Joint Committee of Public Accounts and Audit

Review of Management and Integrity of the Commonwealth's Electronic Information

Table of Contents

Attachments

1 Introduction and Overview

The Australian Taxation Office (ATO) on behalf of the Commonwealth of Australia collects processes and stores a large amount of data about Australian taxpayers.

In a dynamic and evolving electronic environment the ATO has made a commitment to make interactions with the community 'easier, cheaper and more personalised'. Inherent in this commitment is the need to develop and promote secure electronic interactions and storage of data.

The ATO is also moving to progressively make data relating to a taxpayer available to them. For example, we are making account information available to taxpayers and their representatives. This will provide an avenue to significantly improve the accuracy and integrity of our account data.

On the other hand the ATO is aware of the risks to privacy and community confidence associated with the collection, storage and transfer of electronic data and the increase in such risks when an increasing number of people are allowed access to it.

In recognition of this, we have set up a Trusted Access Branch headed by an SES officer whose sole focus is to minimise the risks from external and internal sources by putting in place Defence Signals Directorate (DSD) certified technical facilities, as well as integrated processes, procedures and guidelines. It is worth noting that the ATO was one of the first organisations to gain DSD certification for its gateways in May 1997. DSD has subsequently re-certified ATO systems.

The ATO remains vigilant in ensuring that the privacy, confidentiality and integrity of data it collects, processes, stores and transfers is maintained.

1.1 Strategy for Information Management

The ATO's high level strategy for information management has the following features:

- A continuous process which seeks to identify potential risks;
- Development and review of mitigation strategies;
- Monitoring the success of the strategy to ensure that it is mitigating the risk and if necessary taking corrective action; and
- Best practices are identified, reviewed and used to improve the ATO's strategies and practices for information management. For example, the ATO has taken into consideration the work of the Australian National Audit Office as set out in their *Better Practice Guide* on Internet delivery.

These features will be discussed in the body of this submission.

1.2 Risks

The risks are broadly categorised as internal or external.

1.2.1 Internal Risks

With approximately 20,000 staff situated in some 31 sites around Australia, the ATO is aware of a potential significant risk that staff may pose to information held in terms of:

- manipulation of information held;
- unauthorised access to information; and
- potential unauthorised transfer of information, either to other staff or to persons outside of the ATO.

Risk assessments are regularly carried out. Following the most recent risk assessment, a plan was prepared and documented in the *ATO Security Risk Management Plan*. This plan identifies the potential risks and puts strategies in place to:

- reduce the opportunity for a risk to be realised;
- detect any person attempting to exploit a vulnerability;
- reduce the impact of the risk if it is exploited; and
- deal effectively with any person who acts improperly.

In view of the changing environment, the *ATO Security Risk Management Plan* is under continual review. This ensures that any new or emerging risks will be identified and strategies to address such risks developed and implemented.

1.2.2 External Risks

Risks which are external to the ATO can be brought about by:

- interactions with taxpayers and their representatives;
- transfers of information to and from other Government agencies;
- interactions with third parties.

1.2.3 Strategies to Address the Risks

The ATO has a comprehensive set of strategies, policies and guidelines to address the risks relating to information security. These are discussed later in this document.

1.2.4 Monitoring

The ATO continually monitors data management to ensure that no new risks are emerging and to ensure that the strategies developed are addressing risks. Work also takes place to ensure that all policies and guidelines are adhered to. The ATO has a practice of undertaking Threat and Risk Analysis which is discussed later.

The ATO uses an extensive array of computer systems to enable its activities. These computer systems contain programs which record staff access and staff manipulation of data and enable the ATO to identify:

- the user details of persons accessing particular records or systems;
- the times and dates records were changed;
- the screens that were viewed but not necessarily changed; and
- new information that was added (rather than updated).

This information is used to investigate allegations of inappropriate access to taxpayer information. While the ATO investigated 133 alleged inappropriate access allegations during 2001-02 financial year, 77 (58 per cent) were found to be unsubstantiated. This is an important aspect of audit logging, supporting staff who conduct their activities within the rules. Audit logging is also used to support managers in controlling work practices and output. Where evidence of inappropriate access is detected the matters are either dealt with as a Code of Conduct breach or referred to DPP for prosecution action. During the last year a number of successful criminal prosecutions have been conducted.

2 Policies and Guidelines

The ATO has a number of policies and guidelines which collectively constitute a policy and planning framework in respect of the privacy, confidentiality and integrity of the ATO's electronic data. This framework provides guidance in handling, storing and transferring of information.

2.1 ICT Security Policy 2001

The ATO ICT Security Policy ensures the protection of ICT hardware and software associated with ATO information. The policy:

- ensures the continuity of ATO ICT related services to its clients and business partners in relation to technology security;

- minimises the likelihood and the consequence of threat realisation to information security that may cause loss or damage to the ATO, the Government or its clients and business partners;

- informs all ATO personnel, contractors and those performing services on behalf of the ATO who have access to information of their responsibilities and obligations with respect to technology security;

- provides processes and procedures to ensure staff meet their responsibilities; and

- ensures that security levels of both staff and infrastructure are appropriate to the level of data to be accessed.

