Department of Finance and Deregulation

Australian Government Information Management Office

GATEKEEPER PKI FRAMEWORK

THREAT AND RISK ASSESSMENT TEMPLATE

February 2009

Department of Finance and Deregulation

Australian Government Information Management Office

CONTENTS

1 OVERVIEW

1.1 Threat and Risk Assessment and Public Key Infrastructure

This document provides a template for conducting a Threat and Risk Assessment (TRA) in a Public Key Infrastructure (PKI) deployment. It outlines a standardised set of general threats that may be encountered.

Threats in PKI deployments fall into seven main categories. They are failures of:

underlying EOI

the Registration process

the Certificate production process

the user Key media

the application software using Keys and Certificates

the user's security and business processes for Certificate management and use; and

the infrastructure supporting Certificate management and use.

In general, broad strategies can be applied to address these threats collectively. The broad risk management measures that are available include:

- procedural controls;
- personnel controls;
- financial controls;
- technological controls; and
- development quality controls.

This document includes a list and description of the main categories of risk in PKI that can be used as a template structure for a Gatekeeper TRA. It also contains some suggested risk management measures that can be considered during the TRA process.

All Gatekeeper documents referenced in this document are available at www.gatekeeper.gov.au

1.2 Mandatory Threat and Risk Assessments

Under the Gatekeeper PKI Framework, the conduct of a TRA is generally considered best practice for all categories of digital certificates, where new PKI deployments are being considered or where existing deployments are subject to major changes.

The conduct and submission of a TRA is *mandatory* for Listing as a Threat and Risk Organisation (TRO) under the Gatekeeper PKI Framework.

Where an Organisation wishes to utilise the Threat and Risk Assessment Evidence of Identity Model in the General Category, it must conduct a Threat and Risk Assessment and submit this to the

Gatekeeper Competent Authority for approval in order to become Listed as a Threat and Risk Organisation.

See Appendix 1 for the Threat and Risk Assessment template for compliance with the Threat and Risk Organisations Listing Requirements.

The TRA for TROs (Appendix 1) is designed to measure whether or not the Evidence of Identity (EOI) processes utilised in that particular PKI deployment meet the test of EOI assurance in the General Category. The test is whether the EOI Assurance level is equivalent from a risk perspective to the EOI assurance provided by the Formal Identity Verification EOI Model. Appendix 3 – Threat and Risk Assessment Checklist contains a checklist for use by Organisations ensuring that all relevant issues have been identified and addressed.

1.3 TRA methodologies

This template does not impose a particular TRA methodology, but instead seeks to provide a comprehensive list of issues to be considered by implementers.

Most TRAs in Australia are performed using customised TRA tools, processes and methodologies that are broadly adapted from the Australian Risk Management Standard (AS 4360:2004). It is a relatively straightforward task to add the threat categories contained in this template to such tools and processes.

A common format for TRAs of this type is:

Threat Source	Threat	Risk Likelihood	Risk Impact	Risk Rating	Risk Management Measure

Agencies or Organisations conducting a TRA may choose to include a “residual risk” column in this Table. This column would measure residual risk after management measures have been conducted. This step does sometimes form part of an AS 4360 methodology.

A TRA should use a common approach to the assessment of risk likelihood and risk impact. Numerous individual methodologies based on AS 4360 have been developed. Gatekeeper does not mandate a particular methodology. Samples of Risk Management methodologies based on AS 4360 are provided in this document at Appendix 2 – Risk Management Methodologies.

2 GENERIC THREATS IN PKI

2.1 Underlying Evidence of Identity

2.1.1 Inappropriate EOI

The number of EOI documentation or the EOI process may be inappropriate in comparison with the risk of applications and transactions that are intended to be performed using the digital certificate. This may result from a flaw in either the EOI Assurance process or a flaw in the design and description of the digital

certificate purpose (e.g. in the Certificate Policy).

2.1.2 Accidental submission

Accidental submission of inaccurate identification documents and information by the applicant may be a threat in some circumstances.

2.1.3 Deliberate submission

Deliberate submission of fraudulent identification documents and information by the applicant will be a common threat. In most categories of Gatekeeper this would involve the presentation of false EOI documents. In relation to some Gatekeeper Relationship Certificates, this might also involve fraudulent membership of a community of interest or the presentation of fraudulent credentials.

