U.PORTO

MASTER
IN MANAGEMENT

Implementation of an Identity and Access Management Control Reporting System – The Case Study of NOS Comunicações, S.A

Pedro Miguel Di Nunzio Mota

M

2025

U.PORTO

FEP FACULDADE DE ECONOMIA UNIVERSIDADE DO PORTO

Implementation of an Identity and Access Management Control Reporting System – The Case Study of NOS Comunicações, S.A

Pedro Miguel Di Nunzio Mota

Dissertation

Master in Management

Supervised by

Adelaide Ferreira Leite Martins

2024/2025

Acknowledgements

I would like to express my gratitude to my supervisor, Professor Adelaide Martins, for her continuous guidance and valuable feedback throughout the development of this dissertation.

I am also deeply thankful to the team at NOS, for the opportunity to carry out my internship and for their support, insights, and collaboration, which were essential for the success of this project.

Finally, I am profoundly grateful to my family and friends for their unwavering support, understanding, and motivation during this challenging but rewarding period, and especially to my father and mother for their constant support, which made it possible for me to have the opportunity to write this dissertation.

Abstract

Identity and access management is an important aspect of information security as it ensures that employees have appropriate access to organizational information while mitigating risks of unauthorized access. Especially due to the high volume of data that a telecom company can have.

This study describes the implementation of a reporting system focused on identity and access control at NOS Comunicações S.A., a prominent telecommunications provider in Portugal. NOS faced specific challenges stemming from its operational scale, the diversity of its workforce, and its reliance on external contractors. Due to employing a hybrid Role-Based Access Control and Attribute-Based Access Control model, existing access dashboards offered limited utility for proactive anomaly and error detection, making the daily access management control more difficult.

To overcome these deficiencies, a new reporting system was developed using Microsoft Power BI, a business intelligence tool. The resulting dashboard incorporates a set of personalized indicators and alerts, designed to improve access governance. These include mechanisms to identify duplicate accesses, highlight distinct application attributions (indicating low adoption by peers within functions), and flag distinct profiles. and identify identity accesses suitable for removal or transfer to standardized profiles. These indicators were developed to detect over-privileged accounts, identify instances of role drift, and reveal inconsistencies in access attribution. This solution aims to provide the Quality team with improved visibility into access management health, enabling the detection of misalignments, improving the security posture, and the improvement of operational efficiency in managing user permissions.

Key words: Identity and Access Management (IAM), Access Control, Information Security, Business Intelligence, Reporting system, Dashboards, Telecom, NOS

Resumo

A gestão de identidades e acessos é um aspeto importante da segurança da informação, pois garante que os colaboradores têm o acesso adequado à informação da organização, enquanto mitiga os riscos de acessos não autorizados. Isto é especialmente relevante devido ao elevado volume de dados que uma empresa de telecomunicações pode possuir.

Este estudo descreve a implementação de um sistema de reporting focado no controlo de identidade e acessos na NOS Comunicações S.A., um dos principais fornecedores de telecomunicações em Portugal. A NOS enfrentava desafios específicos decorrentes da sua escala operacional, da diversidade da sua força de trabalho e da dependência de prestadores externos. Devido à utilização de um modelo híbrido de controlo de acessos baseado em funções (Role-Based Access Control) e atributos (Attribute-Based Access Control), os dashboards de acessos existentes ofereciam utilidade limitada para a deteção proativa de anomalias e erros, tornando o controlo diário da gestão de acessos mais difícil.

Para combater estas deficiências, foi desenvolvido um novo sistema de reporting utilizando o Microsoft Power BI, uma ferramenta de business intelligence. O dashboard resultante incorpora um conjunto de indicadores e alertas personalizados, concebidos para melhorar a governação de acessos. Entre estes incluem-se mecanismos para identificar acessos duplicados, destacar atribuições distintas de aplicações, sinalizar perfis distintos e identificar acessos de identidade suscetíveis de remoção ou transferência para perfis normalizados. Estes indicadores foram desenvolvidos para detetar contas com privilégios excessivos, identificar casos de role drift e revelar inconsistências na atribuição de acessos.

Esta solução tem como objetivo fornecer à equipa de Qualidade uma melhor visibilidade sobre a saúde da gestão de acessos, permitindo a deteção de desalinhamentos, reforçando a postura de segurança e melhorando a eficiência operacional na gestão das permissões de utilizadores.

Palavras-chave: Gestão de Identidades e Acessos (IAM), Controlo de Acessos, Segurança da Informação, Business Intelligence, Sistema de Reporting, Dashboards, Telecomunicações, NOS

Table of contents

Figure Index

Table Index

List of Abbreviations

Abbreviation	Definition
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-Based Access Control
ARC	Audit, Risk & Compliance
B2B	Business-to-Business
BI	Business Intelligence
COBIT	Control Objectives for Information and Related Technology
DAC	Discretionary Access Control
DAX	Data Analysis Expressions
DSR	Design Science Research
ETL	Extract, Transform, Load
GDPR	General Data Protection Regulation
GUIA	NOS's Identity and Access Management system
IAA	Identity, Authentication, and Authorization
IAM	Identity and Access Management
IT	Information Technology
ITM	IT Service Management
IoT	Internet of Things
KPI	Key Performance Indicator
MAC	Mandatory Access Control
NIF	Número de Identificação Fiscal (Tax Identification Number)

NIST SP	National Institute of Standards and Technology Special Publication
ODS	Operational Data Store
OrBAC	Organization-Based Access Control
PoLP	Principle of Least Privilege
RBAC	Role-Based Access Control
RLS	Row-Level Security
RPA	Robotic Process Automation
SAP BO	SAP BusinessObjects
SIEM	Security Information and Event Management
SSO	Single Sign-On
SoA	Statement of Applicability

1. Introduction

Identity and access management (IAM) is a critical component of information security systems and is necessary to ensure that individuals only have the permissions required to perform their roles, addressing risks such as unauthorized access, compliance violations, and data breaches (Anderson & Mutch, 2011). IAM is a set of tools, procedures, and guidelines for managing, regulating, and safeguarding access to an organization's resources (Damon & Coetzee, 2013; Devlekar & Ramteke, 2021). To improve security and productivity, it consists of controlling digital identities and their authorization within or across system and enterprise boundaries (Devlekar & Ramteke, 2021).

According to Anderson and Mutch (2011), information technology access abuse can be classified as intentional, accidental, or indirect. Intentional attacks, such as cyberattacks, against the identity and access management system can compromise the entire organization and vital services and infrastructures (Devlekar & Ramteke, 2021). Abuse of access can also have a wide range of negative effects, from significant financial loss and expense to a decline in public trust in the organization (Damon & Coetzee, 2013)

The impact of IAM systems can be measured across three primary areas: reducing costs, increasing operational efficiencies, and improving employee productivity (Rossnagel et al., 2020). IAM systems achieve these benefits by improving access processes and minimizing security risks. Established Identity, Authentication, and Authorization (IAA) programs provide robust tools and processes that not only protect against access abuse but also operational efficiency by reducing administrative overheads, as automated tools replace manual processes, and user identity self-service, enabling employees to manage their credentials with minimal IT intervention (Damon & Coetzee, 2013). IAM systems can also increase overall productivity by ensuring seamless access to necessary resources while ensuring compliance with regulatory requirements (Damon & Coetzee, 2013).

Because modern organizations generate and consume vast volumes of digital identity and access data, managers struggle to maintain oversight of who has permissions, when and why (Singh et al., 2024). A reporting system offers a solution to this challenge by enabling organizations to measure, track, manage, and communicate their performance and progress, through the collection and analysis of information that supports decision-making for stakeholders (Manente et al., 2014). Understanding Business Intelligence (BI) is essential, as it provides the processes, technologies, and framework necessary to build a reporting system.

BI encompasses the extraction and transformation of data, its storage, and its visualization through dashboards, scorecards, or other reporting formats (Wixom & Watson, 2010).

The motivation for this study includes several factors. The first one is the growing importance of information security as personal and proprietary information held by organizations increases and becomes more valuable. IAM systems are also essential to address new cybersecurity threats and to comply with national and European regulations on data protection and privacy. The strategic importance of identity and access control, especially for large organizations, is fundamental to minimize operational risks associated with large numbers of employees, subcontractors, and external partners. There is also a lack of research on the impact of analysis via the use of reporting systems on the ability of a company to better manage identity and access control systems.

This study is based on an internship at NOS Comunicações S.A. (hereinafter referred to as NOS), one of the three biggest telecommunications providers in Portugal. The internship is integrated into a commercial services sales team and focuses on developing an access management reporting system. NOS faces unique challenges in managing its identity and information control due to the scale of its operations, its diverse workforce, and its reliance on subcontractors and external partners for the sale of its services. The objectives of the internship at NOS are the following: 1) to develop a reporting system that can provide insights into access management and security practices; 2) to design and implement dashboards that improve data exploration and support better decision-making processes;3) and finally, to analyze data and identify opportunities for improvement and resolve existing issues within the access control systems.

This study adopts a qualitative single-case study approach (Yin, 2014), focusing exclusively on NOS. Data collection combined semi-structured interviews with five key stakeholders to identify tool limitations and user needs; document analysis of information security policies, access standards and the GUIA user guide to map formal IAM controls; and system logs from SAP BusinessObjects to review errors issues like duplicate permissions. Direct observation of workflows and dashboard usage, together with discussions with the quality teams, served to triangulate data, validate the findings, and ensure that the resulting BI solution aligns with the technical and organizational objectives.

The dissertation is divided into seven chapters. The first chapter introduces the strategic importance of IAM, along with the study's objectives. Chapter 2 presents the literature review on IAM principles, models, and frameworks, and explores how BI supports

monitoring and reporting for access management in telecommunications. Chapter 3 outlines the methodology and describes data-collection methods. The next chapter presents NOS's organizational context, existing IAM processes, and the challenges that prompted the dashboard intervention. Chapter 5 describes the technical development of the Power BI dashboard, including data integration, DAX measure creation, and visualization design. The last chapter summarizes key conclusions, contributions, limitations, and proposes directions for future research on IAM reporting tools.

2.Literature review

This chapter reviews the key concepts of IAM, its application within the telecommunications sector, and the contribution that BI can make to improve the information security with reporting systems. The first part of the chapter focuses on BI literature, the implementation of a BI system, key performance indicators, and the design and deployment of dashboards designed for IAM reporting needs. The second part begins by the examination of some of the principles of IAM, before exploring the most widely adopted IAM models, Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), and the international frameworks that provide the best IAM practices and guidelines for organizations to follow.

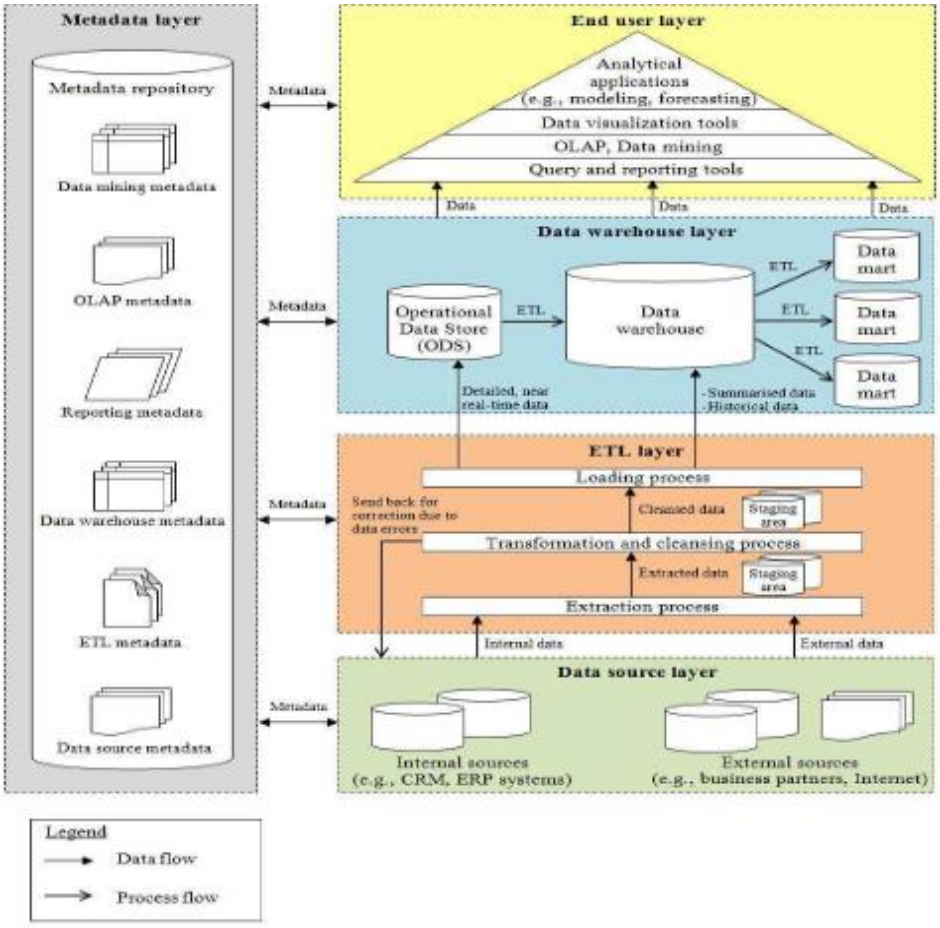
2.1. Business intelligence concept

2.1.1. Concept and architecture of business intelligence

BI is composed of the technologies, tools, and processes that enable organizations to transform raw data into meaningful information, then into actionable insights with the objective of supporting the organization decision-making (Wixom & Watson, 2010). According to this definition, BI is more than just front-end applications such as dashboards, scorecards, or predictive analytics (Wixom & Watson, 2010). It is the entire process of transforming data into actionable insights. Including the extraction of data from source systems, its storage—typically in data marts or data warehouses—and its analysis and visualization using BI technologies (Wixom & Watson, 2010; Zulkifli Abai et al, 2019).