2.2 Policy for the Proper Use of ICT Facilities

The Policy for the proper use of ICT facilities is related to the ICT Security Policy 2001. The proper use of ICT facilities policy describes the conditions under which ATO ICT facilities may be used; and aims to identify the principles behind the permitted use of ICT facilities to make users aware of:

- what constitutes improper use;
- accountability requirements relating to the use of ICT facilities;
- scrutiny and monitoring of the use of ICT facilities; and
- scope for sanctions against users when breaches occur.

2.3 End-to-end Security Architecture

The ATO end-to-end Internet security architecture has been developed in accordance with the following proven methodologies and guidelines:

- The Defence-in-Depth Strategy, which dictates that there should be security check points within each of the layers and sub-systems comprising the ATO ICT environment. The check points are the gatekeepers that ensure that only authenticated and authorised users are able to access that layer and those beneath it;
- The Defence Signals Directorate: Australian Communications – Electronic Security Instruction 33. This instruction has been developed by the Defence Signals Directorate to provide guidance to Australian Government agencies wishing to protect their information systems;
- Gateway certification guide - Defence Signals Directorate;
- Protective Security Manual;
- Detailed guidelines and instructions from our platform supplier, in the form of online and printed documentation and consultation with on-site supplier representatives;
- Australian privacy legislation, using the guidelines set out by the Office of the Federal Privacy Commissioner;
- Authentication mechanisms consistent with the ANAO's Better Practice Guidelines;
- A high level depiction of our security architecture is at Attachment A.

2.4 Evidence of Identity

Evidence of Identity is effectively the key to accessing taxpayer information held electronically by the ATO. The Commissioner, after consultation with the ATO Solicitor, external professional taxation and accounting groups and relevant stakeholders within the ATO has provided firm direction towards greatly improving and streamlining Evidence of Identity procedures for all inbound telephone contact. This builds on other Evidence of Identity improvement work that has been undertaken over the course of 2002.

2.5 ATO Web Centre Gateway Security Policy

The ATO Web Centre represents a single point of management for the ATO's Internet presence. It includes the corporate Internet and Intranet web sites, infrastructure and related services.

A broad threat and risk analysis of the physical and logical implications of existing and future web developments has been carried out. This threat and risk analysis identified a number of existing and potential risks. A security policy to manage these has now been implemented which conforms with the ANAO's Better Practice Guidelines.

2.6 Policies and Guidelines for Call Centres

Staff in call centres are governed by ATO practice statements concerning access and security of taxpayer data. Access to systems is restricted in accordance with the relevant practice statement and this access is regularly checked on site. Taxpayer contact staff receive a significant level of training, coaching and quality assurance, to ensure adherence to all relevant practice statements.

Data which is stored on telephony hardware can only be accessed by appropriate staff/contractors who have undergone the required security checks and all systems are subject to identical security provisions to those of other in house ATO systems.

Ongoing checking and process improvements ensure that the accuracy of data on the ATO reference material systems used in the call centres is high. Access to update or change this information is restricted to a small number of staff whose specific role is to maintain the system and its records.

2.7 Security Clearances

The Commonwealth Protective Security Manual requires people granted access to security classified information to hold a security clearance commensurate with their level of access. The majority of ATO staff with access to classified information either have a security clearance or are undergoing vetting.

The ATO is currently in the process of identifying all of its security assessed positions and security clearing the incumbents. It is anticipated this will be achieved by the end of 2003. This delay does not apply, however, to positions requiring access to 'highly protected' or national security classified matter. Access to such material is dependent on an appropriate security clearance being held or a provisional clearance being granted pending completion of vetting.

2.8 Security Education and Awareness

Security education is included in induction programs and is mandatory for all ATO employees. Contractors who have access to classified information are subject to the same pre-engagement character checks and induction training as ATO employed staff. Security awareness is maintained through internal electronic news articles and log-on-screen reminders. Information security guidelines (including how to classify, handle, store and destroy official information) are published on ATO's Intranet. Security clearance holders are specifically informed of their personal responsibility to protect classified information.

3. Privacy, Confidentiality and Integrity of the Commonwealth's Electronic Data

3.1 Privacy and Confidentiality

Privacy and confidentiality of taxpayer data is protected within the ATO by assigning a security classification to all data and only allowing ATO staff who have undergone appropriate vetting to access data at a particular security classification. Staff need an authorisation to access data and they must abide by the need-to-know principle which restricts them to data which they need to access to perform their authorised work.

3.2 Integrity

There is a number of important aspects of data integrity:

- Data capture techniques to ensure correct data is entered into our systems;
- Ensuring that during transmission the data which is received is identical to the data which was sent;
- Ensuring that only authorised processing is carried out on the data. Part of the authorisation process is to only allow a operator access to those programs and utilities on the ATO's computing systems that the operator needs to do their work.

There is a number of techniques that the ATO uses to ensure systems and data integrity during processing including:

- Intensive edit checks are conducted during capture to ensure integrity of data;

- batch programs run automatically with no human intervention;
- the operator runs a set of predefined batch programs which do all of the permitted processing;
- the operator uses an interactive program to access and transform the data. The program restricts the operator to making just those changes to the data that the operator is authorised to make; and
- audit trails are captured and reviewed regularly to detect and deter anyone attempting to make unauthorised changes.

