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

SIEMENS
Global network of innovation

11 October 2005

Insight Consulting

Management in Confidence

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

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

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 then 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:

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Figure 1 - Annual Loss Expectancy Matrix

These “Annual Loss Expectancy” figures can then be translated into CRAMM measure of risk scale according to the following mapping:

CRAMM Measure of Risk	“Annual Loss of Expectancy”
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

This results in the following risk matrix:

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Figure 2 - CRAMM’s Risk Matrix

Since the measures of risk can be equated to "Annual Loss Expectancies" it is possible for the reviewer to consider, at least at a high level, a brief cost benefit analysis when deciding on which countermeasures should be implemented.

2.2. DETERMINATION OF THE MEASURES OF RISK

The threat and vulnerability assessment is conducted by examining the various threats covered by CRAMM against any group of assets that the reviewer considers to be appropriate for the purposes of investigating those threats.

On the completion of the threat and vulnerability assessment it is necessary to pull together the three key elements of the risk analysis, i.e., the asset valuation and the threat and vulnerability assessments, to produce the "measures of risk".

These measures of risk are based on a combination of the asset valuation associated with the assets, and the levels of threat and the levels of vulnerability that have been derived during the threat and vulnerability assessment.

CRAMM determines measures of risks for:

- each asset that is contained in an asset group;
- each asset that depends on a component of the asset group;
- each asset that a component of an asset group is dependent on.

The measures of risk for components of the asset group are a combination of the asset values associated with the asset and the levels of threat and vulnerability associated with that asset group.

The measures of risk for the assets dependent on a component of the asset group is the asset value associated with that asset and the levels of threat and vulnerability determined for the asset group.

The measures of risk for the assets that a component of the asset group depends on is taken to be the same as the measures of risks for the component of the asset group.

The following table is an example of a completed measures of risk table.

Asset	Value Type	P	1 5 M	1 H	3 H	1 2 H	1 D	2 D	1 W	2 W	1 M	2 M	B	T	I	C	O	S E	W E	D M	In	O r	R c	N d	R p	M r	T m	O s
Threat: Fire																												
Group: !Computer Room																												
	Threat	L	L	L	L	L	L	L	L	L	L	L	L															
	Vul	M	H	H	H	H	H	H	H	H	H	H	M															
Computer Room	Impact	3			1	1	1	3	4	4	4	3	5	3	2		4	3		5								
	Msr of Risk	2			1	1	1	2	3	3	3	2	3															
> Administration Block	Impact	3			1	1	1	3	4	4	4	3	5	3	2		4	3		5								
	Msr of Risk	2			1	1	1	2	3	3	3	2	3															
> Codex Site	Impact	3			1	1	1	3	4	4	4	3	5	3	2		4	3		5								
	Msr of Risk	2			1	1	1	2	3	3	3	2	3															
< Unix Mini System	Impact	3			1	1	1	3	4	4	4	3	5	3	2		4	3		5								
	Msr of Risk	2			1	1	1	2	3	3	3	2	3															

> indicates an asset on which a component of the asset group depends
< indicates an asset which is dependent on a component of the asset group

3. DETERMINATION OF APPROPRIATE COUNTERMEASURES

The process for calculating the recommended countermeasures is based around:

- the threat to countermeasure group table;
- comparing the asset classes associated with the countermeasure with the asset class of assets under consideration;
- comparing the measures of risks determined for each asset with the security levels associated with each countermeasure.

CRAMM contains a comprehensive countermeasure library costing of 3,500 generic controls. This countermeasure library is divided into countermeasure groups, which are divided into different 'security aspects'. Each countermeasure group is further sub-divided into countermeasure sub-groups and within each of these sub-groups there are a number of detailed countermeasures.

