

Title: The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures

Synopsis: The document looks at the CRAMM's Risk Matrix and the determination of appropriate countermeasures.

TABLE OF CONTENTS

- 1. INTRODUCTION.....3**
- 2. ASSESSMENT OF MEASURES OF RISKS3**
 - 2.1. LOGIC BEHIND CRAMM’S RISK MATRIX 3
 - 2.2. DETERMINATION OF THE MEASURES OF RISK 7
- 3. DETERMINATION OF APPROPRIATE COUNTERMEASURES9**

1. INTRODUCTION

This document describes the logic behind CRAMM's assessment of the measures of risk facing an IT system/network and the way these are then used to determine the appropriate countermeasures.

2. ASSESSMENT OF MEASURES OF RISKS

2.1. LOGIC BEHIND CRAMM'S RISK MATRIX

At the heart of CRAMM is the process by which the three major findings of the risk analysis phase, namely the asset valuation and the threat and vulnerability assessments, are drawn together to produce a series of statements about the requirements for security or "measures of risk". The 'measure of risk' is a figure based on a scale of one (low) to seven (high) which represents the need for security.

The manner in which CRAMM draws these elements together is via a 'risk matrix'. In order for CRAMM to achieve consistency there has to be explanation about how this matrix has been derived and what each of the measures of risk actually means.

The basic approach taken to this problem was to consider:

- ◆ the possible frequency with which threats might occur (the level of threat);
- ◆ the chances of the threat succeeding and causing an impact (the level of vulnerability);
- ◆ the potential financial loss that could result if a threat were to succeed (the impact).

CRAMM is fundamentally a qualitative method, however in order to ensure consistency of approach together with sound theoretical background to the CRAMM's measure of risk matrix. The scales used in CRAMM can be converted to quantitative values and then these figures can be combined to produce a value, similar to an "annual loss expectancy" figure.

Several values for the expected frequency of threats and chance that the threat would be successful were tried. The levels that produced the most satisfactory results were as follows:

The levels of threat were equated to the following definitions for frequency:

| | |
|--|----------|
| An incident is expected to occur on average, no more than once in every 10 years | Very Low |
| An incident is expected to occur on average, once in 3 years | Low |
| An incident is expected to occur on average, once in a year | Medium |

Siemens Enterprise - CRAMM Measures of Risk/ Determination of
Appropriate Countermeasures Document

| | |
|---|-----------|
| An incident is expected to occur on average, once every four months | High |
| An incident is expected to occur on average, once every month | Very High |

The levels of vulnerability were equated to the following definitions for probability for success:

| | |
|---|----------|
| If an incident was to occur, there would be no more than a 33% chance of the worst case scenario (assessed during asset valuation) being realised | (Low) |
| If an incident was to occur, there would be a 33% to 66% chance of the worst case scenario (assessed during asset valuation) being realised | (Medium) |
| If an incident was to occur, there would be a higher than 66% chance of the worst case scenario (assessed during asset valuation) being realised | (High) |

The financial values recorded in the Disruption to Activities/Financial Loss guidelines were combined with the threat and vulnerability figures to produce an "Annual Loss Expectancy" figure, as shown on the following matrix:

