Laboratory #2

Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan

Learning Objectives and Outcomes

Upon completing this lab, students will be able to complete the following tasks:

- Identify human nature and behavior patterns of employee types in both hierarchical and flat organizational structures
- Overcome user apathy with security awareness techniques in both hierarchical and flat organizational structures
- Identify how security policies can help shape organizational behavior and culture in both hierarchical and flat organizational structures
- Compare a hierarchical and flat organizational structure to equivalent IT security policy framework structures
- Create an organizational policy implementation plan for the combined organization

Required Setup and Tools

This is a paper-based lab. Internet access and the student's Microsoft Office applications are needed to conduct this lab.

The following summarizes the setup, configuration, and equipment needed to perform Lab #2:

1. Standard onsite student workstation must have the following software applications loaded and Internet access to conduct this lab:
    a. Microsoft Office 2007 or higher
    b. Adobe PDF reader
    c. Internet access

Recommended Procedures

Lab #2 – Student Steps

The student steps needed to conduct Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan:

1. Discuss why the implementation of information systems security policies is difficult within organizations.

2. Discuss what organizations can do to help implement information systems security policies throughout the seven domains of a typical IT infrastructure

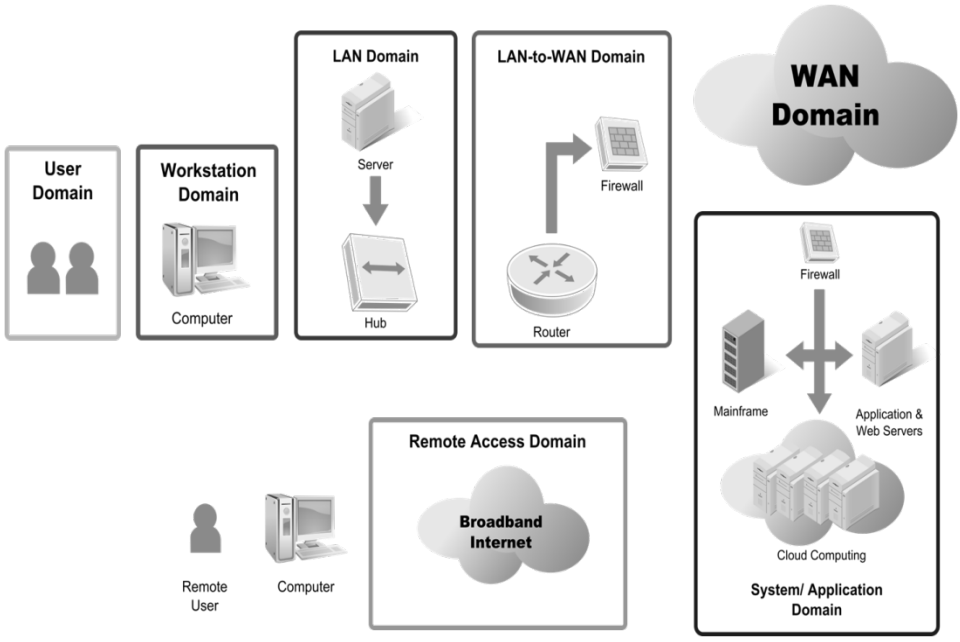

Figure 1 – Seven Domains of a Typical IT Infrastructure

3. Discuss why executive management, IT security policy enforcement monitoring, and human resources must have a unified front regarding disciplinary treatment of policy violations
   - ***Executive Management:*** Policy commitment and implementation must come from the CEO and the president's executive order for the entire organization with policy monitoring and disciplinary action taken for policy violations
   - ***IT Security Policy Enforcement Monitoring:*** Policy monitoring can be conducted via system logging, content filtering logging, and e-mail filtering logging with automated reporting to IT security personnel for monthly or quarterly policy compliance reviews
   - ***Human Resources:*** Employees or contractors/consultants must conform to all organization-wide policies. Violations of policies are considered to be an employer – employee issue upon which proper disciplinary actions must be taken. Repeat or continued violations of organization-wide policies may be grounds for termination of employment depending upon the severity of the violation. Non-employees should be provided with limited access and connectivity as per policy definition