According to Ong et al. (2011), the architecture of a BI system can be divided into five parts: the data source, ETL (Extract-Transform-Load), data warehouse, end user, and metadata layers, as illustrated in Figure 1.

Figure 1- Architecture of a BI system



Source: Ong et al. (2011)

The first layer is the data source layer, which provides the raw data that is necessary for analysis and decision-making, the data can be obtained from both internal and external sources. Internal data sources refer to information generated and maintained within the organization, through operational systems that capture data related to daily business operations and internal processes (Ong et al., 2011). External data sources originate outside the organization and include information from business partners, government databases, market research firms, or online platforms. These external sources are useful for benchmarking, market analysis, and gaining broader contextual insights (Ong et al., 2011; Ranjan, 2009).

ETL comprises three sequential processes: extraction, transformation, and loading. Extraction involves identifying and collecting data from internal and external sources. The datasets obtained can be incomplete, unstructured, and contain duplicates, making integration difficult (Olszak & Ziemba, 2007; Ong et al., 2011; Ranjan, 2009). Once extracted,

the data are transferred to a staging area, where they are held before processing (Ranjan, 2009). Transformation applies a set of business rules—such as aggregation, filtering, or formatting—to convert the raw data into a standardized and consistent structure suitable for analysis (Ong et al., 2011). Finally, in the loading phase, the transformed data are transferred from the staging area into the target repository where they become available for querying and visualization (Ong et al., 2011).

The Data Warehouse Layer includes three main components: the Operational Data Store (ODS), the Data Warehouse, and Data Marts (Olszak & Ziemba, 2007; Ong et al., 2011). The ODS serves as an intermediary repository that integrates data received from the ETL layer. It provides a near real-time, consolidated view of current data, which is necessary for operational reporting and quick decision-making processes (Ong et al., 2011). The Data Warehouse functions as a centralized storage system that aggregates, organizes, and maintains the historical data from both internal and external sources. It stores summarized data and supports complex queries and trend analysis (Ong et al., 2011). Data Marts are specialized, smaller-scale subsets of the data warehouse designed to serve specific business functions. They provide tailored data views optimized for the analytical needs of individual units, such as finance, marketing, or human resources (Bukhbinder et al., 2005).

The Metadata Layer in a BI system provides information about the data itself, it describes where the data is stored and used, its source, any changes made over time, and how it relates to other data elements (Ong et al., 2011). A metadata repository is used to store both technical and business metadata, including data definitions, transformation rules, and business logic. This layer helps ensure consistency, traceability, and clarity in data interpretation and usage across the BI environment (Ong et al., 2011).

The End-User Layer consists of tools that present information in various formats tailored to the needs of different users (Ong et al., 2011). Data visualization tools, such as dashboards and scorecards, provide managers and executives with high-level overviews of business performance. Analytical applications offer advanced functionalities like modeling, forecasting, sales analysis, and what-if scenarios. Query and reporting tools enable users to quickly access data and generate reports to support management activities (Ong et al., 2011).

2.1.3. Implementation of a dashboard

One of the key data visualization tools used within BI systems is the dashboard, which enables users to effectively interpret and interact with data (Ranjan, 2009). Dashboards provide a visual interface that presents information through charts, color-coded metrics, and tables, allowing users to monitor performance indicators in real time. They offer a consolidated view of critical data, enabling decision-makers to quickly identify trends and anomalies (Janes, Sillitti & Succi, 2013). Additionally, dashboards also allow for drill-down functionality, giving users access to more detailed insights behind key performance indicators across different areas of the organization (Janes, Sillitti & Succi, 2013).

According to Yermalovich (2020), the development of an effective dashboard follows a five-stage process designed to align visualization tools with organizational goals. The first stage involves identifying the performance axes, which define the focus areas the dashboard is intended to monitor. The second stage consists of clarifying the dashboard's objectives and the types of decisions it should make. In the third stage, relevant Key Performance Indicators (KPIs) are selected based on organizational needs and data availability. The fourth stage is the construction of the dashboard, where appropriate visual formats, layouts, and user interfaces are developed for clarity and usability. Finally, the fifth stage focuses on testing and validation, ensuring the dashboard performs accurately and effectively in real-world settings before full deployment (Yermalovich, 2020).

The KPIs are quantifiable measures used to assess the performance of individuals, teams, departments, and organizations in relation to defined strategic or operational goals. In the BI, KPIs play a central role in the development of any dashboard. (Nunes et al., 2024). Dashboards visually represent KPIs through charts, gauges, traffic lights, and scorecards, simplifying complex data to support rapid decision-making (Yigitbasioglu & Velcu, 2012). This quick response is critical when an organization is dealing with access control, compliance monitoring, or operational risk management (Yigitbasioglu & Velcu, 2012).

Eckerson (2009) identifies ten fundamental characteristics which make KPIs effective for driving organizational change. First, KPIs should be sparse, meaning that fewer, more focused indicators are preferable to an overwhelming number of metrics. Users should be able to drill down into the data to uncover additional information for better understanding. The measurement criteria should remain straightforward for users to comprehend while providing clear directions about performance influence. The ownership

of KPIs should rest with specific teams or individuals who will maintain responsibility for them. All KPIs need to be referenced because their definitions and data sources and context must be easily accessible to users. The two types of KPIs include correlated indicators which directly impact business results and balanced indicators which combine financial and non-financial metrics to show complete performance. The alignment of KPIs ensures departments work together effectively since they support each other instead of creating conflicting goals. The design of KPIs must include validation features which prevent users from altering or bypassing the metrics according to Eckerson (2009).

For the construction and design of the dashboard there are certain principles that should be considered to ensure usability and clarity. It's critical to prioritize simple visuals, ergonomics and easy to understand analytical elements by ensuring the quick movement through different indicators, choosing suitable colors and fonts for readability and arranging components, like performance axes, indicators, and tooltips in a well-defined and rational format to improve understanding and analysis (Yermalovich 2020). Overloading dashboards with excessive information or complex visuals can overwhelm users, leading to reduced efficiency. Instead, dashboards should prioritize simplicity and adhere to principles like completeness, conciseness, clarity, relevance, and transparency to improve readability and usability, ensuring they support decision-making processes (Janes, Sillitti & Succi, 2013).

According to Eckerson (2009), dashboards can be divided into three main types—strategic, tactical, and operational—each serving different organizational roles (See table 1). Strategic dashboards serve as the primary tool for senior executives to track long-term performance while supporting strategic planning and enterprise-wide decision-making. These dashboards use outcome-based KPIs to consolidate lower-level metrics into high-level summaries of organizational performance, outcome-based KPI is a lagging indicator that reflects the achieved results of past actions. Strategic or planning meetings are typically held to review these dashboards on a monthly or quarterly basis.

Table 1- Types of Dashboards

	Strategic	Tactical	Operational
Focus	Execute strategy	Optimize process	Control operations
Use	Management	Analysis	Monitoring
Users	Executives	Managers	Staff
Scope	Enterprise	Departmental	Operational
Metrics	Outcome KPIs	Outcome and driver KPIs	Driver KPIs
Data	Summary	Detailed/summary	Detailed
Sources	Manual, external	Manual/core systems	Core systems
Refresh cycle	Monthly/quarterly	Daily/weekly	Intraday
"Looks like a..."	Scorecard	Portal	Dashboard

Source: Eckerson (2010)

The implementation of tactical dashboards enables mid-level managers and departments to optimize their team and process performance through alignment with organizational targets. The dashboards show outcome and driver KPIs which integrate information from strategic dashboards and operational systems. The dashboards receive updates between daily and weekly intervals to help teams identify problems early so they can achieve their short-term and medium-term targets (Eckerson, 2009). The main purpose of operational dashboards is to support front-line staff who need to track and manage their daily business operations. The dashboards use real-time data or near-real-time data to show operational metrics and driver KPIs which allow staff to take immediate action when they detect operational issues or inefficiencies. The three dashboard types work together to create a multi-level system which supports performance tracking and decision-making at every organizational level (Eckerson, 2009).

The objective of integrating a dashboard into an identity and access management system is to provide managers, IT professionals and employees with a comprehensive and interactive view of the access control systems anomalies (Damon & Coetzee, 2018). Some of the KPI that could be implemented in any IAM dashboard are Tracking access requests, number of policy violations and time-to-resolve Incidents.

Tracking access requests is a performance metric that reports the number of approvals, denials, and escalations over time, that users experience when they try to request access to files, folders, apps or other digital resources (Peterson, 2006). The objective of this performance indicator is to help organizations identify if they have problems or bottleneck in their approval process, for example a spike in denied requests might indicate overly restrictive policies or misconfigurations that need adjustment (Damon & Coetzee, 2018; Peterson, 2006).

Policy violations measure the frequency of unauthorized login attempts or excessive permissions granted to users. Monitoring policy violations in real-time helps organizations quickly identify security breaches or misconfigurations that could lead to data exposure (Puchta et al., 2019). One example of policy violations is an overprovisioned account, where users have more permission than necessary for their roles (Puchta et al., 2019). Dashboards can flag such accounts by comparing assigned permissions against predefined role templates, ensuring adherence to the Principle of Least Privilege (Kim et al., 2011).

Another KPI for an IAM dashboard will be time-to-resolve Incidents, the objective of this metric is to evaluate the effectiveness of the organization in responding to anomalies or access abuses by measuring the average time to respond to such incidents (Peterson, 2006; Schell et al., 2009). The integration of compliance metrics into the dashboard will improve the organization adherence to regulatory requirements such as GDPR or ISO/IEC 27001 as the tracking of the implementation and enforcement of policies will help the organization identify vulnerabilities or inefficiencies in their access control systems (Hummer et al., 2018; Merchan-Lima et al., 2021).

The implementation of the dashboard will help in the identification of role or attribute drifting, as they occur when a user's permissions extend beyond their original role, often because of role changes or temporary assignments. (Puchta et al., 2019; Schell et al., 2009). Similarly, dashboards can also be used to monitor breaches of segregation of duties policies, which are designed to prevent conflicting responsibilities from being assigned to a single user. For example, the same user should not have the authority to both initiate and

approve financial transactions, and dashboards can help identify and address such violations (Damon & Coetzee, 2018; Devlekar & Ramteke, 2021).

2.2. Identity and access management

2.2.1 Concept of identity and access management

IAM refers to the set of technologies, processes, and policies used to manage, control, and protect access to an organization's information systems and digital resources. (Anderson & Mutch, 2011). Its primary objective is to ensure that individuals and entities have the appropriate level of access at the right time, thereby strengthening security and improving operational efficiency (Devlekar & Ramteke, 2021). IAM is typically structured around three key components: Identity Store, Identity Management, and Access Management (Devlekar & Ramteke, 2021).

The Identity Store is responsible for maintaining unique digital representations of individuals, services, or devices along with their associated attributes and credentials (Devlekar & Ramteke, 2021). Identity Management involves administering the entire lifecycle of digital identities, from creation and modification to deactivation (Devlekar & Ramteke, 2021). Access Management encompasses the technologies and procedures that regulate access to systems and resources. It includes three fundamental activities: identification, which involves uniquely recognizing an entity; authentication, which verifies that the entity is who it claims to be; and authorization, which determines and enforces the rights and privileges granted to the entity (Devlekar & Ramteke, 2021).

The essential principles for any IAM models or frameworks are Authentication, Authorization, and Accounting (AAA) and the Principle of Least Privilege (PoLP). In AAA, authentication verifies a user's identity to ensure only authorized users access systems, and authorization determines the permissions granted based on roles or attributes. And accounting tracks user activities, providing records of activities for auditing and compliance (Kalloniatis et al., 2010). The PoLP reduces security risks by ensuring users, systems, and processes have access only to the resources necessary for their tasks. The principle is based on minimizing excessive permission preventing unauthorized actions and limiting the damages from insider threats or breaches (Kim et al., 2011).

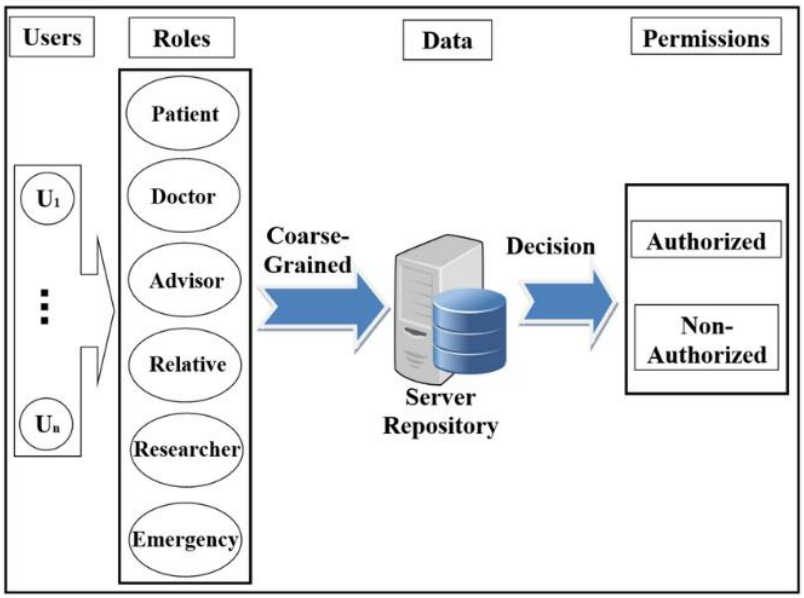
2.2.2. Types of access control models

Access control model is an essential part of IAM, the roles and privileges that a user can possess are based on the access control model that an organization uses for their identity and access systems (Devlekar & Ramteke, 2021). Access control models are a collection of subjects, objects, operations, permissions, and policies (Penelova, 2021). A subject can be a person, a computer process, or a device. The object is a software resource. An operation is when the subject makes an access request for the object. Permission shows that a subject can access an object through an operation. And a policy is a rule that shows if the access request must be granted or denied (Penelova, 2021).