3.3 Ensuring Privacy and Confidentiality of Data Held on ATO Networks

ATO staff use an Australia wide network of desk top personal computers. This network has a security classification of 'in-confidence'. Policy directs that data with a higher security classification is not permitted on the network.

All ATO data sent over these networks is encrypted immediately prior to entry to the networks and decrypted immediately after exit from the networks. This use of a private network and encryption of data transmitted between ATO premises over the networks protects the privacy and confidentiality of the data being transmitted.

3.3.1 Replacement of Current Infrastructure

In February 2003, a new infrastructure for desktop and communication will begin to be rolled out within the ATO. It will use Windows 2000 administrative software and Windows XP Professional on the desktop. It will provide a number of benefits including:

- Addressing an Australian National Audit Office concern about access controls for secure data on the internal network; and
- Improved access control to the network;
- A more secure and stable network.

Network security will also be strengthened by the roll out in 2003 of smart card technology. A user's identity is authenticated by placing a smart card in a smart card reader which is attached to the terminal.

3.3.2 Mobile Computing Platform

ATO staff who work as field officers are issued with lap top computers for use in the field. Other ATO staff who have a need to work away from ATO premises are also issued with lap top computers. Authorised staff with lap top computers have dial in access to the network.

Dial in access is via a Virtual Private Network using public network infrastructure. Further protection is provided by Public Key Infrastructure encryption of all transmissions.

Data held on the lap top hard disk is also encrypted to protect against loss or theft and the user's identity is authenticated by the use of smart card technology.

3.3.3 Network Connection to the Mainframe

Staff access to the mainframe is controlled by User ID and password combinations as well as the Resource Access Control Facility which ensures proper authority is held for any transaction.

3.4 Security and Integrity Measures for Telephone Interaction

Self-help IVR (telephony) applications employ the following security measures:

- They are all conducted within the ATO secure environment and therefore are subject to the same security as all mainframe systems;
- Evidence of Identity requirements for any self help application are in line with the required Evidence of Identity for a 'live' call.

4 Management and Security of Information

4.1 Taxpayer Information Provided Electronically by Third Parties

Discussed below are some examples of the security treatment of information provided by third parties.

4.1.1 Data for Income Matching Purposes.

Taxation laws require investment bodies, companies, Pay As You Go (PAYG) payers and Private Health Insurance funds to report certain information to the ATO. The ATO also receives data on investment income earned by Australians overseas under Organisation for Economic Cooperation and Development (OECD) treaty arrangements.

Typically, information which is reported to the ATO is:

- the full name of the taxpayer;

- the date of birth of the taxpayer where it is available;
- the address of the taxpayer;
- the TFN of the taxpayer where it is available; and
- the relevant account details for the taxpayer which for example, may include details of interest or dividends earned, or private health fund membership details, or the gross amount of payments subject to PAYG withholding and any tax withheld.

This data is held within the ATO secure environment and is subject to the same access protocols as other ATO classified data.

4.1.2 TFN Report Data

Each quarter, investment bodies are required to report to the ATO details of each TFN quotation made during that quarter. Typically information reported to the ATO is the same as that for data matching but the provider also provides the relevant account details for the taxpayer.

4.1.3 TFN Declaration Data

PAYG payers are required to report to the ATO details of each TFN declaration made during a period. Each week TFN declaration data is reported to Centrelink for their assurance purposes using a mainframe to mainframe connection over a private secure link.

4.1.4 Family Tax Benefit Data

To ensure compliance with the arrangements around Family Tax Benefit, information is provided by Centrelink to the ATO using the same mainframe to mainframe connection over a private secure link.

4.1.5 Exchange of Information with Child Support Agency

Both the Child Support Agency and the ATO work within the same physical infrastructure. Similar access protocols apply as to other ATO held data.

4.1.6 Data Matching Program

Data matching processes are conducted by the Data Matching Authority under the provisions of the *Data-matching Program (Assistance Tax) Act 1990*. For the purposes of this program data is transmitted to the agency via a private secure link.

4.2 Measures to Protect Information Being Transmitted by the ATO

The ATO adheres to the principles for the transmission of security classified information that are set out in the Protective Security Manual and ACSI 33 and ACSI 37. In a transfer of data the security classification of the data determines the type of security mechanisms employed. Essentially data with a higher sensitivity is given a correspondingly higher security classification necessitating transmission involving more secure mechanisms to provide greater protection to the data.

Persons who are to receive security classified data need to be vetted to an appropriate level and have a need-to-know in relation to the specific data about to be transmitted.

Audit trail: An audit trail is captured and written to write-once media to reduce the risk of subsequent alteration of the audit logs.

Encryption: Hardware and software based encryption is used for transfers of data to internal business lines and to external clients. PKI is used where appropriate. Virtual Private Networks are used. An example is Fedlink which is a virtual private network solution for connection to Federal, State and Local Government agencies.

Firewalls: The ATO uses multiple firewalls to protect its electronic assets. The firewall devices and the software used are all from the evaluated product list provided by Defence Signals Directorate. The ATO firewall implementations have been inspected and certified by Defence Signals Directorate. In 1997 the Secure ATO Firewall Environment (SAFE) was certified by Defence Signals Directorate at the protected level. In 2000 the Secure ATO Firewall Environment Redevelopment (SAFER) was certified by Defence Signals Directorate at the highly protected level.