4. Review the organizational structure inherent in flat and hierarchical organizations and how people behave in such structures
   - ***Flat organizational structures are characterized by the following characteristics:***
     Management structure that is cross-functional and more open to employee input
     Dialogue and communications between employees may occur across organizational functions
     Employees tend to be more open and communicative
     Employees tend to be more creative and involved in business decisions
     Employees are not as constrained within their role or function and can see and interact across the organization more freely
   - ***Hierarchical organizational structures are characterized by the following:***
     Departments are separated by function, creating multiple functional silos.
     Business decision making performed at the executive management level.
     Dialogue and communications is more "top-down."
     Employees tend to be less communicative and more isolated within their business functions.
     Employees find it difficult to offer additional creativity or input to business decisions
     Employees are constrained within their roles and cannot interact outside of their business functions without going through a chain of command
5. Review the organizational structure inherent within hierarchical and flat organizations and how people behave in such a structure
   - Isolated communication vs. open and free communication
   - Silos vs. flat dialogue and communications
   - Executive managers make business decisions vs. employees provide input into business decisions.
   - Management to employee dialogue and communications vs. employee to employee dialogue and communications.
6. Review why conducting annual audits and security assessments for policy compliance is a critical security operations and management function to help mitigate risks and threats.
   - People constantly change.
   - People gravitate toward repetition and repetitive inputs.
   - Periodic security awareness training coupled with policy compliance monitoring can help mitigate the risks and threats caused by employees within the User Domain.

7. Review the scope of a Policy Implementation Plan and what elements are required for the plan as part of this lab's deliverables.
    - Publish Your Policies
    - Communicate Your Policies
    - Involve Human Resources & Executive Management
    - Incorporate Security Awareness and Training
    - Release a Monthly Organization-Wide Newsletter
    - Implement Security Reminders on System Login Screens
    - Incorporate On-Going Security Policy Maintenance
    - Obtain Employee Questions or Feedback

Deliverables

Upon completion of the Lab #2: Develop an Organization-Wide Policy Framework Implementation Plan, the students are required to provide the following deliverables as part of this lab:

1. Lab #2 – Develop an Organization-Wide Policy Framework Implementation Plan
2. Lab #2 – Assessment Questions & Answers

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #2 that the students must perform:

1. Was the student able to identify human nature and behavior patterns of employee types in both hierarchical and flat organizational structures? – [**20%**]
2. Was the student able to overcome user apathy with security awareness techniques in both hierarchical and flat organizational structures? – [**20%**]
3. Was the student able to identify how security policies can help shape organizational behavior and culture in both hierarchical and flat organizational structures? – [**20%**]
4. Was the student able to compare a hierarchical and flat organizational structure to equivalent IT security policy framework structures? – [**20%**]
5. Was the student able to create an organizational policy implementation plan for the combined organization? – [**20%**]

Lab #2 – Organization-Wide Policy Framework Implementation Plan Worksheet

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name:

Lab Due Date: 12/10/2024

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

Using Microsoft Word, create a Policy Framework Implementation Plan according to the following policy implementation plan outline:

- Publish Your Policies for the Acquired Clinic – {Explain your strategy}
- Communicate Your Policies to the Acquired Clinic Employees – {How are you going to do this?}
- Involve Human Resources & Executive Management - {How do you do this smoothly?}
- Incorporate Security Awareness and Training for the New Clinic – {How can you make this fun and engaging?}
- Release a Monthly Organization-Wide Newsletter for All – {How can you make this short and to the point?}
- Implement Security Reminders on System Login Screens for All – {For access to sensitive systems only}
- Incorporate On-Going Security Policy Maintenance for All – {Review and obtain feedback from employees and policy compliance monitoring}
- Obtain Employee Questions or Feedback for Policy Board – {Review and incorporate into policy edits and changes as needed}

