International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Leveraging SAP HANA Views for Data Governance: Authorization Check Approach in Enterprise Analytics for Data Compliance

Sriramaraju Sagi

NetApp

Abstract: ***This research focuses on exploring ways to enhance data compliance in organizations by implementing authorization checks using SAP Analytics Cloud and SAP HANA views. When companies face the challenge of sharing global analytics reports with employees while meeting authorization requirements, we devised a method that combines business distribution lists with SAP HANA views, for authorization validation. Our study resulted in a process that produces distribution lists containing recipients for regional data access. The efficacy of our approach was thoroughly tested across regions demonstrating the ability to maintain compliance with data access regulations. These findings highlight the advantages of utilizing analytics tools and database technologies to establish data governance and compliance frameworks within firms. This research contributes by presenting a legally compliant framework for distributing sensitive analytics reports ensuring secure data access in accordance with organizational and regional authorization norms. It underscores the importance of data management strategies in addressing data privacy and compliance challenges in today's age.***

Keywords: Enterprise Analytics, Data Compliance, SAP HANA Views, Authorization Checks, Data Governance

1.Introduction

In the paced world of business operations, enterprise analytics and data compliance play a crucial role. As companies increasingly rely on data for decision making, efficiency improvements and fostering innovation safeguarding information is vital for legal business practices.

The advent of analytics tools has ushered in an era of business intelligence, where data is not merely a byproduct but a valuable asset that shapes a company's strategic direction. However, utilizing data for decision making entails responsibilities related to compliance. These obligations stem from the growing number of regulations on data protection, such as the General Data Protection Regulation (GDPR) in the EU, the California Consumer Privacy Act (CCPA) and other region-specific laws. Compliance with these regulations necessitates protocols to ensure that personal and sensitive information is managed transparently lawfully and securely.

Moreover, managing data is an aspect that goes beyond mere legal obligations and involves building trust with consumers, employees and stakeholders. Organizations have a responsibility to create data governance frameworks that cover both administrative aspects of data security, privacy, and adherence, to regulations. This includes implementing cybersecurity measures, setting up data management protocols and providing regular training to staff to minimize the risk of data breaches and unauthorized access.

This research seeks to delve into the facets of ensuring enterprise analytics data compliance and protecting information within companies. Through a mix of real-world studies, analyses and case studies we aim to explore the trends, technologies and regulatory landscapes influencing data compliance practices.

In summary, in navigating the complexities of the age maintaining compliance with data regulations and safeguarding information are critical elements for organizational success. By embracing an approach, data governance organizations can meet their existing obligations while laying the groundwork for a future where data continues to drive innovation and societal progress.

2.Preventing Data Spillage in Corporate Environments

In today's era, where data plays a role, in shaping company strategies and operations it is essential to minimize data leaks to protect the confidentiality, privacy and security of valuable information. Data leaks involve the exposure of data leading to potential financial losses, damage to a company's reputation and legal issues. Within the field of enterprise analytics, where vast amounts of data are processed and analyzed, the risk of data breaches is heightened due to data environments and widespread data sharing among departments and external collaborators. To mitigate these risks effectively organizations, need a security strategy that encompasses solutions as well as organizational policies.

A key step is to prioritize implementing encryption measures for data protection. Encryption serves as a barrier ensuring that both stored and transmitted data remains incomprehensible to individuals. By employing encryption technologies along with key management practices companies can establish a solid foundation for securing confidential information.

Furthermore, it is important to have measures in place to control access and prevent data leaks. Concepts such as granting the amount of privilege necessary and using role based access control ensure that individuals only have access to the data they need for their tasks, reducing the chances of unauthorized access or accidental exposure. Adding factor authentication strengthens security by confirming the identities of users attempting to reach sensitive information. Conducting audits and monitoring data access and usage are

crucial for identifying weaknesses and adhering to data protection regulations. Employing automated tools and systems that detect anomalies can notify organizations about patterns of access or data transfers enabling responses to possible threats.

Maintaining data integrity within systems is vital for preserving the accuracy, consistency, and dependability of information throughout its lifecycle. Data integrity plays a role in decision making processes, operational efficiency, and compliance with industry standards. To uphold data integrity standards companies must establish policies for managing data that address both aspects and operational procedures.