There are multiple examples of access control models, some of which are less commonly used by organizations. These include Mandatory Access Control (MAC), a system that matches a user's security clearance with the security classification assigned to an object. (Devlekar & Ramteke, 2021; Osborn et al., 2000). Discretionary Access Control (DAC), where the owner determines which subjects can access an object based on a defined set of rules (Osborn et al., 2000). Lastly, there is Organization-Based Access Control (OrBAC), a model specifically designed for organizations, where rules are created to define contextual permissions and prohibitions (Penelova, 2021).

According to Devlekar and Ramteke (2021), RBAC and ABAC are among the most widely used access control models in modern organizations. RBAC operates by assigning permissions to users based on their roles in an organization, as shown in Figure 2. Using this model, it is easy for administrators to manage and enforce access controls with consistently and quickly changing permissions for employes (Ferraiolo et al., 2001; Kim et al., 2011). An example that was given by Penelova (2021) is if the user has the job of accountant, in the IAM system, he will be assigned the role of "accountant" and automatically have the permissions that are set for that role.

Figure 2-Scheme of RBAC model.

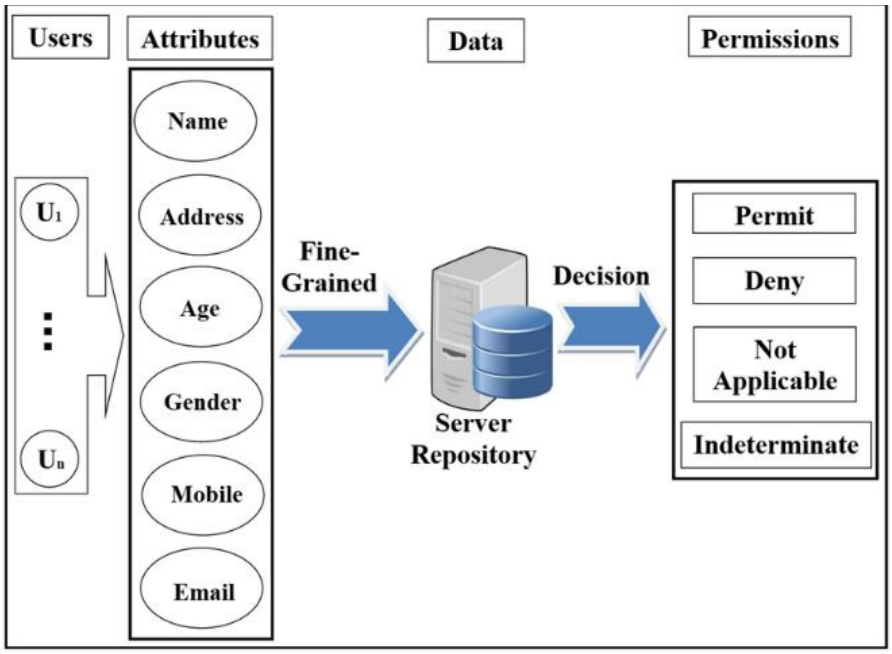


Source: Al-Zubaidie et al. (2019)

The RBAC model is built on five components: users, roles, permissions, operations, and objects, roles represent specific job functions, and users assigned to these roles inherit predefined permissions to access necessary resources (Kim et al., 2011). Some of the features of this model include static and dynamic separation of duties which prevent conflicting roles from being assigned or activated simultaneously and the ability to have hierarchies where roles can inherit permissions and responsibilities, for example a manager role will also have the permissions of subordinate roles (Ferraiolo et al., 2001).

ABAC is an access control model where decisions are made based on the attributes of users, resources, and environmental conditions (Devlekar & Ramteke, 2021) (See Figure 2). This model is ideal for heterogeneous information systems, as ABAC provides a flexible approach that is necessary if an organization has multiple types of data from different sources and requires a complicated set of permissions (Hu et al., 2013; Penelova, 2021). ABAC operates on attributes represented as key-value pairs like role = administrator or age = 34. ABAC will evaluate attributes, the environmental conditions and the internal policies and make an access decision whether access is granted or not. The model allows subjects and objects that do not exist in the system to be included in a policy enabling dynamic and context-aware permissions (Lanus et al., 2023; Penelova, 2021).

Figure 3- Scheme of ABAC model.



Source: Al-Zubaidie et al. (2019)

The advantages that the ABAC model has over the RBAC model are avoiding the need for predefined roles and permissions for every possible scenario that is the cause of "role explosion" in the RBAC Model. The ABAC model has better privacy and security as the process of granting authorization and access is based on attributes rather than identity (Lanus et al., 2023). The main disadvantage of the ABAC model is the need for defining multiple attributes for each user, making its use more complex than the RBAC model (Lanus et al., 2023).

2.2.3. IAM challenges

IAM in telecom companies face multiple challenges, including the integration of diverse identities, complex network architectures, and compliance with privacy regulations (Anawar et al., 2022). As systems expand to include not only human users but also technical entities like devices and Internet of Things (IoT) elements, it has become more difficult to correctly integrated and assigned appropriate access permissions to all the elements to avoid vulnerabilities (Puchta et al., 2019).

Privacy and regulatory compliance are also one of the main challenges for IAM systems, especially with regulations like the European Union General Data Protection Regulation (Merchan-Lima et al., 2021). Organizations must balance providing sufficient information access to users and employees while protecting sensitive identity information to comply with national and international regulations (Merchan-Lima et al., 2021). The

operational complexity of access control systems is also a significant challenge as the management for large numbers of employees, subcontractors, and external partners can be demanding so inefficiencies, such as delays in access provisioning or policy enforcement, can negatively impact operational efficiency (Damon & Coetzee, 2018).

The heterogeneity of identities in modern organizations is a challenge for access management, as diverse attributes across human users, devices, and applications require complex policies that control models like RBAC struggle to adapt, necessitating the transition to models like ABAC, which bring their own implementation complexities (Lanus et al., 2024; Puchta et al., 2019). Data quality and management is another challenge in access management as identity attributes systems must have constant surveillance and maintenance due to the risk incorrect or redundant permissions, that lead to overprovisioned accounts, increasing the risk of unauthorized access (Kim et al., 2011).

Telecom companies face significant challenges with IAM systems, which are essential for securing sensitive data and ensuring operational integrity. According to Anawar et al. (2022) complex network architectures, which are used by modern telecom systems like 5G, face is the identification and management of relevant identities. These networks involve numerous interconnected components, including base stations, routers, cloud storage, and edge computing systems. Each component represents a potential vulnerability that must be secured to protect data privacy. Privacy and regulatory compliance are important issues for telecom companies due to the sensitive nature of telecom data, which includes confidential information such as call detail records, geolocation data, and internet browsing history. The consequences of the improper use of this data can be financial fraud, identity theft, privacy violations, and harm to telecom providers' reputations (Cheng & Bilal, 2024).

Telecom companies also face challenges related to data privacy due to the volume and velocity of data they process daily (Malaka & Brown, 2015; Martucci et al., 2012). As they have large amounts of data flowing continuously between users, devices, and networks there is an increase in the risk of exposure and complicated traditional data security methods (Martucci et al., 2012). Real-time monitoring and encryption are necessary to address these challenges effectively. Telecom companies must implement strict access controls that limit sensitive data access to authorized personnel to reduce these risks (Martucci et al., 2012).

There are privacy and security issues with telecommunications companies' use of external partners, subcontractors, and resellers. As sensitive information can be easily compromised by misuse or negligence from third parties who do not have the necessary training (Anawar et al., 2022). To reduce risks and guarantee that external partners and subcontractors follow the company's data protection policies, it is also crucial to implement thorough employee training programs on privacy practices and potential threats (Damon & Coetzee, 2018).

2.2.4. International Frameworks for IAM

The international frameworks utilized by organizations, for IAM include NIST Special Publication 800–53 (NIST SP 800–53) ISO/IEC 27001 and Control Objectives for Information and Related Technologies (COBIT). These frameworks offer guidance in safeguarding information security through control definitions and best practices to secure data effectively and ensure adherence to regulations while minimizing risks. They emphasize governance structures, resilience building, and access management strategies, to aid organizations in aligning their IT security approaches, with needs and regulatory standards (Merchan Lima et al., 2021).

The ISO/IEC 27001 standard received its first publication in 2005 through joint development by the International Organization for Standardization and the International Electrotechnical Commission to create a process-based framework which unites technical and managerial elements (Culot et al., 2021). The main goal of ISO/IEC 27001 exists to protect information from unauthorized disclosure while maintaining its integrity and ensuring availability. The framework establishes confidentiality as the protection of information from disclosure to unauthorized parties and entities. The framework establishes three core properties for information security: confidentiality protects data from unauthorized disclosure, integrity ensures data accuracy and completeness, and availability always ensures authorized access (British Standards Institution, 2023; Mirtsch, 2023).

Organizations that meet ISO/IEC 27001 requirements can pursue certification through a two-step process. After an internal audit, an external auditor reviews documentation and conducts an audit to verify compliance. Certification is often limited to specific organizational units, such as IT or data centers, and requires a Statement of Applicability (SoA) alongside the certificate (Mirtsch, 2023). Formalization required by this standard may reduce flexibility, negatively impacting labor productivity and responsiveness to client demands (van Wessel et al., 2011). While its value extends to sales performance and

external communication, ISO/IEC 27001 also holds significant implications for profitability and operational efficiency (Culot et al., 2021).

NIST SP 800-53 is a framework that provides comprehensive guidelines for securing access configurations, outlines a robust set of controls to protect sensitive data, ensure operational resilience, and align access management with industry best practices (Putra & Soewito, 2023).The framework categorizes its controls into families, like the Access Control family, which addresses key principles like least privilege, separation of duties, and audit logging (Brickley & Thakur, 2022; Putra & Soewito, 2023). The NIST SP 800-53 guidelines help organizations set appropriate security controls required for the information management systems, and the evaluation methods do determine the effectiveness of the security controls practices (Putra & Soewito, 2023).

The objective of the framework is to help organizations minimize risks from unauthorized access and insider threats while ensuring compliance with regulatory standards and improving communication among the organization. The framework that NIST 800-30 provides for an effective risk management strategy has nine steps, it starts with system characterization, identifying possible treats, identifying vulnerabilities in the IT system, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and the results document of the risk assessment report (Putra & Soewito, 2023).

The COBIT offers effective practices throughout a framework and lays down activities in an organized and flexible structure (Khther & Othman, 2013). Developed by Information Systems Audit and Control Association (ISACA), COBIT focuses on integrating risk management, performance measurement, and compliance (Khther & Othman, 2013). Control objectives exist to assist in building a suitable management and control system into the IT environment and to make sure that a continuous service is provided, which can be established through the implementation of several control procedures, such writing or testing continuity plans. COBIT has 34 IT processes with control objectives listed for each process, and management guidelines provide information to measure, control, and organize particular IT processes (Khther & Othman, 2013).

3. Methodology

3.1. Methodology approach

The objective of this study is to implement an IAM reporting system for monitoring employee access within NOS's systems with the objective of mitigating the risks of unauthorized access. The specific objectives are:

- to develop a reporting system that can provide insights into access management and security practices.
- to design and implement dashboards that improve data exploration and support better decision-making processes.
- and finally, to analyze data and identify opportunities for improvement and resolve existing issues within the access control systems.

The study adopts a qualitative case study as its research strategy. A case study is a research strategy that involves an empirical investigation of a contemporary phenomenon within its real-life context, utilizing multiple sources of evidence (Yin, 2018). It aims to provide an in-depth understanding of a specific issue by conducting an analysis of an individual, group, or event (Yin, 2018).

When choosing between various research strategies for the study one of the most important deciding factors is the type of research objectives that are being asked. According to Yin (2018), a case study is the preferred research strategy when the focus of the research is on questions that start with "how," "why," and "what". So, due to the nature of the research question a case study strategy has been adopted. The second reason for this choice is to better understand the research context and the processes involved (Yin, 2018). In this study, the case study approach is applied due to the significance of NOS's organizational context and the organization's information security systems in implementing identity and access BI reporting model.

According to Yin (2018), there are two main design types for case studies: single-case study and multiple-case study. A single-case study is appropriate when the researcher seeks to conduct an in-depth and focused investigation within a specific, bounded context. In this dissertation, the single-case study design was chosen due to the opportunity provided by the internship at NOS, which enables direct access to internal data, systems, and stakeholders.