Parent Medical Clinic

Acquires Specialty Medical Clinic

Publish Your Policies for the New Clinic

{Explain your strategy}

Để đảm bảo tính rõ ràng và minh bạch, các chính sách sẽ được công bố trên trang intranet của phòng khám. Đây sẽ là phần dành riêng cho các chính sách mới và các quy trình đã được cập nhật, cho phép nhân viên dễ dàng tra cứu. Nhân viên sẽ nhận được thông báo qua email khi có chính sách mới được công bố, với tóm tắt các điểm quan trọng để họ có thể dễ dàng nắm bắt.

Communicate Your Policies to the New Clinic Employees

{How are you going to do this?}

Truyền thông sẽ được thực hiện thông qua các cuộc họp giới thiệu và buổi đào tạo cho nhân viên phòng khám. Trong các buổi này, các bên liên quan chính như trưởng phòng và trưởng nhóm sẽ trình bày về các chính sách và tác động của chúng. Ngoài ra, nhân viên sẽ nhận được sách hướng dẫn điện tử chứa đầy đủ các chính sách và

Involve Human Resources & Executive Management

{How do you do this smoothly?}

Nhân sự (HR) sẽ chịu trách nhiệm chính trong việc phối hợp việc giới thiệu chính sách, trong khi Ban Giám đốc sẽ hỗ trợ bằng cách đảm bảo các phòng ban tuân thủ theo các hướng dẫn mới. Các cuộc kiểm tra định kỳ với các trưởng phòng sẽ được thiết lập để giải quyết các vấn đề hoặc thắc mắc sớm trong quá trình triển khai. Ban Giám đốc sẽ tham gia việc phê duyệt chính sách để nhấn mạnh tầm quan trọng của việc tuân thủ.

Incorporate Security Awareness and Training for the New Clinic

{How can you make this fun and engaging?}

Đào tạo an ninh sẽ được tổ chức một cách tương tác và hấp dẫn bằng cách kết hợp các mô-đun học trực tuyến, câu hỏi trắc nghiệm, và các tình huống mô phỏng thực tế. Các tình huống như các cuộc tấn công phishing, chính sách mật khẩu, và việc xử lý dữ liệu an toàn sẽ được trình bày dưới dạng trò chơi để nhân viên không cảm thấy nhàm chán.

Release a Monthly Organization Wide Newsletter for All

{How can you make this newsletter succinct?}

Bản tin hàng tháng sẽ ngắn gọn, chỉ tập trung vào một hoặc hai cập nhật chính sách quan trọng hoặc mẹo về an ninh. Nội dung sẽ được trình bày dưới dạng các điểm nổi bật, liên kết có liên quan và một phần "Chính sách của Tháng" đảm bảo nhân viên có thể nhanh chóng nắm bắt thông tin quan trọng. Bản tin cũng sẽ nêu bật các sự cố an ninh hoặc thành công để tạo ra cảm giác khẩn cấp và quan trọng

Implement Security Reminders on System Login Screens for All

{For access to sensitive systems only}

Nhắc nhở an ninh sẽ được cài đặt dưới dạng thông báo pop-up khi nhân viên đăng nhập vào các hệ thống xử lý dữ liệu nhạy cảm. Những thông báo này sẽ được tùy chỉnh theo từng loại hệ thống mà nhân viên đang truy cập, nhắc nhở họ về các chính sách như mật khẩu mạnh, bảo mật dữ liệu, và cách xử lý thông tin bệnh nhân an toàn

Incorporate On-Going Security Policy Maintenance for All

Chính sách sẽ được xem xét định kỳ mỗi 6 tháng bởi Ban Chính sách để đảm bảo chúng vẫn phù hợp và hiệu quả.

