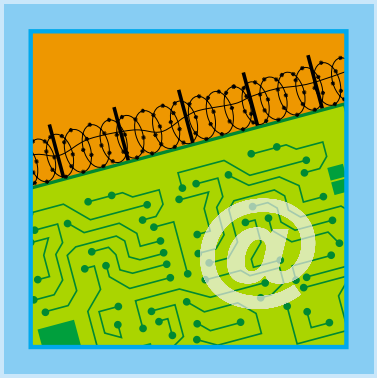
Information (Security)
A Reference Model



Demands on information security are increasing due to complexities from regulatory change, such as the *Privacy Act,* and added requirements to share more information broadly and quickly, as brought on by recent threats to public safety. Organizations and information providers are faced with escalating demands to exchange information, sometimes across jurisdictions or to groups for whom the information was not originally intended. As the Editor of this magazine pointed out in a previous issue, the challenge facing the intelligence community (and others) is one of improving timely information sharing – how do we ensure pertinent and secure information will flow to where it is required (whether that is to an oil rig, a refinery or pipelines, transit systems, or to local border guards and government agencies)? In this context how can we be confident that we recognize which information is true and pertinent and which needs to be secured?

Managers are looking for adaptive business planning and the right mix of governance to accommodate these drivers; Information Security Specialists are looking for a means to add value to these processes, not shackle them; and Transformation Architects are looking for 'the enablers' that address the significant issues and allow the business to achieve its objectives without negative outcomes. Each wants to engage the Information Security issue earlier, and in order to do so it requires a business vocabulary that is common and recognizable to all.

As governments and private organizations begin to transform into more responsive client-focused service entities, they discover which outputs add value to their internal processes and to their external delivery of services. This information assists in the development of strategic reference models that categorize specific aspects related to their clientele (as an extreme example, you may recognize that a prisoner is now a "client" of the correctional facility, though it is difficult to change providers if the client is unsatisfied).

To remain relevant, organizations must provide the information, services and products that are demanded by modern clients. Therefore, information systems must be able to adjust automatically to changes within the business model or security policies. This leads to the need and obligation for organizations to exchange information under differing conditions – assessing and handling the information according to the business /security contexts rather than simply at the document level. But how do we identify and implement these seemingly disparate security criteria when accessing and sharing data?

Analysis of these expectations are often presented in the form of value statements, performance measures, processes and information movement as items that make up the service or value chains.

Reference models, also known as conceptual models, help structure this landscape and provide the basis for a common business language across the organization. They guide the dialogue that relates these interest items with the objectives of any one part of the business. They provide organizations with a means to better understand what information, services or products are of real value to their stakeholders.

The creation of reference models that accommodate evolving business contexts or semantics can help identify what information is at risk or even what information is pertinent. (Semantics being the use of a word, in terms of sense and reference as opposed to the nature of the word itself.)

Recently, while working with the Chief Information Officer Branch at the Treasury Board Secretariat, I was asked to define a concept called the Information Reference Model (IRM). This was seen as an integral part of the Governments of Canada Strategic Reference Model (GSRM) being promoted throughout various federal and provincial jurisdictions.

It was understood that the use of a reference model provides a simplified view of complex areas such as: capital assets, target groups, value statements, service levels and analysis results. Such a standardized presentation assists the interested citizen, business-person, government colleague or even curious researcher to understand policies and find authoritative references from which to obtain services or information.

The design of the IRM addressed the need of analysts to capture authoritative information about items of "shared interest in the Government of Canada." The model had to define associations between different items of mutual interest and place these in an operational or situational context(s). Such contextual adjustments can either be based on the current business interactions or on newly discovered interactions, providing the basis of the required formative security model.

By using reference models, an organization provides a common business language that can be adopted across the whole of the enterprise – where the business objectives align with stakeholders' interests and enables the security specialist to be involved at the outset.

Not having a commonly agreed reference model often leads to trade delays,

failure to communicate, increased operational risk, and losses of tactical advantage due to insufficient or incorrect information exposure. Inconsistency of meaning or understanding between information providers and receivers complicates matters and aggravates information security risks. In addition, satisfying information sharing obligations without clearly defined protocol can lead to ineffective security policies that may not provide the right information when needed or could expose more information than necessary – this can make stakeholders skeptical of its reliability and effectiveness.