The case study method can serve three primary purposes depending on the research objective: descriptive, explanatory, and exploratory (Yin, 2018). Descriptive case studies aim to portray a phenomenon as it exists by describing its characteristics and context. They are used for answering "what" questions, such as documenting how a new organizational process is structured or what is the outcome a policy has produced (Yin, 2018). Explanatory case studies seek to uncover causation, focusing on "how" and "why" events or processes unfold as they do. This approach is suited for understanding mechanisms, such as why a program succeeded or failed. (Yin, 2018). Exploratory case studies are designed to generate insights, identify key factors, and define research questions for further investigation. They used to study new or poorly understood phenomena where the aim is to build a foundation for future research (Yin, 2018).

The most appropriate methodological design for this dissertation is a descriptive single-case study. Because the goal of this study is not to test any propositions or develop any new theory, but to describe the implementation of a BI system developed to aid in the management of IAM. This approach allows for a comprehensive understanding of NOS's current practices, offering valuable insights into the organizational processes and challenges associated with access control reporting (Yin, 2018).

3.2. Data collection

The study utilizes a qualitative research method to gather the data. Qualitative research methodology involves verbal descriptions of real-life situations, utilizing multiple data collection methods like observation, interviews, collection of documents, pictures, audio-visual materials as well as representations of artifacts generating non-numerical data (Silverman, 2011). The use of qualitative data in this study has the objective of understanding how NOS utilizes its IAM systems, what the expectations of future users of the reporting model are for its functionality and usability, and how it can be tailored to meet the specific needs of the different users.

Stake (1995) explains that, to have confidence in the information gathered, a case study should draw data from multiple sources—i.e., data triangulation—to confirm critical assertions or interpretations in the research, or to validate information that may be dubious or contested in a single source. Data triangulation is also an effort to ensure that the information observed or discovered is consistent across different circumstances (Stake, 1995). The three sources of data that this study utilizes are semi-structured interviews, documentation and the use of observation.

According to Silverman (2011), documents are an easily accessible data source that can be used to get an overall picture of how an organization operates, as this data exists without the interference of the researcher it allows an authentic understanding of organizational practices. The documents that were used in this study are focused on NOS information security systems and identity and access systems. This includes documentation about information security frameworks, security guidelines, existing IAM focused dashboards. Training material and user manual about the IAM system were also analyzed to better understand how NOS employees use the IAM system.

Table 2- Documents Analyzed

Document Title	**Type**	**Purpose in Research**	**Source**
Information Security Management System (ISMS) Manual	Internal policy/Framework manual	Analyze the organization's overarching information security framework, roles, and responsibilities, including how access control is governed under ISO/IEC 27001.	Information security department
General information security policy	Internal policy manual	Understand NOS's overarching information security principles, objectives, and governance model	Information security department
Security standard for access management	Technical security standard	To analyze procedures, roles, and rules related to user access provisioning, review, and deprovisioning.	Information security department
Information Classification and Management Standard	Data classification policy	To examine how data is categorized and handled to align access levels with information sensitivity.	Data protection office
GUIA Manual	IAM system Manual	Review how access profiles and user permissions are technically managed.	IT/ Information security department

Source: Own Work

As part of the data collection strategy, semi-structured interviews were conducted with key stakeholders across NOS's commercial and technical departments. These included participants from the commercial sales teams, such as managers and operational staff, as well as IT managers and information systems administrators. The aim of the interviews was to gather insights into their experiences with the IAM systems and to provide contextual depth to complement data collected through other methods.

In total, five individuals were interviewed: the Operations Department Manager, who oversees the four main operational support areas (Quality, Commissions, Automation, and Commercial Support) (E1); the Head of the Quality Team, responsible for managing access rights and internal audits (E2); the Access Manager, who executes operational tasks related to provisioning and revoking access (E3); risk and compliance team leader in the Audit, Risk, and Compliance department, responsible for monitoring user activity through Power BI dashboards (E4); and the IT Auditor , who manages the organization's circularization dashboard used for tracking critical access risks (E5).

Table 3- List of Interviews.

Participant Role	**Department Team**	**Duration**	**Date**
Operations department manager	Operations department	10 minutes	20/03/2025
Head of the quality team	Quality team	15 minutes	26/03/2025
Access manager	Quality team	20 minutes	31/03/2025
Risk and compliance team leader	Audit, risk, and compliance department	20 minutes	02/04/2025
IT auditor	Audit, risk, and compliance department	30 minutes	04/04/2025

Source: Own Work

The semi-structured interviews allowed respondents to elaborate on the strengths, limitations, and expectations regarding IAM systems and reporting tools. Questions were tailored to each participant's role and covered areas such as the structure of their teams, specific responsibilities in access management, the tools currently in use (e.g., Power BI dashboards, Guia, Garra, UiPath), approval workflows, frequency and process of access reviews, and collaboration between departments. Furthermore, the interviews explored how access is currently granted, reviewed, and revoked, as well as perceived gaps or inefficiencies in the current processes. A particular focus was placed on gathering input for the design of a new dashboard, including participants' expectations, preferred usability features, and the types of indicators or alerts they considered most valuable for supporting monitoring and decision-making.

Direct observation was employed to capture real-time interactions and behaviors related to access management. This included analyzing how employees requested access, how approval processes were handled, and how teams monitored IAM compliance. According to Silverman (2011), direct observation helps researchers understand how policies are enacted in practice and how employees navigate access control challenges. The information acquired complements the interview data by identifying discrepancies between documented procedures and actual practices, thereby improving the overall validity and reliability of the findings (Robson, 2016).

During the execution of the activities required for the implementation of the reporting system, it was necessary to utilize a range of software tools to support the development process. These tools played a fundamental role in enabling data modeling, visualization, and performance optimization. Specifically, the project relied on Power BI Desktop for the creation of dashboards and data visualizations, and Power BI Service for publishing and sharing reports within the organization. Microsoft Excel was used for the initial analysis of the available data and detection of possible errors in the dataset.

4. The empirical setting - NOS Comunicações, S.A.

4.1. General information

NOS Comunicações, S.A. is one of Portugal's leading telecommunications and entertainment providers and offers a range of services including fixed and mobile telecommunications, internet, television, and entertainment content. NOS was launched as a rebrand of the merger of ZON Multimedia and Optimus Telecomunicações that occurred in 2013. This merger combined two of Portugal's major communication companies improving their market positions.[1]

In telecommunications, NOS delivers fixed and mobile networks, including broadband internet and 5G technology. Its television services, encompassing cable, satellite, and IPTV, provide access to a diverse range of content, including sports and entertainment channels. NOS is also a leader in the entertainment sector, operating Portugal's largest cinema chain, NOS Cinemas, and distributing films and audiovisual content through NOS Audiovisuals. For businesses, NOS offers tailored solutions such as cloud computing, managed IT services, and data centers, supporting digital transformation and operational efficiency.

The recent financial performance of NOS has been very positive, in the first half of 2024 NOS profits stood at €95.4 million, reflecting an 18.6% increase compared to the same period in 2023. The company invested €185.1 million during this period, equivalent to 22.1% of its telecommunications revenues, focusing on expanding its 5G network, which now covers 96.5% of the national population.[2]

4.2. Organizational structure and responsibilities

The internship took place within the business transformation center, a division responsible for developing products and services for enterprise clients, as well as managing all related operations. This division is organized into three key areas: product segment management, business development, and customer experience.

[1] https://www.nos.pt/en/institutional/nos/history

[2] https://business-it.pt/2024/07/19/receitas-consolidadas-da-nos-cresceram-52-no-primeiro-semestre-de-2024

The business development area is responsible for managing the enterprise product catalog across various market segments. It ensures effective pre-sales conditions tailored to different customer segments and sales channels, while also delivering value propositions for several business lines such as communications, cloud services, consulting, and mobile networks. The product segment management team focuses on market analysis, business analytics, data engineering, digital content, and customer relationship management. The experience area includes departments such as operations and the proposal center, and partnerships. The proposal center is tasked with aligning and ensuring the quality of B2B proposals for NOS. It is also responsible for preparing timely and commercial sound responses and for representing NOS in interactions with strategic partners.

During my internship, I was integrated into the operations department, specifically within the quality team. The operations department is structured into four main teams: automation, commissions, quality, and support to the commercial queue. The Automation team is responsible for identifying opportunities for robotic process automation, evaluating their feasibility, developing business cases, implementing automation solutions, and ensuring ongoing maintenance of the robots. The commissions team handles the calculation and validation of commission cycles for sales teams and channel partners. They also focus on automating commission processes and reporting, as well as analyzing and implementing new commission plans. The support to the commercial queue team is dedicated to assisting sales agents by clarifying questions, providing training, and monitoring non-conformities in the sales and provisioning processes. They also follow up on pending issues and non-conformities, ensuring smooth progression of processes until the activation of services.

The quality team manages user access and commercial structures across various departments, such as the business transformation center (CTE), enterprise channels, and direct sales. Additionally, the team monitors compliance with security, privacy, and data protection policies, and oversees the quality of sales negotiation and formalization processes in remote channels, ensuring proper governance and supporting continuous improvement through training and awareness initiatives. Their main duties involve the creation of new teams and user profiles, as well as handling "I NEED" requests—internal support tickets raised when employees are unable to access essential applications. In these cases, the quality team analyzes the request and resolves the issue, ensuring minimal disruption to business operations. This responsibility spans a significant user base, including approximately 1,000 internal and external collaborators in the enterprise channels division, 120 employees in direct sales, and around 300 employees within the CTE.

The enterprise channel division focuses on sales to small and medium-sized enterprises (SME) and is composed of a wide variety of roles and sales models. It includes in-store sales teams that support businesses directly at NOS retail locations, dedicated agents who sell only NOS services and manage high-value client portfolios, and authorized resellers who, despite not having exclusivity with NOS, are allowed to sell its telecommunications products. Additionally, the division includes internally managed NOS teams focused on customer satisfaction, client retention, and outbound or inside sales aimed at enhancing the existing value of products and services for SME clients.

The direct sales channel is dedicated to large companies and strategic accounts, including public sector entities and enterprise clients with significant long-term relationships with NOS. This channel requires a tailored and high-value approach, given the complexity and critical nature of the clients it serves.

Although the quality team handles most access-related tasks, there are situations where other departments are responsible. For instance, when a new employee joins the organization, the human resources department oversees defining the user's role and assigning the corresponding basic identity and access rights. In other cases, access must be granted exclusively by the owners of specific systems or data. This applies to scenarios such as access to databases, which are restricted to the data owners, or dashboards, which can only be managed and shared by their respective creators or administrators.

5. Design and implementation of reporting system

This chapter outlines the implementation of IAM reporting system. It provides a sequential analysis of each activity, structured as a guide for effective deployment. The discussion begins with the project framework, presenting an overview of the system. Subsequently, the methodologies and technologies employed are described, linking these choices to the literature review. This section examines processes including data modeling, the selection and creation of performance indicators, and the design and development of dashboards. The aim is to illustrate the project's steps and challenges encountered during its execution.

5.1. Framework of the project

For the implementation of the IAM reporting system, it is necessary to consider the layered architecture of BI systems, which typically consists of five key components: data sources, the ETL process, the data warehouse, the metadata layer, and the end-user access layer (Ong et al., 2011). According to Kimball and Ross (2013) the implementation of a new BI system can be divided into three phases. The first phase involves planning and assessing the organization's readiness to support such a system and the requirements that they have for the system. This includes defining business requirements and identifying user needs through interviews or document analysis (Kimball & Ross, 2013).

The implementation process then unfolds along three parallel tracks. The first focuses on technical architecture—designing an integration structure and selecting appropriate tools and technologies. The second centers on data modeling: translating requirements into a dimensional model, then into a physical schema, followed by developing the ETL process to transform and load data. The third phase concerns the development of BI applications. This includes designing templates and analytics features that present key information to users through dashboards and reports (Kimball & Ross, 2013).

5.2. Requirements and expectations for IAM reporting system

The initial gathering of information about the requirements and expectations was done by an interview with the operations department manager and the head of the quality team. The purpose of the interviews was to understand the organization structure of the company, the responsibilities of the quality team and the initial expectations for the systems. The initial expectations according to the quality team leader was a dashboard that could display information about the access permissions and personal information from all the employees that are under the purview of the quality team, with the ability to share that information with the relevant team and department managers. Another objective discussed in the interview was the ability from the dashboard to display alerts about duplicate permissions or outliers in the permission granted with roles or teams.

In the initial interviews two existing PowerBI dashboards were mentioned, access monitoring dashboard and access circularization dashboard. According to E2 e E3 the dashboard has limited utility to them due to their access being restrictive, limited scope of information, their inability to share the information in the dashboard to other departments and teams' managers and lack of tools to compare the permission granted between teams and employees with the same responsibilities. Even with the quality team not regularly utilizing these dashboards it was important to have interviews with risk and compliance team leader responsible for the access monitoring dashboard and a IT auditor responsible for the access circularization dashboard, not only to be able to understand their function but also to be able to understand the programs used in these dashboards, the best origin for their data and the design language at NOS, that the new dashboard should adopt.

The access monitoring dashboard's main objective is to detect unauthorized behavior, such as repeated data searches or access outside normal usage patterns, by displaying data points like the date and frequency of system access, total and distinct queries, and VPN activity of internal and external employees (E4). When predefined thresholds are exceeded, an alert is generated and flagged to their respective team (E4). According to E4, access circularization dashboard focuses on the structural assignment of permissions rather than user behavior. Its core purpose is to support periodic reviews of user access, especially in relation to sensitive or critical systems(E5). The two dashboard have some common features such as only showing information and permissions that are considered as high-risk by the organization, some examples of permission that are classified by the information classification and management standard as high-risk are the ability to mass-checks on

personal data of clients, applications related to reviewing the performance of call center employees by listening on the recording of the calls or the use of VPNs by external contractors.

