GITS SECURITY ENTITLEMENTS

SECURITY ENTITLEMENTS

In an ideal world, management of security concerns would be predicated on providing Security Policy Definition and Security Administration for the corporation (see following page). Unfortunately, it is not an ideal world. Some firms are not even aware of the actual security policy that has been implemented. The logic associated with the security policy is often buried within software application code**. Semantic mismatches and Metadata issues may frequently occur, especially when a Common Business Lexicon does not exist.** Moreover, there is rarely a requirement for software application code to be rigorously documented. Hence, the following must occur to resolve these issues:

a) The board members associated with data governance must define the security policies.

b) Application code must be reverse-engineered and documented to truly understand what policies are already in place.

c) Any gaps existing between a) and b) must be documented and addressed.

d) A **Common Business Lexicon** must be developed to articulate the rules and procedures associated with complying with the edicts provided by the governance board.

The GITS Methodology ensures that common references and lexicons are applied to data items that should be protected and managed properly during enterprise's software application execution phase.

GITS provides intuitive methods to define and manage the Security Entitlement strategy in a comprehensive and cost-effective fashion.

SECURITY POLICY DEFINITION

This phase of the security lifecycle addresses a corporation's definition of the rules associated with grants, encryption requirements, authentication procedures, and temporal policies (i.e., archiving policies, temporary suspension of access rights (e.g., no updates of core data during month end closing, etc.) and other enterprise driven decisions.

The policy definition phase is used to define the explicit security entitlement rules that should be applied to the data assets owned by a particular enterprise. The typical types of rules include:

- Role based security
- Security entitlements as applied to the fields of data owned by an enterprise, and data contained therein.
- Location-driven rules
- Temporal considerations

SECURITY ADMINISTRATION

This phase of the security lifecycle is driven by the actual topology associated with an enterprise's landscape. The options for topology are as follows:

- ***Centralized***
    - Central Security Tsar (CST) Business Unit (BU) defines and manages security entitlement rules for the entire enterprise
    - CST has the option has the option to deploy Regional Security Administrator BUs to manage the DBMS, Network ('Implied' Hub-and-Spoke model), and Application Security Entitlement Rules
- ***Distributed***
    - Each Regional geographical location has complete autonomy of the establishment of Security Entitlements
    - A Core Corporate Security BU still exists, but it is passive – it only receives security entitlement rules, and notifies management when rules are defined that are contrary to corporate policy
- ***Federated***

- Based on melding Centralized and Distributed (Explicit Hub-and-Spoke model); Cross Regional hand-shakes must occur

SECURITY ENTITLEMENT ENFORCEMENT

Enforcement of the security policies can often be performed by commercial off the shelf (COTS) products or custom development. This phase, while not trivial, is perhaps the easiest phase associated with implementing the security policy. Technical expertise pertaining to architecture and enacting security policies is a commodity.

The GITS Methodology has provided assistance in identifying and managing the above. The 'Business Language' is used to ensure that the roles associated with an enterprise's corporate structure, the Administrative Topology, and the relevant business rules are depicted accurately.