

Security Governance and Compliance for IBM Cognos Business Intelligence Software

Business Issues - The Challenge of Governing Information Access

Successful governance of business intelligence related data requires that the business needs comprehensive policies to govern information access. It is critical that the policies that govern such access must be understandable, both to the business and IT. They must be accurately implemented and auditable, so that any risks can be identified and their impact and likelihood understood. Even good policies change from time to time. There may be new legislation, or the business may need to reorganize itself for increased flexibility or efficiency. Such changes impact the design of information access security policies. Barriers to quickly changing policies cannot be allowed to hold up the business' evolution.

It is critical that the policies that govern such access must be understandable, both to the business and IT. They must be accurately implemented and auditable, so that any risks can be identified and their impact and likelihood understood. Even good policies change periodically. There may be new legislation, or the business may need to reorganize itself for increased flexibility or efficiency. Such changes impact the design of information access security policies. Barriers to quickly changing policies cannot be allowed to hold up the business' evolution. Typical policy examples include:

- **Finance.** Policies that govern access to P/Ls by location and business unit within an entity. Because certain information is more confidential than other information therefore certain financial measures might be available to one audience, but not to another.
- **Sales.** Policies for segregating sales pipeline forecasts across departments/divisions from a consolidated company plan. The policy would govern access to revenue information, especially during period end close. Insiders can see what is closing this week, in the last month of the quarter, but product management can only see closed months, and everyone else can only see publicly announced information about previous quarters.
- **Human Resources.** Policies that insuring HR information is only visible to first line managers, and then only some of it. Individual personal information must be secured according to privacy laws. Key measures like Headcount or Base Salary are treated differently because certain data is more confidential than other.

Implementing these policies quickly moves from being a high level business issue to a hands-on technology challenge. Authorizing access in a typical business intelligent reporting application can easily require hundreds of thousands of manual steps to implement. Such information access challenges are shared by all enterprise class products, including IBM Cognos software.

IT Issues - The Challenge of Implementing Data and Content Security

It is critical that the policies that govern such access must be understandable, both to the business and IT. They must be accurately implemented and auditable, so that any risks can be identified and their impact and likelihood understood. Authorizing access to information quickly moves from being a high level business issue to a hands-on technology challenge. Surprisingly, only a few key IT administrators in every large organization really understand how significant the challenge is.

IT needs an integrated and flexible authorization process to access information; however, the business doesn't understand how complex and expensive this is. Authorizing access in a typical BI reporting application can easily require hundreds of thousands of manual steps to implement. Manual processes are not reliable, or repeatable in any timeframe – short or long term.

Implementing “policies” requires that IT create groups to limit access to content and data – these are known as “policy groups.” There can easily be thousands of “policy groups” within a typical business intelligent application. IT needs to be able to design and implement centralized control of the policies to ensure integrity of information access. It needs to know when the changes will be applied and to be able to verify that the changes have been successfully applied. Once that policy groups are created, users are assigned to these groups as “members.”

IT's challenges are as follows:

- **Creating Policies.** Without automation, IT cannot possibly create the policy groups necessary to adequately secure BI applications. The number of steps involved to create and manage policies is staggering and cannot be completed by manual means.
- **Managing Memberships.** IT cannot realistically keep track of memberships in an organization. Which manager took over from which other manager and must now assume their responsibility. Who is on vacation for 2 weeks and must temporarily delegate their information access for that period and then reliably revoke it. These changes are only known by the business
- **Changing Policies.** Because policies change over time, IT needs to be able to design or change policies in the development environment, quality assure them in a test environment and then deploy them into production. Testing, quality assurance, and promotion to production has to happen quickly and reliably. A failure here could lead to unauthorized access (e.g. Kmart seeing Walmart's data) which can be a costly mistake.
- **Limited Human Capital.** A further challenge is that typically an IT organization has very few people responsible for the complex task of security administration. Managing fine-grained security on content and data manually object by object is not cost effective, neither is it very reliable.

The Solution

FirstQuarter Security Studio™, the IBM Cognos specific security policy director that designs sophisticated policies and automates the design, testing and implementation across all IBM Cognos Software.