Mohammed Aljuboor

CYSE 368

10-02-2024 to 10-16-2024

Reflection Paper 3.

I've been tasked to work with the Governance, Risk, and Compliance (GRC) team during the most recent stage of my internship. My knowledge of the relationship between cybersecurity and organizational policy has grown as a result of my role, which focuses on managing access privileges and end-user account oversight. My main duties include assessing access levels, changing permissions as needed, and making sure the business conforms with legal and internal security regulations.

Maintaining the notion of least privilege—making sure that users have access to only the resources required for their roles—has been a crucial part of my work. I must evaluate the suitability of access for different jobs while striking a balance between security requirements and operational efficiency, which calls for a thorough understanding of organizational structure and process. I've improved my technical and communication abilities by directly collaborating with department heads to define access requirements.

Simplifying the procedure for changing user access for sizable groups during position changes or department reorganizations was one of the biggest obstacles I faced. This experience made it clear how crucial automation and thorough documentation are to efficiently managing access control. My managers have appreciated my initiative in creating more effective protocols for managing these changes.

My grasp of the wider ramifications of cybersecurity has greatly expanded as a result of this internship phase, especially with regard to how governance, risk management, and compliance frameworks influence and protect an organization's security posture. I've learned from working in GRC that cybersecurity is more than simply technical protections; it's also about making sure that policies and processes meet internal security standards and regulatory obligations.

Overseeing access control has shown me firsthand how important the notion of least privilege is in reducing potential risks. This experience has also highlighted the need of combining security and usability, ensuring that personnel can execute their duties without undue friction. Moving forward, I am eager to broaden my knowledge of GRC, as I believe that mastering the governance and compliance aspects of cybersecurity will enable me to contribute more holistically to securing digital environments, ultimately preparing me for a career in which both technical skills and policy knowledge are required.