

IOActive's KARMA Risk-Rating Framework

IOActive, Inc.
1426 Elliott Ave W
Seattle, WA 98119

Toll free: (866) 760-0222
Office: (206) 784-4313
Fax: (206) 784-4367

© 2024 IOActive, Inc. All Rights Reserved.



Document Management

Document Revision Information

Date	Version	Author	Revision Details
2024-07-18	1.0	IOActive	Issue of KARMA v1.0



Introduction

Key Attribute and Risk Management and Analysis (KARMA) v1.0 is IOActive's framework for rating a system's ability to avoid negative outcomes based on a limited number of key attributes. The risk-rating framework leverages subject matter expert (SME) knowledge of the particular *system* being rated, and its goal is to find the attributes that best predict negative outcomes in the real world.

We define "*system*" as being the maximum most-likely deployment scenario of the asset (e.g. application, software, device, or component) having undergone security testing and risk evaluation.

KARMA has been in use at IOActive for over 20 years and has proven a simple yet effective method due its preciseness, paired with its flexibility to adapt to different kinds of security assessments, ranging from web/mobile/infra, to embedded penetration tests, code reviews, design reviews and tabletop exercises.

Likelihood and Impact

With KARMA, a vulnerability is assigned two key ratings: one for likelihood and another for impact. The likelihood describes the probability a real-world attacker has of finding and exploiting a vulnerability. The impact assumes an attacker has exploited the vulnerability, and describes the outcome of this exploitation over the affected assets.

The scope of likelihood and impact is contextualized to the scope of the engagement, and reflects the most-likely deployment scenario. For example, a credential sent over plaintext would have a high likelihood of being intercepted by a network attacker, if that's transmitted over the internet; but it may have a lower likelihood if it's only transmitted in a private network with mitigating strict logical and physical access controls. The same considerations apply when reasoning about impact.

Each rating corresponds to a numeric score ranging from 5 (critical) to 1 (informational). The definition of each score, for both likelihood and impact, is provided in the table below.



Table 1. Description of likelihood and impact

Rating (Score)	Likelihood	Impact
Critical (5)	The finding is almost certain to be exploited; knowledge of the issue and how to exploit it are in the public domain	Extreme impact to the entire organization if exploited; or completely defeats a security measure the in-scope asset was designed to provide
High (4)	The finding is relatively easy to detect and exploit by an attacker with low skills	Major impact to the entire organization or a single line of business if exploited
Medium (3)	A knowledgeable insider or expert attacker could exploit the finding without much difficulty	Noticeable impact to a line of business if exploited
Low (2)	Exploiting the finding would require considerable expertise and resources	Minor damage if exploited or could be exploited in conjunction with other vulnerabilities as part of a more serious attack
Informational (1)	The finding is not likely to be exploited on its own but may be used to gain information for launching another attack	Does not represent an immediate threat but may have security implications if combined with other vulnerabilities

Total Risk Rating

KARMA then calculates a total risk score by multiplying likelihood and impact, per the table below.

Table 2. Total risk rating and corresponding aggregate risk scores

Total Risk Rating	Total Risk Score Range (Likelihood × Impact)
Critical	20–25
High	12–19
Medium	6–11
Low	2–5
Informational	1