2.1.4 Failure of proper checks

Staff may accidentally fail to perform proper checks resulting in acceptance of inaccurate identification documents and information. Staff may not be appropriately trained to recognise submitted false or inaccurate EOI documents.

2.1.5 Staff collusion

Staff may deliberately collude with the applicant resulting in acceptance of false EOI documents.

2.1.6 Poor records

Loss of, or poor record keeping and certification may compromise the production and quality of evidence at a later date for legal purposes.

2.2 Registration

2.2.1 Data entry mistake by the RA operator

It is possible that a RA operator may enter incorrect data.

2.2.2 Interception

Whenever a credential is 'pushed out' (for example under the Relationship Certificate model), there is the possibility that it falls into the wrong hands and is subsequently abused.

Technical and procedural security protecting credentials being pushed out may be inadequate to prevent misuse in the event of interception. This type of threat might be addressed with a two-stage activation process. For example, smartcards could be distributed in an inactive state, and only activated after additional application controls that may detect misuse.

2.2.3 Corrupt a member database

In relation to some digital certificates (e.g. Relationship Certificates and Known Customer Certificates), subjects may be automatically registered from an existing membership database and their certificates automatically populated. The possibility that the database contains errors, either by accident or by design of a fraudster, must be considered.

2.2.4 Social engineering attack on the RA operator

A fraudster can possibly obtain a fraudulent digital certificate by bribing, corrupting or otherwise misleading the RA operator, resulting in a fraudulent

digital certificate request.

2.2.5 Social engineering attack on the Help Desk

Where certificates are subject to PIN protection, a fraudster might obtain the digital certificate, and then attempt to have the PIN reset to a value of their choosing by misleading the Help Desk.

2.2.6 Subject fails to revoke

If a digital certificate Subject (i.e. Subscriber or Key Holder) loses control of his/her Private Key such that it may fall into the wrong hands, or if he/she suspects his/her Private Key may have been compromised, then the Subject is required in general to request that his/her certificate be revoked. If a Subject fails to request revocation (or fails to do so in a timely manner) then there is a window of opportunity in which the Private Key might potentially be abused.

2.2.7 Other failures to revoke

In relation to some digital certificates (e.g. Relationship Certificates and Digital Credentials) there may be some additional risks in relation to suspension of credentials or termination of membership (for example, because the Subject's qualifications are withdrawn, they are sacked, or they otherwise fail to meet legitimate requirements imposed by their Organisation). In these circumstances, the relevant authority or Community of Interest is required in general to request the digital certificate to be revoked.

If the relevant administrator fails to request revocation (or fails to do so in a timely manner) then there is a window of opportunity in which the Subject's Private Key might potentially be abused.

2.3 Certificate production

2.3.1 Spoofing the RA

If a fraudulent digital certificate request were to be generated by an attacker and injected into the communication channel between the CA and one of its RAs, then counterfeit certificates could in principle be created. Denial of Service attacks can similarly be mounted if fake revocations can be injected into the CA.

A RA can be spoofed by synthesising digital certificate requests, or by "imaging" a RA workstation and replicating it on an attacker's machine.

2.3.2 Duplicate the CA

The CA could be duplicated ("imaged") by an attacker so as to create any number of counterfeit digital certificates.

2.3.3 Corrupt the CA operation

If the CA operation could be subverted, then an attacker might be able to create counterfeit certificates without spoofing legitimate requests.

There could also be a Denial of Service attack against the CA or compromise of its integrity through unauthorised access.

2.3.4 Social engineering attack on CA staff

Operators at a CA might be bribed, corrupted or otherwise misled into creating counterfeit digital certificates directly at the CA server.

2.3.5 Revocation request is not actioned in a timely manner

There are scenarios where a revocation request is issued appropriately but fails to be actioned by the CA (for example, due to a technical communications breakdown).

2.4 Key media

2.4.1 Private Key is obtained and misused

If the Private Key of a digital certificate Subject is obtained by someone else, that person may be able to act on behalf of the Subject, without authorisation. A Private Key may in principle be obtained by stealing the Subject's Key media or by retrieving a copy of the Private Key from the media in which it is held.

