Lab #2:

Develop an Organization-Wide Policy Framework Implementation Plan

PART A: Organization-Wide Policy Framework Implementation Plan Worksheet

Course Name: Policy Development in Information Assurance (IAP301)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 16/09/2023

Overview

In this lab, you are to create an organization-wide policy framework implementation plan for two organizations that are merging. The parent organization is a medical clinic under HIPAA compliance law. They recently acquired a remote medical clinic that provides a specialty service. This clinic is organized in a flat structure, but the parent organization is organized in a hierarchical structure with many departments and medical clinics.

Instructions

Parent Medical Clinic
Acquires Specialty Medical Clinic

Publish Your Policies for the New Clinic

- Identify the most important policies and procedures that need to be communicated to the new clinic employees. This may include policies on patient privacy, confidentiality, workplace safety, and compliance with regulatory requirements.
- Develop clear and concise versions of these policies and procedures that are tailored to the new clinic's audience. This may involve using simpler language or providing more specific examples.
- Publish the policies and procedures in a variety of formats, including on the organization's intranet, in a welcome packet for new employees, and in training materials. This will ensure that all employees have access to the policies and procedures in a format that is convenient for them.

Communicate Your Policies to the New Clinic Employees

- Send a mass email to all new clinic employees with a link to the policies and procedures. This email should include a brief overview of the policies and procedures, as well as instructions on how to access them.
- Post the policies and procedures on the organization's intranet. This will ensure that employees have easy access to the policies and procedures at any time.
- Provide new clinic employees with a welcome packet that includes a copy of the policies and procedures. This will give new employees a chance to review the policies and procedures at their own pace and ask questions as needed.

- Hold training sessions on the policies and procedures for all new clinic employees. These training sessions should be interactive and engaging, and they should provide employees with the opportunity to ask questions and get clarification.

Involve Human Resources & Executive Management

- Human resources can play a key role in the implementation of the policy framework. They can develop training materials, provide training to employees, and answer questions about the policies and procedures.
- Executive management can also play a role in the implementation of the policy framework. They can show their support for the policies and procedures by communicating with employees about them and by enforcing them consistently.

Incorporate Security Awareness and Training for the New Clinic

- Security awareness and training is essential for all employees, but it is especially important for employees who work in a healthcare setting. This is because healthcare organizations are a prime target for cyberattacks.
- Security awareness and training can be incorporated into the policy framework in a variety of ways. For example, training sessions on the policies and procedures can include a module on security awareness. Additionally, security reminders can be posted on system login screens and in other areas of the clinic.
- To make security awareness and training more fun and engaging, you can use games, simulations, and other interactive activities. You can also offer rewards to employees who complete security training or who demonstrate good security practices.

Release a Monthly Organization Wide Newsletter for All

- A monthly organization-wide newsletter can be a great way to keep employees up-to-date on the latest policies and procedures. It can also be used to remind employees about important security practices.
- To make the newsletter more succinct, you can focus on the most important policies and procedures. You can also use bullet points and other formatting techniques to make the newsletter easy to read.

Implement Security Reminders on System Login Screens for All

- Security reminders on system login screens can be a simple but effective way to remind employees about important security practices. These reminders can include things like changing passwords regularly and being careful about what links you click on.
- To implement security reminders on system login screens, you can use a variety of tools and software. You can also create your own custom reminders.

Incorporate On-Going Security Policy Maintenance for All

- Security policies and procedures should be reviewed and updated on a regular basis to ensure that they are still effective and up-to-date. This is especially important in the healthcare industry, where new threats are constantly emerging.

- To incorporate ongoing security policy maintenance, you can establish a review schedule for your policies and procedures. You can also involve employees in the review process by asking them for feedback and suggestions.
- Additionally, you can monitor compliance with the security policies and procedures. This will help you to identify any areas where improvement is needed.

Obtain Employee Questions or Feedback for Policy Board

- It is important to obtain feedback from employees on the policies and procedures. This feedback can be used to improve the policies and procedures over time.
- To obtain feedback from employees, you can create a suggestion box, conduct employee surveys, or hold focus groups. You can also encourage employees to send feedback directly to the policy board.
- The policy board should review all feedback from employees and incorporate any useful suggestions into the policies

PART B: Develop an Organization-Wide Policy Framework Implementation Plan

Overview

In this lab, you participated in classroom discussions on information systems security policy implementation issues. These issues and questions included the following topics:

- How to deal with people and human nature
- What motivates people
- Understanding different personality types of employees
- Identifying the characteristics of a flat organizational structure
- Identifying the characteristics of a hierarchical organizational structure
- What makes an IT security policy "stick"?
- How do you monitor organizational compliance?
- What is the ongoing role of executive management?
- What is the ongoing role of human resources?
- Why is conducting an annual audit and security assessment for policy compliance important?

