



# Managing CRAMM Reviews Using PRINCE

13 October 2005

**SIEMENS**

Global network of innovation

**Insight Consulting**

Management in Confidence



## TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1.	PURPOSE .....	1
1.2.	WHO SHOULD READ THIS GUIDE.....	2
<b>2.</b>	<b>OVERVIEW OF THE GUIDE .....</b>	<b>3</b>
2.1.	OVERVIEW OF PRINCE .....	3
2.2.	ORGANISATION OF THE CRAMM REVIEW .....	3
2.3.	CRAMM PRODUCTS.....	3
2.4.	PLANS .....	3
2.5.	CONTROL OF CRAMM PRODUCTS .....	3
2.6.	QUALITY MANAGEMENT .....	3
2.7.	CONFIGURATION MANAGEMENT AND CHANGE CONTROL.....	4
2.8.	SUMMARY AND BENEFITS .....	4
<b>3.</b>	<b>OVERVIEW OF PRINCE .....</b>	<b>5</b>
<b>4.</b>	<b>ORGANISATION OF THE CRAMM REVIEW .....</b>	<b>7</b>
4.1.	PROJECT BOARD .....	7
4.2.	PROJECT MANAGER.....	8
4.3.	PROJECT ASSURANCE TEAM .....	8
4.3.1.	Business Assurance Co-ordinator (BAC) .....	8
4.3.2.	Technical Assurance Co-ordinator (TAC).....	9
4.3.3.	User Assurance Co-ordinator (UAC) .....	10
4.3.4.	CRAMM Review Team .....	10
<b>5.</b>	<b>CRAMM PRODUCTS .....</b>	<b>12</b>
5.1.	INTRODUCTION.....	12
5.2.	CRAMM MANAGEMENT PRODUCTS.....	13
5.2.1.	Project Initiation Document for a CRAMM Review .....	13
5.2.2.	Risk Analysis Report.....	15
5.2.3.	Risk Management Report(s).....	17
5.2.4.	Implementation Plan .....	18
5.3.	CRAMM QUALITY PRODUCTS .....	18
5.3.1.	Boundary of the Review Form .....	19
5.3.2.	Data Asset Valuation Forms.....	19
5.3.3.	Contents of Asset Groups.....	20
5.3.4.	Threat/Asset Summary .....	20
5.3.5.	Completed Threat and Vulnerability Questionnaire.....	21
5.3.6.	Measures of Risk Report .....	21
5.3.7.	Installed Countermeasures.....	21
5.3.8.	Prioritisation of recommended countermeasures .....	22
5.4.	CRAMM TECHNICAL PRODUCTS .....	22
5.4.1.	System Security Policy .....	22
5.4.2.	Interchange Agreement .....	23
5.4.3.	Physical Security Document.....	24
5.4.4.	Security Operating Procedures .....	24
<b>6.</b>	<b>PLANS .....</b>	<b>26</b>
6.1.	RESOURCES REQUIRED FOR A CRAMM REVIEW .....	26
6.2.	INTERVIEW MATRIX .....	28
6.3.	AGREEING THE TIMETABLE FOR THE REVIEW.....	30
<b>7.</b>	<b>CONTROL OF CRAMM PRODUCTS.....</b>	<b>33</b>
7.1.	PRINCE CONTROL POINTS.....	33
7.1.1.	Project Initiation .....	33

7.1.2.	End-Stage Assessment .....	34
7.1.3.	Mid-Stage Assessment.....	34
7.1.4.	Highlight Report .....	34
7.1.5.	Checkpoints Report/Meeting .....	35
7.1.6.	Project Closure .....	35
<b>8.</b>	<b>QUALITY MANAGEMENT OF CRAMM PRODUCTS .....</b>	<b>36</b>
<b>9.</b>	<b>CONFIGURATION MANAGEMENT AND CHANGE CONTROL.....</b>	<b>37</b>
9.1.	CONFIGURATION MANAGEMENT .....	37
9.2.	CHANGE CONTROL.....	38
<b>10.</b>	<b>SUMMARY AND BENEFITS .....</b>	<b>40</b>
10.1.	SUMMARY.....	40
10.2.	BENEFITS .....	40

## 1. INTRODUCTION

### 1.1. PURPOSE

For a CRAMM review to be conducted successfully it must be planned and managed effectively. To achieve this objective it is recommended that CRAMM reviews are planned and managed using a well defined project management method such as PRINCE (**PR**ojects **IN** **C**ontrolled **E**nvironments).

PRINCE is a structured method for effective project management. It is a de facto standard used extensively by the UK Government and is widely recognised and used in the private sector, both in the UK and internationally. PRINCE, the method, is in the public domain, offering non-proprietary best-practice guidance on project management. PRINCE is a recommended standard within many government departments and is becoming widely used in the private sector.

PRINCE is capable of being used on a wide range of projects from the very large to the very small. This guide sets out how PRINCE can be used to ensure that a CRAMM review meets its objectives and is carried out within the time and budget allocated. Even if PRINCE was not used to plan and control the project, similar techniques would have to be used to ensure that the review met all its objectives with the allocated time and budget. Many of the concepts embodied in PRINCE are already present in the structure of CRAMM and so the imposition of PRINCE techniques should not cause any difficulties or unnecessary expense. In fact, in many cases using PRINCE can produce savings through improved efficiency and control.

The use of PRINCE adds value to a CRAMM review by:

- ◆ explaining what reports will be produced during the review and helping to ensure that these are produced on time and to budget;
- ◆ improving the planning process, leading to more effective estimation and use of resources;
- ◆ making the project's progress more visible to management;
- ◆ helping to establish the objectives of the CRAMM review and ensuring that these objectives are met;
- ◆ highlighting problems as they occur so that exception plans can be made and management can be kept informed and in control;
- ◆ allowing the review to be suspended and re-started, completely under management control, at any time in the review's life;
- ◆ improving quality assurance, which in turn leads to quality deliverables and the production of deliverables that are aligned with the objectives of the review.

PRINCE requires that every project should have the following:

- ◆ a pre-defined set of end products;

- ◆ a set of activities to construct these end-products;
- ◆ a finite life-span;
- ◆ an organisational structure to control its progress;
- ◆ defined roles and responsibilities.

CRAMM reviews are well suited to those requirements and this guide provides details and guidance about each of these aspects in relation to the management of CRAMM reviews.

It is not the intention of this guide to show how CRAMM should be used for risk analysis in systems development or other projects managed under PRINCE.

Please note, this guide has been written specifically in relation to the use of CRAMM Expert rather than CRAMM Express. CRAMM Express is considered a much simpler method, and a typical CRAMM Express review should be completed in less than half a day, so many of the project management principals set out in this document do not apply. Further information on CRAMM Express can be found on [www.CRAMM.com](http://www.CRAMM.com).

## 1.2. WHO SHOULD READ THIS GUIDE

This guide should be read by:

- ◆ Project Boards and Senior Managers who are responsible for overseeing CRAMM reviews;
- ◆ IT Security Officers or Project Managers who are responsible for managing a CRAMM review;
- ◆ CRAMM reviewers.

It is assumed that readers of this guide have a working knowledge of CRAMM, but no previous knowledge of PRINCE. Background information on CRAMM can be found in the CRAMM User Guide [Ref 3] or [www.cramm.com](http://www.cramm.com). Further information about PRINCE can be found at <http://www.oqc.gov.uk/prince2/>











































































