For each countermeasure the countermeasure library contains the following information:

- a reference number;
- a narrative description;
- the position in the countermeasure hierarchical structure;
- a cross-reference to other related countermeasures (where applicable);
- minimum and maximum measures of risk/security levels for the impacts of:
    - physical destruction,
    - unavailability (for 10 time periods),
    - destruction of data (for 2 categories, total and since last back-up),
    - unauthorised disclosure of data to insiders,
    - unauthorised disclosure of data to contracted service providers,
    - unauthorised disclosure of data to outsiders
    - accidental modification - small scale errors (e.g., keying errors),
    - accidental modification - widespread errors (e.g., programming errors),
    - modification - deliberate,
    - insertion,
    - deletion,
    - replay,
    - out of sequence,
    - repudiation of origin,
    - repudiation of receipt,

    - non delivery
    - mis-routing
    - traffic monitoring

- ♦ the manner in which a countermeasure can operate, i.e. either:

    - reduce threat,
    - reduce vulnerability,
    - reduce impact,
    - detect
    - recover
    - transfer

- ♦ a broad indication of the cost of implementing that countermeasure - either:

    - low,
    - medium,
    - high,

The effectiveness rating as defined as "the degree to which a countermeasure meets the objectives of the sub-group that it is contained in".

For example, the sub group "Room Fire Detection" might have three countermeasures:

- Manual Fire Alarm
- Smoke Detector
- Very sensitive smoke detecting equipment

The effectiveness rating would be indication of how effective each countermeasure is of meeting the aim of "Fire Detection".

The permissible values of effectiveness ratings are:

- Low
- Medium
- High

- ♦ references to any alternative countermeasures;
- ♦ references to any related countermeasures;
- ♦ the asset classes that the countermeasure should be applied to.

For each asset that the countermeasure may apply to there is also:

- a flag indicating whether the countermeasure is recommended, superseded by an alternative countermeasure or not recommended;

- an indication of the current status of the countermeasure.

The method of identifying precisely where a countermeasure should be applied is a three step process.

The first step is to compare the asset classes associated with the countermeasure to the asset class of the components of the asset group. Where there is a match the countermeasure would be considered further for that asset.

The second step is to compare the asset classes associated with the countermeasure with the asset class of the assets which the components of the asset group are dependent on (and assets which these assets are dependent on). Where there is a match the countermeasure will be considered further for those assets.

The asset classes associated with the countermeasure are then compared with the asset class of the assets which are dependent on the components of the asset group. Where there is a match the countermeasure will be considered for those assets.

For example, the reviewer has chosen to investigate the threat of fire against an asset group called “!Computer Room” which contains a location asset called “Computer Room”. Measures which apply at the room level would be applied to that asset. Countermeasures, such as a “Fire Prevention programme”, which are applicable at the site level, would be considered further for the location asset “Codex Site” that the computer room is dependent upon. Measures such as those in the contingency planning countermeasure groups would be considered further for any Host Systems which were dependent on the “Computer Room”.

Having identified that the asset is of the appropriate class, the next step is to identify if the measures of risk are sufficient to justify the recommendation of the countermeasure.