In general, hardware media are more resistant to theft than software media, if only because the Subject is generally in a better position to realise when the Key has been lost or stolen. In addition, hardware media can usually be PIN protected.

2.4.2 Private Key unavailable because of media failure

Damage can arise if an important transaction cannot be undertaken because at the desired time the user cannot access his/her Private Key due to media failure (or sabotage). This applies not only to the media on which the Private Key is stored, but any hardware in which this media is contained.

2.4.3 Private Key lost because of user error

Damage can arise if the user loses his/her Private Key media or the availability of associated hardware and is unable to use his/her Key at a critical time.

2.4.4 Relying application fails to check revocation status

While revocation is required under various circumstances, it is generally the responsibility of any Relying Party that relies upon a digital certificate to check the status of that digital certificate before accepting an associated transaction. Relying Party application software may fail to do so for a number of reasons, including design or programming error.

2.4.5 Relying application cannot reach revocation status

In general, authoritative revocation status information is held at the CA and is accessed by Relying Parties either by downloading the Certificate Revocation List (CRL) or by sending a real time Online Certificate Status Protocol (OCSP) inquiry. It is possible that due to a communications outage, for example, Relying Party software cannot access revocation information at a particular instance and might therefore suffer from misuse of a digital certificate that was in fact revoked at the time.

2.4.6 Relying application fails to correctly validate certificate path

Digital certificates chain back through a series of certificate issuers to terminate at a "trust anchor". The digital certificate pathway should in general be checked by Relying Party software to make sure that all issuers are valid, and that the trust anchor has not been tampered with. There are a number of actual as well as theoretical cases where an attacker can corrupt the certificate path so as to insinuate a fraudulent digital certificate into a transaction.

2.4.7 User and Relying Party Business Procedures

Users and issuers may establish inadequate procedures to ensure that only they have access and use of their digital certificate.

2.4.8 Supporting Infrastructure

The security of the hardware and the networks crucial to provide PKI services must be considered to ensure that they are kept available, and that confidentiality and integrity of essential data is maintained.

2.4.9 Loss of availability of critical hardware

An event could occur to make critical business applications and/or networks unavailable. This could affect the availability of any number of vital components of the PKI's operational software and hardware, including the CA database, CRLs and the X.500 directory or any other mechanism by which certificates are made available.

2.4.10 Compromise of devices used for Key Management

The compromise of systems used for Key management presents the possibility for private Key data to be obtained by an unauthorised entity, or the ability to compromise Key systems related to the management of Key information. This threat must also be considered not only for operational machines, but also data stored on backup media. Compromise of hardware could also facilitate other threats previously described, giving the ability to affect the confidentiality, integrity and availability of PKI infrastructure.

GENERIC RISK MITIGATION MEASURES IN PKI

3.1 Underlying EOI

3.1.1 Inappropriate EOI

- Risk rating.

3.1.2 Accidental submission

- Risk rating
- Duplication checks
- Matching
- Random sample checking.

3.1.3 Deliberate submission

- Risk rating
- Duplication checks
- Matching
- Random sample checking.

3.1.4 Failure of proper checks

- Post transaction integrity controls
- Secondary checks
- Random sample checking.

3.1.5 Staff collusion

- Vetted operations staff, background checks, strict HR policies
- Post transaction integrity controls
- Secondary checks
- Random sample checking.

3.2 Registration

3.2.1 RA operator procedures

- Good documentation of RA operations
- Secondary checks.

3.2.2 RA personnel security

- RA operators should be resistant to corruption
- Logging, auditability.

3.2.3 RA physical security

- Access to RA operator workstations should be restricted.

3.2.4 RA logical security

- RA operator workstations should be protected against misuse, through logical access controls (perhaps two factor authentication)
- Strong authentication of RA operators
- Digitally sign all digital certificate requests.

3.2.5 Key activation

- Take extra steps to activate Keys/Certificates (especially under push distribution models) so that if a Key falls into the wrong hands, it might not be usable.

3.3 Certificate production

A reasonable working assumption seems to be that all backend related threats and risks are adequately addressed by Gatekeeper's suite of Accreditation criteria which emphasise physical, logical and personnel security. It may therefore not be necessary to conduct an additional comprehensive TRA against these risks.