The analysis of the documentation provided was also important to establish the requirements for the IAM reporting system. According to the ISMS manual, the organization uses the ISO/IEC 27001 framework with the organization following the guidelines set by the standard with the objective of safeguarding confidentiality, integrity, and availability of information (British Standards Institution, 2023). In the ISMS manual and the security standard for access management it is clear that NOS utilizes a hybrid access control model of RBAC and ABAC by combining the characteristics of both models in the IAM model. With some permissions being predefined according to job function, as in a RBAC model (Kim et al., 2011). While other permissions are granted to employees based on the user position in the company, the team that they are assigned to, or the company responsible for their management in the case of external contractors, these are characteristics of an ABAC model (Devlekar & Ramteke, 2021).

The hybrid nature of the IAM control model gives it flexibility and ease of use when assigning permissions to a large number of employees that have similar responsibilities but belong to different teams or are assigned to manage different types of corporate clients (E2). As each employee according to the GUIA manual, has two types of permissions, the identity permissions that are individually granted based on the individual need for a certain application or permission, and the profile that is a predefined set of access permissions associated with a specific role or function within the organization. According to the head of the quality team and the access managers this flexibility also has drawbacks, the ability to assign permission to the profile and the identity can lead to duplication of permission, permission being inconsistent between employees with the same responsibilities, different permission within the same teams and errors in the assignment of permission when they are placed in the wrong category. These errors were verified by the large number of duplicated permissions and the inconsistency of granted permissions by the multiple analyses done in Excel with the GUIA database.

So, the initial requirements are the ability for the quality team to easily access the general information about the permissions of all the employees and be able to share that information with other department managers. The dashboard also needs to highlight potential errors, such as duplicate access, direct permissions bypassing profiles, or

discrepancies in role-based access across similar job titles. Finally, the ability to update and change the system without asking other departments for permission (E2).

5.3. Planning of the Power BI project

The implementation process begins with the focus on technical architecture, designing an integration structure and selecting appropriate tools and technologies (Kimball & Ross, 2013). The BI platform selected for this project is Microsoft Power BI, as it is already deployed organization-wide for dashboard creation and sharing, ensuring integration with existing workflows and user familiarity (E4, E5). Microsoft Power BI is a cloud-based BI platform designed to enable self-service data analytics and visualization (Microsoft Corporation, 2024). Its primary function is to provide users with the ability to connect to a wide range of data sources, transform and model data using Power Query and Data Analysis Expressions (DAX) and create interactive reports and dashboards that can be shared across the organization. It comprises two main components: the Power BI Desktop, where the BI solution was developed; the Power BI Service, for sharing reports.

Once the initial business requirements were established, there was a need to define some of the necessary components to begin the development of the new reporting system. The critical aspects were the identification of the target audience, data sources, the security and access controls necessary for the report and the data refresh frequency necessary for the dataset. Some questions were answered in the first series of interviews; others were clarified during the internship. The primary target audience is the quality team members, with the ability to send the report about the information to other department managers being of secondary importance. Due to the requirement for the visualization tools to be able to show anomalies in the granted permissions and tables with information, the dashboard with its ability to have a consolidated view with KPIs, tables, charts, gauges, and color-coded alerts to highlight trends and anomalies (Yermalovich, 2020). It is the ideal choice for visualization tools.

After evaluating several data source options, the most flexible solution was to export multiple Excel datasets from the SAP BusinessObjects platform, NOS's existing BI tool for data storage from multiple IT systems, including the IAM system GUIA universe. This approach allows the Quality team to modify and refresh the underlying data set on demand, ensuring that the BI solution remains both current and adaptable to evolving requirements.

The downside of this approach is the inability from SAP BO to update the data in real-time, so the data refresh frequency would be once per day in the morning or weakly.

Among the three types of dashboards strategic, tactical and operational, the solution that was chosen was the strategic dashboard. According to Eckerson (2009), tactical dashboards serve mid-level managers and departments by helping them optimize team and process performance in alignment with broader objectives and are updated on a daily or weekly basis. According to E1, this type of dashboard aligns with the objective of the quality team for tools to improve the performance of the access management in the CTE division.

5.4. ETL process and data modeling

ETL process comprises three sequential processes: extraction, transformation, and loading. Extraction involves identifying and collecting relevant data from diverse internal and external sources (Ong et al., 2011). Transformation applies to a set of business rules—such as aggregation, filtering, or formatting—to convert the raw data into a standardized and consistent structure suitable for analysis (Ong et al., 2011). The loading phase, the cleansed and transformed data are transferred from the staging area into the target repository (Ong et al., 2011). This process was done with the PowerBI Desktop as it can connect to different types of data sources and make the necessary transformations of the data, so that they are loaded correctly.

ETL process began by exporting all operational data from the SAP BusinessObjects GUIA universe into Excel workbooks, which were then loaded into Power BI Desktop to construct a dimensional data model. Four key files formed the core dataset:

a) **Dashboard Identity**: Contains user-level identifiers (e.g., UserID, NIF), profile creation and modification timestamps, and direct access assignments. This file underpins analyses of individual access changes over time.
b) **Basic Information** Provides demographic and organizational details—such as name, department, and employment status—serving as the primary lookup for user attributes.
c) **Profile Aggregator**: Lists each role or profile alongside its linked applications and aggregators, enabling profile-based permission mapping and role-based access analyses.

d) **Dashboard commercial hierarchy**: Captures the commercial hierarchy, including channels, sub-channels, and directorates, which allows reporting on access patterns across business units.

Once data is imported into Power BI, it often requires restructuring before it can be used effectively in reports. Power Query Editor addresses this need by providing a suite of transformation tools that let users clean and shape their data. Common operations include changing column data types, removing empty rows, renaming columns or tables, and designating the first row as headers. Crucially, Power Query Editor records every action in a transformation log, allowing users to review and modify each step of the ETL process. This process begins by importing and cleaning the raw spreadsheets, then progressively merging them to build a single, unified dataset that supports the dashboard's analytical needs. Initially, user attributes are combined with profile information, after which organizational hierarchy data is joined and enriched to reflect both formal and non-formal structures. A duplicate of this consolidated dataset is then maintained—without automatic refresh—to serve as a "previous version" baseline, enabling comparison over time.

To improve the performance of the Power BI dashboard, several columns were deleted. This included personal information, such as employees' NIFs, which were deemed irrelevant for the dashboard's purpose. Additionally, columns that registered individual permissions were removed. This is because, according to the GUIA manual for the NOS IAM system, permissions are not granted individually but as part of an aggregator. An aggregator groups multiple permissions or access rights into a single assignable unit, simplifying access management. Therefore, deleting individual permission columns does not result in information loss but significantly reduces the database's complexity.

Another way performance was improved was by utilizing tables that extracted only the necessary information to calculate specific indicators. For example, to generate the creation of new users overtime chart, a new table in PowerBI was created containing only the user's creation date, user identification and organizational structure, thus optimizing the data used for that visualization.

5.5. KPI used in the dashboard

Following data preparation, the next phase involves creating measures to represent the KPI within the Power BI report visuals. A critical aspect of this stage was the strategic selection of indicators that would be useful in the analysis of the access management at NOS. This selection process was informed by initial interviews with quality team, aided by the information about the existing dashboards and the indicators that they use. Furthermore, a review of indicators used in existing literature about existing IAM dashboards and their suitability for this specific context was conducted.

KPI are quantifiable measures used to assess the performance of individuals, teams, departments, or entire organizations in goals, playing a central role on the development of dashboard (Nunes et al., 2024). As highlighted during the interviews, the objective was for the indicator in the BI solution to provide a holistic overview of the access management status within the CTE division access management, therefore, not only will flag specific deviations but also contribute to a general awareness and continuous monitoring of access management health.

To effectively generate the necessary indicators for the dashboard, Power BI Desktop offers a crucial tool: DAX . DAX functions as a comprehensive language, comprising a diverse set of functions, operators, and constants. These are combined within formulas or expressions to compute and return either single values or entire sets of values. Beyond their primary use in defining report measures, these DAX formulas are also integral to crafting calculated columns, calculated tables, and implementing sophisticated row-level security (see Figure 4). The application of DAX throughout the report enabled complex data combinations and precise filtering of the data model, thereby enhancing analytical capabilities.

Figure 4- Example of the use of DAX

```
Numero_Identidades_Suspensas =
CALCULATE(
    DISTINCTCOUNT('Dados Totais'[User GUIA]),
    'Dados Totais'[Estado da Identidade] IN {"Suspenso", "Suspenso por Prova de Vida"},
    ALLSELECTED('Dados Totais')
)
```

Source: Power BI Desktop

The selection of critical KPI is a foundational step in implementing a BI solution. According to Eckerson (2009), these indicators must be simple, to ensure user comprehension, and actionable, to demonstrate how behavior and decisions influence outcomes. An indicator must be well-documented. Its precise definition, the source of the

data, and the context should be transparent and easily accessible to all users. They also be aligned, meaning they support rather than conflict with one another. Proper alignment prevents situations where contradictory efforts exist (Eckerson ,2009).

Due to the limitations with the information available there are access indicators that are impossible to implement in this IAM reporting system. Access request is an indicator that reports the number of approvals, denials, and escalations over time, that users experience when requesting digital resources (Peterson, 2006). While it can be a useful indicator for the new IAM dashboard, it has already been implemented within NOS in the access monitoring dashboard and the quality team does not have use for this metric (E2 ,E3, E4).

Policy violations measure the frequency of unauthorized login attempts or excessive use of digital resources (Puchta et al., 2019). This is another IAM indicator that, while relevant, is already implemented by both the monitoring dashboard and the access circularization dashboard, as policy violation is the responsibility of the Audit, Risk, and Compliance department (E4, E5). The data extracted from SAP BO also does not have the information necessary for the dashboard to include KPI like policy violation or access request, as the platform GUIA only has information on the personal data, organizational structure, and permissions granted to users in the CTE division.

The objective for the reporting system will be the use of indicators that can flag overprovisioned accounts, where users have more permission than necessary for their roles, and so are not following the principle of least privilege (Kim et al., 2011). The use of an KPI that can help the identification of role or attribute drifting, as they occur when a user's permissions extend beyond their original role, often because of role changes or temporary assignments (Puchta et al., 2019; Schell et al., 2009).

Table 4- List of indicators

Category	Indicator
General Overview	Total Users
	Average Accesses per User
	Average Applications per User
	Total Suspended Users
	Total Users in Provisioning Context
Alert: Duplicate Accesses	Number of users with duplicate accesses
	Proportion of users with duplicate accesses
	Total number of duplicate accesses
	Proportion of duplicate access compared to total existing accesses
Alert: Distinct Profiles	Number of Distinct Profile
	Proportion Profiles in Alert
Alert: Identity Accesses to Remove	Number of Identity Accesses to Remove
	Proportion of Identity Accesses to Remove
Alert: Identity Accesses to transfer to Profile	Number of Identity Accesses to Transfer to Profile
	Proportion Identity Accesses to Transfer to Profile
Alert: Distinct Assigned Applications	Total Number of Applications in Alert
	Proportion of Applications in Alert
	Total Number of Users with Alert
	Proportion of Users with Alert

Source: Own Work

The principal indicator in the general view is the Total Users. Total users quantify the aggregate number of individuals with a registered account in the system, serving as the baseline figure for further analysis. To provide deeper insight into user permissions, this is complemented by the Average Accesses per User, a metric representing the average quantity of access aggregators assigned to each user. The Average Applications per User indicator calculates the average number of distinct applications allocated to an individual, encompassing both Identity-based and Profile-based access types. Both indicators are important metrics for access management. The ideal scenario is the lowest amount of aggregators attribute to each user to prevent errors; they are also useful metrics to compare between teams or roles.

The dashboard includes metrics on user status. The Total Suspended Users metric enumerates the number of individuals who currently lack active system access, a state which can be attributed either to a planned administrative suspension or a failure to complete a required liveness validation protocol. Total Users in Provisioning Context metric quantifies the number of user accounts that are still in the initial provisioning phase and have not yet been formally associated with a commercial entity or business unit within the system. Collectively, these indicators offer a simple way to determine the important user status in the IAM system.

The KPIs for duplicate assess are the number of users with duplicate accesses, so the number of individual users have redundant or overlapping access permissions, by having the same aggregator assign to both identity and profile. Another is the proportion of users with duplicate access in relation to total number of users. It helps to understand the prevalence of the issue across your entire system. Total number of duplicate accesses moves beyond individual users; this indicator measures the volume of redundant access permissions. Since one user might have multiple duplicate accesses, this number can be significantly higher than the number of affected users, highlighting the overall scale of the problem. Lastly, is proportion of duplicate access compared to total existing accesses, expresses the total duplicate accesses as a percentage of all granted accesses.

The KPIs for the application alert category are the total number of applications in Alert, it quantifies every instance where a user has access to an application that's rarely used by their direct peers. Proportion of Applications with Alert shows what percentage of all applications assigned across the organization fall into this "alert" category. Total Number of Users with Alerts shifts the focus to the individuals. This counts every user who holds access to at least

one application deemed "in alert," meaning it's not common to more than 30% of their colleagues in the same team and function. The last KPI is the proportion of Users with Alerts. These alerts can help by distinguishing between broadly used, essential tools and niche applications that might only be needed by a few. By highlighting low commonality, these KPIs push you to evaluate if access is truly needed or just an oversight and help determine if there are applications that are rarely used or excessively assigned in certain contexts, pointing to potential inefficiencies or security risks.

