Top of Form

Bottom of Form

**Unit 5: Risk, Business Continuity and Disaster Recovery**

**In this unit we shall:**

* + Review how and why to create business continuity (BC) and disaster recovery (DR) plans.
  + Discuss the main determining factors in BC/DR plans – including Business Impact Assessments (BIA), Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
  + Discuss emerging trends in Information Risk Management.

**On completion of this unit, you will be able to:**

* + Explain what is meant by BC, DR, RTO and RPO.
  + Suggest the most suitable solutions to meet specific recovery objectives.
  + Discuss some of the factors driving the future of the Information Risk Management field.

**Reflection**

* A **business continuity plan**, often known as a BCP, is a method that describes the potential impact of disaster scenarios on an organization's activities. It guarantees that a corporation to recover from a crisis in a timely way by developing rules that are adaptable to several conditions. The fundamental goal of a business continuity strategy is to safeguard people, property, and investments (BCP). In addition, it positions your firm to recover from unplanned business interruptions, property damage, financial impact, and even loss of life in the wake of an emergency (Akita Box et. al., 2020).
* A **disaster recovery plan (DRP)** is a collection of guidelines that may be used to secure the continuation of an organization's information technology activities. A comprehensive DRP will include recovery procedures for data records, IT hardware and equipment, and the physical location of the IT infrastructure. Natural disasters, such as fires and floods, and man-made disasters, such as computer hacking and malfunctioning equipment, are two sorts of situations that might benefit from a disaster recovery plan (DRP) (Beal, V. (2004)).
* The term "**Recovery Time Objective**" refers to the maximum length of time that a computer, system, network, or application may remain down after a breakdown or disaster has taken place (RTO). The RTO is determined by determining the degree to which the disruption creates a disturbance in usual operations and the amount of money that is lost per unit of time because of the disaster. Additionally, the RTO considers the length of time that the disruption lasts. These factors, in turn, are dependent on the piece of machinery and the application that are being influenced (Michael Kerner, S. (2020).
* **Recovery point objective (RPO)** is the greatest quantity of data – measured in time – that may be lost following a recovery from a catastrophe, failure, or similar event before the amount of data loss exceeds an organization's tolerable threshold. RPO is the maximum amount of data that may be lost after recovering from a catastrophe, failure, or similar occurrence. A RPO specifies the maximum age of data or files held in backup storage in the case of a network or computer system failure. This is required to achieve the RPO's intended objective (Druva (2021).

For every recovery method each have its own different scenarios, like RTO, or "Recovery Time Objective," is the goal that your firm sets for the maximum length of time it should take to restart normal operations after a service disruption or the loss of data. The RPO metric estimates the amount of data an organization can afford to lose before it is deemed a failure (Insights, R. (2021). So, both these are better in different scenarios.

**Factor Analysis of Information Risk** is a taxonomy of the aspects that contribute to risk and their interactions with one another. The major objective of this task is to provide exact probabilities for the frequency and magnitude of data loss. It is not a method that can be used to analyze the risk of a company (Dobson, et. al., 2011). These factors include Threat Event Frequency, Contact Frequency, Probability of Action, Vulnerability, Threat Capability, Difficulty, Loss Event Frequency, Primary Loss Magnitude, Secondary Loss Event Frequency, and Secondary Risk (Wikipedia (2022).

**References:**

AkitaBox (2020). *The Importance of a Business Continuity Plan (Plus a Free Guide) – AkitaBox*. [online] Available at: https://home.akitabox.com/blog/importance-of-business-continuity-plan/ [Accessed 26 Jun. 2022].

Beal, V. (2004). *What is DRP?* [online] Webopedia. Available at: <https://www.webopedia.com/definitions/drp/>.

Michael Kerner, S. (2020). *What Is A Recovery Time Objective And How Does It Work?* [online] WhatIs.com. Available at: <https://www.techtarget.com/whatis/definition/recovery-time-objective-RTO#:~:text=The%20recovery%20time%20objective%20(RTO>.

Druva (2021). *What is a recovery point objective? Definition and related FAQs*. [online] Druva. Available at: <https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/>.

Insights, R. (2021). *The Difference Between RTO & RPO*. [online] Rubrik. Available at: https://www.rubrik.com/insights/rto-rpo-whats-the-difference [Accessed 26 Jun. 2022].

Dobson, I. and Hietala, J. eds., 2011. Risk Management-The Open Group Guide. *Van Haren Pub*.

Wikipedia (2022). *Factor analysis of information risk*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Factor\_analysis\_of\_information\_risk#cite\_note-OGC081-1 [Accessed 26 Jun. 2022].