3.3.1 CA physical security

- [Gatekeeper Accreditation and ongoing audit]
- Physical security standards, perimeter security, monitoring, guards
- Secure network design, defence in depth, segmentation etc.
- High availability Internet connection
- Redundant electricity, telecommunications supplies.

3.3.2 CA technological security

- [Gatekeeper Accreditation and ongoing audit]
- Hardware security modules to protect CA Private Key, Root Private Key etc.
- Common Criteria or similar certification of CA, against accepted target of evaluation.

3.3.3 CA procedural security

- [Gatekeeper Accreditation and ongoing audit]
- Two person access controls over critical modules, such as private Keys
- Key generation ceremonies
- Event logging and regular audit.

3.3.4 CA personnel security

- [Gatekeeper Accreditation and ongoing audit]
- Vetted operations staff, background checks, strict HR policies.

3.3.5 CA financial security

- [Gatekeeper Accreditation and ongoing audit]
- Vetted management staff.

3.4 Key media

3.4.1 Choice of Key media

- Consider hardware tokens
- Loss evident
- Private Keys harder to extract
- Hardware Key generation less corruptible, especially when private Key retained inside hardware
- Certification of tamper resistance and of cryptographic quality (e.g. FIPS 140).

3.4.2 Password protection

- To limit damage if media falls into the wrong hands
- Strength/weakness of proposed passwords.

3.4.3 Contractual measures

- Prohibitions on sharing Keys or allowing a third party to use the Keys.

3.5 Application software

3.5.1 Relying application fails to check revocation status

- Good documentation and specifications
- Software development quality controls, design review, code inspection, testing
- Security certification.

3.5.2 Relying application cannot reach revocation status

- Good documentation and specifications
- Software development quality controls, design review, code inspection, testing
- Security certification.

3.5.3 Relying application fails to correctly validate certificate path

- Good documentation and specifications
- Software development quality controls, design review, code inspection, testing
- Security certification.

3.6 User and Relying Party Business Procedures

- Contractual requirements for technical and procedural security over certificates and Keys

- Education of users and relying parties.

3.7 Supporting Infrastructure

3.7.1 Loss of availability of critical hardware

- [Gatekeeper Accreditation and ongoing audit]
- Implement business continuity and recovery plans to deal with outages
- Design networks to include redundancy for increased availability.

3.7.2 Compromise of devices used for Key management

- [Gatekeeper Accreditation and ongoing audit]
- Hardware modules in place to protect vital network components, including CA Private Key, Root Key, etc.
- Secure network hosts through patching and other software security measures
- Utilise logging and auditing to detect compromise, and incident response procedures for dealing with any detected incidents
- Appropriate training and management to ensure network and host security is maintained.

4

Appendix 1 – General Certificates TRA Template

4.1 Objective of the TRA

Under the Gatekeeper PKI Framework, the submission of a TRA is ***mandatory*** where an Organisation wishes to utilise the TRA EOI Model in the General Category. The Organisation must conduct an independent TRA and submit this to the Gatekeeper Competent Authority for approval. This Appendix focuses solely on the EOI TRA that must be conducted for Listing as a Threat and Risk Organisation.

This TRA is designed to measure whether or not the EOI processes utilised in that particular PKI deployment meet the test of EOI Assurance in the General Category.

The following headings and supporting information provides guidance for how the TRA document should be written.

The TRA for an Organisation seeking to be listed as a Threat and Risk Organisation will be performed by a member of the Gatekeeper Audit Panel, selected by the Organisation seeking listing as a Threat and Risk Organisation. All costs incurred in conducting the TRA will be met by the Organisation.

4.2 Description of the PKI Deployment

In this section the TRA would include a broad description of the PKI deployment being assessed, including the main participants and the objectives of the deployment.

For the purpose of the TRA it will be important to determine two Key factors:

- **Target assets**
  These are the assets that require protection in the PKI deployment. They may be Individual applications, transactions or data sets. More broadly, assets include the reputation and operation of projects, programs or entire Agencies.
- **Target period**
  In order to determine the likelihood of a risk occurring, a target period must be defined. In PKI deployments this is typically a very long period, as PKI is designed to enable checks against data over a substantial period of time.