Profiles are fixed sets of aggregators assigned to users with the same organizational role. However, according to both the interview with the Head of Quality Management and the GUIA manual, two users with the same function at NOS can have different profiles. This is because each profile is also linked to the company responsible for managing the user, which is relevant given that many NOS sales collaborators are external contractors.

The Total Number of Profiles with Alert indicator counts profiles possessing at least one access aggregator flagged as an "alert." An access aggregator is in alert if it's found in 20% or fewer of its peers. This helps identify the overall number of user profiles exhibiting these unusual access patterns. The Proportion of Profiles with Alert is simply the percentage of all profiles that have at least one access in alert.

The objective of the Alert: Identity Accesses to transfer to Profile is to identify common access privileges that, due to their widespread nature within specific groups or teams, might be better managed through standardized profiles, rather than assigned individually. The indicators are number of Accesses to transfer to Profile counts the total instances of access where these are aggregators shared by 80% or more of users within the same function and team. The proportion of access to transfer to profile: this indicator presents the percentage of all assigned access aggregators that are common within a role and team.

The objective of the Alert: Identity Accesses - Evaluate for Removal is to identify individual access privileges that deviate from the standard patterns observed within a user's peer group (those with the same function and team), indicating potential inconsistencies or unnecessary assignments and reducing security risks. The KPI total number of accesses in Alert counts the total instances of access where these are aggregators shared by 20% or less of users within the same function and team. Proportion of accesses in alert: This indicator presents the percentage of all assigned access aggregators that are uncommon within a given role and team,

5.6. Building the dashboard

The final step after the integration of the data and the creation of the relevant indicators is the creation of the dashboard. As the last phase of the BI implementation framework is the designing templates and analytics features that present information to users through dashboards. (Kimball & Ross, 2013). The objective of a dashboard is to enable the user to access and visualize the information in a quick and easy manner. Having the correct KPIs is one of the ways that this objective could be achieved as they are a critical part of any BI system (Nunes et al., 2024).

This dashboard is going to often use the drill-down functionality. This function allows users access to more detailed insights behind KPI across different areas of the organization (Ranjan, 2009). As one main purpose of this dashboard is to compare the access given to different roles and teams the filters and drill-down functionality as essential. The design and colors of the dashboard are also an important part as the construction of any dashboard, have to consider appropriate visual formats, layouts, and user interfaces to have better information clarity and a more usable tool (Yermaloich, 2020).

The BI system incorporates a permission system designed to control which users can view specific information within the report. This system is built upon Power BI's Row-Level Security (RLS) feature. RLS allows dynamically filtering the data that a user sees based on their identity and predefined roles, ensuring that users only have access to the information they are authorized to view. RLS is implemented by defining specific roles within the Power BI data model and applying filters to individual tables that contain sensitive information. Permissions are applied granularly to relevant information tables, ensuring that the security rules are enforced at the data level.

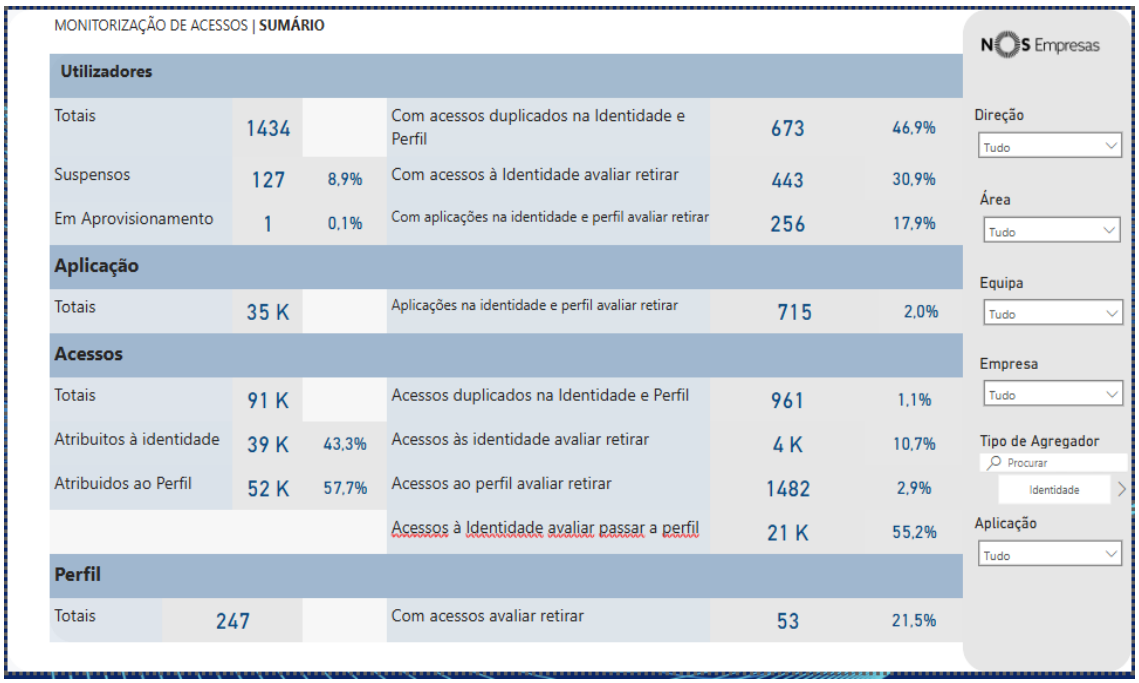
The configuration and management of these security measures are performed within Power BI Desktop through the "Manage Roles" interface. After the security rules, including the permissions table and DAX functions, are configured in Power BI Desktop, the report is published to the Power BI Service. In the online service, these RLS rules are activated and managed by assigning specific users or Microsoft Entra ID (formerly Azure Active Directory) groups to the roles defined in Power BI Desktop. This final step in the Power BI Service ensures that the configured permissions are enforced when users access the published dashboard.

The dashboard is organized into several distinct pages, each serving a specific purpose in presenting information and highlighting potential issues related to user access. The first section of the report is the glossary; this section serves as a fundamental reference point for users of the dashboard. It defines the basic concepts and terminology used throughout the report. The next part of the dashboard is the summary of the information presented in this report; this page provides a high-level overview of the report's key information and metrics. Its main objective is to offer the necessary context for interpreting the various alerts presented in the dashboard.

5.6.1. Summary page

As shown by figure 5, summary page of the dashboard provides a high-level overview of key access metrics, it displays total counts for critical entities such as the number of users, total attributed accesses, profiles, applications assigned to profiles, and accesses granted directly via identity. Additionally, it highlights the number of suspended users and those currently in the provisioning process. Beyond these baseline indicators, the page also summarizes key alerts that help identify potential access governance issues. These include the number and proportion of duplicate access, users with overlapping permissions, and the presence of distinct applications—defined as applications not commonly shared among users with similar functions or within the same area. It also tracks profiles that contain uncommon permissions.

Figure 5- Summary

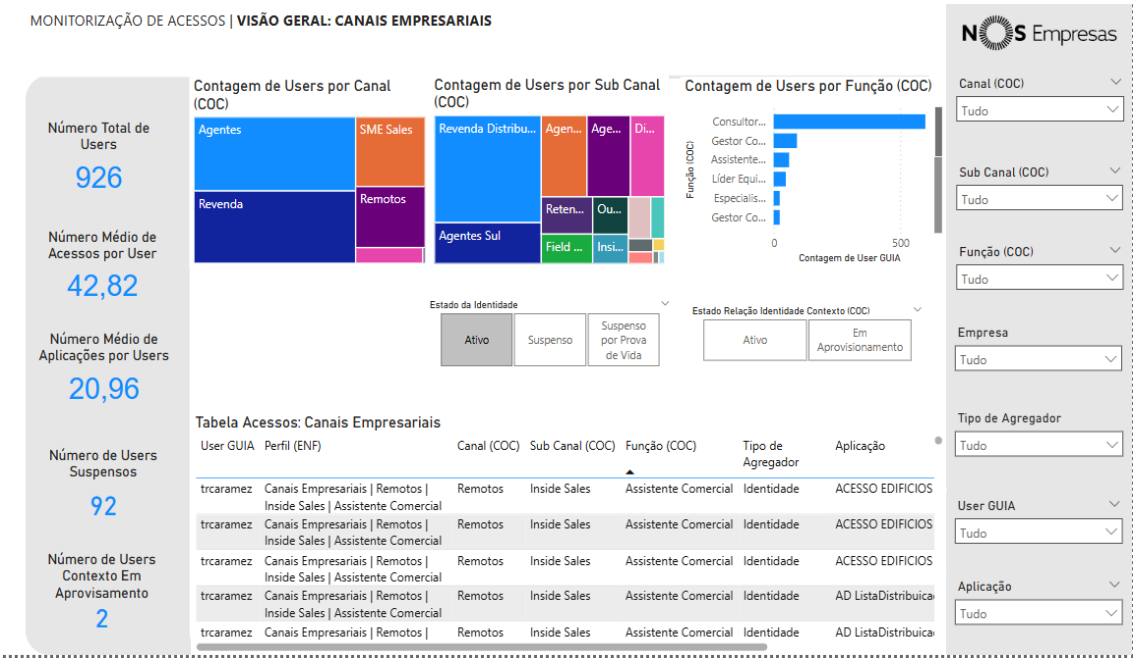


Source: Power BI Desktop

5.6.2. General view

The General View was designed to provide a more intuitive and visual presentation of user access and permissions compared to raw data tables (see Figure 6) It aims to offer a clear and accessible source of information. General View is divided into multiple pages, each focusing on a specific organizational channel or structure, with different pages for the Center of enterprise transformation, direct sales, and enterprise channels.

Figure 6- General View

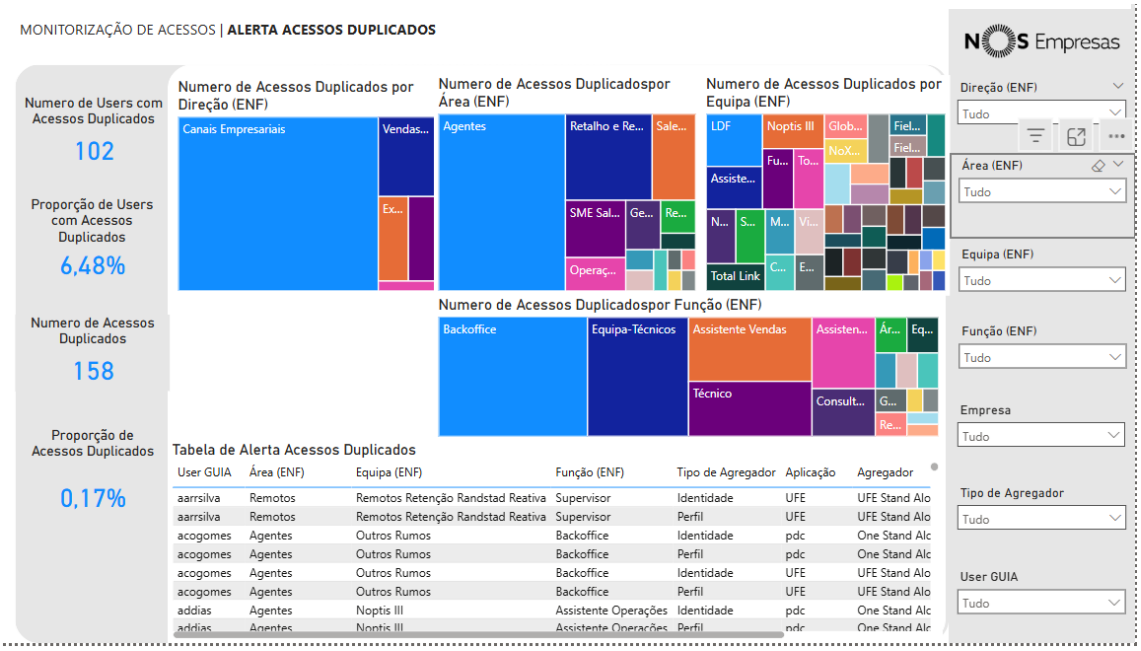


Source: Power BI Desktop

5.6.3. Duplicate Accesses alert

The Duplicate Access Alert page serves to identify instances where a user possesses the same access aggregator simultaneously through both their profile and their individual identity. (see Figure 7). This often signals redundant access or misconfigurations in permission assignments, posing potential security and efficiency concerns. The page's organization facilitates clear analysis. Visual filters and segmentation, primarily using treemaps and slicers, allow users to navigate data based on the non-formal organizational structure (Direction, Area, Team, Function) and company. These visuals dynamically display the number of users affected by duplicate access within each organizational unit.

