Business Continuity Planning (BCP) Terms Explained

Are you part of the 52% of companies that do not have a Business Continuity Plan?

With the height of the COVID-19 situation, you must have learned by now that having a BCP in place should have been a pro-active measure rather than a reactive one (and that BCP is not just for pandemics but for major disruptions like - economic downturns, bad publicity, cyber-attacks, data breaches and many more.

To better understand BCP and not be overwhelmed with all the information out there, we'll explain the common terms you will encounter while learning and planning for BCP. If you ever found yourself confused or unsure about certain terms here's a quick guide for you:

1. **Business Continuity Planning (BCP)**

Business Continuity Planning is a proactive business activity to identify, avoid, and mitigate risks associated with a disruption of operations. It details steps to be taken before, during and after an event to maintain the financial and operational viability of an organisation.

2. **Business Continuity Management (BCM)**

A framework for identifying an organisation's risk of exposure to internal and external threats. It's a way to predict the consequences of disruptions to a business and its processes and systems by collecting relevant data, which can be used to develop strategies for the business to recover in the case of an emergency.

3. **Business Disaster Recovery Plan**

A document that specifies exactly what should happen to minimize the impact and return the company to working order as quickly as possible after a disaster occurs that impacts the company.

4. **Contingency Plan**

The act of developing responses in advance for various situations that might impact business. Contingency Planning ensures that proper and immediate follow-up steps will be taken by a management and employees in an emergency. Its major objectives are to ensure (1) containment of damage or injury to, or loss of, personnel and property, and (2) continuity of the key operations of the organization.

5. Crisis

A singular event that places employees at personal risk (whether physical or psychological), threatens the integrity of critical infrastructure, may lead to the loss of sensitive materials or information, hinders the operational productivity of a project, and presents a threat to the business interests and reputation of the company.

6. Grading Risks

The assessment of risk involved in the daily activities of a business and classifying them on the basis of the impact on the business. Grading Risks enables organisations to look for control measures that would help in curing or mitigating the impact of the risk and in some cases negating the risk altogether

Grading Risks in BCP:

- Negligible Level of Risk — Highly Unlikely to Occur
- Low Level of Risk — Remote Chance of Occurrence
- Medium Level of Risk — Some Chance of Occurrence
- High Level of Risk — Likely to Occur
- Extreme Level of Risk — Expected to Occur

7. Incident Management Plan (IMP)

An Incident Management Plan or IMP is a documented plan of action to respond and manage an incident and also to return to the business in a reasonable amount of time following an interruption. This plan details how the incident will be managed from occurrence to back-to-normal operation.

8. Incident Response Plan

A systematic approach taken by an organisation to prepare, detect, contain, and recover from disruptions. An incident response plan helps ensure an orderly, effective response to unwanted incidents, which in turn can help protect an organisation's data, reputation, revenue and assets.

9. Problem

An everyday occurrence that does not affect an individual's safety, the integrity of critical infrastructure, or the protection of sensitive materials or information, and does not undermine significantly the operational productivity of a project, nor devalue the business interests or reputation of the company.

10. Risk

A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

Risk Calculation

$$\text{Risk} = \frac{\text{Asset Cost + Likelihood + Impact}}{3}$$

Types of Risk

1. Strategic Risk
2. Man-Made Risks
3. Natural Risks

11. Risk Mitigation

The process by which an organisation introduces specific measures to minimize or eliminate unacceptable risks associated with its operations. Risk mitigation measures can be directed towards reducing the severity of risk consequences, reducing the probability of the risk materializing, or reducing the organisations exposure to the risk.

12. Risk Quantification

The process of evaluating the risks that have been identified and developing the data that will be needed for making decisions as to what should be done about them.

13. Vulnerability

The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of risk, event or another occurrence.