The CORAS Tool supports the CORAS methodology for model based security risk assessment, combining established methods for risk assessment and modelling techniques like UML with domain knowledge from the security field. The CORAS Tool is open source and freely available at: http://coras.sourceforge.net/

The methodology explained

1. **Context Identification**
   - Activity 1.1: Identify areas of relevance
   - Activity 1.2: Identify and value assets
   - Activity 1.3: Identify policies and risk evaluation criteria
   - Activity 1.4: Approval

2. **Risk Identification**
   - Activity 2.1: Identify threats to assets
   - Activity 2.2: Identify vulnerabilities of assets
   - Activity 2.3: Document unwanted incidents

3. **Consequence Evaluation**
   - Activity 3.1: Consequence evaluation

4. **Frequency Evaluation**
   - Activity 4.1: Frequency evaluation

5. **Risk Evaluation**
   - Activity 5.1: Determine level of risk
   - Activity 5.2: Prioritise risks
   - Activity 5.3: Categorise risks into risk themes
   - Activity 5.4: Determine interrelationships among risk themes
   - Activity 5.5: Prioritise the resulting risk themes

6. **Risk Treatment**
   - Activity 6.1: Identify treatment options
   - Activity 6.2: Assess alternative treatment approaches

The CORAS Tool provides the end user with administrative functionality, such as creating new security risk assessment projects and managing the reusable experience packages. Many entities of a security risk assessment, e.g. assets, stakeholders and threats, appear in several different assessment documents, tables and forms. It is therefore important to ensure that the various elements of the documentation are mutually consistent with regards to these entities. The CORAS Tool contains functionality for carrying out consistency checks for the stored data.

A wide variety of UML modelling tools and risk analysis tools are in use by security analysts and system engineers. The CORAS Tool provides flexible support for integration with such external tools. The CORAS Tool offers an integration layer with a well defined API to facilitate integration of external tools, utilising standardised XML formats for data integration.

The CORAS Tool is based on XML data formats, such as XMI for the interchange of UML models. The CORAS Tool contains two repositories for documenting risk assessment results and reusable experiences, which are implemented on top of the open-source XML database eXist.

Documentation of Risk Assessment results

Documentation of Risk Assessment experiences

Assessment Repository (AR)
documents completed risk assessments and risk assessments in progress.

Reusable Elements Repository (RER)
contains reusable elements represented in the XML format, which help the risk analyst document future assessment.

The CORAS Tool provides the end user with administrative functionality, such as creating new security risk assessment projects and managing the reusable experience packages. Many entities of a security risk assessment, e.g. assets, stakeholders and threats, appear in several different assessment documents, tables and forms. It is therefore important to ensure that the various elements of the documentation are mutually consistent with regards to these entities. The CORAS Tool contains functionality for carrying out consistency checks for the stored data.