Figure 7- Duplicate Accesses Page

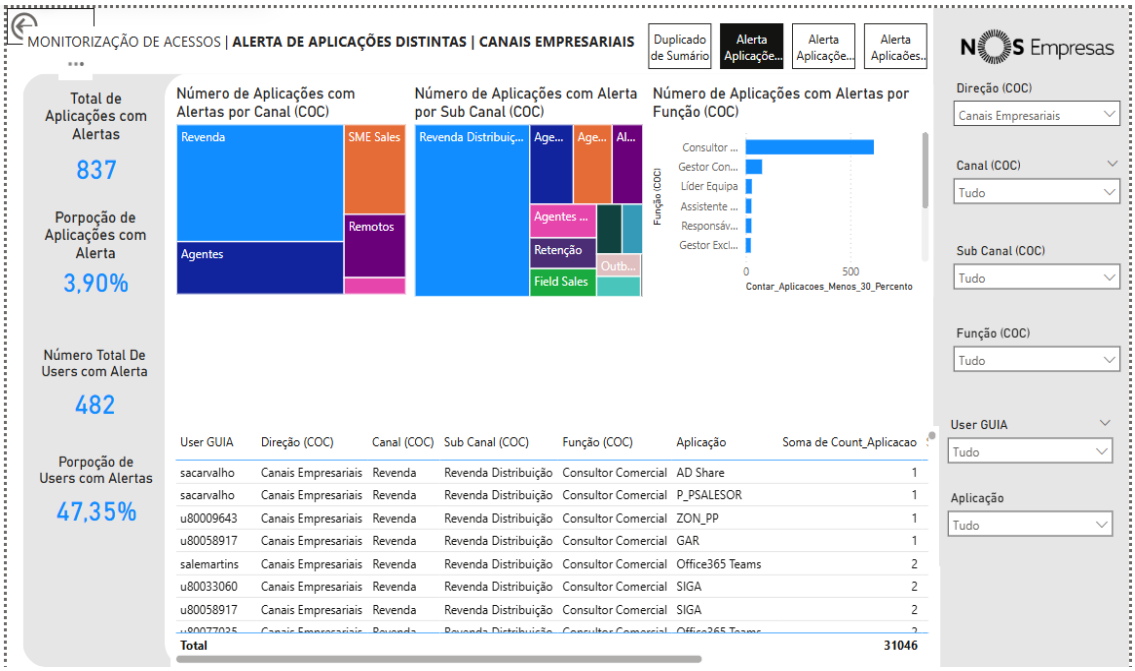


Source: Power BI Desktop

5.6.4. Alert distinct applications

The objective of this page is to identify applications that are accessed by a low percentage of users within the same function and team. This suggests these applications might be candidates for review or removal, as they are not commonly used by peers in similar roles (see Figure 8). The page incorporates Visual Filters/Segmentation through treemaps and slicers, allowing for data exploration based on both commercial and non-formal organizational hierarchies, as well as specific applications and User IDs. The treemaps represent the number of applications with alerts within each organizational unit, providing a quick summary of areas with potential over-provisioning. The information table details instances where users have access to applications with low adoption rates among their peers.

Figure 8- **Alert distinct applications page**

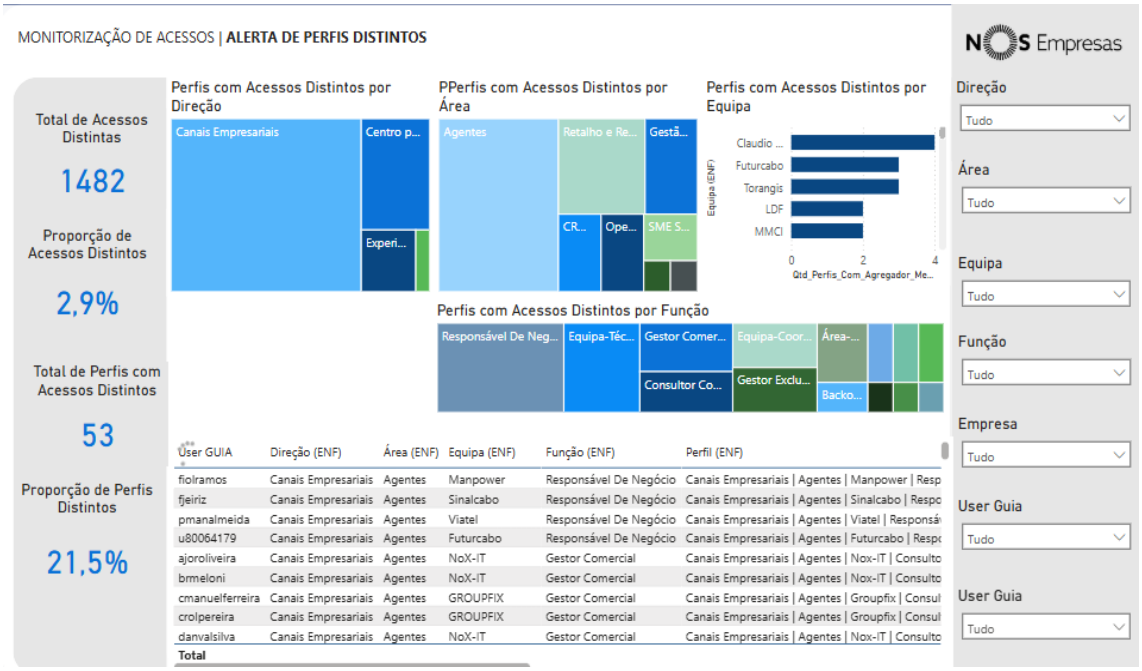


Source: Power BI Desktop

5.6.5. Distinct Profiles Alert

The objective of this page is to identify profiles with aggregators that deviate from the standard pattern for profiles sharing the same function and area (see Figure 9). These deviations signal uncommon access configurations, highlighting inconsistencies, especially relevant for external contractors where profiles might vary by outsourcing agency. Visual Filters/Segmentation utilize treemaps and slicers based on the non-formal hierarchy, applications, and User IDs. The Information Table details profiles with uncommon accesses. filtered to display only those below a defined threshold (e.g., less than 20%). This pinpoints profiles needing review.

Figure 9-Alert distinct profiles page

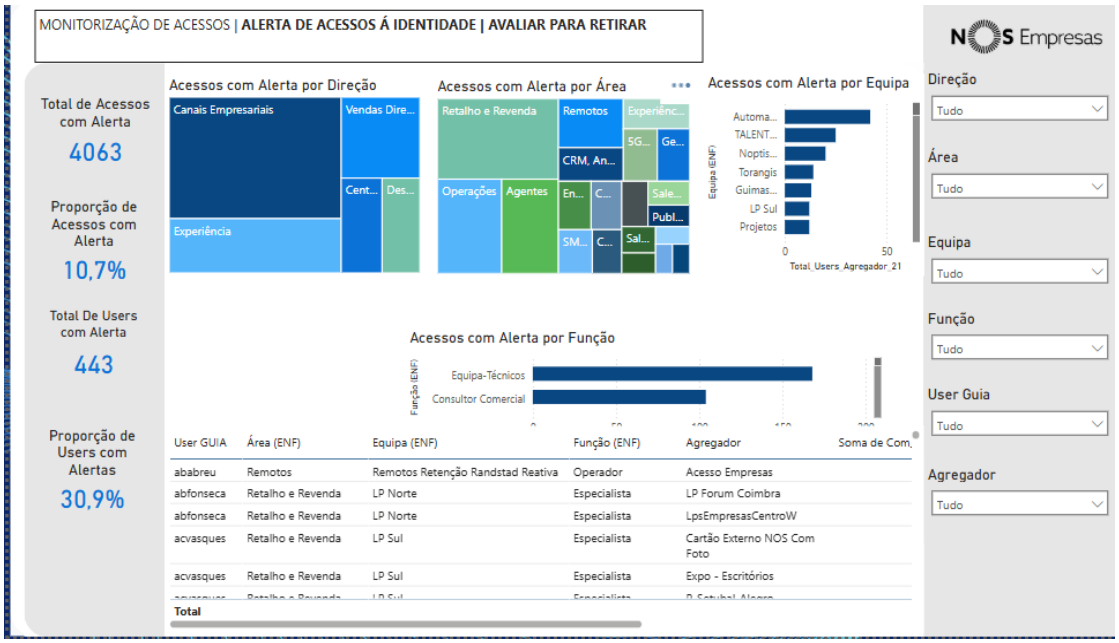


Source: Power BI Desktop

5.6.6. Identity accesses to evaluate removal Alert

The objective of this page is to identify individual identity accesses that are uncommon among users with the same function and team (see Figure 10). Visual Filters/Segmentation leverage treemaps and slicers based on the non-formal hierarchy, aggregators, and User IDs. Treemaps display the count of accesses with alerts within each organizational unit. Page-level filters are applied to specifically include only 'Identity' type aggregator. An Information Table lists instances of users with uncommon identity access within their function and team. The table is further filtered to display only rows where the percentage of users with the aggregator is below a defined threshold (e.g., less than 20%), pinpointing specific cases for review.

Figure 10-Identity Accesses to Evaluate Removal Alert page

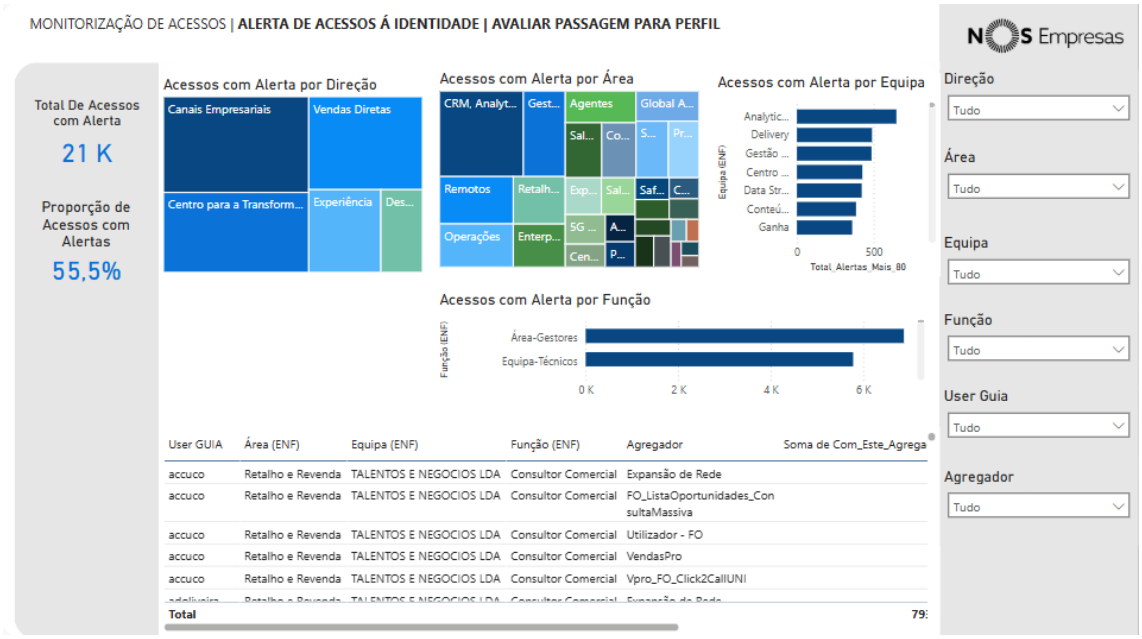


Source: Power BI Desktop

5.6.6. Identity Accesses to Transfer to Profile Alert

The objective of this page is to identify accesses that are commonly shared among a majority of users within the same function and team (see Figure 11). Visual Filters/Segmentation are provided through treemaps and slicers, enabling navigation by non-formal hierarchy, aggregators, and User IDs. The treemaps represent the number of accesses flagged for potential transfer within each organizational unit. An Information Table details instances where identity access is common among users in the same function and team. This table includes key attributes such as "User GUIA," full organizational hierarchy details, "Application," and "Aggregator." It also features calculated columns that show the count of users with that specific aggregator in each context, the total number of users in that context, and the percentage of users sharing that aggregator.

Figure 11-Identity Accesses to Transfer to Profile page



Source: Power BI Desktop

6. Conclusion

This study aimed to explore how BI tools could address key challenges in Identity and IAM at NOS. The focus was on implementing an IAM reporting system that would improve visibility, monitoring, and governance of access permissions across a large and diverse workforce. This objective led to the development of a Power BI dashboard, designed to improve the quality team's ability to control and monitor the organization's access management systems.

The research was guided by three main objectives:

1) to develop an IAM reporting system that can provide insights into access management and security practices.
2) to design and implement dashboards that improve data exploration and support better decision-making processes.
3) and finally, to analyze data and identify opportunities for improvement and resolve existing issues within the access control systems.

To answer these objectives, a single-case study approach was used. The research combined document analysis, semi-structured interviews, direct observation, and technical implementation. Interviews with stakeholders across operations, quality, risk & compliance, and IT audit departments provided the business context, while documentation and user manuals informed the technical framework. The dataset was extracted from SAP BO and included user information from the NOS's GUIA IAM system. The dashboard's primary purpose was to visualize and assess identity and access configurations within the Business CTE, which includes over 1,400 internal and external collaborators. The solution successfully integrated data from various organizational units—internal employees, contractors, and outsourcing partners—allowing the Quality team to evaluate users' access rights in real time.

The reporting system provided better visibility into NOS's access control landscape. Through indicators such as total users, average access per user, suspended users, and users in provisioning context, the dashboard quantified key aspects of identity management. It also highlighted inconsistencies, such as duplicate access and unusually assigned permissions, revealing that NOS's IAM systems and practices are prone to errors. The information obtained highlighted the disadvantages of the IAM control model used by NOS.

