

**Application Security Guide For CISOs**

**2013 (Draft v0.1)**

Author

Marco Marona

Editor

Stephanie Tan

Other Contributors and Reviewers

Tobias Gondrom, Eoin Keary, Andy Lewis and Colin Watson

Chief Information Security Officers (CISOs) are responsible for application security from governance, compliance and risk perspectives. The Application Security Guide For CISOs seeks to help CISOs manage application security programs according to their own roles, responsibilities, perspectives and needs. Application security best practices and OWASP resources are referenced throughout the guide.

© 2013 OWASP Foundation

This document is licensed under the Creative Commons Attribution-ShareAlike 3.0 license

**Contents**

Preamble to Guide 1

Introduction 2

Executive Summary 3

Foreword 4

The CISO Guide 5

Part I : Reasons for Investing in Application Security 6

Part II : Criteria for Managing Application Security Risks 7

Part III : Application Security Program 8

Part IV : Metrics For Managing Risks & Application Security Investments 9

Supporting Information 10

References 11

About OWASP 12

CISO Guide Appendixes 13

Appendix A: Value of Data & Cost of an Incident 14

Appendix B: Quick Reference to OWASP Guides & Projects 15

**List of Figures**

Figure 1 A Figure 6

**List of Tables**

Table 1 A Table 6

# Preamble to Guide

## Introduction

### ???

???

## Executive Summary

### ???

???

## Foreword

### ???

???

# The CISO Guide

???

## Part I : Reasons for Investing in Application Security

???

1. A Figure
2. A Table

| **???** | **???** |
| --- | --- |
| ??? |
|  | * Instead of a GET or POST request, the user sends a TRACE request to the application.
 |

## Part II : Criteria for Managing Application Security Risks

???

## Part III : Application Security Program

???

## Part IV : Metrics For Managing Risks & Application Security Investments

???

# Supporting Information

???

## References

???

## About OWASP

???

# CISO Guide Appendixes

## Appendix A: Value of Data & Cost of an Incident

### ???

???

## Appendix B: Quick Reference to OWASP Guides & Projects

### ???

???