Discuss how your security, compliance, and privacy strategies should integrate with each other. How would you ensure that these three strategies stay integrated?

Security, compliance, and privacy are terms that can be defined in different ways. Nevertheless, they all build upon the following crucial concepts:

Security: The primary responsibility of the Information Security Officer and generally understood to focus on protecting data from un unauthorized access, including malicious attacks. Security is vital for both compliance and privacy. For example, regulations such as HIPAA and GLBA require the implementation of certain security controls. On the other hand, organizations maintain the privacy of their customers' data by having security protocols in place to prevent against external threats and data breaches.

Compliance: This includes the development of policies and procedures so that individuals have the information they need to act accordingly to meet the organization’s security and privacy objectives.

Privacy: is generally focused on the use and governance of personal data and personally identifiable information. It might include putting policies in place to ensure that personal data is being collected, shared, and used in appropriate ways.

Hence, while security, compliance, and privacy necessarily seem separate and distinct disciplines with potentially different responsibilities, the strategies they entail overlap significantly and complements each other in various ways. That is, organizations must design robust security strategies to comply with regulations and prevent incidents, including data security breaches involving customers and employees. At the same time, such security strategies help to keep consumers' data private.

As a result, security, compliance, and privacy strategies should integrate with each other by allowing these strategic functions within an institution to work together. Additionally, making sure security awareness is a teamwork, training staff, and establishing a transparent and account environment plays a critical role in integrating the three strategies. During this process, the organization must also properly keep any compliance plans and procedures.

In order to ensure security, compliance, and privacy stay integrated, the legal team (Compliance subject matter experts) of the organization plays a critical role. The team must address the organization’s obligations to protect customer and employee personal data. It must also understand the risk of breaching these obligations, and the security measures needed to remedy any gaps or deficiencies. Furthermore, the team must review policies to ensure that it's up to date with respect to the various state and federal laws the institution must comply with.

References

https://er.educause.edu/blogs/2017/1/compliance-privacy-and-security-whats-the-difference

https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-a-compliance-strategy-can-mitigate-cyber-threats