CONTINGENCY PLANNING

Prepared by:
Bicomong, Grazziela Antoniette
De Castro, Mar Kian P.
Hanapi, Russel Amin Kadra P.
Jalos, Mithi Anianna Gabrielle O.
Magcawas, Jayvee
Manguerra, Jan Misael K.
Rivera, John Paul
Pajavera, Robin

Mrs.

WHAT IS A CONTINGENCY PLAN

A **contingency plan** is a course of action designed to effectively address significant future incidents, events, or situations that may or may not happen. It is implemented to minimize potential negative impacts and ensure a timely and effective response.

Contingency planning is a strategic approach implemented to minimize the impact of potential disruptions on system and service availability. Its primary objective is to ensure the continuous and reliable functioning of critical systems by anticipating and preparing for various risks and uncertainties. This involves the identification of potential threats, such as natural disasters, cyberattacks, hardware failures, or human errors, and the development of comprehensive strategies to address these challenges. Contingency planning goes beyond mere risk assessment; it involves creating actionable and well-documented plans that outline specific steps to be taken in the event of an unexpected event. These plans typically include measures for backup and recovery, redundancy, alternative communication channels, and crisis management protocols. By adopting contingency planning, organizations aim to enhance their overall resilience, minimize downtime, and maintain seamless operations even when faced with unforeseen disruptions, thereby ensuring the continuity of critical services and systems.

CHARACTERISTICS OF A CONTINGENCY PLAN

A contingency plan should have the following characteristics:

1. **It is a plan for an uncertain or unknown event.**
    - The contingency plan ay ginagawa para harapin ang mga unexpected events o unpredictability (kawalan ng katiyakan) na nagpapakita ng hindi katiyakan ng ilang mga sitwasyon.
2. **It is designed to mitigate the effects of the event and provide a solution.**
    - One main objective is to reduce the impact of an event and provide a solution to ensure that the organization can continue its critical activities.
3. **It is composed of steps that need to be taken, actions that need to be taken, and resources needed for the plan's implementation.**

- The contingency plan outlines specific steps, actions, and the allocation of necessary resources such as funds needed to implement a proper response to the event.

4. **The plan should not create new risks, but rather reduce the risks caused by the original event.**
    - A well-designed contingency plan considers possible unexpected effects and strives to reduce or eliminate the creation of new risks while implementing the plan.
5. **It is typically used in the event of an emergency or disaster**
    - Contingency plans are typically released in response to emergency situations, disasters, or unexpected events that may affect the normal operations of an organization.
6. **It uses resources and personnel**
    - Usually, it involves the use of various funds, personnel, equipment, and other assets to carry out the specified responses.
7. **It often involves the use of equipment**
    - Depending on the type of event, contingency plans may require the use of specific equipment to effectively implement the plans.

DIFFERENT TYPES OF CONTINGENCY PLAN

The specific types of contingency plans can vary based on the **nature of the organization**, its **industry**, and **potential risks** it may face. Since it varies based on different aspects, there is no fixed or actual number of plans but listed below are sample types of contingency plans.

1. **Business Continuity Plan (BCP)**
    - Provides procedures for sustaining mission/business operations while recovering from a significant disruption.
2. **Continuity of Operations (COOP) Plan**

- Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.

3. **Crisis Communications Plan**
    - Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.
4. **Critical Infrastructure Protection (CIP) Plan**
    - Provides policies and procedures for the protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.
5. **Cyber Incident Response Plan**
    - Steps to reduce the impact of a security incident: Isolate affected systems and clean up by removing malware, minimizing information loss through data backup, and restoration against cyber attacks.
6. **Disaster Recovery Plan (DRP)**
    - It's a plan for moving an information system to a backup place if needed. It focuses on getting individual systems back in a bigger plan for system continuity. You can use one or more plans for this.
7. **Information System Contingency Plan (ISCP)**
    - It's a plan to get an information system back on track. Whether it's in the usual spot or a backup, this plan works on its own and can team up with other organization plans based on what happened.
8. **Occupants Emergency Plan (OEP)**
    - It gives coordinated steps to reduce harm to people and property from physical threats. It focuses on specific places, activated right after an incident to minimize loss of life, injury, and property damage.

