Discussion-7 Contingency planning

Discussion Topic:

Contingency planning consists of four major components: The Business Impact Analysis, the Incident Response Plan, the Disaster Recovery Plan, and the Business Continuity Plan. Whether an organization adopts one plan or multiple plans, each of these components must be addressed and developed entirely.

Taking into consideration the material from this module, discuss your experience with these four components of Contingency Planning. Additionally, discuss whether your organization has adopted the one-plan method or multiple-plan method. Do you think one method is better than the other?

My Post:

Hello Class,

I have no real-life experience with the four components of Contingency Planning (CP), and I do not know if the organization I work for has adopted the one-plan method or multiple-plan method.
However, from this module's material, I can provide an overview of CP. Contingency planning is a process utilized to prepare for, anticipate, and plan for the recovery of events, human and/or natural (CSU Global, 2025). The goal of CP is to have procedures and steps in place to respond to circumstances that compromise the availability of a system. This process integrates four components or plans: the Business Impact Analysis (BIA), the Incident Response Plan (IRP), the Disaster Recovery Plan (DRP), and the Business Continuity Plan (BCP).

Business Impact Analysis (BIA) is a risk assessment plan that uses a quantitative or qualitative process to investigate the impact that various adverse events can have on an organization (Chapple, 2022a; CSU Global, 2025). While risk management identifies threats and vulnerabilities to prevent incidents, the BIA is utilized after preventive measures, that is, after risk management measures have failed and an attack has succeeded.

Incident Response Plan (IRP), on the other hand, is a set of processes and procedures that anticipate, detect, and mitigate the effects of an event that might compromise information and assets (CSU Global, 2025). IRP's two goals are to control or contain the damage caused by the incident and then to eradicate the threat, that is, to remove any traces of the incident from systems and networks (Chapple, 2024b).

When an IRP can no longer handle the recovery from loss effectively and efficiently, the Disaster Recovery Plan (DRP) is activated (CSU Global, 2025). The DRP's primary goal is to restore IT, OT, communications, and other information processing capabilities into a safe, secure, and reliable operating condition (uCertify, n.d.).

Concurrently with the DRP, the Business Continuity Plan (BCP) is used to ensure that critical business functions can continue if a disaster occurs (CSU Global, 2025). It is a living document that is regularly tested, maintained, and updated. I should include the organization's mission and the resources required to maintain operations, even if the primary business location is unusable (uCertify, n.d.).

While these plans are related and support one another, they represent distinct areas of CP. For example, an IRP focuses on a single incident, while a DRP handles severe events that can put an organization out of business. Additionally, these plans can be implemented and adopted with a “one-plan” or “multiple-plan” approach. For example, a single document approach might be adopted by a very small organization, but for larger and more complex organizations, a single document probably will not be sufficient, necessitating separate plans. This multiple-plan approach is more flexible and more focused on the specifics of each module and component of the organization. In other words, it delegates responsibilities, is more modular, and is more focused on specific challenges/incident responses, disaster recovery, and overall business continuity, making the multiple-plan method a more appropriate contingency planning approach for medium to large businesses and corporations.

-Alex

References:

Chapple, M. (2022a, September 6). Business continuity planning (BCP) [Video]. *ISC2 Certified in Cybersecurity (CC) Cert Prep*. LinkedIn Learn.https://www.linkedin.com/learning/cert-prep-isc2-certified-in-cybersecurity-cc/business-continuity-planning?autoAdvance=false&u=2245842

Chapple, M. (2024b, April 25). Incident eradication and recovery. *ISC2 Certified Information Systems Security Professional (CISSP) (2024) Cert Prep*. LinkedIn Learn

CSU Global (2025). Module 7: Business Continuity [Interactive Lecture]. Canvas. https://csuglobal.instructure.com/courses/110243/pages/module-7-overview-2?module_item_id=5721044

uCertify (n.d). Lesson 11: Business Continuity via Information Security and People Power. *(ISC)² SSCP Certification Training Guide*. uCertify. ISBN: 976164493776.