



CERT® Resilience Management Model



A Maturity
Model for
Managing
Operational
Resilience

SEI SERIES • A CERT® BOOK

Richard A. Caralli

Julia H. Allen

David W. White

CERT[®] Resilience Management Model

CERT Resilience Management Model (CERT-RMM): A Maturity Model for Managing Operational Resilience

Table of Contents

Cover

Title Page

Copyright Page

CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

ACKNOWLEDGMENTS

PART ONE ABOUT THE CERT RESILIENCE
MANAGEMENT MODEL

1 INTRODUCTION

1.1 The Influence of Process Improvement and Capability Maturity
Models

1.2 The Evolution of CERT-RMM

1.3 CERT-RMM and CMMI Models

1.4 Why CERT-RMM Is Not a Capability Maturity Model

2 UNDERSTANDING KEY CONCEPTS IN CERT-RMM

2.1 Foundational Concepts

2.2 Elements of Operational Resilience Management

2.3 Adapting CERT-RMM Terminology and Concepts

3 MODEL COMPONENTS

Table of Contents

3.1 The Process Areas and Their Categories

3.2 Process Area Component Categories

3.3 Process Area Component Descriptions

3.4 Numbering Scheme

3.5 Typographical and Structural Conventions

4 MODEL RELATIONSHIPS

4.1 The Model View

4.2 Objective Views for Assets

PART TWO PROCESS INSTITUTIONALIZATION AND IMPROVEMENT

5 INSTITUTIONALIZING OPERATIONAL RESILIENCE MANAGEMENT PROCESSES

5.1 Overview

5.2 Understanding Capability Levels

5.3 Connecting Capability Levels to Process Institutionalization

5.4 CERT-RMM Generic Goals and Practices

5.5 Applying Generic Practices

5.6 Process Areas That Support Generic Practices

6 USING CERT-RMM

6.1 Examples of CERT-RMM Uses

6.2 Focusing CERT-RMM on Model-Based Process Improvement

6.3 Setting and Communicating Objectives Using CERT-RMM

6.4 Diagnosing Based on CERT-RMM

6.5 Planning CERT-RMM Based Improvements

7 CERT-RMM PERSPECTIVES

Using CERT-RMM in the Utility Sector

Addressing Resilience as a Key Aspect of Software Assurance Throughout
the Software Life Cycle

Raising the Bar on Business Resilience

Measuring Operational Resilience Using CERT-RMM

Table of Contents

PART THREE CERT-RMM PROCESS AREAS

ASSET DEFINITION AND MANAGEMENT

ACCESS MANAGEMENT

COMMUNICATIONS

COMPLIANCE

CONTROLS MANAGEMENT

ENVIRONMENTAL CONTROL

ENTERPRISE FOCUS

EXTERNAL DEPENDENCIES MANAGEMENT

FINANCIAL RESOURCE MANAGEMENT

HUMAN RESOURCE MANAGEMENT

IDENTITY MANAGEMENT

INCIDENT MANAGEMENT AND CONTROL

KNOWLEDGE AND INFORMATION MANAGEMENT

MEASUREMENT AND ANALYSIS

MONITORING

ORGANIZATIONAL PROCESS DEFINITION

ORGANIZATIONAL PROCESS FOCUS

ORGANIZATIONAL TRAINING AND AWARENESS

PEOPLE MANAGEMENT

RISK MANAGEMENT

RESILIENCE REQUIREMENTS DEVELOPMENT

RESILIENCE REQUIREMENTS MANAGEMENT

RESILIENT TECHNICAL SOLUTION ENGINEERING

SERVICE CONTINUITY

TECHNOLOGY MANAGEMENT

VULNERABILITY ANALYSIS AND RESOLUTION

Table of Contents

PART FOUR THE APPENDICES

A: GENERIC GOALS AND PRACTICES

B: TARGETED IMPROVEMENT ROADMAPS

C: GLOSSARY OF TERMS

D: ACRONYMS AND INITIALISMS

E: REFERENCES

BOOK CONTRIBUTORS

INDEX