

# Improving Common Security Risk Analysis

## (RTO-TR-IST-049)

### Executive Summary

This report is the final report resulting from the four meetings of the working group called “Improving Common Security Risk Analysis” (IST-049 – RTG-021). The report describes the different methods used by various NATO countries such as EBIOS for France, CRAMM for UK, ITSG-04 for Canada, MAGERIT for Spain. As a first conclusion, the report shows that these methodologies, even if based on similar principles, differ in their knowledge bases (assets, threats, vulnerabilities, ...) or type of results (quantitative or qualitative). This makes the risk assessments difficult or impossible to compare when different methods have been used.

In a second part, the report identifies the main steps which are considered as mandatory for a method to be used by NATO.

Then the report identifies recommendations which should be taken into account by the existing methods and tools in order to solve the interoperability problem identified in the first part of the document but also to be able to take into account the new NATO concepts such as NNEC. These recommendations mainly concern the integration of dynamic risk analysis and improvement of information exchange. A proposal list of evolution for existing methods and tools concludes this part. The main results are:

- Methods should be based on documented models and should be modular.
- Methods should use a technical repository for assets, threats and vulnerabilities.
- Methods should be quantitative instead of qualitative.
- Methods should use the principle of refinement (more depth).
- Methods should allow reusability: it should be possible to reuse the result of a previous risk analysis on a system, sub system or component and to include these results in a new analysis.
- Methods should allow the reuse of the vulnerabilities analysis done during a product evaluation (CC, FIPS 140-1) or a system security testing (vulnerabilities scan, IDS, ...).
- Tools should be able to implement accurately the methods, to interface with external repositories, and to offer a user friendly interface.
- When performing risk assessment or when identifying countermeasures, tools shall be able to take into account the standard NATO security measures (physical, procedural) and the NATO technical security requirements.
- Tools should offer functionalities to conduct high level risk analysis in a time frame coherent with the new needs for system deployment and accreditation. Detailed risk analysis should be refined from these high level ones if necessary.
- Tools should offer simulation capabilities or at a minimum extended “What if” functions, in order, for example, to select the most appropriate countermeasure or to identify the impact of a change in threat level, in system architecture / configuration.

The final chapter of the report identifies the follow on activities to be conducted within RTO/IST or within other NATO entities.

# Amélioration d'un processus commun d'analyse de risques sécurité (RTO-TR-IST-049)

## Synthèse

Ceci est le rapport final clôturant les quatre réunions du groupe de travail intitulé « Amélioration d'un processus commun d'analyse de risques sécurité » (IST-049 – RTG-021). Il décrit les différentes méthodes utilisées par diverses nations de l'OTAN, telles que EBIOS pour la France, CRAMM pour le Royaume-Uni, ITSG-04 pour le Canada ou MAGERIT pour l'Espagne. La première conclusion de ce rapport démontre que ces méthodologies, même si elles sont fondées sur des principes similaires, divergent dans leurs bases de connaissances (atouts, menaces, vulnérabilités, ...) ou leur type de résultats (quantitatif ou qualitatif). Lorsque des méthodes différentes ont été employées, il devient difficile, voire impossible, de comparer les évaluations de risques.

Dans une deuxième partie, ce rapport identifie les principales étapes considérées comme obligatoires pour qu'une méthode soit utilisée par l'OTAN.

Ce rapport détermine ensuite les recommandations qui devraient être prises en compte par les méthodes et les outils existants afin de résoudre les problèmes d'interopérabilité recensés en première partie du document, mais également afin de pouvoir intégrer les nouveaux concepts de l'Alliance, tels que la capacité en réseau de l'OTAN (NNEC). Ces recommandations concernent principalement l'intégration des analyses de risques dynamiques et l'amélioration des échanges d'informations. Une liste de propositions d'améliorations pour les méthodes et outils existants conclut cette partie. Les principaux résultats sont les suivants :

- Les méthodes devraient être basées sur des simulations documentées et devraient être modulaires.
- Les méthodes devraient utiliser un référentiel technique pour les biens, les menaces et les vulnérabilités.
- Les méthodes devraient être quantitatives et non qualitatives.
- Les méthodes devraient utiliser le principe du raffinement (plus de profondeur).
- Les méthodes devraient permettre la réutilisation : il devrait être possible de réutiliser le résultat d'une précédente analyse de risques sur un système, un sous-système ou un composant et d'inclure ces résultats dans une nouvelle analyse.
- Les méthodes devraient permettre la réutilisation de l'analyse des vulnérabilités réalisée lors de l'évaluation d'un produit (CC, FIPS 140-1) ou des tests de sécurité d'un système (scanner de vulnérabilités, IDS, ...).
- Les outils devraient être capables d'implémenter les méthodes avec précision, d'interfacer avec les référentiels externes et de proposer une interface conviviale.
- Lors de la réalisation d'une évaluation des risques ou de l'identification de contre-mesures, les outils devraient être capables de prendre en compte les mesures de sécurité standard de l'OTAN (physiques, de procédure) et les exigences de sécurité techniques de l'OTAN.
- Les outils devraient proposer des fonctionnalités permettant de réaliser des analyses de risques de haut niveau dans un cadre temporel cohérent avec les nouveaux besoins en matière d'accréditation

et de déploiement de système. Des analyses de risques détaillées devraient être affinées à partir de ces analyses de haut niveau si nécessaire.

- Les outils devraient proposer des capacités de simulation ou, au minimum, des fonctions « What If » (quoi si) avancées afin, par exemple, de sélectionner la contre-mesure la plus appropriée ou d'identifier l'impact d'une modification du niveau de menace, dans l'architecture ou la configuration du système.

Le dernier chapitre de ce rapport identifie les activités de suivi à mettre en place au sein de la RTO/IST ou d'autres entités de l'OTAN.

