archTIS

# Trusted Information Sharing

*Secure **your data***

*Share **your information***

*Take control of **your enterprise***

ARCHITECTING **TRUST** INTO YOUR ENTERPRISE

# Table of Contents



# The Challenge of Delivering Information Value

Chief Information Officers (CIOs) throughout the world are continually faced with the same challenge:

*How can information services be better and more deliberately aligned to deliver value and support organisational outcomes?*

Intuitively, CIOs know that there is a difference between managing ICT risk and strategically leading an ICT organisation. In fact, success in this role is measured by an ability to achieve both.

The enterprise is measuring the performance of the CIO by their ability to deliver value to the business through the provision of information services. Yet the time of so many CIOs is occupied by operational issues such as infrastructure upgrades, controlling costs and running projects while their business clients are clamouring for tangible improvements to information access and productivity.

Quick and easy access to current and reliable information is the foundation of a strong decision-making capability. This facilitates the development of effective organisational strategies and operational outcomes. An efficient, secure information management capability should therefore be the goal of all CIOs.

The true power of information is realised through its ability to inform or influence the decision-making process and support the execution of business objectives. However, these goals cannot be achieved when information is kept in information silos. Information must be shared. Security policies and controls, therefore, should not impede our ability to share information with authorised personnel nor should they be allowed to prevent or hinder the meeting of business requirements and obligations.

To deliver information value within risk-driven environments, CIOs need to establish flexible and agile information service platforms that *enable and control* the flow of information between people, systems and partners in a secure and 'trusted' manner.

Securing data and sharing information are complex goals to achieve and manage in practice. How do we determine when information should be shared, with whom and via what means? How can we know what impact a new service, capability or ICT upgrade will have on regulatory compliance and the achievement of the organisation's mission?

Trusted Information Sharing (TIS) is an approach that addresses information sharing and security as complementary requirements. This is achieved by looking at information management (security and sharing) through a 'top to bottom' enterprise architecture that aligns the CIO's information vision with the mission and business outcomes of the organisation. It captures the agreed business goals, information strategy, security policies, and functional ICT expectations of the organisation in order to architect a 'One Enterprise' view of its information services.

Architecting a TIS capability ensures that an ICT program is directly aligned to delivering an agreed organisational capability. That is, investments are implemented and operating in full alignment with the needs, maturity, risk appetite and resources of the organisation. Most importantly, a TIS-enabled organisation has the agility to respond to a rapidly changing environment, and possesses the confidence and competitive advantage that come from being in control of the enterprise and its information.

> *"A lack of trust, not technology, is the primary stumbling block to information sharing."*
>
> Officials from coalition countries, speaking at the 2007 Network Centric Warfare Conference.
>
> Source: http://fcw.com/articles/2007/01/29/crossdomain-solutions-needed-in-iraq.aspx

# The Trusted Information Sharing Advantage

The concepts of 'Trust' and 'Sharing' are human values placed on how people use, exchange, create and store sensitive information. While often the act of sharing is seen as running counter to the concepts of 'Protection' and 'Security', in reality, sharing and securing information are not mutually exclusive nor are they competing objectives. Rather, they are two complementary benefits of good information management practices. If you can manage your information so that it is actionable and you are sharing data only with the person intended, then you are maintaining the security of your information as well.

Enabling or controlling the flow of information in an assured manner will assist in achieving multiple benefits for the organisation:

- Better, more informed decision-making capability based on dependable information;
- Consistent, traceable sensitive data flows within and beyond the organisation;
- Effective alignment with business outcomes;
- Greater exploitation of information assets through the ability to discover, consume and share those assets in an assured and timely manner;
- Lower total cost of ownership including ICT governance and maintenance costs; and
- Increased return on investment.

**Information management and sharing need to be considered from three perspectives:**

**People — Processes — Technology**

Trust must be understood and established across these three views so that the information flows support organisational performance and productivity. The extent to which those information flows are enabled and controlled will depend on the nature and value of these information assets, the context of the organisation within which the information resides, and with whom the sharing occurs.

