SECURITY, INTEGRATION AND DATA MANAGEMENT : WHY ALIGNMENT IS CRITICAL…

Written by:
Andrew Swindell

orbus software

INTRODUCTION

Information is the life-blood of modern digital organisations with government agencies and major corporate's now the custodians of a large and ever increasing amount of personal information, payments data and other sensitive information. Organizations need to adopt new and more holistic patterns to effectively secure, integrate and manage their information assets.

The rationale for adopting more effective patterns is due to a number of issues including:

- We manage billions of records and transactions
- There are now many ways to access our information and move large amounts of it around, instantly
- Protecting our customers and customer-facing services increasingly depends on protecting our information and digital assets
- In addition to insiders with a personal agenda, our information is also attractive to organized criminals, nation-state actors and others

It is critical to understand the data and risks involved (Security Management), how important key data is to the business (Data Management) and which system components rely upon which data and who needs access to the information (Integration Management). The opportunity exists to align your Data, Security and Integration Management functions to ensure that all new projects are scoped to protect your information assets during the design and build phase and that management disciplines are in place to actively secure, integrate and manage your data assets.

If your organization is making security, data and integration decisions in isolation then you are exposing a range of risks, compliance and duplicated costs over your portfolio and creating potentially more spaghetti and complexity across your architecture. In this white paper, I will explore the reasons why an integrated approach is required across these three key disciplines and how they can work together to effectively manage your technology and data assets.

Firstly, I will explore each discipline and the key constructs and through this will identify numerous alignment opportunities and the rationale for each. There is a logical order for presenting these three disciplines as follows:

- Data Management provides visibility of what data (structured and unstructured) is important and who owns it across the organization and how the data ecosystem is architected
- Integration Management identifies how data is moved around the organization
- Security Management provides the discipline for managing the security of that data across the ecosystem

For the purposes of this paper, I will use the generic term "Data or Information Management" to reflect both structured data and unstructured data such as Records and Documents.

DATA MANAGEMENT

It is important to have an inventory of Information assets to guide your Architecture Reference points and support the data conversations across your enterprise.

Information asset descriptions incorporate a range of inputs including Information about the business e.g. Business Owner, Information about technical infrastructure, systems and applications and the Information Assets Input and Output.

An Information Management Framework and Enterprise Information Model are also critical tools to support stakeholder discussions and engagement. Maturing these artefacts is a critical first step in driving uplift in approach to IM disciplines.

A well designed Information Management Framework will signpost key information capabilities and inputs required to effectively manage information as an asset across your organization. The DAMA Framework provides a good working model of what IM capabilities should be addressed and below is an example of an Information Management Framework that simplifies the conversations and creates focus and uplift opportunities.

DATA MANAGEMENT (CONT...)

Definition of the key layers enables a story to be created around Information Management at your organization and brings stakeholders together to strategize, plan, understand challenges and deploy inputs that contribute to the broader organizational information agenda.

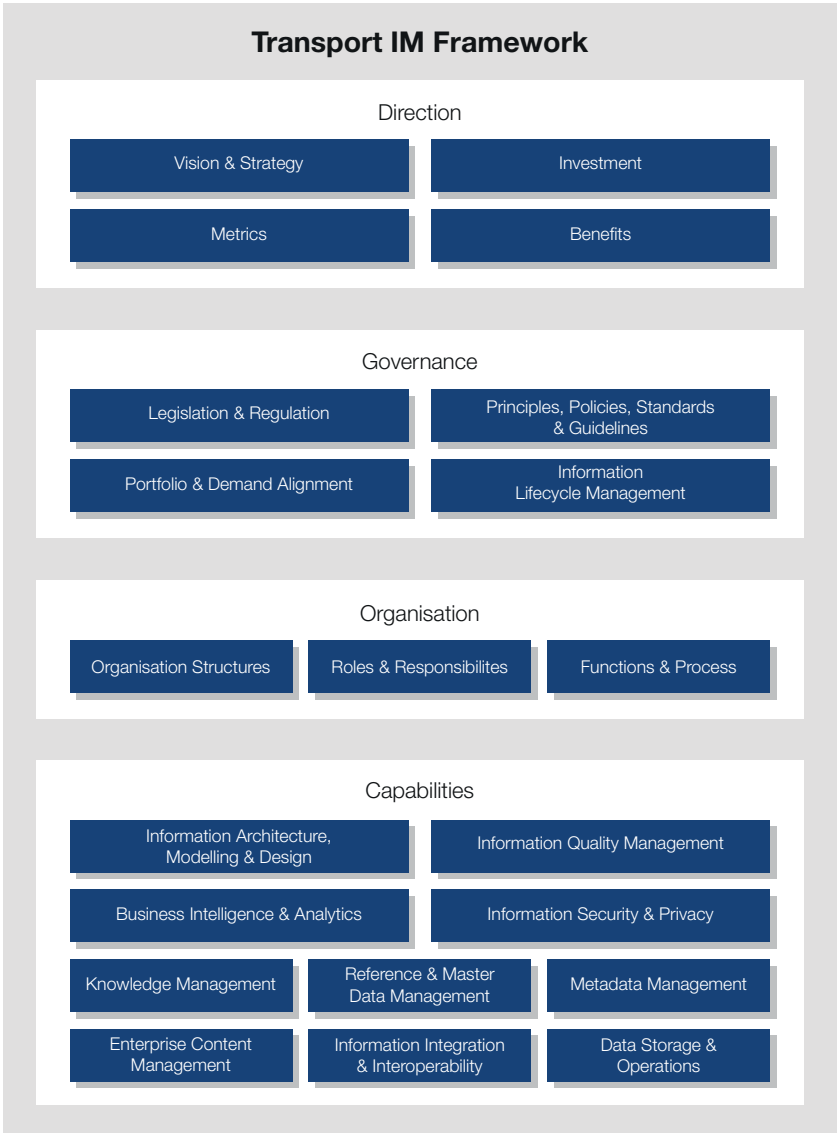
Definitions for each layer is as follows:

- **Direction** - Strategy and direction of key IM priorities established through executive leadership, with input and agreement from all stakeholders. Unified, organizational-wide understanding of the importance of shared information, the parameters within which it can be shared and the business benefits which are derived as a result.

- **Governance** - The development and monitoring of principles, processes, policies, standards and technologies to drive the effective and efficient use of data for achieving business objectives. Authority and control must rest with the corporate executive with clear lines of delegation and responsibility down to the operational level.

- **Organization** - Establishment of Organization Structures, key Roles and Responsibilities and mature Functions and Processes to provide formal opportunities for collaboration and alignment on organizational-wide IM standards.

- **Capabilities** - The current environment can be a confusing combination of terms, methods, tools, opinion and hype and thus the world wide DAMA-DMBOK Framework capabilities can be used as a guide for the standardization of data management disciplines to help the organization perform more effectively and consistently.



Source - NSW Transport Information Management Framework

INTEGRATION MANAGEMENT

Integration Management enables the integration of different applications and services and the Integration Platform should consist of a number of technology components including:

1. Enterprise Service Bus (ESB) – software infrastructure used for designing and implementing the interaction and communication between software systems.
2. Data Integration – is used to collect, aggregate, transform and transport data used by people, processes and systems.
3. Service Gateway provides gateway functionality for interactions with external partners and customers.
4. Complex Event Processing (CEP) combines data from multiple sources to infer events or patterns that suggest more complicated circumstances.
5. Business Rule Management System (BRMS) is a system used to define, deploy, execute, monitor and maintain the variety and complexity of decision logic that is used by operational systems within an organization.
6. Business Process Management & Workflow is the automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules. BPM/Workflow automates the sequence of actions or activities required to complete a business process.
7. Data Transformations is the ability to transform messages or data from one system format into the format required by another system.

The fundamental vision of Integration Management is to provide:

- An enterprise integration platform which provides the technology environments required to support the integration of systems and data and to automate business processes and information flows spanning the organization to provide the relevant, accurate and available information for the right users in the right context.

Source: NSW Transport Integration Reference Architecture

The primary goals of the Integration Platform are:

- Interoperability: Provide better access to core information and critical business services across a heterogeneous application and technology landscape.
- Responsiveness: Enable IT responsiveness to effectively incorporate changes to business and technology.

INTEGRATION MANAGEMENT

- Maintainability: Modular application systems which are easy to use and maintain.
- Affordability: Reduced cost and complexity in integration of existing and new applications.
- Visibility: Providing clear and traceable visibility of services and related assets (with linkages to business functions and information models).

The fulfilment of any integration service requirement may be achieved through the capabilities of a combination of one or more layers in the Integration Reference Architecture. Within each layer, the architectural building blocks are a means to fulfil the architectural capabilities.

'The fulfilment of any integration service requirement may be achieved through the capabilities of a combination of one or more layers in the Integration Reference Architecture.'

The identification of service requirements and the mapping of those requirements to each of the layers of the Integration Reference Architecture is a key aspect in developing an integration service for an enterprise. The underlying requirements which determine the capabilities that the Enterprise Integration Platform supports are determined by:

- A set of functional and non-functional requirements on a service.
- Documented capability that a service needs to deliver or is expected to deliver.
- The provider view of a service requirement which represents the business and technical capability that a given service needs to deliver given the context of all of its consumers.
- The consumer view of a service requirement which represents the business and technical capability that the service is expected to deliver in the context of that consumer alone.