Virus management controls: The ATO deploys virus management controls to provide assurance that the ATO neither receives nor transmits viruses.

E-mail filtering: The ATO employs e-mail filtering to reduce the incidence of spam, to detect viruses, trojans and worms and thereby ensure as much as possible that its networks are available to perform its work.

Patches: The ATO applies the latest security patches to its software to mitigate the risks of denial of service and trojan attacks.

Mainframe to Mainframe

Leased lines which provide the ability for the ATO to have a Wide Area Network also enable connections between the ATO mainframe and other mainframes such as that held by the Australian Security and Investment Commission. Such mainframe to mainframe communication is always carried out by batch programs and never by individuals running individual enquiries.

Icon Network

Icon is a fibre optic network which has been laid in Canberra. It provides communication links between Government agency mainframe computers. It has two distinct and separate circuits as follows:

- Icon black - this circuit is security classified at in-confidence
- Icon red - this circuit is security classified at protected and as further protection the circuit is enclosed in a steel pipe to prevent anyone from tampering with the fibre optic cables

4.3 Measures to Protect Stored Information

Disaster recovery and business continuity plan: The ATO has developed and tested its disaster recovery and business continuity plans for its applications, systems and electronic data.

Backups: The ATO uses industry best practice to ensure that it has back up copies of its data. It ensures that the data has the correct security classification, there are protective markings indicating the appropriate security classification.

Storage mechanisms: The ATO ensures that the material holding its data is protected properly by appropriately vetted storage and archiving contractors.

Destruction of storage media: Where appropriate, media used to store classified data are securely destroyed

Staff awareness: The ATO has developed in-house policies and procedures and uses an education approach to increase staff awareness of security best practice.

5 Adequacy of the Current Legislative and Guidance Framework

Substantial protections exist within taxation law and other laws of the Commonwealth designed to protect information held by the ATO. These provide a very tight legal and administrative framework within which the ATO operates.

6 Monitoring and Governance

6.1 Technical Monitoring

Secure ATO Internet based systems are located within ATO's own Defence Signals Directorate certified environment which is designed to protect various types of data including highly protected data. Major systems include ATOassist (ATO's main web site), Electronic Client Interface for Business Activity Statement, Australian Business Register and Tax Agent Portals. This environment is currently being upgraded to an

ATO wide Internet Security Framework to support a range of “Fit for Purpose” authentication and access control type business requirements.

The ATO's gateways and critical Internet systems use leading technology that detects unauthorised attempts to access ATO systems and alerts the operational staff to take preventive measures. This capability is available around the clock and the ATO is assisted in operating this facility by a leading Australian security organisation.

Incidents are categorised in accordance with Defence Signals Directorate guidelines. Every week the ATO detects and prevents thousands of such attempts from damaging its systems. Weekly reports are produced and circulated to key stakeholders. The ATO ensures that all new systems connected to the Internet have this capability.

It is our understanding that the Defence Signals Directorate are highly satisfied with ATO's capability in this respect. The ATO strictly follows Defence Signals Directorate guidelines to ensure that the risk to its various online systems from the Internet is acceptable to the business users.

6.2 Threat and Risk Analysis

The ATO follows the Defence Signals Directorate recommendation that agencies adopt a risk management approach by determining the source of threat and level of risk to its systems from various potential sources. The sources could be either based on the Internet or other deficiencies in internal procedures or other capabilities.

There are various levels of the Threat and Risk Analysis process. Less complex Threat and Risk Analyses are performed by the ATO's Trusted Access Branch. More complex analysis is done with the assistance of Defence Signals Directorate approved security consultants. During the last twelve months, the ATO has completed 51 internal and 4 external formal Threat and Risk Analyses and has 23 internal and 6 external Threat and Risk Analyses in progress for various systems.

For each new application development a doctrine is developed to ensure that vital roles and responsibilities are carried out, a system security plan is developed and physical and logical access management controls are deployed.

6.3 Defence Signals Directorate Accreditation in relation to PKI

The Baltimore UniCERT product used in the ATO Certification Authority is evaluated to the E3 level. As part of Gatekeeper accreditation, Defence Signals Directorate were responsible for accrediting the security of the ATO Certification Authority. The ATO PKI has maintained Gatekeeper full accreditation since 16 June 2000.

6.4 Defence Signals Directorate Accreditation in relation to Firewalls

The ATO firewall implementations have been inspected and certified by Defence Signals Directorate. In 1997, the Secure ATO Firewall Environment (SAFE) was certified by Defence Signals Directorate at the protected level. In 2000 the Secure ATO Firewall Environment Redevelopment (SAFER) was provisionally certified by Defence Signals Directorate at the highly protected level.

6.5 Australian National Audit Office Recommendations

The ATO maintains a register of Australian National Audit Office (ANAO) recommendations and factors them into its ICT plan. Senior ATO management including the ATO Audit Committee regularly reviews the register of ANAO recommendations to ensure that these recommendations are actively being followed up.

6.6 Australian National Audit Office Audit of ATO Internet Security Management

In 2001 the ANAO conducted a performance audit of Internet security management of various Commonwealth agencies, including the ATO.

The ANAO considered that the ATO Internet and PKI risk management and security policy framework adequately addressed issues of confidentiality, integrity and availability of ATO ICT systems and data holdings. The ANAO also provided some suggestions for improvement which have been adopted by the ATO.

