Attain Insight
Security 4X

Security Governance and Compliance for Business & IT

The challenge of governing information access for business

Business Analytics has the capability to yield a significant amount of highly valuable insights. The process of cleansing and formatting raw data ultimately leads to actionable datasets — each of these datasets can then produce game-changing business visualizations and insights. In short, analytics and Business Intelligence (BI) data are like diamonds: intrinsically valuable.

The core challenge for any organization, however, is not necessarily discovering relevant information; rather, how can it be safeguarded? Those “diamonds” are valuable because they offer unique data views that—in the wrong hands—could potentially compromise an organization’s integrity. The critical nature of key business data has given rise to a need for comprehensive security governance and compliance in terms of policy management.

Characteristics of effective security policies

The effective governance of BI-derived data requires the creation and implementation of comprehensive security policies that govern access to company information. Some key characteristics of effective security policies include:

- Understandable to both Business and IT user profiles;
- Accurately implemented and auditable so that risks can be quickly identified and their impact understood;
- Flexibility and adaptability of security policies when change occurs.

The last point is of particular note. Security policies must be flexible and malleable — there are always forces of change, such as new legislation and business reorganization. Given the reality of a non-static environment, security policy changes should not pose a risk to business continuity. Ideally, security policies must be flexible enough to change when needed, but without compromising the overall security needs of the organization.

Common types of security policies

There are a variety of security policies commonly implemented in BI settings, such as:

- **Finance:** Policies that govern policy & loss statements by location and business unit within an entity. Due to the varied security levels assigned to financial data, some measures may be available to one policy group but not another.

- **Sales:** Policies that govern access to sales pipeline forecasts across departments/divisions, particularly as time periods come to a close. Insiders can see what is closing this week or in the last month of a quarter, but product management may only see closed months. Other audiences may only see publicly announced information about previous quarters.

- **Human Resources:** Policies may govern access to employee data in order to remain compliant with privacy laws. Key measures, such as Headcount or Base Salary, are treated differently due to the variable nature of data confidentiality.




The challenge of implementing data and content security for IT

The Business side of the coin may be responsible for high-level strategic BI security initiatives, but it is the IT side that is responsible for their tactical implementation. Unfortunately, only a few key IT administrators in every large organization truly realize the significance of the challenge.

In a typical BI reporting application, it is not uncommon for access authorizations to require hundreds of thousands of manual steps — this is not only difficult to repeat, but is highly unreliable over both the short and long-term.

Policy implementation requires the creation of groups to limit access to content and data. In a large organization, the number of policy groups can number in the thousands. In order to ensure the integrity of data access, IT departments need to be able to design & implement centralized control over security policies.

Key IT personnel need to know when changes will be applied and be able to verify their application. After policy groups are created, users (aka “members”) are assigned to the groups based on access requirements.

The process of creating groups, aligning accessibility with business requirements, and managing group memberships requires an integrated and flexible authorization process. This process has to be streamlined and scalable as the organization’s security needs grow.

IT security administration challenges

Some key challenges in the management and implementation of security policies include:

- **Creating Policies:** The sheer volume of policy groups required in large-scale BI applications effectively negates their manual creation. The only answer is an automated solution that can adequately secure the BI environment while remaining responsive to authorization requirements.
- **Managing Memberships:** The scope of membership management in a large BI environment is typically beyond the capability of an IT department to manually handle. The number of variables involved are simply too numerous: changes in management, delegation hand-overs, role changes, and so on.
- **Changing Policies:** Over time policies change. In order to accommodate these changes, an efficient policy lifecycle process must be enacted. This would include designing policies in a development environment, quality controlling them in a test environment, and then deploying them into the production environment. This has to happen quickly, yet without error.
- **Limited Human Capital:** IT departments are typically pulled in many different directions... from employee onboarding to network management, both time & resources are typically in short supply. Given this, IT departments usually have very few people responsible for security administration. Manually managing fin e-grained security on content and data is neither cost-effective nor reliable.

The solution?

Attain Insight Security 4X, the centralized security administration and compliance reporting solution that handles the most sophisticated enterprise security polices across the full suite of IBM Analytics products Learn more at www.security4x.com or contact us for a demonstration at +1 (613)-235-0200 or info@attaininsight.com.

Attain Insight

IBM Gold Business Partner