Moreover, architecting TIS throughout the organisation ensures that the resulting capability corresponds with its risk context and the criticality of those needs.

*A Trusted Information Sharing capability is one that controls and enables the flow of information between parties so that the business value of information assets is maximised, and unauthorised disclosure, modification or access is prevented.*

# Securing your Data: Why the old ways no longer work

Traditionally, high value information has been controlled via two means: personal trust relationships and the use of perimeter security to segregate and protect information domains. Therefore, a focus on sharing information - increasing the access, availability, discoverability and consumability of tightly controlled information - can be confronting to those whose role it has been to control and prevent that data from being inappropriately shared.

This approach no longer works. It does not meet the demands of the business and has bred a culture of mistrust. As a result, data is often confined within expensive perimeter security models (e.g. isolated networks, stand-alone machines, or compartmented modes of operation within a system). Within the perimeter, access is relatively unrestricted. A lack of internal restrictions implies a potentially unwarranted level of trust within the organisation itself: insiders are trusted, but outsiders are not. History has shown this premise to be flawed, with incidents of internal leaks, or 'insider threats', becoming more prevalent over the last decade.

Events such as 9/11, the Bali bombings and even the Global Financial Crisis have called for a re-balancing of the need-to-know requirements against the business imperative to share information. WikiLeaks and the Edward Snowden affair have highlighted the need to address the old paradigm that insiders are trusted. Security models must now be redesigned to reduce both costs and risks while enabling the sharing of information from within existing perimeter protected domains. Often these attempts result in higher costs and unnecessary complexity.

Redesigning the security model is further complicated by the proliferation of data, the way we source services, and the mobile workforce. Smart phones, tablets and other mobile devices have spearheaded a cultural change in the way we work and consume information. While perimeter and network security models are still relevant, organisations now need to extend security controls to the information itself so the data can be both *mobile and secure*.

*A TIS-capable organisation embeds security capabilities into its enterprise architecture to facilitate, and not inhibit, information sharing.*

# The Values and Attributes of Trusted Information Sharing

**In an initial step toward securing data and sharing information, the ICT organisation must first understand the qualities and attributes that are valued by the business for each of the different information holdings it produces. Identifying who will consume these holdings, and for which purposes, will contribute to establishing the needs and key priorities of the organisation.**

Each of the three words – Trusted – Information – Sharing – embodies a core TIS value statement that, in turn, can be associated with three core business attributes:

| TRUSTED | INFORMATION | SHARING |
|---|---|---|
| • Integrity<br>• Confidentiality & Privacy<br>• Provenance | • Efficiency<br>• Traceability<br>• Discoverability | • Timeliness<br>• Consumability<br>• Interoperability |
| **Value Statement:** There is business, social and/or economic value in being able to: **assure the credibility and reliability of information, its source, and its destination.** This value underpins the concept of TIS and enables the application of investment to mitigate risk and meet the level of confidence required. | **Value Statement:** There is business, social and/or economic value in being able to: **locate, use, manage, and take action on trusted information.** Conversely, there are costs associated with the ad-hoc management and the ineffective use or disclosure of information. | **Value Statement:** There is business, social and/or economic value in being able to: **make information available, accessible, and useable to those who can benefit from it, when they need it.** This value plays an integral role in an organisation's ability to be proactive in the face of threats and opportunities. |

From strategy to operations, the TIS business attributes must be reflected through all of the complex dynamics involved in sharing information within and between enterprises. By using these attributes to map the organisation's people, processes and technologies, gaps can be identified and ICT Programs can be aligned to deliver the identified capability requirements against the agreed business need. As a result, the process will also determine the value that a TIS capability will deliver. While many organisations may only want to address a particular attribute, others may want to achieve all three values, by addressing each set of three attributes, across all three layers of the organisation - People, Processes and Technology.

