1.1 Risk Assessment

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.

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

A common format for TRAs of this type is:

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