Information Security practitioners would do well to investigate the reference models being constructed in their organizations, since modeling is the basis for transforming the management of information. Service and value chains that result from transformation projects can provide organizations with clear definitions of who produces what, when, and where it goes. Reference models as well as value chains can benefit from having information security concepts and services added.

Semantic-based security models would allow for the evaluation of information within a business or situational context, such as: who requested it; for what purpose; under what authority; and in conjunction with what other information? This type of service support would allow information security specialists to examine the multiple level security problems in a new light – based on the data value and its context.

As an Information Security practitioner, I find it worrisome that there is limited discussion on how to place the information into measurable contexts, how to better assess the information value and pertinence, or how to establish its threat-risk level.

There is a real need to identify specific contexts that place discreet information into composite forms that distinguish one situational context from another when evaluating the risk level, and then determine the appropriate level of security.

Attempts to resolve this quandary by means of document tagging sometimes results in too much information being exchanged or held back. Using a discreet record-level tagging approach can determine the appropriate security level for information in more, but not all, contexts.

Information must be defined first by employing concepts like inferential-role semantics in order to understand the situation correctly. In the case of the reference models being promoted at the provincial and federal government levels, the identification of the fundamental components does provide the basis from which an effective information security model can be oriented towards protection, sensitivity and security.

A reference model augmented by security measures and criteria can define the constraints under which controls can be implemented across the enterprise. It allows an enterprise to produce security policies that define which information can be accessed or released, and that provide a rational modern basis to deploy and apply access controls across the application portfolio rather than being driven by them.

Engaging in transformation efforts early, with an eye to information security and applying the various reference model elements, allows security specialists to set proper security measures around legitimate and expected business transactions or information exchange. Further, it allows the evaluation of risk, thereby setting conditions under which information can or cannot be shared. This inherent flexibility is critical to future successes of new legislation, regulations and the evolving demands for physical and information level security at any jurisdictional level.

One key to success is an iterative approach, one which focuses on targeted projects of quantifiable business value that are relatively easy to implement. Business transformation involves improving a service-oriented architecture and is therefore far more than an overnight project. Embracing business transformation initiatives will improve understanding of the information and its flow, and by extension – its security.

These concepts, when combined with adaptable reference models, provide the foundation for value-based and context-oriented information security models.

An Information Security Model within the overall business transformation process will enable the organization to respond more effectively to a changing world. Similarly, reference models incorporating security precepts will help structure the transformation strategies and lead to solutions that result in the necessary amount of information being exchanged securely, thus ensuring that the client is best served.

Those of us who are either directly involved in re-structuring the business or who provide the security policies and the mechanisms to protect information across the enterprise must operate from a commonly agreed or controlled business "semantics." Effectively establishing this vocabulary will only be achieved when information security is a recognized factor in the transformation process and reflected in the resulting context models. Perhaps then the border guard will get the information he or she needs in time to stop the next Ressam (aka "the millennium bomber") without compromising other security needs. S

Kevin MacLean is the Director of Business Analytics at Macklin Information Resources (www.macklinir.com). He has collaborated on NATO/SHAPE interoperability efforts, contributed to the Multilateral Interoperability Programme for both Canada and the United Kingdom, and has been involved in the development semantic-based security models. He can be reached at kmaclean@macklinir.com

Evaluating the Information Security Reference Model Process

	Internal Factors	External Factors
Positive Factors	**Strengths** – overcomes "Info Silos" – presents a common vocabulary for Executive, Managers, IT/IM and IS – models information distribution by context as well as content – unified imposition of security constraints across application base.	**Opportunities** – brings IS into business planning – aligns terminology between IS and business managers – allows for value and context-based information release – identification of pertinent information by context
Negative Factors	**Weaknesses** – difficult to understand how to implement change or transformation – organization has to accept change – introduces new design and application requirements	**Threats** – resistance to cost of change – inconsistent executive support – weak application suite implementation of security controls or policy base governance