In order to TRUST our information, we require assurance concerning the integrity, confidentiality and privacy of our identities, information, systems and workflows. Our INFORMATION must be managed efficiently so that we can trace and discover the information we need when we need it. In order to ensure that information can be SHARED, the information management architecture must make the information available to the right people in a timely manner and in a format that is easily consumed. Moreover, across multiple networks, systems and organisations, appropriate controls need to be in place to enable the flow of information between them (interoperability).

# Trusted Information Sharing Attributes in Context

| | | |
|---|---|---|
| TRUSTED | **INTEGRITY** | To say that data or information has integrity, means that there is a high level of confidence that the data has not been corrupted, tampered with or modified by unauthorised persons. Making decisions based on compromised or incorrect data exposes organisations to a range of strategic and operational risks. |
| | **CONFIDENTIALITY & PRIVACY** | Ensuring an organisation's data is not disclosed to unauthorised persons is key to being able to retain commercial advantage, protect trade secrets, protect people from harm or exposure, and meet legal and regulatory obligations. As the impact of breaches is significant, the general public expects that all organisations who collect, store, use and share their personal information will do so in accordance with confidentiality requirements and privacy regulations. |
| | **PROVENANCE** | Provenance is the historical record of a piece of data or information. Knowing the information's history is one way of proving or checking whether the data has retained its integrity over time. Within a compliance context, provenance can also help track changes and updates that have been made to policies and procedures. |
| INFORMATION | **EFFICIENCY** | In terms of TIS, efficiency represents the consideration of cost and resource utilisation. It assumes cost-effectiveness of design so that the total cost of ownership remains low, systems design parameters are aligned with business objectives, workflows and rules, information management systems are integrated and interoperable, and that systems' maintainability is sufficiently streamlined to provide both continuity and resilience at the lowest possible cost to the organisation. |
| | **TRACEABILITY** | The ability to track, or trace, information within the business and technical architecture enables organisations to monitor their compliance and to maintain the coherence between their information, processes and systems. It also assists them in understanding how a change to one aspect of the business, for example a policy update, will affect all other aspects of the organisation. |
| | **DISCOVERABILITY** | To make informed decisions, organisations need to readily locate accurate and relevant information, via a search mechanism or process, which exist across diverse systems and locations. This attribute is particularly relevant for organisations that incorporate a wide variety of mobile devices and need to gain access to a range of internal and external information warehouses and databases. |
| SHARING | **TIMELINESS** | Key to making informed decisions is the ability to receive or access the right information at the most suitable, most opportune time. Within an ICT framework, timeliness refers to the distribution time from when the information becomes available to when it is made available to those who need it. The system must be designed to reflect the criticality requirement each person has for that information. |
| | **CONSUMABILITY** | Referring to the use and reuse of data or information, this attribute involves all aspects of being able to view/read and modify the data. Essentially, it refers to the adaptability of the presentation layers and how they are integrated into a system of knowledge so that one is able to readily exploit the available information assets for a specific context, purpose, or platform. |
| | **INTEROPERABILITY** | The challenge of information sharing is complicated by the fact that organisations can differ in the way they not only trust and value information but also in the types of risks they face. This is a major impediment to information sharing. Interoperability ensures that diverse systems and organisations can work together in a controlled manner to exchange information. |