One important strategy involves setting up systems to manage data quality effectively. These systems provide methods for entering, handling, and maintaining data to reduce errors and discrepancies. Conducting reviews of data quality helps identify and resolve issues ensuring that the data remains accurate and consistent over time. Another critical aspect is implementing backup and disaster recovery measures. These processes protect data from loss or corruption due to hardware failures, cyberattacks or natural disasters. By backing up data and testing recovery methods organizations can quickly restore information ensuring smooth operations. Prioritizing backup and disaster recovery as practices is crucial for maintaining Data Compliance standards.

3.Best Practices for Data Compliance in Corporate Settings

Ensuring compliance with data protection standards is a vital aspect of business governance. Companies need to navigate through the evolving landscape of local regulations to avoid legal penalties and build trust with customers and stakeholders. Developing strategies for data compliance necessitates a comprehensive approach to managing data.

The first step involves gaining an understanding of regulations like GDPR, CCPA and industry specific laws. Organizations must translate these requirements into policies and procedures that govern the collection, processing, storage and sharing of data.

Conducting data protection impact assessments (DPIAs) for projects or technologies involving data processing can help identify potential compliance issues in advance. DPIAs play a role in demonstrating an attitude towards privacy and adherence to regulatory standards.

Training programs and awareness campaigns are crucial in ensuring that employees grasp their roles in upholding data compliance. Regular training sessions coupled with communication of data protection policies help foster a culture of adherence and accountability, across the organization.

In essence successfully averting data leaks upholding data accuracy and adhering to data regulations, in business environments necessitates a strategy encompassing security protocols streamlined data handling practices and stringent adherence to compliance guidelines. By emphasizing these aspects companies can safeguard their data assets, maintain credibility, with stakeholders and navigate the complexities of the landscape with assurance.

4.Literature Review

Various studies have explored how enterprise architecture (EA) plays a role in ensuring data compliance within analytics. Burmeister (2019) and Kim (2007) both emphasize the importance of EA models that incorporate aspects of analytics, security and privacy. Kim specifically highlights the use of ontology-based models to simplify compliance assessments. The research identifies a gap in existing EA meta models regarding the management of data. Suggests a privacy centric EA meta model to align with GDPR requirements and enhance transparency in data handling. The research illustrates how ontology-based enterprise models provide structured representations, for compliance assessment reducing bias and catering to a range of enterprises.

Knuplesch (2010) and Delbaere (2007) in their research discuss the significance of integrating data compliance testing and creating a data structure throughout a company to simplify regulatory reporting responsibilities. In their study they outlined about how compliance checks should support enforcing compliance regulations that consider the processed data. And also the challenge of state explosion can be reduced by adopting an abstraction method, which can also enhance the efficiency of compliance check algorithms. They identified how businesses need to establish a data structure across their organization to centralize regulatory reporting duties and consolidate data from various business sectors. Implementing data modeling techniques and standards organization wide can aid in addressing compliance challenges. One of the Examples from the financial services industry demonstrate how implementing enterprise information management strategies utilizing industry models and technology can effectively tackle compliance requirements.

Hashmi (2012) and Schleicher (2011) delve into the significance of annotations and compliance domains, in expanding business processes and outlining data constraints within cloud environments. The research paper introduces a method to automatically extract annotations to data schema and templates associated with tasks in a business process to ensure compliance from the start. The proposed approach, based on queries is aimed at extracting data for control tags to annotate process models. The study highlighted in the paper focuses on achieving compliance through the extraction of data annotations from schema linked to tasks within a process. It also addresses the evolving compliance demands in business process design due to cloud computing stresses enterprise accountability for data when stored externally and offers guidance on aiding human process designers in crafting business processes.

These studies collectively emphasize the role of enterprise analytics models, data aware compliance verification and semantic annotations in upholding data compliance within enterprise analytics.

5.Results

We carried out a study to explore how global analytics reports are shared within a organization based on permissions. Our investigation yielded insights to showcase the effectiveness and adaptability of SAP Analytics Cloud as a reporting solution, in addressing the data governance and compliance requirements of diverse business sectors. By introducing an authorization verification mechanism using SAP HANA views we enhanced data access accuracy and security across the organization. Our approach primarily concentrated on merging business distribution lists containing recipient details with SAP HANA views for authorization verifications. This integration facilitated the creation of an updated distribution list comprising of individuals authorized to access regional data.