7 ATO Performance Against ANAO *Better Practice Guide*

The ANAO *Better Practice Guide* provides best practices in a number of areas. The four which are most relevant to security and integrity of information have been referred to in developing the following section.

7.1 Monitoring and Evaluating Internet-delivered Government Programs and Services

The ATO constantly monitors and evaluates its Internet delivered programs and services. With Gatekeeper accredited PKI for instance the ATO provides a monthly report including statistics, fault reports and analysis to NOIE about its PKI operations.

7.2 Internet Systems Security and Authentication for ATO Programs

The ATO strictly follows the guidelines contained in the Privacy Act, the Protective Services Manual and Australian Communications - Electronic Security Instructions to protect its data. Its gateways to the Internet have been certified by Defence Signals Directorate. It uses Gatekeeper accredited PKI for authenticating businesses online and communicating with them.

It has the ability to identify, record and analyse incorrect or anomalous activities on its information technology based systems. This ability is supplied by the ATO having the necessary tools and techniques such as firewalls, intrusion detection systems, logging and regularly auditing activity on important systems and system integrity verification tools.

Guided by its Disaster Recovery and Business Continuity Plans the ATO has the ability to react effectively and appropriately to security issues or incidents as they emerge. Where a high degree of authentication is required the ATO uses PKI to reliably authenticate parties.

7.3 Legal Considerations for ATO Internet Service Delivery

The ATO has consulted extensively on legal risk with the Australian Government Solicitor and the ATO's legal professionals in relation to the Australian laws which apply generally to significant aspects of electronic service delivery.

7.4 Privacy Issues, the Internet and the ATO

The ATO is well aware of its responsibilities in relation to privacy issues and complies with guidelines 1 to 4 of the Australian National Audit Office *Better Practice Guide*. It enforces compliance with guidelines on workplace email, web browsing and privacy.

8 Conclusion

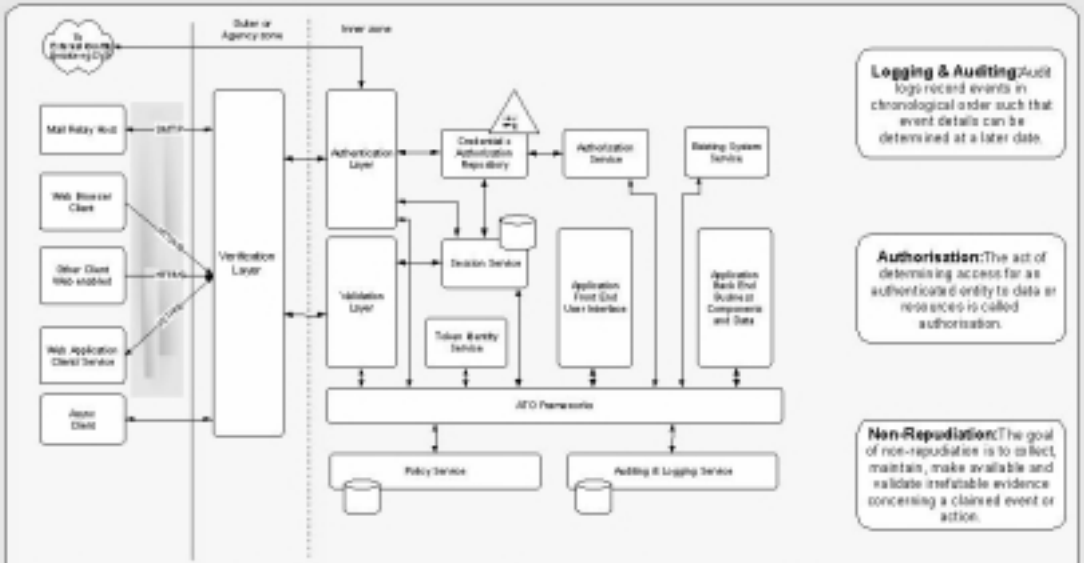
We live in a dynamic and very challenging environment. The ATO sees information security as essential to continued community confidence in our administration and see this as critical to the effective operation of the tax system.

We are satisfied that we have the necessary legislative and administrative frameworks including policies and guidelines in place. We are satisfied that we have the correct tools to help us comply with these frameworks. We are confident that we have the governance arrangements in place to ensure that we comply with our security obligations.

ATO Internet Security Framework (ISF)

Attachment A

Overview



Logging & Auditing: Audit logs record events in chronological order such that event details can be determined at a later date.

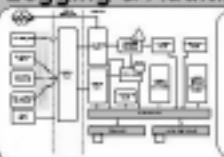
Authorisation: The act of determining access for an authenticated entity to data or resources is called authorisation.

Non-Repudiation: The goal of non-repudiation is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action.

Authentication: The process by which one entity verifies with another that they are who they claim to be. The claim is enforced by using credentials.

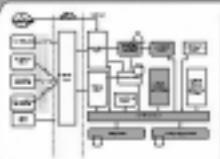
Confidentiality & Integrity is concerned with maintaining the privacy and reliability of data or information and is generally achieved on the Internet by utilising cryptographic technologies.