CONTINGENCY PLANNING PROCESS

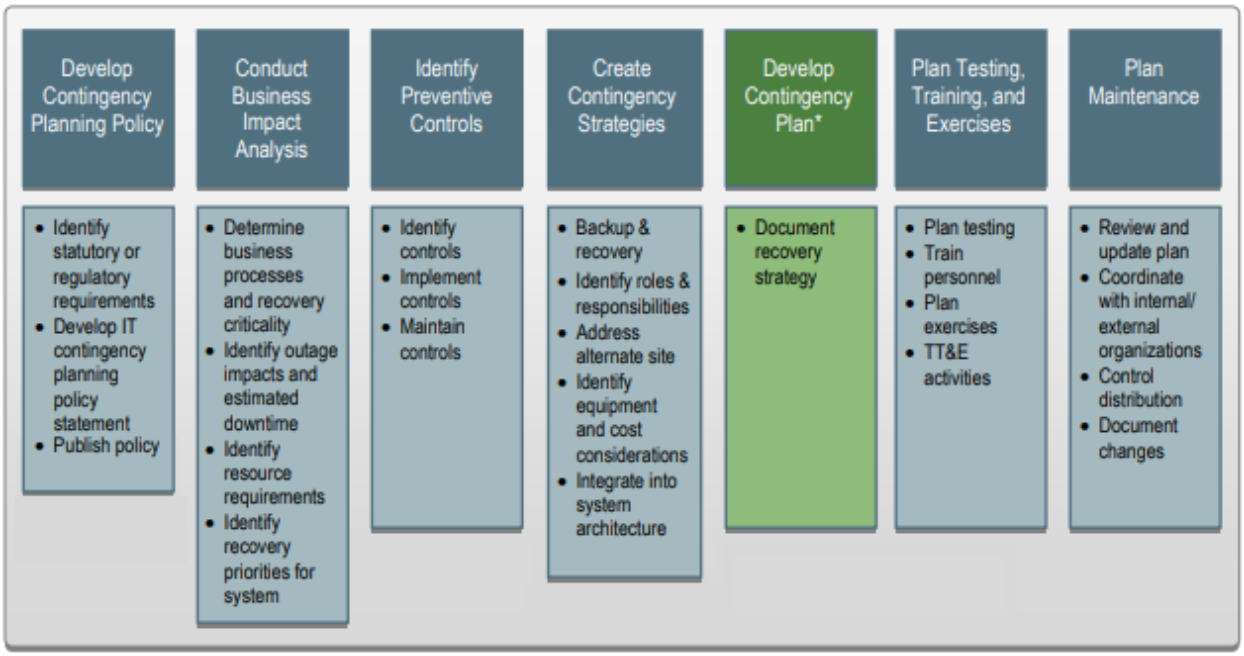

Figure 1: Contingency Planning Process

1. **Develop Contingency Planning Policies**
    - Contingency planning assigns yearly responsibilities to individuals within an organization, involving regular training and testing, to prevent and address potential disruptions in systems and ensure ongoing operational stability.

2. **Conduct Business Impact Analysis**
    - Determine business processes and recovery criticality
        - An organization employs various workflows and activities to attain its goals and objectives.
    - Identify outage impacts and estimated downtime
        - Since businesses and organizations have goals and objectives, the occurrence of downtime is possible. Downtime can significantly impact the organization's business processes.

    - Identify resource requirements

- In a business or organization, a comprehensive evaluation of the resources required for business processes is necessary.

- Identify recovery priorities for system resources
  - Regularly check and update the system for effective contingency planning

3. **Identify Preventive Controls**
   - In essence, the purpose of identifying preventive controls is to detect and mitigate potential impacts on the system, prioritizing preventive measures over recovery actions.
4. **Create Contingency Strategies**
   - Backup and recovery
     - There are methods and strategies in place to quickly restore system operations.
   - Identify roles and responsibilities
     - It is important for the Information Systems Contingency Plan (ISCP) coordinator to effectively designate teams for the implementation of the strategy
   - Address alternate site
     - In the event of downtime, it is crucial for the ISCP coordinator to ensure that management, operations, and technical controls are compatible with the prospective site.
   - Identify equipment and cost consideration
     - The ISCP Coordinator should consider whether the purchase of equipment will be effective or if it will create unnecessary overhead.

   - Integrate into the system architecture
     - All methods and strategies are applied to the design and structure of the system.

5. **Develop Contingency Plan**

   Why is this important? Contingency planning helps us deal with risks in our computer systems. Imagine that it is a backup plan or Plan B when things go wrong in our computer systems.

Contingency Strategies:

- Backup and Recovery
    - Make a copy of your important files.
- Backup Methods and Offsite Storage
    - Employees should be regularly backing up data, and looking for potential off-site storage.
- Alternate Sites
    - A storage place that can be either in a different place or online (cloud).
- Equipment Replacement
    - This makes agreements with companies for fast repairs, having spare equipment ready, or using similar stuff from backup places.
- Cost Considerations
    - Make a budget, analyze costs, and use a template to figure out what's the best plan without spending too much.
- Roles and Responsibilities
    - We have different teams for different jobs.
    - There's a big team led by important people, and smaller teams for specific tasks like fixing servers or getting new equipment.

6. Plan Testing, Training, and Exercises

- The plan should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the Information System Contingency Plan.