Lab Assessment Questions & Answers

1. What are the differences between a Flat and Hierarchical organizations?

Answer:

- Flat organizations have few or no levels of management between top management and employees. This means that employees have more autonomy and decision-making power. Flat organizations are often more agile and responsive to change.
- Hierarchical organizations have many levels of management between top management and employees. This means that employees have less autonomy and decision-making power. Hierarchical organizations are often more stable and predictable.

- Which type of organization is better depends on the specific needs of the organization. Flat organizations can be more effective in fast-paced and dynamic environments, while hierarchical organizations can be more effective in stable and predictable environments.

2. Do employees behave differently in a flat versus hierarchical organizational structure?
Answer:
- Yes, employees can behave differently in a flat versus hierarchical organizational structure.
- In a flat organization, employees have more autonomy and decision-making power. This can lead to employees being more engaged and motivated, as they have more control over their work. Employees in flat organizations are also more likely to be proactive and take initiative, as they are not micromanaged by their supervisors.
- In a hierarchical organization, employees have less autonomy and decision-making power. This can lead to employees being less engaged and motivated, as they feel like they have less control over their work. Employees in hierarchical organizations are also more likely to be passive and wait for instructions from their supervisors.

3. Do employee personality types differ between these organizations?
Answer:
- Yes, employee personality types can differ between hierarchical and flat organizations.
- In hierarchical organizations, employees may be more likely to be compliant, deferential, and traditional. This is because hierarchical organizations tend to be more structured and hierarchical, which can create a culture of compliance. Employees in hierarchical organizations may also be more likely to defer to authority and to follow traditional norms and values.
- In flat organizations, employees may be more likely to be independent, creative, and entrepreneurial. This is because flat organizations tend to be more flexible and less structured, which can create a culture of innovation and creativity. Employees in flat organizations may also be more likely to be independent and to take initiative.

4. What makes it difficult for implementation in flat organizations?
Answer:
There are a few key factors that can make it difficult for organizations to implement policy compliance in flat organizations, including:

- Lack of hierarchy: In flat organizations, there is no clear hierarchy of authority. This can make it difficult to identify who is responsible for enforcing policies.
- Lack of accountability: In flat organizations, employees may not feel accountable to a specific manager or supervisor. This can make it difficult to hold employees accountable for policy violations.
- Lack of communication: In flat organizations, communication can be more informal and less structured. This can make it difficult to communicate policies to employees effectively and to ensure that everyone is aware of the policies that apply to them.
- Lack of buy-in: In flat organizations, employees may be more likely to question the need for policies or to believe that the policies are not relevant to their jobs. This can make it difficult to get employees to buy into policy compliance.

5. What makes it difficult for implementation in hierarchical organizations?
Answer:
There are a few key factors that can make it difficult for organizations to implement policy compliance in hierarchical organizations, including:

- Lack of communication: In hierarchical organizations, communication can be top-down, which can make it difficult for employees to understand and comply with policies. Employees may not

be aware of all of the policies that apply to them, or they may not understand what is expected of them.

- Lack of ownership: Employees in hierarchical organizations may not feel ownership of policies, which can make them less likely to comply with them. This is especially true if employees feel that the policies are not relevant to their jobs or that they are unfair.
- Lack of accountability: Employees in hierarchical organizations may not feel accountable for compliance, especially if they believe that their managers are not held accountable. This can lead to a culture of "passing the buck" and a lack of responsibility for policy compliance.
- Lack of resources: Employees in hierarchical organizations may not have the resources they need to comply with policies, such as training, tools, or support. This can make it difficult for employees to comply with policies, especially if they are complex or challenging.
- Lack of buy-in from senior management: If senior management does not buy into policy compliance, it will be difficult to implement and enforce policies effectively. This is because employees will see that senior management does not value policy compliance.