Logging & Auditing



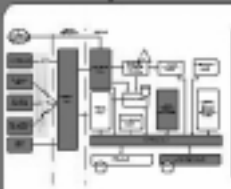
Auditing and Logging Service: The auditing and logging service provides transaction based logging. It allows transactions that span many systems to be coherently reconstructed for auditing purposes.
It also provides non-repudiation logging which captures and stores evidence about an entity's actions.
Security components and applications utilise the eATO frameworks to log events to this service.
The policy service enforces security and business rules for events that are logged to the service.

Authorisation



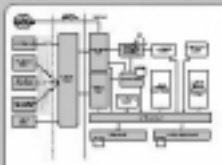
Authorisation: Once a request has been authenticated it may be processed by any number of application layers. The identity that is created as part of the authentication process is used by authorisation to determine access to resources.
The authorisation repository provides a centralised system for grouping user identities into roles.
Applications utilise the eATO frameworks to take advantage of the ISF authorisation capabilities.
The policy service supports authorisation by enforcing organisational authorisation rules.

Non-Repudiation



Non-repudiation: A number of ISF components work together to support non-repudiation.
At the client, when a critical action occurs, evidence is generated by a process. Typically by creating a digital signature.
The evidence is then transferred via the verification to the authentication layer where it is verified for integrity. The application also has the opportunity to verify the evidence.
The evidence and transaction data is then passed to the tamper proof auditing and logging service to store for later use.

Authentication



Web Browser Client: This represents an end user who uses web browser software to interact or transact with the ATO online environment. In business terms people who may use this are individuals, Tax Officers, Agency users and Intermediaries.

Other Client Web Enabled: This represents end user software that utilises web technologies to communicate but is not a web browser. Typically this is a piece of software like Quicken/ MYOB or a third party developed application.

Mail Relay Host: This component simply provides a relay facility for incoming secure Email. Acting as a gateway this component would scan for malicious content and could enforce policy on only allowing mail that contained secure content.

Web Application Client/ Service: This represents a piece of software running on a server. The software utilises web technologies to transact with the ATO. Typically web application clients would use SOAP/XML technologies.

Async Client: Client technology that allows asynchronous communications with the ATO. These clients typically use MQSeries or MSMQ transport technologies.

Auditing & Logging Service: see Auditing & Logging section.

Verification Layer: This layer processes incoming requests and messages to ensure that they conform to a set of security requirements. If they conform requests and messages are allowed to enter the Inner SAFER zone.

Session Service: The Session Service component creates, manages and verifies session tokens. Session tokens represent identities that have been previously authenticated at the authentication layer.

Authentication Layer: The Authentication layer undertakes the authentication process for incoming requests and messages. This is capable of supporting a number of different credentials. The process output adds an identity token to support authentication.

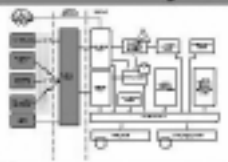
Credential and Authorization Repository: This represents the repository that holds identity credentials and how they are related to authorisation. This component also assists the session service by storing information that maps external credentials to ATO internal identities.

Validation Layer: The validation layer processes requests from users that have been previously authenticated. This layer uses authentication session tokens created by the session service. The process output adds an identity token to support authorisation.

ATO Frameworks: The ATO frameworks allows applications and security services to interoperate seamlessly.

Policy Service: Allows ATO security & business rules to be consistently applied to components of the security architecture.

Confidentiality & Integrity



Integrity: Where data traverses untrusted paths integrity mechanisms are implemented to ensure that data is not maliciously or unintentionally modified.
The ISF employs cryptographic technologies to ensure data maintains reliability across untrusted paths.

Async Link Confidentiality: Async clients in this situation rely upon a trusted network connection that utilises hardware encryption to secure data.
In the future transport across the internet will need to employ message encryption technologies.

Verification Layer & Confidentiality: This layer understands that information for specific resources must be kept confidential. It only accepts such information using specific guidelines.

Web Client Confidentiality: Internet where the security classification of data is rated at In-Confidence and below then SSL 3.0 is used.
Agency Link: Trusted network connections which implement hardware encryption are used in this case.

Mail Relay Confidentiality: As the mail relay host is not the originator of the mail message, the client who originates the mail must apply confidentiality technologies.
Typically with email S/MIME is used to allow sensitive data to traverse untrusted paths.

Attachment B - Glossary of terms

ABN	Australian Business Number
ABR	Australian Business Register
ANAO	Australian National Audit Office
ASCII	American Standard Code for Information Interchange. A coding scheme using 7 or 8 bits that assigns numeric values to up to 256 characters, including letters, numerals, punctuation marks, control characters and other symbols
ATO	Australian Taxation Office
ATOassist	ATOassist is the ATO's web site, available to the general public at www.ato.gov.au . It is based on a user-centred design. It aims to provide reliable information through intuitive navigation.
Authentication	The purpose of authentication is to prove the identity of the sender of a message.
BAS	Business Activity Statement
Browser	A software application which enables users to access the Internet.
Certificate	A certificate (also called a digital certificate) is sent when a message is digitally signed. The certificate proves the sender's identity and provides the public key used to decrypt the encrypted signature. Refer also to public key encryption.
CSA	Child Support Agency
e-commerce	(Electronic commerce) A method of conducting or managing business-related transactions using computer and telecommunications technology.
e-mail	(Electronic mail) A means to send messages, with or without documents or other information, electronically.
e-tax	(Electronic tax) e-tax is the ATO's Internet based income tax preparation and lodgment system.

