsible for helping those same individuals return to normalcy.

The Basics of BCM

4. What is Business Continuity Management (BCM)?

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 disrupted aspects of business functions and processes that relate to or support the delivery of core products or services to a customer. Business resumption processes focus on the evaluation of people, processes, technology and other resources vital to the organisation's operations. 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 towards business as usual.
- **IT disaster recovery (ITDR)** – This discipline addresses restoration of critical IT assets, including systems, applications, databases, and storage and network assets. An ITDR strategy also should encompass all technology service provider relationships (e.g., cloud providers) to ensure that all technical stakeholders remain aligned.

In addition to the traditional BCM disciplines listed above, many organisations manage other closely related programmes as part of their overall BCM programme. These programmes 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 programmes 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, a phishing attempt or a 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, and safety and environmental health teams may have input in developing recovery strategies. Integration of these enterprise-impacting functions, depending on the organisation or industry, can be confusing.

5. What is the value to an organisation in designing and deploying BCM programmes?

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 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
- 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 programme 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 programme. 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 credit worthiness or reputation. Generally, companies that violate regulations or compliance requirements face:

- Fines, penalties and judgements.
- 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.

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, a measured, empathetic, rapid and relevant response to any event is crucial to maintain a positive reputation. A mature BCM programme drives value by protecting a company's brand and adeptly managing the ever-changing business landscape in the face of growing competition.

6. 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 programme. A building evacuation plan is an example of an emergency response action.
- **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 programmes 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 programme 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 –** The 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 programme, 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 disaster. 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 programme.

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

7. 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, human resources and investor relations 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 COVID-19, 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.

Programme Development and Strategies

8. Is there a best practice approach to business continuity planning?

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

- **BCM programme governance** – This involves identification and formalisation of the BCM steering committee and executive-level risk management oversight to determine BCM programme requirements.
- **BCM programme and implementation design** —This includes definition of policies, standards and tools to support business continuity efforts. In addition, an effective BCM programme should define the operating model, which includes who is accountable and responsible for each key discipline of the programme (e.g., crisis management, business resumption and IT disaster recovery), technology tools used to monitor and manage the programme 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 programme, enables organisations to capture and effectively measure the potential business impacts of a disruption (i.e., operational, reputation, 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 programme 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 programme.

- **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 those not directly engaged on a recovery team.
- **Compliance monitoring and audit** – Conducting regular and objective reviews of the BCM programme allows for programme changes, if needed, while following a reasonable cadence. Also, the reviews will enable easy-to-maintain compliance with internal and third-party business continuity standards.

9. 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 programmes. 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 programme 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.
- **Programme scope** – Defines programme tenets and recovery priorities via the continuity risk assessments and a business impact analysis. Further, this foundational effort establishes the criteria for the type and scale of incidents to be addressed in the BCM programme.
- **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.
- **Plan development and maintenance** – Specifies the standards regarding the review and maintenance of all programme and planning documentation.
- **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.
- **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 assessment** – 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 programme 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 programme effectively.

10. 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, man-made, 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 hours, as opposed to many weeks, using the input of business leaders throughout the organisation.

With regard to 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 above provide a way to jumpstart 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.

Ownership and Governance

11. Who is the right person in the organisation to own the BCM programme?

As organisations begin to develop their BCM programme capabilities and plans, they are confronted with a common question and dilemma: Who should own the overall programme? A successful BCM programme 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 programme, many choose to utilise existing resources and/or personnel.

Organisations typically provide leadership to the BCM programme through one of three roles: sponsors, owners and 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 programme 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 programme 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 programme 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 programme. The nuances of a company's industry, risk profile, culture and operations can influence the decision about where the BCM should reside. 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 programme.
- **Information technology –** The CTO's, CIO's or CISO's organisation or vertical.

As a matter of practice, it is recommended that BCM programme 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 programme.

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
- Number 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 programme 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." As such, when it comes to ensuring that a business impact analysis or a resumption plan for a department is current and actionable, the BCM lead (or leads) must solicit input and involvement from those individuals on the ground.

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 programme.

