TOPIC: Risk Assessments & Security Assessments
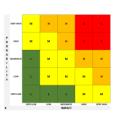
Risk Assessments should be carried out for each business case proposing the development of a new system, or a significant change to an existing system or process. Organizations should define their risk assessment process and distribute it internally so that it is known throughout the organization. Reduction strategies should be defined for each risk identified in a risk assessment. There are various ways of managing risks: **transfer** the risk to a third party, **avoid** the risk by not engaging in the activity, **accept** the risk if it falls within the organization's risk tolerance, or **mitigate** the risk with internal controls.

Risks should be rated as part of the risk assessment process. Risks are rated by multiplying **probability** by **impact**. There are usually four risk ratings: Low, Medium, High, and Critical.

Security Assessments are health checks for an organization's overall security posture. The assessments should be conducted annually as both a self assessment and a third-party assessment (to ensure independence). Assessments should follow a published security standard, and gaps that are identified should be built into a plan which is reviewed by executives and implemented.

UPCOMING SECURITY EVENTS:

- **Monthly Defensible Security Conference Call: Nov 28, 2018**
At the next conference call, 3 control areas of Defensible Security will be discussed; Risk Appetite & Register, Risk Assessments, and Security Assessments.

- **20th Annual Privacy and Security Conference: Feb 6-8, 2019**
This three-day conference is recognized as one of the top tier events in North America, drawing an international audience of some 1,000 delegates with an interest in cutting edge policy, programs, law, research, and technologies aimed at the protection of privacy and security. Visit the Privacy and Security Conference website for more information.