Firewall	A security system intended to protect an organisation's network against external threats such as hackers coming from another network such as the Internet. Usually a firewall is a combination of hardware and software which prevents computers in the organisation's network from communicating directly with computers external to the network and vice versa. Instead all communication is routed through a proxy server outside the organisation's network. The proxy server decides whether it is safe to let a particular message or file pass through to the organisation's network.
FTB	Family Tax Benefit
Gatekeeper	Gatekeeper is the Commonwealth Government's Public Key Infrastructure (PKI) strategy. It was set up to provide a mechanism for the implementation of public key technology by Government agencies and enables agencies to choose from a panel of accredited service providers. The Gatekeeper Accreditation and Interoperability (cross recognition) processes ensure that the products and methods of delivery of accredited Certification Authorities (CAs) and Registration Authorities (RAs) comply with appropriate Commonwealth policies and meet prescribed Government standards for integrity and trust.
Gateway	A secured connection between an internal network and an external network such as the Internet.
Internet browser	A software application which enables users to access the Internet.
Internet Protocol Security (IPSec)	A security mechanism developed by the Internet Engineering Task Force to ensure secure packet exchanges at the IP layer. IPSec is based on two levels of security: AH (Authentication Header), which authenticates the sender and assures the recipient that the information has not been altered during transmission, and ESP (Encapsulating Security Protocol), which provides data encryption in addition to authentication and integrity assurance. IPSec protects all protocols in the TCP/IP protocol suite and Internet communications by using Layer Two Tunnelling Protocol and ensures secure transmissions over virtual private networks.

Internet	The world wide collection of networks and gateways that use the TCP/IP suite of protocols to communicate with one another. At the heart of the Internet is a backbone of high-speed data communication lines between major nodes or host computers consisting of thousands of commercial, Government, educational and other computer systems which route data and messages.
Intranet	A private network designed for information management within a company or organisation. An intranet uses the same technologies as the Internet but is strictly internal to the organisation. Some intranets offer access to the Internet, but such connections are directed through a firewall that protects the internal network from the external Internet
Intrusion Detection System	A type of security management system for computers and networks that gathers and analyses information from various areas within a computer or network to identify possible security breaches both inside and outside the organisation. An Intrusion Detection System can detect a wide range of hostile attack signatures, generate alarms and in some cases cause routers to terminate communications from hostile sources.
ICT	Information and communication technology
Keys	A set of two keys, one public and one private, as used in public key encryption.
local area network (LAN)	A group of computers and other devices, such as printers and large hard disks, dispersed over a relatively limited area and connected by a communications link that allows any device to interact with any other on the network.
Mainframe	A high-level, typically large and expensive computer designed to handle intensive computational tasks.
non-repudiation	Non-repudiation ensures that the sender of a message cannot later deny that they sent the message.
PAYG	Pay as You Go
public key encryption	An asymmetric scheme that uses a pair of keys for encryption: the public key encrypts data, and a corresponding private or secret key decrypts it.

Public Key Infrastructure (PKI)	A public key infrastructure enables users to exchange data securely and privately through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority. A PKI consists of • a certification authority (CA) that issues and verifies digital certificates to requestors; • a registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor; • one or more directories where the certificates, with their public keys, are held; and • a certificate management system.
RSA encryption	Rivest-Shamir-Adleman encryption – the public key encryption algorithm introduced by Ronald Rivest, Adi Shamir and Leonard Adleman in 1978.
Secure Sockets Layer	A protocol developed by Netscape Communications Corporation for ensuring security and privacy in Internet communications. Secure Sockets Layer uses public key encryption and supports authentication of client, server, or both, as well as encryption during a communications session.
TFN	Tax File Number
Virtual private network	Nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorised users as if the nodes were connected by private lines.
wide area network (WAN)	A geographically widespread network, that relies on communications capabilities to link the various network segments. A WAN can be one large network, or it can consist of a number of linked LANs (local area networks).
X.25	A recommendation published by the ITU-T international communications standards organisation that defines the connection between a terminal and a packet-switching network.

Attachment C - List of relevant source documents

ACSI 33

Australian Communications - Electronic Security Instruction 33 maintained by the Defence Signals Directorate. Commonwealth of Australia 2000. Available at www.dsd.gov.au/infosec/acsi33/acsi-index.html

ANAO *Better Practice Guide* – Internet Delivery Decisions

Commonwealth of Australia 2001. ISSN 1036-7632.
ISBN 0 642 44227 4.
AS/NZ 4360:1999

Australian/New Zealand Standard. Risk Management. Standards Australia 1999. ISBN 0-337-2647-X

This standard provides a generic guide for the establishment and implementation of the risk management process involving the identification, analysis, evaluation, treatment and ongoing monitoring of risks.

ATO End-to-End Internet Security Solution Design

Version 2.0, 29/10/2002, prepared by ATO Trusted Access ATEC. This solution recommends a full Public Key Infrastructure to supply confidentiality and integrity of client data transmitted over insecure public networks such as the Internet.

