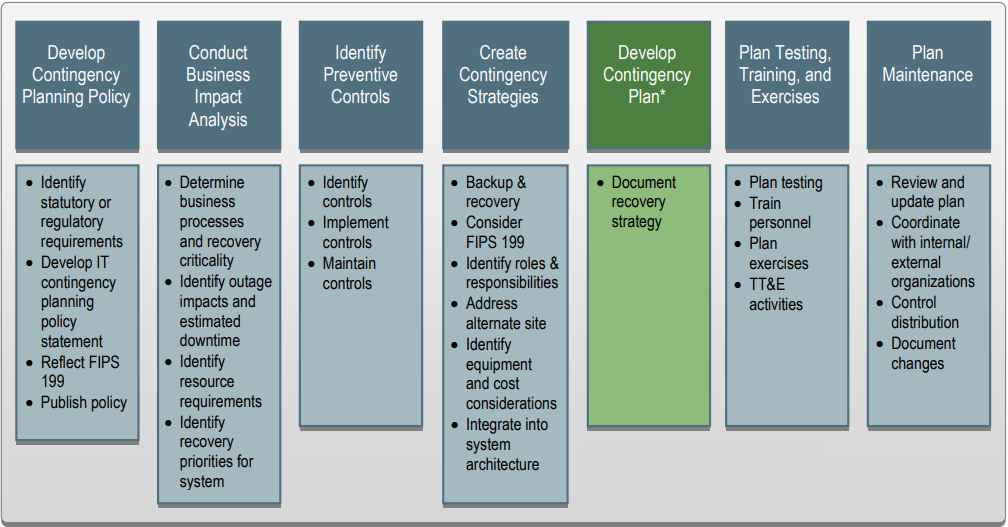
Project Topic: Contingency Planning

Author: Paul McGlothlin & Emily Harrison

Information:

A contingency plan is a plan designed to take a possible future event or circumstance into account- it is a plan for your other plans in case they fail. You may think of them as the backup defense mechanism put in place in case of emergency. The National Institute of Standards and Technology, or NIST, has regulated 7 exact steps to take when developing a proper contingency plan:

1. **Policy Requirement:**Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
2. **BIA(Business Impact Analysis):** The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business functions. A template for developing the BIA is provided to assist the user.
3. **Preventative Controls:** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
4. **Contingency Strategies:** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. **Contingency Plan:** The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
6. **Plan Training:** Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.
7. **Plan Maintenance:** The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes. 

Below is a simple example of a completed contingency plan using the 7-step program\*

Situation: System X controlled at an off-site location suddenly goes down as the site experiences a power outage. What kind of contingency plan could be in place to ensure that the data in system X was safely preserved?

1. **Policy Requirements:** Incase of an event of a power outage were to occur, System X requires that all important data is to be backed up appropriately before. It is also important that all managers/supervisors and IT support employees know and understand the contingency plan beforehand.
2. **BIA:** Failure to complete plan would lead to destruction of back-up data, losing company resources.
3. **Preventative Controls:** On-site backup generators in case of major power outage. Utilize surge protectors in case of minor power outages. Ensure that all important data is backed up.
4. **Contingency Strategies:** Ensure that there is enough storage available for any backups. Assign an employee in IT support to be an emergency contact number in case a power outage does occur. Hard drives and generators will cost around $10000.
5. **Contingency Plan:** Evaluate the situation and turn on backup generators. Ensure that all of the data is safe and not missing. If so use the data that was backed up before the incident. If the person is unsure of what to do, contact either IT support or a supervisor/manager.
6. **Plan Training:** Regularly go through the plan with others to know the procedure incase of a power outage. Ensure that everyone is properly following the plans correctly.
7. **Plan Maintenance:** Ensure that backup generators are working correctly and important data is being backed up regularly.

*\*For an example of a full template of a contingency plan please view the Information Technology Contingency Plan. Also found here:* [*https://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Contingency-Disaster%20Recovery%20Plan/eplc\_contingency\_plan\_template.doc*](https://www.hhs.gov/ocio/eplc/EPLC%20Archive%20Documents/36-Contingency-Disaster%20Recovery%20Plan/eplc_contingency_plan_template.doc)

**Hands-On Assignment**

Try your hands at creating two simple contingency plans for yourself using the following example situations:

1.

Situation: Employees working have received notice that a fire has broken out within the building. The fire ended up damaging most of the servers that were stored within the server room. What kind of contingency plan could be in place to ensure that the company will be able to continue to operate without those servers ?

1. **Policy Requirements:**
2. **BIA:**
3. **Preventative Controls:**
4. **Contingency Strategies:**
5. **Contingency Plan:**
6. **Plan Training:**
7. **Plan Maintenance:**

2.

Situation: Employees at Google have just discovered that their software has been hacked. During this incident more than 20,000 users had their personal data stolen. What contingency plan do you believe should be in place to protect the users personal data.

1. **Policy Requirements:**
2. **BIA:**
3. **Preventative Controls:**
4. **Contingency Strategies:**
5. **Contingency Plan:**
6. **Plan Training:**
7. **Plan Maintenance:**