1. **Security Planning**

Suppose you are in the InfoSec program of a large bank with several branches, and tasked to handle contingencies and plan for Business Continuity.

1. identify main steps to develop the BC program.
2. Form the BC Team
3. –Develop the BC planning policy statement
4. –Review the BIA
5. –Identify preventative controls
6. –Create relocation strategies
7. –Develop the BC plan
8. –Ensure BC plan, testing, training, and exercises
9. –Ensure BC plan maintenance
10. identify major BCP components (at least five) and develop a high-level plan.

Business Continuity Plan Every bank or financial institution shall develop and maintain a comprehensive business continuity plan (BCP) based on their business impact analysis, risk assessment and recovery objectives. In developing BCP, a bank or financial institution shall ensure that: (i) The plan is institution-wide and it is disseminated so that the relevant groups of personnel can implement it in a timely manner; (ii) The business continuity plan addresses the staff requirements and relocation to the alternate site in the event of a major disruption; (iii) The plan is documented and contains a minimum of the following key elements: a. A business continuity plan awareness program; b. a risk management program that includes clearly defined roles and responsibilities for resumption of business processes, including support organization functions; c. procedures for mitigating interdependency risks between departments within the institution and with other institutions; d. Trigger points and/or dates to activate the continuity plan; e. Data back-up and recovery (hard copy and electronic); f. Processes to deal with the loss of information that are not available from backup data; g. Manual processes for continuing operations until technology is repaired; h. Accessible recovery locations and emergency operations centers; i. A process for automatically switching telephone and data lines; j. Testing of the business continuity plans on an end-to-end basis; k. A review process to ensure that the business continuity plan is feasible and up-to-date; l. Specific incident/emergency management responses that identify assembly areas at a safe distance from the site of the incident; Annual statement by Senior Management on whether the recovery strategies adopted are still valid and whether the documented BCPs are properly tested and maintained; and n. Regulatory approval.

Critical Elements

There are 10 critical elements of a BCP specified in FINRA Rule 4370. Each firm need only address the elements applicable to its business, but if you do not include a specified element in your firm’s plan, your plan must document why it is not included:

(1) Data back-up and recovery (hard copy and electronic);

(2) All mission critical systems;

(3) Financial and operational assessments;

(4) Alternate communications between customers and the member;

(5) Alternate communications between the member and its employees;

(6) Alternate physical location of employees;

(7) Critical business constituent, bank, and counter-party impact;

(8) Regulatory reporting;

(9) Communications with regulators; and

(10) How the firm will assure customers’ prompt access to their funds and

securities in the event that the member determines that it is unable to continue its

business.

https://www.boj.or.jp/en/announcements/release\_2003/data/sai0309a.pdf

1. **Security Policy**

Management focuses on and decides policy issues for a specific system. Such SysSPs are often codified as standards and procedures. Imagine you are the Chief Information Security Officer of KU, and responsible for developing a policy regarding to the use and protection of electronic health records in KU research projects. Please read KU Information Technology Security Policy and related issue-specific security policies, and identify/discuss:

1) what are the roles responsible for the development and implementation of this policy?

2) what are the existing ISSPs and laws related to the development of this policy?

3) what are the security objectives (please be more specific than CIA) for such system using EHRs? Describe security actions and/or operational rules.