6. How do you overcome employee apathy towards policy compliance?

Answer:

There are a number of things that organizations can do to overcome employee apathy towards policy compliance, including:

- Make sure policies are clear, concise, and easy to understand. Employees should be able to easily understand what is expected of them and the consequences of violating policies.
- Get input from employees when developing policies. This will help to ensure that policies are realistic and achievable.
- Communicate policies effectively to employees. Policies should be communicated in a way that is clear, concise, and engaging.
- Provide training on policies. Employees should be trained on how to comply with policies and the consequences of violating policies.
- Enforce policies consistently. When employees violate policies, they should be disciplined consistently.
- Create a culture of compliance. This means making it clear that policy compliance is important and that employees are expected to comply with policies.

7. What solution makes sense for the merging of policy frameworks from both a flat and hierarchical organizational structure?

Answer:

The best solution for the merging of policy frameworks from both a flat and hierarchical organizational structure will vary depending on the specific needs of the organization. However, there are a few general principles that can be followed:

- Start by understanding the policy frameworks of both organizations. This will help to identify any areas of conflict or overlap.
- Identify the key principles that are important to both organizations. This will form the basis for the new policy framework.
- Develop policies that are clear, concise, and easy to follow. Policies should be written in a way that is understandable to employees at all levels of the organization.
- Get feedback from employees on the new policy framework. This will help to ensure that the policies are realistic and achievable.
- Communicate the new policy framework to employees clearly and concisely. Employees should know what is expected of them and the consequences of violating policies.

8. What type of disciplinary action should organizations take for information systems security violations?

Answer:

The type of disciplinary action that organizations take for information systems security violations will vary depending on the severity of the violation, the employee's past disciplinary record, and the organization's policies and procedures.

9. What is the most important element to have in policy implementation?

Answer:

The most important element to have in policy implementation is buy-in from senior management. If senior management is not committed to implementing policies, it will be difficult to get employees to follow them.

Senior management can demonstrate their commitment to policy implementation by:

- Communicating the importance of policies to employees. Senior management should explain to employees why policies are important and how they help to protect the organization.
- Setting a good example. Senior management should follow the policies that they implement.
- Providing resources for policy implementation. Senior management should provide the resources that are needed to implement and enforce policies, such as training, budget, and tools.

10. What is the most important element to have in policy enforcement?

Answer:

The most important element to have in policy enforcement is consistency. If policies are not enforced consistently, employees will not take them seriously and they will be more likely to violate them. Consistency means that all employees are held to the same standards, regardless of their position or department. It also means that policies are enforced fairly and impartially.

There are a number of things that organizations can do to ensure consistency in policy enforcement:

- Have a clear and well-defined policy enforcement process. This process should outline the steps that will be taken when a policy violation is suspected or confirmed.
- Train all employees on the policy enforcement process. Employees should know what to do if they suspect a policy violation and how they will be disciplined if they violate a policy.
- Monitor employee activity regularly. This can be done through network monitoring, web filtering, and other security solutions.
- Investigate all suspected policy violations promptly. If an employee is suspected of violating a policy, the organization should investigate the matter promptly and take appropriate disciplinary action.

11. Which domain of the 7-Domains of a Typical IT Infrastructure would an Acceptable Use Policy (AUP) reside? How does an AUP help mitigate the risks commonly found with employees and authorized users of an organization’s IT infrastructure?

Answer:

An Acceptable Use Policy (AUP) would reside in the User Domain of the 7-Domains of a Typical IT Infrastructure.

The User Domain includes all users of the IT infrastructure, including employees, contractors, and guests. It also includes all devices that users use to access the IT infrastructure, such as laptops, desktops, smartphones, and tablets.

The AUP is a document that defines what is and is not acceptable use of the organization's IT resources. It is important to have an AUP in place to help mitigate the risks commonly found with employees and authorized users of an organization's IT infrastructure. These risks include:

- Unauthorized access: Employees and authorized users may accidentally or intentionally give unauthorized users access to the organization's IT resources. For example, an employee may click on a phishing email and give their password to a scammer.
- Data loss: Employees and authorized users may accidentally or intentionally lose data. For example, an employee may accidentally delete a file or send it to the wrong person.
- Malware infection: Employees and authorized users may accidentally or intentionally infect the organization's IT systems with malware. For example, an employee may download a file from the Internet that is infected with malware.
- Security breaches: Employees and authorized users may exploit security vulnerabilities in the organization's IT systems. For example, an employee may use a weak password or fail to install security updates.

12. In addition to the AUP to define what is acceptable use, what can an organization implement within the LAN-to-WAN Domain to help monitor and prevent employees and authorized users in complying with acceptable use of the organization's Internet link?

