

# Risk Management: Business Continuity Management

With the shift in business goals, work locations, processes, and associated IT usage, IT should consider how these changes may require enhancements to existing Business Continuity Management (BCM) and supporting capabilities. Working through a structured series of questions can identify gaps and areas to enhance Business Continuity Management (BCM) to align with the business needs of the “New Normal”.



## GOVERNANCE AND PROGRAM MANAGEMENT

In this rapidly changing environment, it is likely a risk analysis performed last year could not have identified or accurately evaluated many of today's risk scenarios. Review the full BCM cycle from Objectives to Risk Analysis to Training and Testing considering the current business operating environment.

Have your business goals changed? Are your Business Continuity Management (BCM) goals/strategy aligned to maintain business continuity?

Have you audited the BCM program and objectives to confirm effectiveness and alignment with measurable, realistic, and achievable objectives and SLAs/SLOs?

Have additional sources of risk been identified and prioritized? Have risk assessments been refined reflecting likelihood and impacts?

Have Business Impact Analysis been updated to align with changing risks and recovery needs?

Has Business Continuity training been updated and executed?

Are legal and regulatory requirements understood and accommodated?



## CRISIS/EMERGENCY MANAGEMENT

Ensure the Business Continuity Plan considers critical resources, processes, and tools needed to manage through a crisis. Timely communication is essential, be proactive in establishing communication plans.

Do you know the key areas requiring resiliency? Do you have the capabilities/resources to support those areas? (e.g., infrastructure, 3rd parties, personnel, etc.)

Is there sufficient capacity to support the way you are working today?

Have BCM-related responsibilities changed? Do you have the right representation in BCM within each Business Unit/Area? Are key resources to support BCM activities enabled and available?

Do you have a robust communications plan and formal crisis communications methods in case of failure?



## BUSINESS RECOVERY/CONTINUITY

Review recovery scenarios with impacted parties, ensuring alignment and understanding will help enable a fast recovery.

Have Business Continuity Plans (BCP) been updated/refined and accessible?

Are protocols for business recovery and continuity effective? Have they been refined?

Are all impacted parties aware of the plan and understand their role and expectations?

Have Business Continuity Plans been tested?



## IT DISASTER RECOVERY AND SERVICE CONTINUITY MANAGEMENT\*

Alignment between the BCP and the IT DR plan is important. Confirm priorities, recovery time objectives, and availability of critical resources in the current operating environment.

Are IT Disaster Recovery (DR) and Service Continuity processes and capabilities refined and captured?

Are technology recovery teams distinct from the business process recovery teams?

Does the IT DR plan align with updated Business Risk Assessments, Business Impact Analysis, and Recovery Time objectives?



## SUPPLIER/SUPPLY CHAIN RISK AND CONTINGENCY MANAGEMENT

In evaluating supply chain risk, consider business and IT supply chains, supplier/partner capabilities, and customer needs.

Have risks and single points of failure been identified in your global supply chain and contingencies deployed?

Are critical suppliers and partners aware of their role in the organization's Business Continuity Plan?

How confident are you in your supplier's BCP/DR plans? What contractual mechanisms are in place to mitigate risks?

Has the organization's role in the broader supply chain environment been considered, understanding and minimizing impacts to partners and customers?



## FAILURE PREVENTION

Preventing failures through robust processes and up to date technology can prevent outages that impact business.

How mature is your IT change management process?

Are your platforms supported (e.g., regularly patched, supported hardware)?

Do you know where your equipment resides?

Do you understand the true root cause of outages?

\* Further detail on IT Disaster Recovery can be found at [jabian.com/planahead/risk-management-it-disaster-recovery-planning](http://jabian.com/planahead/risk-management-it-disaster-recovery-planning)

By examining your answers to the questions above, you can get initial visibility into areas of greatest risk and opportunity. If you haven't reviewed your Business Continuity Management program, take the following approach:

1

Review your program and supporting materials;

2

Identify weak spots;

3

Develop processes/capabilities to address those weak spots;

4

Document those enhanced processes/capabilities;

5

Test and verify your Business Continuity Management Program.

## JABIAN IS HERE TO HELP

To learn more about how Jabian can help you align your Business Continuity Management to the “New Normal” or improve IT capabilities with Business needs, simply contact us at [planahead@jabian.com](mailto:planahead@jabian.com).