Risk Appetite:

A consideration of risk appetite is typically one of the first steps in enterprise-wide risk management. **Risk Appetite** is defined as the "amount of risk an organization is willing to accept, on a broad level, in pursuit of its objectives, given consideration of costs and benefits." (Federal Playbook, p.23). Looked at from another point of view, risk appetite "embraces the level of exposure which is considered tolerable and justifiable should it be realized." (The Orange Book: Management of Risk – Principles and Concepts).

Without considering and engaging in this step, organizations may take on more or less risk than is appropriate to achieve its objectives. Clearly defined statements on risk appetite can provide guidance on the amount of reasonable risk, and help managers make informed decisions along the way. Each program should have its own risk appetite level, so that all levels fall into the risk appetite for the entire organization.

The Orange Book further defines risk appetite as "a series of boundaries, appropriately authorized by management," which provide each level of the organization clear guidance on the limits of risk which they can take. When properly undertaken, the risk appetite process helps drive decisions by setting agreed-upon boundaries for running the organization.

In this way, the risk appetite discussion can help a firm or government entity make better decisions with regard to funding, staffing, and new projects.

Risk Appetite Process:

There are several key components to this process. It begins of course with a discussion of the company's strategic goals and objectives. This is essential because risk must be considered in relation to the goals and tasks undertaken. Here are several aspects of this process:

- **Risk Profile** – An upper level assessment of a company's top risks and the capability of the firm to manage those risks.
- **Risk Capacity** –The actual amount of risk that a firm could bear. This includes qualitative and quantitative aspects.
- **Qualitative risk assessment** – A categorization of risk items relative to each other. This takes into account risk mitigation.
- **Quantitative risk analysis** – This may involve estimates, a rating scale, heat maps, benchmarking, and probability models such as VaR (value at risk) models.

Risk Tolerance:

Although the consideration of risk analysis may have some quantitative aspects, it is typically expressed in more broad, general statements. That is not always the case with risk tolerance, in which a risk limit is identified and possibly reached.

Risk Tolerance is defined as "the acceptable level of variation in performance relative to the achievement of objectives," (GAO Green Book p. 36). This defines the specific maximum risk that an entity is willing to take regarding each relevant risk category. Often this is expressed as a risk limit, or in quantitative terms. This helps management determine what thresholds to monitor to make sure the actual risk exposure does not deviate too much from the desired level. Breaching a risk limit may signal a warning, or corrective action.

Risk tolerance is often measured in the same terms as performance measures – such as % of achievement, or progress milestones. Tolerance levels are generally defined for specific risks, and can be based on the importance of the objectives to the operation of the entity.