Trusted Information Sharing (TIS)
Bringing business, information management and security together to share information securely
Copyright Statement

The information developed in this document remains the property of archTIS and, apart from any use permitted under the Copyright Act 1968, all other rights are reserved.

The intellectual Property Rights of other companies’ information presented within this document remain the property of the company so represented. This document acknowledges all trademarks and copyrights. While we make every effort to ensure that material in this document is accurate and up-to-date (unless denoted as archival material), you should make independent inquiries before entering any commitment based on material published here. The information in this document is general in nature. We specifically disclaim responsibility for any loss you may suffer as a result of relying on the information in this document.

Links to websites are provided in good faith, but we can give no assurance of the quality, accuracy or relevance of materials on such sites.

Copyright © archTIS 2014
Organisations must share information, however, the risks involved in sharing are often seen to outweigh the benefits: sensitive information could be exposed, financial data stolen, a competitive advantage or even a reputation lost. As a result, organisations are often reluctant to share as openly as they would like, and they hope that their ICT systems can be trusted to keep their information assets safe. While information exists in many forms, organisations tend to expect ICT to enable information sharing while protecting it at the same time.

These expectations are based on the assumption that secure information sharing is an ICT problem. It’s not. It is a business problem. The sharing of accurate and timely information is integral to decision-making, profit-generation, and innovation. Organisations simply make better decisions and respond more quickly to new threats and opportunities when information is reliable and available.

The information sharing challenge

Secure sharing implies and requires a level of trust. While digital information once flowed primarily within the perimeter of an organisation and information was only shared hand-to-hand between people who knew each other, today’s information is being shared at great speed, with people we do not know, and often with less thought as to the risks presented by these exchanges. To compound the fear of exposure, events such as Snowden and Wikileaks have shown that we cannot always trust our own people with the organisation’s most prized information.

Fear of information exposure, arising from mistrust in people and in systems, constrains our preparedness to share. Without trust, we hesitate to share for fear of the consequences, which means the value and power of our information is diminished, and we may not be able to meet the strategic and operational objectives of our organisation. Therefore to do business, we must find a way to share information in an assured manner.

Despite the need to better manage and share information, organisations often only address individual ICT symptoms, typically at the network or presentation layers. The problem with this approach is that the real threat is either already inside or can gain broad-base access to information by breaching the perimeter. Placing stronger security controls around an organisation is not sufficient to address the threat of the trusted insider. Perimeter security controls are a reactive method of dealing with information security – one that was designed to wrap around the network as an afterthought. In fact this method often works counter to today’s businesses need. Instead of facilitating the exchange of information between people, systems and organisations, perimeter security controls inhibit information sharing and even encourage people to circumvent security in order to ‘do their job’.

Key business questions the organisation needs to answer:

- What information does it have?
- What is the value of that information?
- Which high-value information assets and services does the business consume to make decisions?
- What information does it need to share with others outside the organisation?
- Which information might outsiders consider worth targeting?
- What governance and authority structures guide the terms and conditions required for sharing to take place?
To do its job for the business, ICT must be able to deliver the right information services when and where the organisation needs them. Identifying the information that is of most value to the business, and that needs to be protected, is not a trivial activity. It involves many information stakeholders from across the business units, information management and security domains. All of these information stakeholders must develop a deep understanding of, not only their own roles and responsibilities, but also their interrelationships within and beyond the organisation.

**Who supports whom?**

**What needs to be shared and when?**

**Are the people, systems and workflows trusted to manage critical business information?**

The process of bringing an organisation’s information assets and services under control cannot be achieved overnight. There is no single technology or product that can correct years of poor information management, or resolve the complexity introduced by disparate networks of systems and applications. Instead a whole-of-enterprise approach is required to grow a single, integrated information environment that encourages confident collaboration and delivers a richer, more informed decision-making capability.

Improving and reshaping the way a business consumes, manages, delivers and protects its high-value information involves effort, risk and investment. For many organisations, making changes to a system that supports business-as-usual (BAU) activities is akin to changing the wheels of a car while it’s travelling down the road. However maintaining legacy systems on life support indefinitely also carries significant risks for the organisation. Siloed systems and information assets limit the organisation’s ability to share high-value information across business functions, and diminish its ability to respond to the business environment. They are also expensive to maintain.

All stakeholders need to work together to:

- better understand the organisation’s high-value information requirements
- implement a trusted information management capability that both enables AND controls information availability and access, and
- develop a unifying framework for operating BAU, undertaking programs of work and responding to changing information needs.

By taking a whole-of-enterprise approach, a trusted information sharing capability can be achieved by integrating the business operational needs, good information management practices and dynamic security controls in a symbiotic way.

Establishing trust is key to managing and sharing information in a way that enables responsive, innovative and proactive decision making. An assurance framework establishes trust by enabling people to make good, risk-based decisions concerning the information being shared. It provides the context for understanding security and the business value of information sharing. Without it there is no context to help people assess risk and make informed judgments about the information they generate, access and share.