4.3 Description of the EOI Assurance Model

In this section the TRA would include a broad description of the EOI Assurance Model for the PKI deployment. The description would include details of the level of EOI in the following categories:

- Face-to-face checks;
- current photograph;
- signature matching;

- EOI documents presented;
- referees;
- background checks;
- pre-population or matching from other internal data sets; and
- pre-population or matching from external data sets.

4.4 Description of post transaction integrity controls

In this section, the TRA would include a broad description of the post transaction integrity controls that were utilised (or available) for the EOI Assurance Model. These checks will vary greatly from Organisation to Organisation, but a starting list might include:

- additional background checks or referee requests;
- duplication checks (checking for duplicate names, numbers photos or other entries);
- matching (to internal and external data); and
- random sample checking (for accuracy and completeness).

In some deployments, a form of risk rating may also be implemented. This would result in additional post transaction integrity checks being undertaken for applicants in pre-identified high-risk categories.

4.5 Risk assessment for underlying EOI

In PKI deployments, risks can occur at multiple stages of the deployment. However, for the purposes of an EOI Assurance, TRA in the General Certificate Category, only the underlying EOI checks are relevant.

There are five specific risk categories in the underlying EOI in a PKI deployment.

This template TRA provides guidance about the main types of risk in each category, and some suggested risk management measures that might be considered.

4.5.1 Inappropriate EOI

Threat Source	Threat	Risk Likelihood	Risk Impact	Risk Rating	Risk Management Measure

Inappropriate EOI	The level of EOI documentation or the EOI process may be inappropriate in comparison with the risk of applications and transactions that can be performed using the Certificate.		Dependant on the nature of the application or specific high-risk transactions.		Risk rating process - This involves pre-determining the risk of particular categories of applicants and requiring EOI documentation or processes that are appropriate to that risk. This can sometimes be a mix of risk rating tools rather than a single risk rating process.

4.5.2 Accidental submission

Threat Source	Threat	Risk Likelihood	Risk Impact	Risk Rating	Risk Management Measure

Accidental submission	Accidental submission of inaccurate identification documents and information by the applicant may be a threat in some circumstances.	Reduced for face to face submission	Often only results in inconvenience or need for re-entry – low risk of fraud. Somewhat dependant on the nature of the application or specific high-risk transactions.		Risk rating process Duplication checks (checking for duplicate names, numbers photos or other entries). Matching to internal or external data sets. Random sample checking.

4.5.3 Deliberate submission

Threat Source	Threat	Risk Likelihood	Risk Impact	Risk Rating	Risk Management Measure
Deliberate submission	Deliberate submission of fraudulent identification documents and information.	Dependant on the nature of the application or specific high-risk transactions.	Likely to be high as the intention is to commit fraud. Dependant on the nature of the application or specific high-risk transactions.		Risk rating process Duplication checks (checking for duplicate names, numbers photos or other entries). Matching to internal or external data sets. Random sample checking.

4.5.4 Failure of proper checks

Threat Source	Threat	Risk Likelihood	Risk Impact	Risk Rating	Risk Management Measure

Failure of proper checks	Staff may accidentally fail to perform proper checks resulting in acceptance of inaccurate identification documents and information. Staff may not be appropriately trained to recognise submitted false or inaccurate EOI documents.	Can be higher for new deploy ments.	Likely to be high as a possibl e intentio n is fraud. Somew hat depend ant on the nature of the applicat ion or specific high-risk transact ions.		Staff training. Documentation of processes. Duplication checks (checking for duplicate names, numbers photos or other entries). Matching to internal or external data sets. Random sample checking by a person other than the staff member who initially performed the checks.
					Secondary checks (e.g. for new staff or staff assigned to new roles).

4.5.5 Staff collusion

Threat Source	Threat	Risk Likelih ood	Risk Impact	Risk Rating	Risk Management Measure

Staff collusion	Staff may deliberately collude with the applicant resulting in acceptance of false EOI documents.	Somewhat dependant on the nature of the application or specific high-risk transactions.	Somewhat dependant on the nature of the application or specific high-risk transactions. Note: Impact can be very broad due to reputation damage if staff collusion is revealed.		Vetted operations staff. Strict HR policies. Transaction logging. Secondary checks. Random sample checking by a person other than the staff member who initially performed the checks.

