

Veracode SecurityReview® Assurance Level Worksheet

This Worksheet helps you determine the business criticality of your applications. The business criticality is a critical component in Veracode's Ratings approach as we believe that applications need to be rated in the context of their security risk to the organizations deploying them. Review the following questions and then review the table at the end to see a summary of the application assurance levels (business criticality).

Determine Potential Impacts:

For each of the six potential impacts below determine if the impact is **low**, **moderate**, or **high** based on the definitions following the potential impact.

1. Potential impact of *inconvenience, distress, or damage to standing or reputation*:

- **Low**—at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- **Moderate**—at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **High**—severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

2. Potential impact of *financial loss*:

- **Low**—at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or an insignificant or inconsequential organization liability.
- **Moderate**—at worst, a serious unrecoverable financial loss to any party, or a serious organization liability.
- **High**—severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic organization liability.

3. Potential impact of *harm to organization programs or public interests*:

- **Low**—at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness, or (ii) minor damage to organizational assets or public interests.
- **Moderate**—at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- **High**—a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

4. Potential impact of **unauthorized release of sensitive information**:

- **Low**—at worst, a limited release of personal, organization sensitive or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.
- **Moderate**—at worst, a release of personal, organization sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.
- **High**—a release of personal, organization sensitive or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

5. Potential impact to **personal safety**:

- **Low**—at worst, minor injury not requiring medical treatment.
- **Moderate**—at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- **High**—a risk of serious injury or death.

6. The potential impact of **civil or criminal violations** is:

- **Low**—at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- **Moderate**—at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- **High**—a risk of civil or criminal violations that are of special importance to enforcement programs.

Determine Assurance Level: Using the table below, determine the assurance level by placing Low, Moderate or High for each potential impact category in the table and then selecting the Assurance level that corresponds to the highest level for any category. For example if personal safety is Moderate then the assurance level is Very High even if other potential impacts are low.

Assurance Level Impact Profiles				
Potential Impact Categories	Low	Medium	High	Very High
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to organization programs or stakeholders	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod or High
Civil or criminal violations	N/A	Low	Mod	High

Ref: U.S. Govt. OMB Memorandum M-04-04 December 16, 2003