For the second research objective, prior to this project, the quality team had limited access to existing dashboards and often relied on Excel files to perform access reviews. With the introduction of the new reporting model, which includes drill-down features, dynamic filters, and tailored KPIs, the quality team can now more easily review entire teams' permissions and share information with relevant department managers. The addition of detailed visual alerts that automatically highlight situations requiring further investigation not only supports autonomous decision-making within the quality team but also enables faster and more targeted investigations by teams whose primary responsibilities extend beyond access management and the use of the IAM system GUIA

Regarding the last research objective, data analysis revealed critical opportunities for operational improvement. Duplicate permissions that are caused by permissions being simultaneously assigned through profiles and identity, were prevalent across multiple user segments. In some cases, these duplicates exceeded 7% of total assigned permissions. Moreover, the system identified profiles with unusual aggregators, applications granted to users without clear justification, and due to the frequent change in responsibility and roles that users can have, especially if they are contractors, a lot of cases of old permission that the user did not need anymore. These findings can help on the to streamline role definitions and find the best balance between permission assign individuals and permissions assign to the profile.

This research reinforces the potential of reporting systems as operational tools for IAM governance. While IAM frameworks such as RBAC and ABAC are well-established, this study contributes by demonstrating how dashboards can make these models actionable and measurable in a large, real-world organization. Indicators such as duplicate permissions, uncommon aggregators, and profile inconsistencies provided tangible insights into policy compliance and deviations from expected behavior. The study also aligns with literature advocating for proactive access monitoring (Devlekar & Ramteke, 2021). It illustrates how BI tools can move IAM processes beyond manual audits and static reports toward dynamic, continuous monitoring that enhances transparency and control. This approach adds a practical dimension to academic discussions about the role of data visualization and analytics in risk management and compliance (Puchta et al., 2019).

The most immediate practical contribution was the delivery of a tailored Power BI dashboard for NOS's quality team, designed to analyze identity-based and profile-based permissions across more than 1,400 users in the CTE division. The solution improved access

visibility helped detect redundant and inconsistent permissions and empowered the team to independently assess risks and share findings with other departments. By addressing gaps in existing tools (such as the inability to compare users within the same function or detect overprovisioning) the dashboard supported NOS in aligning its access control practices with internal security standards and external frameworks like ISO/IEC 27001 (Mirtsch, 2023). It also laid the foundation for developing more standardized access profiles and review routines, contributing to long-term governance improvements.

This project also demonstrated the broader organizational value of BI in access management and supported NOS's digital transformation strategy. It serves as a model that can be scaled across other departments or adapted to different IAM challenges.

While the reporting system offered valuable insights, the scope was limited to the CTE division. It did not include access data from other business areas or cover permissions outside of SAP BO exports. The data was also not updated in real-time, relying instead on manual refreshes, which limited the system's responsiveness to immediate risks. Additionally, the dashboard focused on structural access data—who has what—rather than behavioral data—how accesses are used. As a result, it could not detect inappropriate usage or potential policy violations threats that go beyond configuration errors. Finally, the internship duration did not allow for a full audit cycle post-implementation, so long-term impact on decision-making, risk reduction, or policy enforcement could not be measured.

Future work should focus on real-time integration with live systems would improve the solution's effectiveness in identifying emerging risks and automating alerts. Further development could also incorporate behavioral analytics, such as frequency of application usage or unusual access patterns, enabling risk-based prioritization of user reviews. These enhancements would elevate the dashboard from a compliance support tool to a strategic asset in security operations. Finally, future research could examine how dashboard usage influences organizational behavior and culture around IAM. Understanding how visual tools affect accountability and cross-department collaboration may provide further insights.

References

Anawar, S., Othman, N., Selamat, S. R., Ayop, Z., Harum, N., & Abdul Rahim, F. (2022). Security and privacy challenges of big data adoption: A qualitative study in telecommunication industry. *International Journal of Interactive Mobile Technologies (iJIM), 16*(19), 81–97. https://doi.org/10.3991/ijim.v16i19.32093

Anderson, B., & Mutch, J. (2011). *Preventing good people from doing bad things: Implementing least privilege*. Apress.

Becker, L. T., & Gould, E. M. (2019). Microsoft Power BI: Extending Excel to Manipulate, Analyze, and Visualize Diverse Data. *Serials Review, 45*(3), 184–188. https://doi.org/10.1080/00987913.2019.1644891

Brickley, J., & Thakur, K. (2022). Policy of least privilege and segregation of duties, their deployment, application, & effectiveness. 10.112-119.

British Standards Institution. (2023). *Expert commentary for BS ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements*.

Büdel, V., Fritsch, A., & Oberweis, A. (2020). Integrating sustainability into day-to-day business. *Proceedings of the 7th International Conference on ICT for Sustainability*, 56–65. https://doi.org/10.1145/3401335.3401665

Bukhbinder, G., Krumenaker, M., & Phillips, A. (2005). Insurance Industry Decision Support: Data Marts, OLAP, and Predictive Analytics. In *Casualty Actuarial Society Forum* (pp. 171–197).

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Damon, F., & Coetzee, M. (2013). Towards a generic Identity and Access Assurance model by component analysis - A conceptual review. https://doi.org/10.1109/ES.2013.6690086

Damon, F., & Coetzee, M. (2018). The design of an identity and access management assurance dashboard model. *12th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS)*, LNCS, 123–133. https://doi.org/10.1007/978-3-319-99040-8_10

Devlekar, S., & Ramteke, V. (2021). Identity and access management: High-level conceptual framework. *Revista Gestão Inovação E Tecnologias, 11*(4), 4885–4897. https://doi.org/10.47059/revistageintec.v11i4.2511

Eckerson, W. W. (2009). Performance management strategies. *Business Intelligence Journal, 14*(1), 24–27.

Eckerson, W. W. (2010). *Performance dashboards: Measuring, monitoring, and managing your business*. John Wiley.

Feng, N., Chen, Y., Feng, H., Li, D., & Li, M. (2020). To outsource or not: The impact of information leakage risk on IS strategy. *Information & Management, 57*(6), 103215. https://doi.org/10.1016/j.im.2019.103215

Ferraiolo, D. F., Kuhn, D. R., & Sandhu, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC), 4*(3), 224–274. https://doi.org/10.1145/501978.501980

Hu, V. C., Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2013). *Guide to attribute-based access control (ABAC): Definition and considerations*. NIST Special Publication 800-162. https://doi.org/10.6028/NIST.SP.800-162

Hummer, M., Groll, S., Kunz, M., Fuchs, L., & Pernul, G. (2018). Measuring Identity and Access Management Performance - An Expert Survey on Possible Performance Indicators. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0006557702330240

Janes, A., Sillitti, A., & Succi, G. (2013). Effective dashboard design. *Cutter IT Journal, 26*, 17–24.

Kalloniatis, C., Mouratidis, H., & Islam, S. (2010). An identity and access management approach for SOA. *Information Management & Computer Security, 18*(5), 310–322. https://doi.org/10.1108/09685221011095262

Kamariotou, M., & Kitsios, F. (2023). Information systems strategy and security policy: A conceptual framework. *Electronics, 12*(2), 382. https://doi.org/10.3390/electronics12020382

Khther, R. A., & Othman, M. (2013). Cobit framework as a guideline of effective IT governance in higher education: A review. *International Journal of Information Technology Convergence and Services, 3*(1), 21–29. https://doi.org/10.5121/ijitcs.2013.3102

Kim, S., Kim, D.-K., Lu, L., & Park, S. (2011). A feature-based approach for modeling role-based access control systems. *Journal of Systems and Software, 84*(11), 2035–2052. https://doi.org/10.1016/j.jss.2011.03.084

Kimball, R., & Ross, M. (2013). *The data warehouse toolkit: The definitive guide to dimensional modeling* (3rd ed.). John Wiley & Sons.

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37

Lanus, E., Colbourn, C. J., & Ahn, G. J. (2024). Guaranteeing anonymity in attribute-based authorization. *Journal of Information Security and Applications, 87*, Article 103895. https://doi.org/10.1016/j.jisa.2024.103895

Martucci, L. A., Zuccato, A., Smeets, B., Habib, S. M., Johansson, T., & Shahmehri, N. (2012). Privacy, Security and Trust in Cloud Computing: The Perspective of the Telecommunication Industry. *2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing*. https://doi.org/10.1109/uic-atc.2012.166

Manente, M., Minghetti, V., Mingotto, E., & Casarin, F. (2014). Consumer Confidence in Responsible Tourism. *Advances in Marketing, Customer Relationship Management, and E-Services Book Series*, 264–285. https://doi.org/10.4018/978-1-4666-5880-6.ch013

Malaka, I., & Brown, I. (2015). Challenges to the organisational adoption of big data analytics. *Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists - SAICSIT '15*. https://doi.org/10.1145/2815782.2815793

Merchan-Lima, J., et al. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. *Annals of Telecommunications, 76*(4), 255–270. https://doi.org/10.1007/s12243-020-00783-2

Microsoft Corporation. (2024). *What is Power BI?* Retrieved July 5, 2025, from https://learn.microsoft.com/power-bi/fundamentals/power-bi-overview

Mirtsch, M. (2023). Adoption of the information security management system standard ISO/IEC 27001: A study among German organizations. *International Journal for Quality Research, 17*(3), 747–768. https://doi.org/10.24874/ijqr17.03-08

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & Security, 109*, Article 102383. https://doi.org/10.1016/j.cose.2021.102383

Nunes, F., Alexandre, E., & Gaspar, P. D. (2024). Implementing Key Performance Indicators and Designing Dashboard Solutions in an Automotive Components Company: A Case Study. *Administrative Sciences, 14*(8), 175. https://doi.org/10.3390/admsci14080175

M. Olszak, C., & Ziemba, E. (2007). Approach to Building and Implementing Business Intelligence Systems. *Interdisciplinary Journal of Information, Knowledge, and Management*, *2*, 135–148. https://doi.org/10.28945/105

Ong, I., Siew, P., & Wong, S. (2011). A Five-Layered Business Intelligence Architecture. *Communications of the IBIMA*, *2011*(695619), 1–11. https://doi.org/10.5171/2011.695619

Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security, 3*(2), 85–106. https://doi.org/10.1145/354876.354878

Penelova, M. (2021). Access control models. *Cybernetics and Information Technologies, 21*(4), 77–104. https://doi.org/10.2478/cait-2021-0044

Puchta, A., Böhm, F., & Pernul, G. (2019). Contributing to current challenges in identity and access management with visual analytics. *IFIP DBSec 2019, LNCS 11559*, 221–239. https://doi.org/10.1007/978-3-030-22479-0_12

Putra, A. P., & Soewito, B. (2023). Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector. *International Journal of Advanced Computer Science and Applications, 14*(4). https://doi.org/10.14569/ijacsa.2023.0140468

Ranjan, J. (2009). Business intelligence: Concepts, components, techniques and benefits. *Journal of Theoretical and Applied Information Technology, 9*(1), 60–70.

Robson, C., & McCartan, K. (2016). *Real world research : A resource for users of social research methods in applied settings* (4th ed.). Wiley.

Fritsch, L. (2020). Identity management as a target in cyberwar. In H. Roßnagel, C. Schunck, S. Mödersheim, & D. Hühnlein (Eds.), *Open Identity Summit 2020* (pp. 61–70). Gesellschaft für Informatik e.V. (*Lecture Notes in Informatics*). https://doi.org/10.18420/ois2020_05

Schell, F., Dinger, J., & Hartenstein, H. (2009). Performance Evaluation of Identity and Access Management Systems in Federated Environments. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 90–107. https://doi.org/10.1007/978-3-642-10485-5_7

Silverman, D. (2011). *Interpreting qualitative data*. SAGE.

Singh, A. P., Kuzminykh, I., & Ghita, B. (2024). Industry Perception of Security Challenges with Identity Access Management Solutions. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2408.10634

Solak, S., & Zhuo, Y. (2020). Optimal policies for information sharing in information system security. *European Journal of Operational Research, 284*(3), 934–950. https://doi.org/10.1016/j.ejor.2019.12.016

van Wessel, R., Yang, X., & de Vries, H. J. (2011). Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study. *Technology Analysis & Strategic Management*, *23*(8), 865–879. https://doi.org/10.1080/09537325.2011.604155

Wahyudi, I., & Widyasari, Y. D. L. (2022, October 1). Improving company performance by the correctness of management decision through implementation dashboard using Power BI tools (Case study at company Y). *IEEE Xplore*. https://doi.org/10.1109/ICET56879.2022.9990634

Wixom, B., & Watson, H. (2010). The BI-Based Organization. *International Journal of Business Intelligence Research*, *1*(1), 13–28. https://doi.org/10.4018/jbir.2010071702

Cheng, Y. W., & Bilal, A. (2024, March 30). *Regulatory data privacy concerns in proliferating IoT era of telecommunication data monetization: A systematic literature review*. TechRxiv. https://doi.org/10.36227/techrxiv.171177247.79933157/v1

Yermalovich, P. (2020). Dashboard Visualization Techniques in Information Security. IEEE. https://doi.org/10.1109/ISNCC49221.2020.9297291

Yigitbasioglu, O. M., & Velcu, O. (2012). A review of dashboards in performance management: Implications for design and research. *International Journal of Accounting Information Systems, 13*(1), 41–59. https://doi.org/10.1016/j.accinf.2011.08.002

Zulkifli Abai, N. H., Yahaya, J., Deraman, A., Hamdan, A. R., Mansor, Z., & Yah Jusoh, Y. (2019). Integrating Business Intelligence and Analytics in Managing Public Sector Performance: An Empirical Study. *International Journal on Advanced Science, Engineering and Information Technology*, *9*(1), 172. https://doi.org/10.18517/ijaseit.9.1.6694

FACULDADE DE **ECONOMIA**