i. **For access control, MAC, DAC, and RBAC are the popular options. In the context of ABC, Inc., state which of these are appropriate, with a brief justification.**

Since ABC Inc. is a large company, using MAC and RBAC would be the most beneficial access control types. These two access control types give the company a lot of control over what information and applications employees have access to. In turn, this would prevent employees from accessing applications they otherwise would not need to complete their role or job. This would also be an additional line of defense if an employee's computer or ID were to be compromised. Limiting employee access across the network also prevents threat actors from making use of a compromised account. Limiting what the attacker can reach out and do with the account that was originally compromised. MAC is great for limiting what types of documents or data employees have access to—making sure that only authorized individuals can obtain information that is deemed to be restricted.

ii. **ABC Inc. is trying to purchase advanced authentication servers to accommodate the increasing customer activity. The CFO (chief financial officer) prefers to go with the lowest bidder. However, the CSO (chief security officer) prefers a more systematic approach. On behalf of the CSO, write a brief note to the CFO stating the aspects that need to be taken into account in the choice. ABC Inc. has a COO and a CSO. While the COO (chief operations officer) is responsible for the overall operation of ABC Inc., the CSO (chief security officer) is responsible for the security. Both report to CEO who, in turn, reports to the Board of Directors and to the Shareholders.**

While going with the lowest bidder may sound like an appealing offer there is much to be considered. Appealing to the lowest bidder may save money upfront but in the long run, could set the company up to have lackluster authentication servers. When considering an advanced authentication server spending more money to ensure that it meets all requirements will be more beneficial. Taking a more systematic approach will allow the company to understand what areas need to be improved upon. Allowing them to pick the best server that would fit what it needed for the company. Since the company has a lot of online traffic it would be best to purchase a reliable and secure authentication server over a cheaper alternative. This will ensure that customers are protected and threat actors aren't able to compromise accounts.

iii. **Is there a need for intrusion detection in ABC Inc.? Which type(s) of products do you recommend? Justify.**

NIDS and HIDS should be implemented in order to provide a well-rounded IDS for ABC Inc. This will allow the company to monitor activity that is occurring on the network. Letting them look at what is being sent across the network to determine if anything is unusual. Snort is a popular IDS that is being used across many companies. This would be a good product to go with for NIDS features. Tripwire is a good product that provides tools and interfaces for HIDs features. This is necessary because it would allow the company to monitor files and ensure that files haven't been accessed or altered. Also allowing the company to see what hosts have been comprised or who made the changes.

iv. **Do you think the defense-in-depth is relevant for ABC, Inc.? Justify.**

Yes, defense in depth should be implemented in any company that is collecting data from its customers. This also is a great practice to have to ensure that the company is preparing for potential threat acts. Setting the company up to be able to defend itself against potential attacks. It is best to prepare and set forth various levels of security features to create a more complex and secure system. If an attacker can get passed one security feature there will be even more features they would have to get passed. This overall prevents attackers from gaining access or control of a system by only bypassing one security feature. Additionally, defense in depth will allow the company to prepare itself for various types of attacks by implementing multiple levels of security. Adjusting what features need to be implemented and which ones need to be improved upon based on what is happening in the general field.