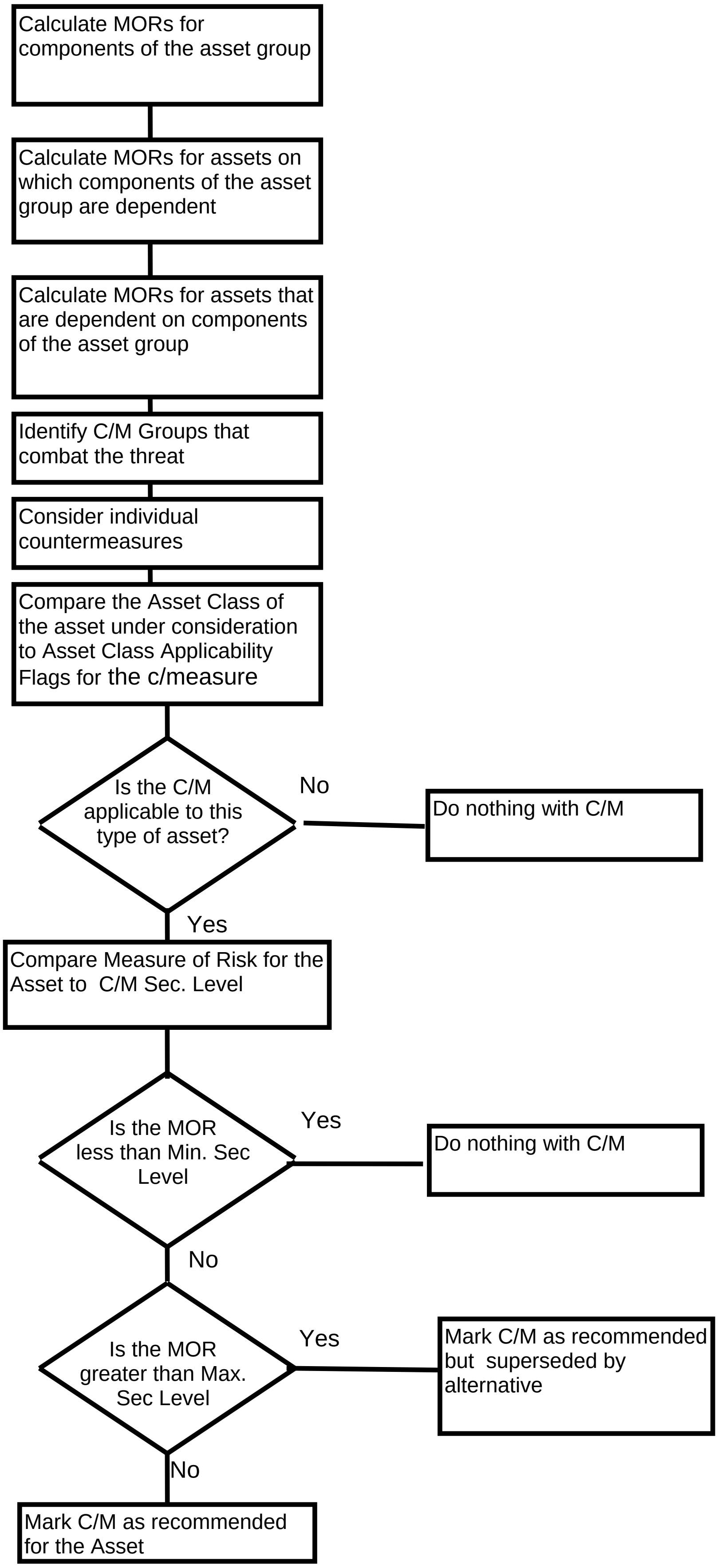
Every countermeasure has a set of security levels (two for every impact that the countermeasure protects against) associated with it. These security levels represent the threshold values at which the countermeasure is to be recommended and at which the countermeasure would be superseded by an alternative countermeasure.

For each relevant threat/asset pairing the CRAMM software compares the measures of risks that are associated with this threat/asset pairing to the minimum security levels associated with each countermeasure which protects against that threat (as defined by the threat /countermeasure group table).

If one or more of the measures of risk is greater than or equal to the minimum security level for the corresponding impact then the countermeasure is recommended.

The software then compares the measures of risk that are associated with this threat/asset pairing to the maximum security levels associated with each countermeasure that protects against that threat. If one or more of the measures of risk is greater than or equal to the maximum measure of risk/security level for the corresponding impact then the countermeasure is marked as superseded.

The process for determining recommended countermeasures is shown below:


Calculate MORs for components of the asset group
Calculate MORs for assets on which components of the asset group are dependent
Calculate MORs for assets that are dependent on components of the asset group
Identify C/M Groups that combat the threat
Consider individual countermeasures
Compare the Asset Class of the asset under consideration to Asset Class Applicability Flags for the c/measure
Is the C/M applicable to this type of asset?
No
Do nothing with C/M
Yes
Compare Measure of Risk for the Asset to C/M Sec. Level
Is the MOR less than Min. Sec Level
Yes
Do nothing with C/M
No
Is the MOR greater than Max. Sec Level
Yes
Mark C/M as recommended but superseded by alternative
No
Mark C/M as recommended for the Asset