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

- **Centralised** – Under this model, a central continuity office serves the business units by providing policy, guidance, tools, templates, metrics and maintenance.
- **Divisional** – Multiple continuity offices serve the different region and business lines.
- **Federated** – A central continuity office, linked to various centres of excellence, provides dedicated services to different regions and business lines.

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

When not a compliance need, BCM is often viewed as discretionary, since the value of time and resources spent planning, training, documenting, testing and validating all aspects of a programme 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., the business continuity risk assessment and business impact analysis, or 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).

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 programme. Programme 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 and enforce BCM.

The Regulatory Environment

14. How should regulations and standards shape the development of a BCM programme?

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 of 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 protections for employees and all those who depend on an organisation's services (e.g., customers, clients and patients).

Regulations and standards are used to support BCM programme development, measure adherence and assess maturity. While regulations and standards often provide guidance on required or suggested 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 towards financial services. Using these more rigorous guidelines, it is not uncommon for other industries to apply the relevant controls and strategies as they model all best practices.

15. What is the connection between operational resilience and business continuity management?

Regulators around the world are developing new rules and expectations aimed at strengthening the operational resilience of the financial services sector, an effort being 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 through which an operational resilience programme 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 programmes, 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 their important business service.
- **Testing** – Testing various aspects of a BCM programme 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 event. 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 programme. 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, skillsets, processes, technology, data, third parties, operations, reporting requirements and legal entities, along with clearly defined cross-functional/business dependencies and hand-offs.
    - 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 programmes, there are no formal or consistent definitions of important business services, testing or severity levels.

Glossary

KEY TERM	DEFINITION	SOURCE
BCM programme governance	The system of rules, practices and processes by which a business continuity programme 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)	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
	Documented 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
	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 timeframe following a disruption.	BCI/DRJ
Business resumption planning	[One of the 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 (BRP). The audience of these plans is the first-line personnel.	Protiviti, based on best practices

KEY TERM	DEFINITION	SOURCE
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 communication 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 defence in-depth strategy. If, for any reason, proactive defences fail, reactive defences assume the full burden of organisational security. Where mature proactive defences 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 towards 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 the three core disciplines of BCM.] Also known as IT disaster recovery (ITDR), a set of processes, policies and procedures related 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 amidst disruptive events. Disaster recovery is a subset of business continuity.	BCI/DRJ
Emergency management/ operations	See **Crisis Management**.	FFIEC
	Regarding healthcare: 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 the systems critical to providing care, treatment and services in the most expeditious manner possible.	The Joint Commission

KEY TERM	DEFINITION	SOURCE
	The facility used by the incident or crisis management team after the first phase of a 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
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 impact, 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
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 (FISMA) or that processes any information the loss, misuse, disclosure or unauthorised access to or modification of would have a debilitating impact on the mission of an agency.	NIST

KEY TERM	DEFINITION	SOURCE
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 from external events such as regulatory changes.	BCI/DRJ
Pandemic	Worldwide spread of a new disease.	WHO
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 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 towards 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

KEY TERM	DEFINITION	SOURCE
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
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 programme.	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

Glossary Sources

BCI/DRJ	www.drj.com/images/BCI-DRJ-glossary-of-BC-terms-2018-03-09.pdf
FFIEC	ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx
NIST	csrc.nist.gov/glossary?index=A
ISO 22300:2018	www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en
ISACA	support.isaca.org/app/answers/list/p/451
FFIEC Web	www.ffiec.gov/
FINRA	www.finra.org/about
GDPR.EU	gdpr.eu/what-is-gdpr/
HHS	www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
ITIL	www.axelos.com/corporate/media/files/glossaries/itil_2011_glossary_gb-v1-0.pdf
NASD	www.finra.org/sites/default/files/Corporate/p009762.pdf
OSHA	www.osha.gov/faq
The Joint Commission	www.jointcommission.org/standards/standard-faqs?p=1
WHO	www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/

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 our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 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.

Contacts

Matt Watson
Managing Director, Technology Consulting
+1.571.382.9707
matthew.watson@protiviti.com

Dugan P. Krwawicz
Associate Director, Technology Consulting
+1.469.374.2439
dugan.krwawicz@protiviti.com

protiviti®
Face the Future with Confidence