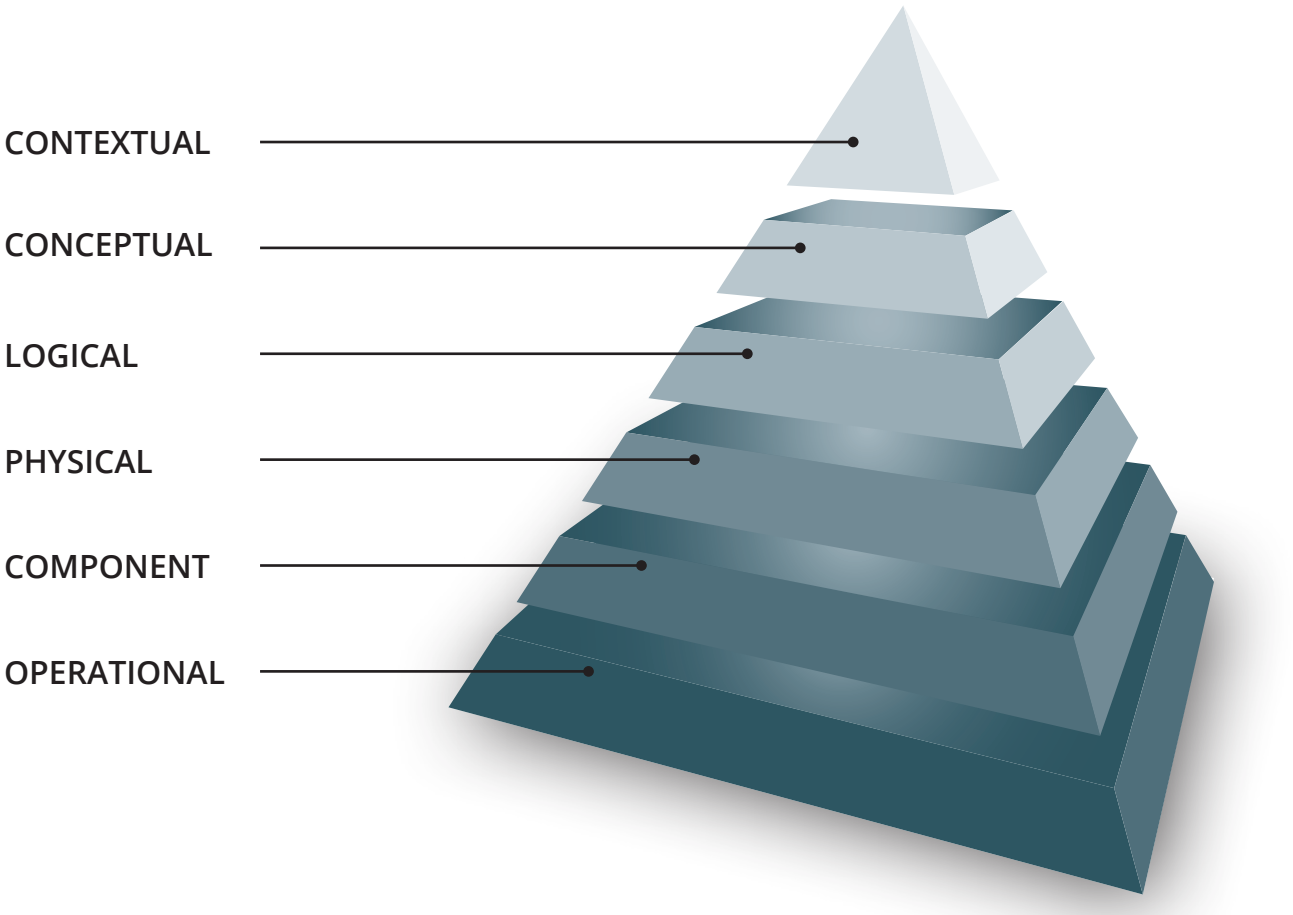
# Architecting Trust: Taking Control of Your Enterprise

By understanding the organisation's current capability, maturity, risk appetite and resources, it is possible to architect and implement a 'One Enterprise' view and take control of the enterprise.

An architectural approach consists of the coherent alignment and integration of all aspects of the business in support of its ongoing and often dynamic mission, vision, goals and objectives. This approach can be applied to assure the quality of the information being collected, used, shared and stored throughout an organisation. Moreover, it leverages existing ICT investments and makes use of commercial off-the-shelf (COTS) products to achieve this goal.