SECURITY MANAGEMENT

Protecting your information is far more complex than it used to be and a strategic approach to Security Management is paramount to marshal the internal forces and awareness amongst your Executive community. Actively undertaking risk assessments and closing the gaps across your organization is a real time exercise to keep your organization safe.

Some key security areas to be addressed include:

- Identification - An information asset is any piece of information that is created, utilised or updated within the scope of the project. The architect should consider both information assets which already exist and may be impacted by the project as well as those which are new and will be introduced by the solution.

- Classification - Once identified, the project's information assets should then be classified to determine their importance. Ideally, your organization's information should be formally classified, under the official guidance of the Information Security and Classification and Labelling Standard.

A security classification includes a combination of:

1. The confidentially requirement for the information
2. The integrity requirement for the information.
3. The availability requirement for the information.

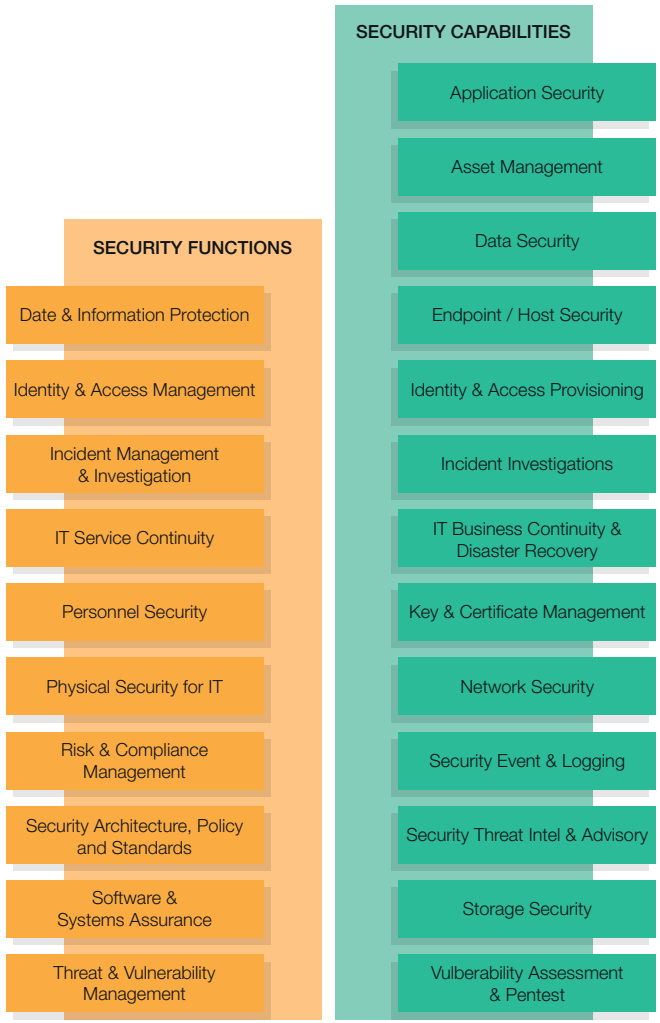
- CONFIDENTIALITY is a characteristic that applies to information. To protect and preserve the confidentiality of information to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

- INTEGRITY: To preserve the integrity of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it.

- AVAILABILITY is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the context of this standard, assets include things like information, systems, facilities, networks, and computers. All of these assets must be available to authorized entities when they need to access or use them.

SECURITY ARCHITECTURE

Below is an example of a Security Architecture that provides guidance on core Security Functions and Capabilities to be addressed:



Source - NSW Transport Information Management Framework

The 10 security functions are logical groupings to clearly convey that a layered approach has been used. Organizations must have at least one, and may have multiple, strategy documents per function.

There may be multiple levels of controls within security architectural functions, as well as controls that potentially span functions. This is determined by your guiding security principles, strategy and objectives, the Information Security Policy and the secure by design criteria for each function.

PATTERNS

A number of business problems provide the backdrop for co-ordinating your activities across these three disciplines including:

- Business units and project teams have to engage three separate specialist groups to ensure agreement and endorsement of solution designs.
- Three separate Governance approaches need to be deployed with different expertise and approach:
- Unless co-ordinated not all data is known, secured and moved according to agreed principles;

Defining Patterns is a key lever for bringing the three disciplines together.

The process for identification and harvesting of a pattern for future reuse provides significant benefits to scoping, designing, building and deploying your projects. .