{Review and obtain feedback from employees and policy compliance monitoring}

Nhân viên sẽ được khuyến khích cung cấp phản hồi thông qua các khảo sát ẩn danh, và những phản hồi này sẽ được đánh giá trong các cuộc xem xét chính sách

Obtain Employee Questions or Feedback for Policy Board

{Review and incorporate into policy edits and changes as needed}

Nhân viên sẽ có cơ hội gửi câu hỏi hoặc phản hồi thông qua một địa chỉ email dành riêng, mẫu đơn trực tuyến hoặc trong các cuộc họp toàn công ty. Các ý kiến này sẽ được nhân sự thu thập và trình bày trước Ban Chính sách để xem xét. Khi cần thiết, các thay đổi sẽ được thực hiện đối với chính sách dựa trên phản hồi từ nhân viên, đảm bảo chính sách sẽ phát triển cùng với nhu cầu của phòng khám và nhân viên.

Note: Your policy framework implementation plan should be no more than three pages long.

Lab #2 – Assessment Worksheet

Develop an Organization-Wide Policy Framework Implementation Plan

Course Name: IAP301

Student Name: Nguyễn Quốc Vượng

Instructor Name:

Lab Due Date: 12/10/2024

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?

+ Loại cơ cấu được tổ chức lựa chọn được xác định bởi nhiều yếu tố. Những yếu tố này bao gồm quy mô của tổ chức, kỹ năng của nhân viên, phong cách lãnh đạo, mục tiêu kinh doanh và công nghệ được sử dụng

+ Tổ chức phân cấp còn được gọi là 'cơ cấu cao'. Nó được đặc trưng bởi một số lượng lớn các tầng lớp giữa ban quản lý cấp cao và các cấp bậc thấp hơn trong tổ chức. Cơ cấu này có mô hình tổ chức theo bố cục hình kim tự tháp. Cơ cấu phân cấp thường được áp dụng bởi các tổ chức lớn.

+ Tổ chức phẳng còn được gọi là tổ chức ngang. Tổ chức phẳng có ít hoặc không có các cấp quản lý trung gian giữa các giám đốc điều hành và nhân viên. Có thể chỉ có một hoặc một vài lớp giữa ban lãnh đạo cao cấp và nhân viên cấp thấp. Cơ cấu phẳng thường được áp dụng bởi các tổ chức nhỏ

2. Do employees behave differently in a flat versus hierarchical organizational structure?

+ Mô hình tổ chức phân cấp có các vai trò và vị trí được xác định rõ ràng. Một nhân viên trong tổ chức như vậy biết rõ ai là người mà họ phải báo cáo và ai sẽ báo cáo cho họ.

+ Trong tổ chức phẳng, có sự nhấn mạnh nhiều hơn vào sự sáng tạo, cá nhân hóa, tự động viên và

3. Do employee personality types differ between these organizations?

+ Các loại tính cách của nhân viên có thể khác nhau giữa các tổ chức do nhiều yếu tố, bao gồm tính chất công việc, văn hóa tổ chức, yêu cầu của ngành và phong cách lãnh đạo.

+ Ngoài ra, các công ty có thể cố ý tuyển dụng những loại tính cách cụ thể phù hợp với mục tiêu chiến lược của họ.

4. What makes it difficult for implementation in flat organizations?

+ Có rất nhiều điều cần thay đổi đối với các nhà lãnh đạo muốn chuyển sang phong cách này. Nhà lãnh đạo sẽ phải loại bỏ các tầng lớp quản lý, thay đổi vai trò, và hy vọng rằng nhân viên sẽ chấp nhận những thay đổi này

+ Nếu một công ty có số lượng lớn các nhà quản lý trung gian, phong cách lãnh đạo này sẽ yêu cầu loại bỏ các vị trí đó

+ Nhân viên có thể thích thú với việc không phải trải qua nhiều thủ tục hành chính và cách giao tiếp thoải mái hơn với ban lãnh đạo cấp cao. Tuy nhiên, họ có thể cảm thấy bực bội do các vai trò không được xác định rõ ràng

