Chapter 7
Auditing Customer Identity and Access Management

Sushmita Podugu
University at Buffalo, SUNY, USA

Vamsi Krishna Rayapureddi
University at Buffalo, SUNY, USA

Manish Gupta
University at Buffalo, SUNY, USA

ABSTRACT

Customer identity and access management (CAIM) is an emerging field that is a subset of traditional identity and access management. Authenticating, authorizing, and granting access to company systems to employees is the foundation of traditional IAM. Contrarily, CIAM is a specialist field that allows organizations to authenticate, authorize, and provide access to their customers/consumers for on-premises or cloud-based organizational systems. By granting customers access, it becomes necessary to control the degree of access granted to customers; as a result, auditing is a crucial component of CIAM. Auditing aids in directing businesses towards establishing control environment, assessing risk, developing, and monitoring relevant IT controls; and keeps an eye on laws that are imposed by governing authorities. The chapter begins with an introduction to audit and customer identity access management. It addresses the risks associated with CIAM, strategies for implementing security controls and the importance of implementing these controls.

DOI: 10.4018/978-1-6684-8766-2.ch007

INTRODUCTION

Customer Identity and Access Management, also known as CIAM, is all about maintaining the customer's identity and providing them with appropriate access to enterprise customer applications. The driving factor for CIAM is the need to engage with customers and improve business output. CIAM helps organizations enable a seamless and secure customer experience while also maintaining compliance with regulatory requirements (Rasouli, 2020).

Consumer Identity and Access Management was created in response to the growing demand for better user interaction and experience with organizational applications and systems. To guarantee the security and management of access to internal systems and applications within an organization, traditional identity and access management (IAM) procedures were created. Yet, as online services and digital technology proliferated, the emphasis changed to giving customers a more safe and centered experience.

The requirements of applications and services that are intended for customers are met by CIAM, a specific type of IAM. It comprises extra functions and features like social login, single sign-on (SSO), and self-service account management that are intended to enhance the user experience with identity systems. Building trust and loyalty with clients requires offering them a simple and secure experience when dealing with a business.

Customers have high expectations for their interactions with businesses in today's digital age. Consumers desire a seamless experience with few barriers that is simple to use and navigate. Also, they are more concerned than ever about the security of their data and privacy. Organizations must therefore offer a simple and safe registration process that satisfies these demands. By streamlining the registration process, minimizing the number of steps needed, and providing practical authentication mechanisms like social network logins, CIAM assists companies in achieving this. CIAM assists businesses in forging solid relationships with their clients and boosting client loyalty by making it simple for customers to set up and maintain their accounts.

CIAM has developed into a crucial tool for businesses looking to engage and improve how their clients use their systems and applications. CIAM assists companies in cultivating consumer trust and loyalty through the provision of a seamless and safe experience, which is crucial for success in today's digital economy. First, it helps businesses to identify their customers accurately and securely, which is essential for providing personalized services and experiences. This can be particularly important in industries such as retail and e-commerce, where customers expect a seamless and convenient experience. Second, CIAM helps businesses to protect their customers' personal and sensitive information, which is essential for maintaining trust and