

Subject	IAP301
Student's name	Dang Hoang Nguyen
Instructor	Mr. Mai Hoang Dinh
Student's id	SE171946

1. What are the differences between a Flat and Hierarchical organizations?
Flat companies have fewer levels of management, with a focus on liberty and independence. Hierarchical organizations have multiple layers of control and decision-making power, with a top-down system.
2. Do employees behave differently in a flat versus hierarchical organizational structure?
Employees generally have more freedom and authority in flat groups, boosting creativity and innovation. In bureaucratic companies, workers may have more clear jobs and tasks, resulting in more organised decision-making processes.
3. Do employee personality types differ between these organizations?
Employee personality types may not greatly vary between the two types of organizations; however, flexible and independent people might thrive in flat organizations, while those who prefer order and clear standards may perform better in hierarchical organizations.
4. What makes it difficult for implementation in flat organizations?
In flat organizations, the lack of defined management roles and decision-making processes might make policy implementation difficult, as employees may be less likely to adhere to a centralized policy.
5. What makes it difficult for implementation in hierarchical organizations?
In hierarchical organizations, resistance to change or bureaucratic processes might make policy implementation difficult, as navigating multiple levels of management can be time-consuming and complex.
6. How do you overcome employee apathy towards policy compliance?
To overcome employee apathy towards policy compliance, stress the value of the policies through regular contact, training, and showing the effects of non-compliance. Engage workers in the policy creation process to create a feeling of ownership and responsibility.
7. What solution makes sense for the merging of policy frameworks from both a flat and hierarchical organizational structure?
When combining policy frameworks from both flat and hierarchical organizational structures, build a mixed answer that combines the need for centralized control with the freedom present in flat organizations. Involve workers and managers from both types of companies in the creation and execution process to create buy-in and support.
8. What type of disciplinary action should organizations take for information systems security violations?
Disciplinary measures for information system security violations should be related to the seriousness of the violation and may include verbal or written warnings, removal of access rights, firing, or court action, based on the nature of the violation.

9. What is the most important element to have in policy implementation?
The most important aspect in policy execution is effective communication that ensures workers understand the policies, their value, and their individual duties for compliance.
10. What is the most important element to have in policy enforcement?
The most important aspect in policy implementation is accuracy in applying consequences for non-compliance, as well as tracking and reporting to ensure ongoing obedience to policies.
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?
An Acceptable Use Policy (AUP) lives within the User Domain. By clearly describing and sharing acceptable activities and user behavior, an AUP helps minimise risks associated with employee actions and use of IT resources.
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?
Within the LAN-to-WAN Domain, companies can implement firewall rules, content blocking, and tracking tools to help ensure compliance with acceptable use policies and avoid illegal activities.
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. To minimise risks in the Workstation Domain, adopt strong password policies, encryption, user access controls, regular software changes, and security awareness training for workers.
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. To reduce risks in the LAN Domain, use network division, attack detection/prevention systems, strong access controls, and frequent vulnerability reviews.
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?
To share the suggestions for both flat and hierarchical organization, use a mix of email, online tools, town hall events, and training classes. Adapt the communication style to fit the company mindset, while ensuring a uniform message across the organization