5. What makes it difficult for implementation in hierarchical organizations?

+ Một công ty vận hành trơn tru khi có một hệ thống phân cấp để tuân theo

+ Mặc dù có thể dễ dàng hiểu được cấu trúc phân cấp cơ bản của công ty từ chủ sở hữu hoặc chủ tịch xuống đến các thành viên trong ban điều hành, nhưng hệ thống phân cấp giữa các quản lý và giám sát viên sẽ bị rối loạn nếu không có một cơ cấu tổ chức rõ ràng

+ Khi bạn triển khai khung làm việc cho công ty, sẽ có những trường hợp khi các quản lý hoặc giám sát viên đảm nhận những vai trò quyền lực mà họ không được dự định nắm giữ, điều này có thể gây ra sự nhầm lẫn cho nhân viên

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

+ Làm cho chính sách thân thiện với người dùng - Mặc dù các từ ngữ pháp lý là cần thiết, nhưng chính sách cũng có thể được trình bày một cách sáng tạo và tương tác.
+ Giao tiếp - Việc truyền đạt các chính sách hiện có là rất quan trọng. Thường xuyên, sự thiếu hiểu biết về chính sách có thể dẫn đến vi phạm.
+ Nhấn mạnh những rủi ro - Nhân viên cần được cảnh báo về những rủi ro có thể xảy ra. Điều này có thể là tiền phạt và các vụ kiện cho công ty hoặc hậu quả cá nhân đối với người vi phạm chính sách.
+ Xem xét chính sách bắt buộc - Việc xem lại các chính sách và làm một bài "Quiz" ngắn ở cuối có thể giúp nhân viên hiểu được tầm quan trọng của chính sách và những gì họ cần tuân thủ.
+ Tinh giản chính sách - Sự quá tải về chính sách có thể gây mệt mỏi thực sự. Tổ chức cần phải rất rõ ràng về những chính sách nào là cần thiết, loại bỏ các chính sách cũ và giữ chính sách đơn giản, dễ tiếp cận, và tối thiểu nhất có thể.
+ Tìm kiếm phản hồi - Tìm kiếm phản hồi từ nhân viên giúp tạo ra sự tham gia, giao tiếp và phá vỡ sự thờ ơ.

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

Có ba giai đoạn trong quá trình hợp nhất. Giai đoạn đầu tiên là nhận thức, trong đó nhân viên từ cả hai công ty hiểu rõ hướng đi mới của công ty và những điều này có ý nghĩa gì đối với họ. Mục tiêu của giai đoạn thứ hai là chấp nhận, khi đội ngũ tích hợp làm việc để xây dựng các mối quan hệ mới và nhân viên ở mọi cấp độ chuyển sang các vai trò và phương thức làm việc mới. Ở giai đoạn cuối cùng, quá trình hợp nhất hoàn tất và cấu trúc tổ chức mới được áp dụng đầy đủ.

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

Các tổ chức nên áp dụng các hình thức kỷ luật từ cảnh cáo đến trách nhiệm pháp lý, tùy thuộc vào mức độ nghiêm trọng của vi phạm bảo mật hệ thống thông tin
Ví dụ: + Cảnh cáo: Nhân viên vô tình chia sẻ thông tin nhạy cảm qua email không bảo mật.
+ Kỷ luật: Nhân viên cố ý truy cập trái phép vào hệ thống bảo mật.
+ Trách nhiệm pháp lý: Nhân viên sử dụng thông tin hệ thống cho mục đích cá nhân, gây thiệt hại cho công ty.

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

Yếu tố quan trọng nhất trong việc triển khai chính sách là đảm bảo tất cả nhân viên đều nhận thức và hiểu rõ chính sách. Điều này rất quan trọng vì nếu nhân viên không hiểu rõ về các quy định, quy trình và yêu cầu của chính sách, họ có thể vô tình vi phạm hoặc không tuân thủ đúng. Để đảm bảo chính sách được thực thi hiệu quả, tổ chức cần có các biện pháp truyền đạt rõ ràng, đào tạo, và theo dõi thường xuyên.