4.5.6 User and Relying Party Business Procedures

Threat Source	Threat	Risk Likelihood	Risk Impact	Risk Rating	Risk Management Measure

Adequacy of Subscriber and Relying Party Business Processes.	Security practices of the Subscriber and Relying Party may leave Certificates accessible by other staff members. Staff members and management may informally allow sharing of Certificates.	Somewhat depends on the Organisation's security culture and other variables such as size, number of staff involved etc. In general the likelihood is expected to be high.	Somewhat dependant on the nature of the application or specific high-risk Transactions. However, it will invalidate, the Certificates once uncovered and reduces the assurance that can be had for non-repudiation purposes.		Specific clauses within policy statements and Subscriber agreements. Continuing education. Best practice/ benchmarking. Audit checks by the Subscriber and Relying Party.

4.6 Comparison with Formal Identity Verification Model

The final step in the TRA for the General Certificate Category is a comparison with the Formal Identity Verification EOI Model and in particular the requirements to meet the bindings as set out in the Gatekeeper EOI Policy.

5 Appendix 2 – Risk Management Methodologies

A TRA should use a common approach to the assessment of risk likelihood and risk impact. Numerous Individual methodologies based on AS 4360 have been developed, as the standard has been interpreted in a variety of ways.

Samples of Risk Management methodologies based on AS 4360 are provided below.

5.1 Risk Likelihood

The following table is a typical example of an AS 4360 risk likelihood assessment tool that indicates quantitative measures of likelihood, i.e. the

probability of a given threat or opportunity occurring.

In some Individual methodologies these tools also include an exact probability in the form of a percentage score (e.g. level 3 is represented by a 50% probability; level 5 is presented by a 100% probability).

Rating		Likelihood of Occurrence
Almost Certain	**5**	The threat ***is expected to occur*** within the target period
Likely	**4**	The threat ***is likely*** to occur within the target period
Possible	**3**	The threat ***may occur*** within the target period
Unlikely	**2**	The threat ***could occur some time*** in the target period
Rare	**1**	The threat ***may occur in exceptional circumstances***

5.2 Risk Consequence

The following table indicates qualitative measures of impact, i.e. the specific damage or consequence to a PKI Deployment of a given threat occurring. (Note: this sample table is customised for an Agency application. The consequences may be slightly different for private sector Organisations.)

If the consequences would	Then an appropriate consequence rating is
Threaten the survival of not only the program but also the agency, possibly causing major problems for Clients and for a large part of the Australian Public Service	**Catastrophic**
Threaten the survival or continued effective function of the program or project and require top level management or ministerial intervention	**Major**
Not threaten the program but would mean that the program could be subject to significant review or changed ways of operating	**Moderate**
Threaten the efficiency or effectiveness of some aspect of the program but would be dealt with internally	**Minor**
Negligible impact on the program or the reputation of the agency	**Insignificant**

5.3 Risk Analysis Matrix

By combining the Likelihood and the Impact rating, the following risk analysis matrix is achieved. (In this sample matrix the scores are represented by colours and numeric values – in some methodologies the matrix scores are represented as letters.)

Likelihood **Impact**	**Rare (1)**	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Almost Certain (5)**
Catastrophic (5)	**5**	**10**	**15**	**20**	**25**

Major (4)	**4**	**8**	**12**	**16**	**20**
Moderate (3)	**3**	**6**	**9**	**12**	**15**
Minor (2)	**2**	**4**	**6**	**8**	**10**
Insignificant (1)	**1**	**2**	**3**	**4**	**5**

The following table explains the legend used in this sample risk analysis matrix:

Risk	Required Actions
Extreme Risk	**Significant Risk** – Immediate treatment required.
High Risk	**Significant Risk** – Treatment required as high priority.
Moderate Risk	**Accepted Risk** – Manage by specific monitoring or response procedures, with management responsibility specified and strategies implemented as part of day-to-day project management.
Low Risk	**Rejected Risk** – Manage and monitor by routine internal procedures.