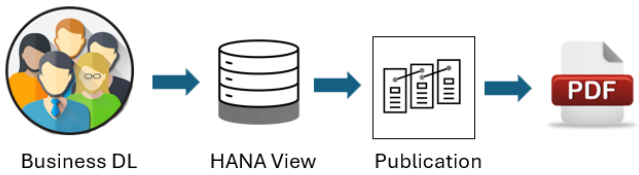

Figure 1: Current Process without Data Compliance

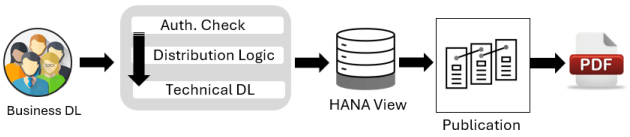

Figure 2: New Process with Auth check for Data Compliance

Upon deploying this methodology and leveraging it through SAP Analytics Cloud for report distribution, we conducted comprehensive testing across various regions. The testing phase was aimed at evaluating the effectiveness of our approach in segregating compliant from non-compliant users based on their authorization levels to access certain data segments.

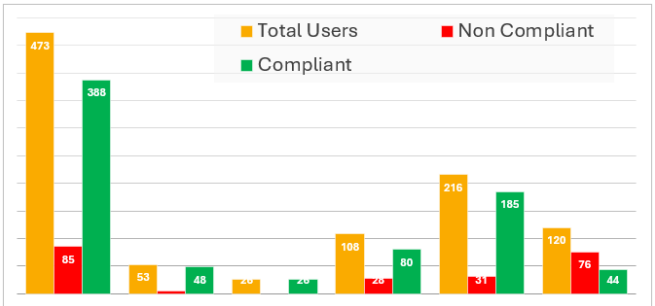

Figure 3: Compliance vs noncompliance users

The results were clearly positive, demonstrating the system's ability to accurately distribute analytics reports to employees based on their permissions. By linking SAP HANA views with business distribution lists the reports were shared with authorized recipients who had access rights. This was evident as there were no access incidents during testing. Testing in regions showed that the system effectively managed complex authorization structures. Each region verified receipt of analytics reports by properly authorized individuals. The graph from the test data clearly showed a distinction between non-compliant users. Compliant users received reports as per their permissions while non-compliant users, who did not meet authorization criteria were excluded by the system.

The success of this scenario underscores the potential of leveraging analytics tools, like SAP Analytics Cloud along with SAP HANAs robust data management features to establish detailed data governance and compliance frameworks in large organizations. This approach enhances data delivery security and accuracy while aligning with data privacy regulations and corporate governance standards.

The results of this research showcase a clear illustration of how companies can navigate the complexities of distributing and ensuring compliance with data across the globe. The proven approach offers a reliable and lawful structure for disseminating confidential analytical reports guaranteeing secure data access that aligns with both the business authorization standards and regional requirements.

6.Conclusion

Our study highlights the importance of using strategies for managing data and ensuring compliance in enterprise analytics. Through the utilization of SAP Analytics Cloud and SAP HANA views we. Successfully put into practice a new method for authorization checks that greatly improves the security and compliance of data sharing within a company. Our results demonstrate that this approach reduces the risks related to unauthorized access and data leaks but also aligns with strict global regulations on data protection. The effective implementation of this method in regions proves its efficiency providing a practical solution for businesses dealing with data compliance challenges in today's interconnected world. Future studies could explore how this method can be adapted to enterprise analytics platforms and databases evaluating its flexibility in various technological settings. Furthermore, examining the influence of data protection laws on this method could offer more insights into its sustainability and adaptability, over time.

References

[1] Burmeister, Fabian et al. "A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation." Hawaii International Conference on System Sciences (2019).
[2] Kim, Henry M. et al. "How To Build Enterprise Data Models To Achieve Compliance To Standards Or Regulatory Requirements (and share data)." J. Assoc. Inf. Syst. 8 (2007): 5.
[3] Knuplesch, David et al. "On Enabling Data-Aware Compliance Checking of Business Process Models." International Conference on Conceptual Modeling (2010).
[4] Delbaere, Marc and Rui Ferreira. "Addressing the data aspects of compliance with industry models." IBM Syst. J. 46 (2007): 319-334.
[5] Hashmi, Mustafa et al. "Business Process Data Compliance." International Web Rule Symposium (2012).
[6] Jugulum, Rajesh. "Importance of Data Quality for Analytics." (2016).

[7] Schleicher, Daniel et al. “Institute of Architecture of Application Systems Compliance Domains : A Means to Model Data-Restrictions in Cloud Environments Institute of Architecture of Application Systems , University of Stuttgart Germany.” (2011).
[8] Ramezani, Elham et al. “Compliance Checking of Data-Aware and Resource-Aware Compliance Requirements.” OTM Conferences (2014).