Business & Decision | expert opinion

BUSINESS INTELLIGENCE | CUSTOMER INTELLIGENCE | E-BUSINESS | MANAGEMENT CONSULTING

Information system security: identity and role management through regulatory compliance

*by **Jérôme Chagnoux and Jean-Luc Rizk***
IT Agency, Business & Decision Group

The most suitable method to increase the global level of security requires identity and access management for each user. *This is also one of the evolution axes upon which companies are subject to regarding rule and regulation compliancy:* ***Sarbanes-Oxley, Basel II, LSF...***

Today, the information system is at the core of every company's economic activity. Applications are numerous and diverse and they are a solution to constant productivity and innovation constraints. As time goes, information system security has become indispensable, and is even beyond network and telecommunications security challenges.

Identity management solutions

"Who's who", "who does what", "who gets access to what", "who gave access rights to who and for what purpose"… Before understanding what is happening inside the information system, some simple questions, that are sometimes forgotten, need to be answered.

Even though applications are accessible to all actors across every business (employees, suppliers, clients, services providers), identity management is the solution to a company's complex and growing organization.

The solution executed is dependent on an architecture based on the three following elements:

- **The basic building bloc is a repository** that stores all components of the digital identity and parameters helping to locate an employee in the organization, such as phone numbers, job title, department, office, geographic location…
- **Synchronization solutions** complete this infrastructure in order to guarantee an intelligent and industrialized data update closely related to events like HR system entries, transfers, phone allocations…
- After, an **authorization management infrastructure** is setup, which aims to build a tool capable of structuring the information system's security around an authorization model close to the company's organization. As an essential part of an identity management infrastructure, it depends on the identity life cycle in order to ensure the "provisioning" of user repositories through the information system's applications.

Setting up this type of infrastructure provides the following advantages:

- **Management of access and authorization rights** (to a computer resource) for a given user, that are generally related to his role in the organization (business role);
- **Management of the modifications impacted on the responsibility scope** in the application, through a detailed follow-up of the allocated authorizations (*"who has the right to delegate what", "who delegated what to who"*);
- **Tracking the movement of users**: authorization revocation during employee departure or transfer, most commonly called user "deprovisioning";
- **Improve of the level of service** provided to users.

Therefore, the information system is equipped with a common repository that guarantees the identity quality, traceability and *auditability*.

Attaining regulatory compliance

The recent financial scandals (Enron, Andersen, Worldcom or Parmalat) have revealed a lack of control in large organizations. Both national and international regulations have been created in order to guarantee control. Whether it's *Sarbanes-Oxley*, *Basel II* or *LSF*, everything is now organized by the legislator to ensure total transparency of the company's financial activity, as well as the responsibilities carried out by the directors. Internal and external audits have become a necessary key to success.

Traceability and *auditability* make great sense in this highly regulated context. Beyond an in-depth documentation of every company's business processes, it is necessary to be able to identify in an organization which individuals have tried to access sensitive and non-authorized data. Furthermore, it is important to understand why these access attempts are in violation of the current governance policy and regulatory constraints.

Without a detailed view of the activity and performance of every individual, the company risks a fraudulent use of its information system (diversion of sensitive information, destruction of documents…) that might lead to substantial financial losses or the interruption of its economic activity.

Therefore, companies need to monitor their information system activity in order to identify and investigate all accidental or deliberate violations of enforced rules, with an overall objective of complying with regulations.

The access and authorization management infrastructures provide essential elements needed to achieve conformity. By ensuring the integrity of the user repository and access control (provisioning and deprovisioning of accounts), increased global security is facilitated.

By adopting a business authorization model, implementing responsibility partitioning rules becomes possible in the information system.

It then becomes possible to participate in an audit, by supplying, for example, formatted reports for the use of auditors…

Company organization at the core of IAM

The approach carried out, even though it is complex, most often clashes with constraints related to the company's organization: it is a matter of implicating each and every actor of the system into security, by describing authorization management generic processes and business responsibilities.

The methodology for establishing such a management authorization infrastructure, as well as all the related elements of business responsibilities, requires a pragmatic iterative approach that aims to continually improve the system's quality.

The above model is known as *"Deming's Wheel"* or the PDCA model (Plan Do Check Act). After defining the overall objectives, action is taken. Afterwards, the quality of the results is checked and new objectives are fixed in order to maintain efficiency.

Above all, an identity management project is business oriented and associated with the company's organization. Its success is also closely linked to every actor's will and motivation inside the company. If the project is carried out wisely with all managers implicated in regulatory compliance, it then becomes the key to company governance success.

Contacts IT Agency, Business & Decision Group

Jean-Luc Rizk – *Agency Director*
jean-luc.rizk@businessdecision.com

Jérôme Chagnoux – *IAM Business Developer*
jerome.chagnoux@businessdecision.com

Phone: +33 0(1) 56 21 21 21
Fax : +33 0(1) 56 21 21 22

About Business & Decision

Founded in 1992, Business & Decision is an international engineering and consulting firm specializing in Business Intelligence, Customer Relationship Management (CRM) and E-Business. The Group works with clients to facilitate system implementation to assist business performance management (dashboards, reporting, consolidation etc.); customer relationship management (sales force automation, call centers, campaign management, analytical CRM); and E-Business (intranet and extranet portals, directories and Meta directories, e-commerce, knowledge management, Open source technologies...).

Business & Decision has been listed on the Euronext Paris since 6 February 2001 (compartment C / Isin code: FR 00000 7895 8 / Symbol: BND). Business & Decision is also listed in the NextEconomy segment as well as the IT-Cac (technology market).

With more than 1,800 employees (in Europe and North America), Business & Decision has developed a 'complete project approach' that ranges from consultation to implementation. The Group has a reputation for its functional and technological expertise and has forged partnerships with the key technology vendors. Today Business & Decision has more than 1,200 clients.

For more information visit: www.businessdecision.com & www.businessdecision.fr

Press contact:

Isabelle Serra
Communications manager
Business & Decision
Tel: +33 (0)1 56 21 21 25
Fax: +33 (0)1 56 21 21 22
E-mail : isabelle.serra@businessdecision.com