Up to six different views of an organisation can be used to better understand, build and accredit an architecture against organisational requirements. These views enable the consistent delivery of predictive and risk management capabilities, viability and flexibility within a dynamic service-driven environment.

*Six views of the TIS enterprise architecture*



# Building Trust in People, Systems, and Technology

**To achieve 'trusted' information sharing, we need to establish the degree to which we are prepared to trust. We then must be able to demonstrate with assurance:**

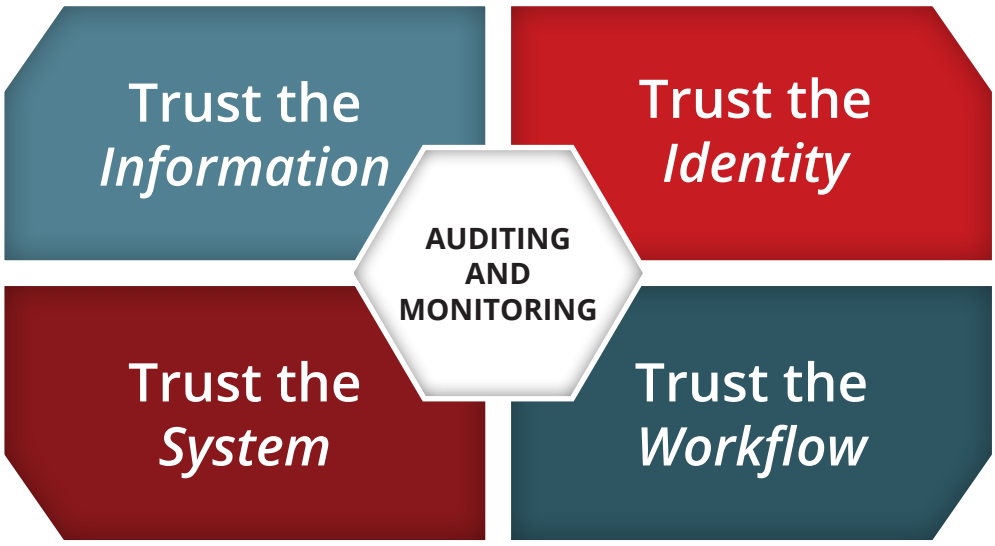
- Who we are sharing information with;
- What information they are entitled to access;
- The terms and conditions of where and how they can access that information; and
- Transparent traceable actions (what and when) that provide us with evidence should there be a breach of security.

This can be achieved by defining and applying business rules that define who does what, to/for whom, how, when, where and why.

At each of the architectural layers of a TIS capability, information, identity, systems and workflow management are executed in a manner that imbues trust without inhibiting operational performance.

Business policies, processes and rules become extremely powerful when combined with a metadata schema. They can embed automated controls throughout the architecture that assure the integrity, confidentiality and provenance of the organisation's information through rigorous access control and monitoring capabilities. Compliance with a particular policy, or contribution to an operational strategy, can be traced through all three organisational views: people, processes, and technology. The organisation can be assured that the controls are consistently adhered to, can be relied upon, and are trusted.

As a result, the TIS architectural approach not only assists organisations to meet stakeholder expectations but also to meet compliance and security obligations: implementing policies coherently throughout the organisation, and keeping sensitive data safe.




**Architecting trust assures the integrity, confidentiality and privacy of all identities, information, systems, and workflows within an enterprise.**

*archTIS is recognised as the world thought leader in TIS, and works with organisations to address their TIS requirements to secure their data, share their information, and take control of their enterprise.*

> *"Information is a source of learning. But unless it is organized, processed, and available to the right people in a format for decision-making, it is a burden, not a benefit."*
>
> William Pollard

**www.archtis.com**

Level 3, 10 National Circuit
Barton ACT 2600
AUSTRALIA

**Phone 1300 ARCHTIS**

Tel +61 2 6162 2792
Fax +61 2 6162 2718
Email info@archtis.com

ACN 123 098 671