ATO End-to-End Security Architecture

Document number SEC0019, version 3.01, 10/10/2002, prepared by ATO Trusted Access ATEC.
Where clients are transmitting data over insecure public networks such as the Internet there is a need to protect the confidentiality and integrity of the data that is being transmitted. This document describes a security architecture which is intended to solve perceived Internet security problems.

ATO End-to-End Security Architecture Requirements

Document number SEC0113, version 3.01, 5/10/2002, prepared by ATO Trusted Access ATEC.
This document describes the requirements of an end to end security architecture for the ATO and its business systems that are directly or indirectly accessed via Internet technologies.

ATO Security Risk Management Plan

This document details how the ATO deals with identified internal risks related to privacy, confidentiality & integrity of the ATO's electronic data.

Certificate Policy Statement for the ATO OCA

Section 2.8 of this document deals with confidentiality and privacy in relation to Public Key Infrastructure.

Commonwealth Protective Security Manual

ISBN 0 642 45506 6
Published 1991, Reprinted November 1991

The purpose of the Protective Security Manual (PSM) is to provide general guidance and broad advice on protective security matters.

Defence in Depth Strategy

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/windows/windows2000/staysecure/secops02.asp

Defence Signals Directorate Australian Communications-Electronic security instruction 33

http://www.dsd.gov.au/infosec/acsi33/acsi_index.html

Evaluated Products List

Produced by Defence Signals Directorate's
Information Security Group (2002)

It provides information about products evaluated and certified under the Australasia, UK, Canadian, French, German an US schemes. Products listed have undergone a process of detailed examination of their security features to ensure they work correctly and effectively.

ISO 17799/2001

Information technology – Code of practice for information security management. Standard published by the International Organization for Standardization (ISO).
This standard provides recommendations for information security management for use by those who are responsible for initiating, implementing of maintaining security in their organisation.

IT security policy and guidelines 2002

The Information Technology (IT) Security Policy has been developed by the ATO's Trusted Access Branch (ATA) to ensure the protection of IT hardware and software associated with this information.

IT security policy 2001

IT Sub Plan Risk Statement

The main risks for IT Security are identified in the IT Sub Plan Statement. These risks being inappropriate integrated controls on ATO IT sub systems and increasing exposure to security breaches through expanded e-commerce functionality.

Office of the Privacy Commissioner

http://www.privacy.gov.au/index.asp

Proof of Identify

Proof of Identity (POI) documentation - Policy
This policy advises ATO staff of acceptable documentation to determine an individual client's 'proof of identity.

Proper use policy for ATO
The Proper Use of Information Technology Facilities

This policy describes the conditions under which ATO technology (IT) facilities maybe used.
Policy endorsed 30 May 2001

Secure ATO Firewall Environment (SAFE) - Gateway Security Management

Gateway Security Management Policy for the Secure ATO Firewall Environment (SAFE). This document describes how the Gateway is managed.

Security policy and services - physical security design brief

This is a pro forma document indicating the various criteria considered in the process of conducting a physical security assessment.

Service Agreement for provision of Lodgment Compliance Services for the Child Support Agency by the Client Account Management, Receivables Management, ATO

These guidelines have been developed to assist Child Support Agency staff identify and refer cases to the ATO, Client Account Management Lodgement Enforcement section to obtain lodgement of tax returns.

Use of Data Matching in Commonwealth Administration – Guidelines

The guidelines provide the following:

- A summary of process
- Requirements for programs not covered by the guidelines
- Data-matching with non-Commonwealth organizations
- Programs inconsistent with the requirements of the guidelines

WGS02 ATO Web Centre Gateway Security - Security Policy

This document describes security requirements for confidentiality, integrity, availability, accountability and evolving technology. (WGS02)
5 June 2001
Prepared by E Security.

WGS03 ATO Web Centre Gateway Security - Security Plan

ATO Web Centre Gateway Security Plan (WGS03)
18 June 2001
Prepared by: E Security

The security plan describes the practices to ensure the security and integrity of the AWC environment, including the establishment of standards of all ATO BSL Web Development Projects that will utilize – in part or in full – functionality of the AWC.

ATO PKI certificate policy documentation

ATO PKI Infrastructure: Guidelines for Agencies using PKI to communicate or transact with individuals.
Prepared by: The office of the Federal Privacy Commissioner, December 2001.

This paper and the guidelines it includes, compliment the standards of the Privacy Act by addressing the privacy issues that are specific to PKI.

http://www.ato-pki.ato.gov.au

PKI Gatekeeper accreditation documentation

Conditions of Use (CO01)

Certificate Policy Statement for Non Individual Type 2, Grade 2 Certificates (PO01)

Certificate Policy Statement for the ATO CA, ATO OCA, and for Keys and Certificates Issued and Used by Other Parts of the ATO PKI (PO01a)

Certificate Practice Statement for the ATO PKI (PO02)

Policy Management Authority (PMA)

Glossary

Personal information and privacy principles for Gatekeeper Accreditation

Manner and Extent of Collection of Personal Information (PC01)

Security safeguards in relation to personal information (PC02)

Openness About the Types of Information Held and Holding Policies (PC03)

Procedures for correction of personal information by subjects (PC04)

Accuracy of personal information (PC05)

Personal information is used only for relevant purposes (PC06)

Limits placed on the use of personal information (PC07)

Limits placed on disclosure of personal information (PC08)

Privacy protection for publicly accessible information (PC09)