RISK ANALYSIS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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. |
|  | | | | | |
| **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. |
| **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. |
|  | | | | | |
| **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 deployments. | Likely to be high as a possible intention is fraud.  Somewhat dependant on the nature of the application or specific high-risk transactions. |  | 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. |
| **Staff collusion** | | | | | |
| **Threat Source** | **Threat** | **Risk Likelihood** | **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. |
|  | | | | | |
| **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. |