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

Yếu tố quan trọng nhất trong việc thi hành chính sách là việc áp dụng chính sách một cách nhất quán và công bằng đối với tất cả nhân viên, đảm bảo rằng các vi phạm được xử lý kịp thời và hợp lý

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?

Chính sách AUP (Chính sách Sử dụng Chấp nhận) sẽ nằm trong phạm vi của miền Máy trạm. Chính sách này sẽ xác định những hành vi sử dụng chấp nhận được và các hậu quả đối với các vi phạm chính sách. AUP cũng là một công cụ giáo dục để thông báo cho nhân viên về bảo mật và tầm quan trọng của nó.

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?

Ngoài chính sách AUP để xác định hành vi sử dụng chấp nhận được, tổ chức có thể triển khai một số biện pháp trong miền LAN-to-WAN để giám sát và ngăn chặn nhân viên cũng như người dùng có quyền truy cập vi phạm quy định về việc sử dụng liên kết Internet của tổ chức. Các biện pháp bao gồm:
+ Lọc Nội Dung: Sử dụng các giải pháp lọc web để chặn truy cập vào các trang web không phù hợp hoặc không liên quan đến công việc.
+ Công Cụ Giám Sát Mạng: Triển khai phần mềm ghi lại và giám sát hoạt động internet để phát hiện vi phạm trong thời gian thực.
+ Quản Lý Băng Thông: Giới hạn băng thông cho các hoạt động internet không thiết yếu hoặc không liên quan đến công việc để đảm bảo sử dụng tài nguyên hợp lý.
+ Tường Lửa: Cấu hình tường lửa để hạn chế truy cập internet trái phép và ngăn chặn tải xuống nội dung độc hại.
+ Hệ Thống Phát Hiện Xâm Nhập (IDS): Thiết lập các hệ thống để nhận diện các hoạt động mạng bất thường hoặc trái phép.

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.

Để giảm thiểu rủi ro, mối đe dọa và lỗ hổng trong miền Workstation, có thể thực hiện các biện pháp sau:
+ Bảo mật đầu cuối: Sử dụng phần mềm chống virus, chống malware và EDR
+ Quản lý bản vá: Cập nhật thường xuyên hệ điều hành và phần mềm
+ Xác thực đa yếu tố (MFA): Thực thi MFA để tăng cường bảo mật
+ Quản lý quyền truy cập: Áp dụng nguyên tắc quyền tối thiểu (POLP) cho người dùng
+ Mã hóa ổ đĩa: Mã hóa dữ liệu để bảo vệ khi mất thiết bị

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.

+ Phân đoạn mạng: Chia miền LAN thành nhiều phân đoạn để hạn chế việc di chuyển ngang và cô lập các mối đe dọa tiềm ẩn trong các khu vực cụ thể
+ Kiểm soát truy cập: Áp dụng chính sách kiểm soát truy cập nghiêm ngặt bằng cách sử dụng kiểm soát truy cập dựa trên vai trò (RBAC) để đảm bảo người dùng chỉ truy cập vào các dữ liệu và tài nguyên cần thiết cho vai trò của họ.
+ Tường lửa và Hệ thống phát hiện xâm nhập (IDS): Triển khai tường lửa và IDS/IPS để giám sát lưu lượng giữa LAN và các mạng bên ngoài, ngăn chặn các cuộc tấn công trái phép vào mạng
+ Mã hóa: Sử dụng mã hóa (như VPN hoặc SSL/TLS) cho các kết nối trong LAN để bảo vệ dữ liệu nhạy cảm khi truyền tải.

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?

+ Đối với tổ chức phẳng: Vì tổ chức nhỏ, tôi có thể tổ chức một ngày họp để đào tạo và giới thiệu về chính sách.
+ Đối với tổ chức theo kiểu phân cấp: Vì tổ chức có quy mô lớn, tôi có thể giới thiệu chính sách cho các quản lý, sau đó họ có thể gửi thông báo đến nhân viên của mình. Sử dụng nhiều ngày hơn để đào tạo với các bộ phận khác nhau.