An assurance framework rationalises information sharing fears by promoting a greater understanding of the level of risk involved in sharing, and the risk posed by not sharing information. It also gives people a means of comparing and assessing competing risks. In short, it helps people to make informed decisions.
The Business-Information-Security Nexus

Trust is achieved when an information management capability is implemented to meet an organisation’s required level of assurance and particular business context. When applied consistently across the organisation, this capability enables people to confidently share their valuable knowledge with colleagues and partners, protect their IP and sensitive information, and shape the way they interact and operate within the organisation and the broader market. Trust cannot be achieved through an ICT solution alone – it must be delivered consistently through an assurance framework and architecture. ICT is just an enabler.

Trusted Information Sharing (TIS)

Trusted Information Sharing (TIS) addresses the nexus of the business, information management and security domains. Many organisations are trying to treat each of these domains in isolation. When it comes to sharing high-value information, these domains cannot be treated in isolation of one another. Elements from each of these three domains must be aligned in order to share and protect information appropriately.

As a result, TIS requires an enterprise perspective regardless of whether the organisation wishes to apply it to a specific community of interest or to the entire organisation. A TIS approach views the organisation holistically as a single system of multiple dynamic relationships that are made up of, driven by and reliant upon high-value information. It provides a means of building today’s required information services in a way that ensures that these services can integrate into, interoperate with and be assured within both the existing and future information environments. To achieve this, TIS necessarily spans all layers of the organisation - strategic, operational and tactical – to identify, guide and implement this capability consistently from the top to the bottom of the organisation.

Business Value:

- What information do we need?
- When, where and why do we need it?

Information Management:

- How do we manage, create, share, present and consume information so that it delivers value to the organisation?

Security:

- Can this information be shared?
- What are the risks of sharing versus not sharing this information?
- What are the terms and conditions of sharing it?

The business and economic costs of NOT sharing information are significant
Implementing Trusted Information Sharing (TIS) starts with identifying and bringing together all of the stakeholders of the organisation’s high value information and information services. This initial step ensures that all stakeholders have a common understanding as to what and who is contributing to the organisation’s mission. It also helps the executive team to prioritise projects and programs of work and to allocate their limited resources to what matters the most to the organisation. Once a trusted information management and sharing capability is established to facilitate the high-value, public-facing business outcomes, the organisation can then address lower priority activities. While low priority outcomes fall outside the scope of the trusted information sharing approach, TIS implementations can be built upon and further extended to meet the wider needs of the organisation. This approach empowers organisations to address the most important business needs first, while providing them with a coherent pathway for future capability development.

Architecting TIS ensures that the resulting capability corresponds with the organisation’s risk context and the criticality of its business needs. Architecture provides each individual with their context in the delivery of organisational outcomes. Who they provide services and information to? What is the responsibility of their service? What are the consequences of not providing that service or information? It identifies information services and the technical capabilities required to support and/or deliver those critical information services, and pinpoints where efficiencies, cost reductions and the most critical investments need to be made.

An agile trusted information platform can then be implemented to bring all of the disparate systems together under one roof and maximise their utility across the organisation. This platform provides the foundation for new services and more dynamic information management. It describes the extent to which the credibility and reliability of the information must be assured; how it needs to be used, and managed; and how it should be made available, accessible and shared so that it’s usable by those who need the information, when and where they need it.

What are the benefits?

Enabling and controlling the flow of information in an assured manner delivers multiple benefits such as:

- Better, more informed decision-making
- Consistent, traceable data flows within and beyond the organisation
- Better alignment of business outcomes and information services
- Improved and trusted information discovery, management, and sharing
- Scalable, extendable information services (the ability to grow a TIS capability throughout an organisation according to need and resourcing)
- Lower long-term ICT governance and maintenance costs, and
- Increased return on investments.

TIS applies a consistent assurance framework throughout the enterprise that enables information access and availability, while simultaneously preventing unauthorised access or disclosure.
Where to begin?

Establishing trust consistently throughout an organisation requires an enterprise approach that takes information, people, workflows, outcomes and systems into account.

To implement Trusted Information Sharing, there are three phases:

- **understand your business** (strategic vision, planning and guidance),
- **architect the solution required to achieve your business outcomes** (an architectural assessment of current state and design of interim and future states),
- **select and implement the technology that will deliver those business outcomes** (the implementation of the architectural design - selecting those technical functions (not just products) that will achieve the required capabilities).

The scale of a TIS implementation will vary according to the business needs. A strategic assessment can determine the most suitable starting point for a TIS implementation. An organisation can start small, focusing on a very specific or short-term need, with the knowledge that they can scale readily to enterprise level if and when they require it. A TIS capability can be achieved by working with either a single provider experienced in delivering services across these three phases, or a consortium of specialist service providers that can seamlessly assess, guide, design, build and accredit a TIS solution from top to bottom and from start to finish.

archTIS - Architects of Trusted Information Sharing

archTIS is the only company in Australia to have implemented TIS within a high security government agency using Attribute Based Access Control (ABAC). This solution was accredited by the Australian Signals Directorate and complied with all of the relevant standards and legislation governing data management and information security.