- Information System Contingency Plan
    - Keep them ready, we need to train our team, practice our plans, and test our systems. It's like making sure everyone knows their role and our tools work well.
- Assessing Security Controls
    - We follow guidelines such as NIST SP 800-53A, to make sure our controls are effective in protecting our information systems.
- Test, Training, and Exercise (TT&E)

    - Manual and guide that helps us design exercises to improve our ability to handle tough situations.
- TT&E in Action
    - TT&E activities mostly happen during the Operations/Maintenance phase. But we also do some training during the Implementation/Assessment phase to make sure our recovery plans work well.

7. **Plan Maintenance**
    - Must be always up to date and ready for tasks, employees from training would be able to apply what they've learned.
    - So, we need to review and update our ISCP regularly, to keep everything in top shape.
    - Risk Management Framework helps us keep an eye on our security plans, assessment reports, and action documents.
    - ISCP should be reviewed often. This means looking at things like operational requirements, security needs, and technical procedures.
    - Always update the team for feedback and reviews.
    - Protect sensitive information, keep it top secret.

ROLES AND RESPONSIBILITIES IN CONTINGENCY PLANNING

Creating a Contingency Plan involves several key Roles and Responsibilities. The following Roles listed are integral to a comprehensive contingency plan. Each role plays a crucial part in ensuring a swift and organized response to unexpected events, mitigating potential risks, and safeguarding the well-being of individuals, assets, and the overall continuity of operations. These roles not only define specific responsibilities but also establish a framework for collaboration, communication, and efficient decision-making in times of crisis.

1. **Team leader** - Define the overall strategy, allocate resources, and provide guidance throughout the planning process.
2. **Risk Assessor** - Identifies potential risks and vulnerabilities to the organization's operations, considering various scenarios.
3. **Communication Coordinator** - Outline communication strategies to keep internal and external stakeholders informed during a crisis.

4. **Data Collector** - Gather critical information about the organization's infrastructure, processes, and key stakeholders.
5. **Plan Developer** - Formulate a comprehensive contingency plan that includes steps to be taken in response to different types of disruptions.
6. **Testing and Training Coordinator -** Regularly test the contingency plan through simulations and drills, and provide training to relevant personnel.
7. **Documenter** - Maintain clear and detailed documentation of the contingency plan, ensuring it is accessible to those who need it.
8. **Review and Update Manager** - Regularly review and update the contingency plan to account for changes in the organization, technology, and external factors.

STEPS IN CONTINGENCY PLANNING

Since we do have different types of contingency plans and each of them have their own unique purpose, the execution of the actual plan varies but there are still steps to be considered in general when the crisis or the purpose of the plan itself arises.

1. **Activation** - Trigger the contingency plan when the predefined conditions or events that necessitate its activation occur. The goal of activation is to mobilize the necessary resources, personnel, and processes to address and mitigate the impact of an unexpected or disruptive incident This could be a natural disaster, a cybersecurity breach, a financial crisis, or any other disruptive event.

2. **Communication**. During a crisis, clear and consistent communication is vital. Identify who needs to know (employees, customers, authorities), craft messages tailored to each audience, and utilize multiple channels (email, social media, hotlines) to keep everyone informed. Adapt your approach as the situation changes, and remember, transparency and ongoing support are key to building trust and navigating towards recovery.

3. **Assembly of the Crisis Management Team**. Those who have the authority when crisis occurs are also those who hold the power in decision-making. Assembling the Crisis Management, the folks with the authority to make tough calls and the brains to navigate the storm. It's not just about gathering people in a room; it's about bringing together the

right skills, the right experience, and the right mindset to make quick decisions and keep the organization afloat.

4. **Assessment**. Conduct a thorough assessment of the situation. Understand the extent of the impact, potential risks, and available resources. This step involves gathering information, analyzing data, and continuously monitoring the situation.

5. **Prioritization**. Prioritize actions based on the severity and urgency of the situation. Identify critical functions and prioritize the allocation of resources to ensure the most essential aspects of the organization continue to operate.

6. **Implementation of Response Strategies**. Put into action the specific strategies outlined in the contingency plan. This may involve activating backup systems, relocating personnel, engaging external support services, or other predefined measures to address the crisis.

7. **Resource Management**. Having activated the plan, identified priorities, and secured resources, the next crucial step is Resource Management. This involves effectively allocating personnel, equipment, and finances, ensuring their efficient use aligns with the priorities established during the assessment phase.

8. **Monitoring and Adjustment.** Continuously monitor the situation and adjust the response strategies as needed. Regularly assess the effectiveness of the implemented measures and make modifications based on real-time information.

9. **Documentation.** Once all is managed, documentation of the incident is important. Keep detailed records of all actions taken during the contingency response. This documentation is essential for post-event analysis, reporting to stakeholders, and improving future contingency plans.

10. **Deactivation and Recovery:** Once the crisis is under control, initiate the process of deactivating the contingency plan. Transition back to normal operations and implement recovery plans to restore the organization to its pre-crisis state.

11. **Post-Incident Review:** Conduct a comprehensive review of the entire incident response process. Identify strengths and weaknesses, gather lessons learned, and update the contingency plan based on the insights gained.