Answer:

In addition to the AUP to define what is acceptable use, an organization can implement the following within the LAN-to-WAN Domain to help monitor and prevent employees and authorized users from complying with acceptable use of the organization's Internet link:

- Network monitoring and intrusion detection/prevention systems (IDS/IPS): These systems can be used to monitor network traffic for suspicious activity, such as attempts to access blocked websites or download malware.
- Web filtering: Web filtering solutions can be used to block access to certain websites or categories of websites, such as social media, gambling, or adult content websites.
- Content filtering: Content filtering solutions can be used to block access to certain types of content, such as images, videos, or audio files.
- Email filtering: Email filtering solutions can be used to block spam and phishing emails, as well as emails containing attachments that may be infected with malware.
- Application control: Application control solutions can be used to control which applications are allowed to run on company devices and which applications are allowed to access the Internet.
- User activity monitoring (UAM): UAM solutions can be used to monitor employee activity on company devices, including their internet browsing history, email usage, and file transfers.

13. What can you do in the Workstation Domain to help mitigate the risks, threats, and vulnerabilities commonly found in this domain? Remember the Workstation Domain is the point of entry for users into the organization's IT infrastructure

Answer:

- Implement strong access controls. This includes using strong passwords, multi-factor authentication, and role-based access control (RBAC) to ensure that only authorized users have access to workstations and data.
- Keep software up to date. Software vulnerabilities are a common entry point for attackers, so it is important to install updates for operating systems, applications, and security software as soon as they are available.
- Educate users about security best practices. This includes teaching users how to identify and avoid phishing attacks, how to create strong passwords, and how to protect their data when working remotely.
- Deploy security solutions. This includes deploying firewalls, intrusion detection systems, and antivirus software to protect workstations from malicious traffic and malware infections.

14. What can you do in the LAN Domain to help mitigate the risks, threats, and vulnerabilities commonly found in this domain? Remember the LAN Domain is the point of entry into the organization's servers, applications, folders, and data

Answer:

- Implement a firewall. A firewall is a network security device that monitors and controls incoming and outgoing network traffic. It can be used to block unauthorized access to the LAN and to prevent malware from spreading.
- Use intrusion detection and prevention systems (IDS/IPS). IDS/IPS systems monitor network traffic for suspicious activity and can block malicious traffic.
- Implement network segmentation. Network segmentation divides the LAN into smaller networks, each with its own security controls. This can help to limit the spread of malware and unauthorized access.
- Use strong passwords and multi-factor authentication. All devices on the LAN should have strong passwords and users should be required to use multi-factor authentication to log in.
- Keep software up to date. Software vulnerabilities are a common entry point for attackers, so it is important to install updates for operating systems, applications, and security software as soon as they are available.
- Educate users about security best practices. This includes teaching users how to identify and avoid phishing attacks, how to create strong passwords, and how to protect their data when working remotely.

15. What do you recommend for properly communicating the recommendations you made in Question #13 and Question #14 above for both a flat organization and a hierarchical organization?

Answer:

In a flat organization, communication is more horizontal and collaborative. This means that you can communicate your recommendations to employees at all levels of the organization. You can do this through a variety of channels, including:

- Town hall meetings: This is a great way to communicate your recommendations to a large group of employees at once. Be sure to leave time for questions and answers.
- Email: Email is a convenient way to communicate with employees individually or in small groups. Be sure to craft your email carefully and to explain your recommendations clearly.
- Slack or other team communication tools: If your organization uses a team communication tool such as Slack, you can use it to communicate your recommendations to specific teams or groups of employees.
- One-on-one meetings: If you have a trusting relationship with your employees, you can also communicate your recommendations to them one-on-one. This can be a good way to have more in-depth conversations and to answer any questions that employees may have.

In a hierarchical organization, communication is more top-down. This means that you should start by communicating your recommendations to senior management. Once you have their support, you can then communicate your recommendations to other levels of the organization. You can do this through a variety of channels, including:

- Executive meetings: This is a great way to communicate your recommendations to senior management all at once. Be sure to leave time for questions and answers.
- Email: Email is a convenient way to communicate with employees at all levels of the organization. Be sure to craft your email carefully and to explain your recommendations clearly.
- Cascade meetings: Cascade meetings are a type of meeting where information is passed down from senior management to lower levels of the organization. You can use cascade meetings to communicate your recommendations to managers and supervisors, who can then communicate them to their teams.

- One-on-one meetings: If you have a trusting relationship with your employees, you can also communicate your recommendations to them one-on-one. This can be a good way to have more in-depth conversations and to answer any questions that employees may have.