The Data, Integration and Security architecture should be transposed to the Pattern template and 'washed' to be more generically applicable to projects beyond the current initiative.

A Data, Integration and Security pattern catalogue and related patterns forms a significant part of the reference architecture. The development and adoption of these patterns will accelerate the delivery of initiatives and improve Data, Integration and Security Management outcomes through the reuse of effective solutions to common problems, and provides a basis for governance to ensure the consistency and applicability of technology use within your organization.

To develop an effective set of Reference Architectures and deliver the desired benefits, there is a heavy dependency on the foundational capabilities within the over-arching enterprise Data, Integration and Security architecture. Without these foundational capabilities, it becomes difficult to define a consolidated set of Reference Architectures and articulate patterns in a way meaningful to the organization. These mandatory dependencies provide the core building blocks for which a successful reference architecture and pattern framework can be established.

TYPES OF PATTERNS

Within the context of your organization the pattern catalogue can be initially divided up into two broad categories: Solution Patterns, and Control Patterns.

- **Solution -** Cover common broad business needs, such as access by agencies to information, or Integration between systems i.e. Access Integration, Application Type, Remote Access

- **Control** - The Control Patterns cover specific discrete capabilities or controls such as Authentication, IP whitelisting. Authentication Certificates & PKI Platforms, Identity Management, Inspection & Enforcement

Solution Patterns

Solution Patterns cover common broad business needs, such as access by agencies to information, or Integration between systems.

For example, a business need for a customer facing application that uses a mobile app, might use a solution pattern such as customer facing mobile access solution. Another solution pattern might be that of an externally-hosted cloud Service, which is consumed by internal applications. Often, solution patterns will be more complex than control patterns as they cover an entire end-to-end solution that is likely to be supported by numerous security controls.

Control Patterns

Control Patterns cover specific discrete security capabilities or controls such as Authentication, whitelisting, logging i.e. authenticating a user using a mobile device. Within the pattern type, there are listed sub categories, which are there to assist in selection and descriptions of the patterns, as the pattern library grows.

PATTERN COVERAGE / GENERALITY

Patterns may have different levels of generality, by this, a pattern may be generic across a solution type, and within, have an extensive documentation discussing the different alternatives that need to be considered. Alternatively, another approach would be to write several similar versions across that solution type, each version dealing with the specific variations.

Patterns are expected to reference or link to other patterns. Therefore, the issue of pattern coverage can also be dealt with by creating a pattern of common elements, and creating separate patterns for aspects which are different. The separate patterns then reference the common pattern.

There is no simple rule for determining the extent of pattern coverage. Where there are significant differences it is likely to make more sense to separate them into multiple patterns. Where they are similar, then including them in the same pattern with commentary or decisions may be the better option. Consideration should also be given to authoring the pattern in a way that directs architects to preferred solution outcomes.

PATTERN USEAGE METRICS

Metrics and measures, are intended on being able to show the usage, and value of the patterns. The metrics collected will depend on the needs and resources available to collect the metrics. The collection of metrics is important, but equally the collection will consume resources. Therefore, they could be collected, when updating the Pattern with documentation, or in a post Solution Architecture document review.

Pattern usage metrics can be collected from information entered by Solution Architects, as part of the process of using a pattern, the pattern must be updated when used in a solution design, or if used in another pattern.

The value of patterns is a powerful discipline to combine the three disciplines and should be part of any mainstream Architecture function.

LAST WORD ON ARCHITECTURE RESPONSE

Architectural decisions relating to Data, Integration and Security Management can be quite similar in nature to other architectural decisions, and should therefore follow a similar set of Principles and Standards. The combination of Reference Architectures, Principles, Standards, Patterns and Governance enable a more holistic approach to defining and securely moving data around your organization.

In my experience, most sets of well-defined Architecture Principles and Standards are designed to enable a focus on securely moving key data around the organization, however, many organizations are yet to realise the full value of co-ordinating their responses across these three disciplines

As organizations mature their technology management disciplines and the need to securely integrate and manage their data assets increases and the risks become greater to the organization, they will need to adopt new and more efficient patterns of governance, stakeholder engagement and compliance monitoring that leverages elements of the Security, Integration and Data Management disciplines.

© Copyright 2018 Orbus Software. All rights reserved.

No part of this publication may be reproduced, resold, stored in a retrieval system, or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

Such requests for permission or any other comments relating to the material contained in this document may be submitted to: marketing@orbussoftware.com

Orbus Software
Portland House, Bressenden Pl, Westminster, London SW1E 5BH

+44 (0) 20 3824 2907
enquiries@orbussoftware.com
www.orbussoftware.com