Appendix 3 – Threat and Risk Assessment Checklist

6.1 Background Information

This information is to be provided by the Organisation seeking Listing as a Gatekeeper Threat and Risk Organisation to the Authorised Auditor conducting the TRA. Its purpose is to provide a basic overview of the Organisation's identity management practices against which the TRA will be conducted.

- Are there legislative requirements for EOI collection – yes / no
  - If yes, what are key provisions in relation to establishing identity of Clients?
  - If no, are there other enforceable requirements (e.g. cabinet decisions)?
    - If yes, what are the enforceable requirements?
- What policies and practices are employed to manage identity fraud?
- Does the Organisation have a publicly available Privacy Policy?
  - If yes – where is it available, (e.g. on the website, desktops, printed copies distributed to staff)?
- What are the security arrangements (physical logical personnel) relating to the Organisation's EOI / transaction data holdings?
- Does the Organisation maintain an up to date risk assessment matrix in relation to EOI / authentication as a basis for enabling on-line transactions?

6.2 Checklist – Evidence of Identity and Data Management

The following is a checklist of questions that should be asked when establishing the nature and integrity of the Organisation's EOI and data management processes. It is provided as a guide only, however, the Organisation undergoing the TRA must be able to demonstrate that all the issues identified below have been satisfactorily addressed.

The threats and risks identified as a result of completing this checklist (together with the identified risk mitigation measures) should then be subject to the risk assessment methodology set out in Section 3.

6.3

Does the Organisation Perform an Initial Client Identification?

If YES how is the initial identification made?

EOI DOCUMENTS

- Which documents must be submitted?
- Is a document list prescribed?
  - List documents prescribed/acceptable
- Is a current photograph required?
- Do its EOI processes comply with the Gatekeeper EOI Policy?
- Is the Client's signature required to be verified?
- How are exceptions managed (e.g. Individuals unable to present documentation)?
- How are documents submitted?
  - Mail
  - Email
  - Over the counter
  - Via third party
- Are originals required?

FACE-TO-FACE

- Does the Organisation conduct a face-to-face interview?
- Is training provided to staff by the Organisation in relation to identifying fraudulent identity documents submitted by Clients?

OTHER PROCESS

- What process does the Organisation use to initially identify the Client?
  - Third party references (data sharing)
  - Use of approved referees

If none of the above, what process does the Organisation employ to establish the identity of the Individual?

If the Client is an Organisation/business represented by an Individual, is the Organisation/business identified?

If YES

- How is the Organisation/business identified?
- Is the relationship between the Individual and the Organisation/ business established?

If YES

- How is the relationship established?

- Is authorisation required to establish the relationship?

If YES

- Who provides the authorisation?
- How is the authorisation provided?
- Is the authoriser identified?

6.4 Is the Client Issued a Unique Credential (e.g. Token, number) once Enrolled/Registered?

If YES

- Is the credential bound to the Individual?
- Does the credential become the sole basis for identifying Individuals in subsequent interactions?
  - If NO, are additional authentication processes employed?
- Is the credential intended to be used as the sole basis for issuance of a digital certificate?
  - If NO, is there a subsequent EOI check or authentication process for the issuance of a digital certificate?

6.5 Is EOI Information/Client Record Maintained by the Organisation?

If YES

- Where is the information stored?
- How is the information stored?
- What security/access controls are in place for the protection of EOI data?
- Do Individuals handling the EOI data have the appropriate security clearances?
- Does the Organisation have designated staff for collecting/handling/storing/retrieving EOI data?
- Are duplications checks conducted?
- Does the Organisation update policies (e.g. name, addresses)
- Does the Organisation conducted data cleansing?
  - How often is data cleansing conducted?
  - Does data cleansing involve cross checks (verification) with other agencies?
- Does the Client have access to its personal records in order to update information?

6.6 Does the Organisation Maintain a Transaction History for Each Client?

If YES

- Is the frequency of the transactions regular?
- What kind of transactions does this include?
- Does the Organisation conduct cross checks with past transactions?

6.7 Does the Organisation Maintain a Published Privacy Policy?

If YES

- Is the Privacy Policy publicly available?
- Does the Policy comply with Gatekeeper privacy requirements?