TECHNOLOGY & PRODUCT REVIEW FOR IDENTITY GOVERNANCE & ADMINISTRATION

Author

Professor’s Name,

Course Title

Institution

Date.

Overview of the Identity Governance & Administration

The company’s recommendation of the Identity Governance & Administration (IGA) is indeed a sure bet for the company’s productivity in its quest of ensuring there is security management in the enterprise. The Identity Governance & Administration is a security technology which is designed to help the in the management of Information Technology related security as it ensures there are efficient identity administration and access control. Notably, the identity governance products are entirely different from the identity and access management systems through their capabilities of facilitating the organization to define, enforce, review and audit IAM policy. Also, they enable the mapping of IAM functions to their compliance requirements and also facilitate the auditing of user access to support compliance reporting.

Moreover, although the Identity Governance and Administration may prove to be a complex discipline, it provides significant value to the business which has initiated the technology to maintain security. Additionally, the Identity Governance and Administration provides a single identity governance ground platform to assist the company to have knowledge, control, and make strategic business decisions that are linked to user access and risks access. Moreover, the security tool provides the business activity approach that enables effective communication between the auditors and Information Technology staffs. Besides, the tool also assists in determining segregation of responsibilities violations across business applications, including the SAP. Nonetheless, the recommended security tool enables better visibility and user access management by consolidating access entitlements from the target applications and integrating the sophisticated algorithms for the role mining, modeling, and optimization in the corporation. Besides, the Identity Governance and Administration promotes the five pillars of information assurance, including confidentiality, integrity, availability, authentication, and non-repudiation (Mowbray, 2014).

There is no doubt the Identity Governance and Administration has proved to be integral in many organization due to its various capabilities. Firstly, the security tool is capable of enabling Access governance. The device provides the identity management infrastructure which is based on the business requirements rather than on the Information Technology processes. Notably, the users are categorized by the company’s roles, group membership, job functions and the needs of access.

Secondly, the Identity Governance and Administration also has the capability of Access to risk assessment and management. Apparently, the security mechanism assists in the mitigating risks and also Segregation of Duties violations by its Access Risk control module found in its features. It is also evident that its capability of Access risk assessment and management minimizes the risks by using the five pillars of information security. The five pillars include protection, detection, reaction, documentation, and prevention of the computer security risks.

Thirdly, the security tool boasts of the capability to access certification. The access certification capability ensures that the entitlement and rights to access are provided to the authorized personnel only. Mainly, it monitors and certifies that the users’ have accesses which are to up-to-date and also at the most appropriate levels. Moreover, when the user access and entitlement are approved, the potential Segregation of Duties violations are determined (“IBM knowledge center,” n.d.).

Fourthly, the security mechanism is also capable of providing audits and reports which are essential in meeting the government and industry legislations. Besides, efficient tracking and internal and external auditing are significance in gaining in-depth knowledge and exceptional visibility into all accounts, access privileges, and rights across all users. Access optimization is also one of the capabilities of the Identity Governance and Administration that has enabled the various companies using the security tool to reduce chances of any security incidents in the organization. Moreover, the security mechanism is also capable of ensuring effective workflow and policy management in the business operations.

The various features of the Identity Governance and Administration include; simplifying access governance, streamlining access request and fulfillments, govern unstructured access to data, speed deployment at relatively lower costs, leveraging identity as a business risk control factor and achievement of sustainable identity and access management program (Evidian, 2013).

However, apart from the benefits of the security tools, there are some notable deficiencies or shortcomings of using the Identity Governance and Administration. Some of the weaknesses in the implementation of security tool include distributed applications, productive provisioning, problems with passwords, and the regulatory compliance.

Indeed, the Identity Governance and Administration will be significant in supporting the cybersecurity objectives by reduction of risk, increasing the company’s resistance to threats or attacks and reducing the possible vulnerabilities. A holistic Identity Governance and Administration will provide assistance to the managers or administrators in consolidating, controlling, and simplifying the privileges to access the vital computer systems in the company which could, therefore, translates to reduced vulnerabilities to the cyber criminals. Moreover, a robust Identity Governance and Administration technique can enable full automation of both the provision and de-provisioning procedures. The automated provisioning will enhance the enforcement speed of the company’s robust cyber security policies and strategies. The plans may be integrated to reduce the threats to computer systems and specifically counter the growing threats from the cyber criminals. Lastly, the integration of the IGA enables the company to make the system of equipment’s vulnerability due to password issues a thing of the past. The approach effect this by its capability of federating the identity of the users and ensuring there is password security through the use of single-sign-on (SSO) capabilities of the security tool (Velazquez, 2016).

References

Velazquez, M. (2016, February 24). The challenges and benefits of identity and access management. Retrieved February 10, 2017, from https://f5.com/resources/white-papers/the-challenges-and-benefits-of-identity-and-access-management-17862

Mowbray, T. J. (2014). Cybersecurity: Managing systems, conducting testing, and investigating intrusions.

IBM knowledge center. Retrieved February 10, 2017, from https://www.ibm.com/support/knowledgecenter/en/SSGHJR\_5.2.0/com.ibm.igi.doc/product\_overview/cpt/cpt\_feat\_overview.html

Evidian. (2013, August 30). IGA 10 for identity governance and administration. Retrieved February 10, 2017, from http://www.evidian.com/products/identity-governance-and-administration-iga-10/