

Chapter 5 – RISK ANALYSIS TOOLS

5.1 EXISTING TOOLS

5.1.1 EBIOS Tool

The EBIOS tool is available on the DCSSI web site: <http://www.ssi.gouv.fr/document/docs/EBIOS/ebios.html>.

The software highly helps users to:

- Record results, to produce tables and to make some calculations automatically;
- Produce outputs based on different templates: study report, security objectives form, synthesis, security policy, strategic note for security, SSRS, security targets, ...;
- Learn intuitively how to use the software with a self-training module (case study named @rchimed included); and
- Customize knowledge bases: constraints, threats, vulnerabilities, metrics, security requirements...

This is an Opensource Software (UML, Java, XML): the software and its source code are free, easily available (ebios.dcssi@sgdn.pm.gouv.fr) and improvable if a return to DCSSI is done.

5.1.2 CRAMM

The CRAMM software is distributed by a UK company called Insight Consulting. An interactive walkthrough presentation is available for free (www.insight.co.uk).

NB: the NC3A has bought a CRAMM software. Contact: J-L AUBOIN, NC3A ACQ INFOSEC, +32 2 707 8238.

NATO has 20 to 25 software licenses.

5.1.3 RISKAN

The RISKAN tool is a Microsoft Excel ® based product. It is distributed by T-Soft Novodvorská 1010/14, 142 01, Praha 4 (tsoft@tsoft.cz, <http://www.tsoft.cz>).

5.1.4 PILAR / EAR

The product is available on a commercial basis. A read only version can be downloaded from: <http://www.ar-tools.com/en/download/index.html>.

The product can be customised by the user. The structure of all the tables (XML files) is included in the documentation.

5.1.5 Comparative Analysis

The analysis will focus on CRAMM, PILAR and EBIOS, the three tools which have been analysed in detail by the WG.

Table 5-1: Comparative Analysis

	+	-
CRAMM	Ease of use Very large CM database	High level threats No access to databases and algorithms Only one type of system modelling No identification of system vulnerabilities
EBIOS	Open source software Configurable databases	User interface No default system modelling
PILAR / EAR	Configurable databases Hierarchical representation Graphical outputs Complete documentation Risk management module included	Confusing strategy for managing vulnerabilities (the word vulnerability is not used)

General comments can be issued on these tools:

- As stated in Chapter 3.3 Alternative methods there is a risk of combinatory explosion when used on large systems.
- These tools should be used only by trained and skilled experts as they are to be considered as a help but cannot replace the human experience. The use of such tools by unskilled people can lead to irrelevant results.