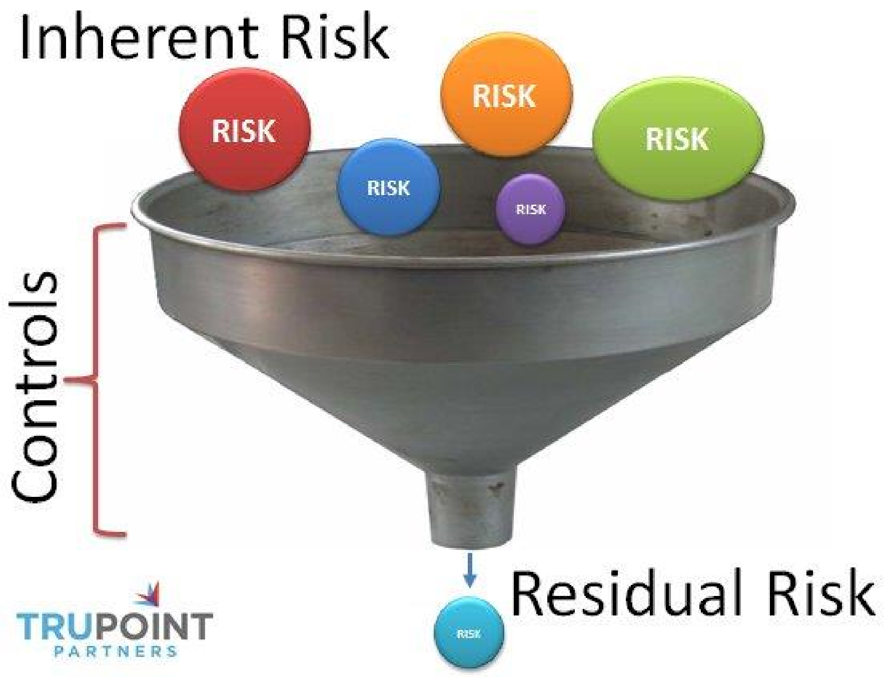
Overview:

Consideration of both inherent and residual risk is one of the most important aspects of enterprise risk management**.** **Inherent Risk** is typically defined as the level of risk in place in order to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood. **Residual Risk** is the remaining level of risk following the development and implementation of the entity's response.

Inherent vs. Residual Risk:

The difference between the inherent and residual risk may be imagined or visualized as water flowing through a filter. Inherent risk is above the filter, which constitutes management controls. A smaller pool of residual risk remains.

Inherent risk is established only after the entity's key objectives have been defined, and steps have been taken to identify what could go wrong to prevent the entity from achieving those objectives. In addition to impact and likelihood, management considers the nature of the risk, whether the risk results from fraud, natural events such as storms, or complex or unusual business transactions. The origin and character of the risk contributes to understanding its potential impact and likelihood of occurrence.



Risk Assessment:

The risks included in the initial risk identification process are usually referred to as a "risk universe," – a listing of the risks that entity faces. These risks are typically organized by standard risk categories such a strategic, financial, operational, compliance, but may also be divided into sub-categories based on function, division, sections, etc.

The steps between the assessment of inherent risk and the final evaluation of residual risk may vary somewhat from entity to entity. They typically include much of the core process of enterprise risk management, and will typically involve the following steps:

- **Risk Response** – Management designs risk responses at various levels based on the analysis of the risk (impact and likelihood) and on the defined level of risk tolerance. The response typically includes the categories of acceptance, avoidance, reduction, and sharing.
- **Establishment of Controls** – Controls are typically established in those operations areas that are essential, and acceptance is too risky, and avoidance and sharing are not possible or practical. A control is any activity which mitigates or reduces risk, but typically it involves an additional activity to ensure that a process occurs as it should. Cost vs benefit is always considered in the establishment of controls.
- **Testing and Assessment of Internal Controls** – To ensure that controls are operating efficiently, testing is usually necessary, particularly in automated processes. The testing provides confidence that controls have reduced risk to a tolerable level.
- **Corrective Action** – Corrective action is warranted when a control is weak, not in place, or not functioning properly. These actions are documented and added to the entity's risk assessment plan with a timeline for action. Testing can be time-consuming and not always possible, and an alternative is to combine on-going monitoring with a regular review of control design to provide assurance that activities are being carried out in a timely and accurate manner.

The Revised COSO Enterprise Risk Guidance (Aligning Risk with Strategy and Performance, June, 2016) identified a new principle – the organization identifies "risk in execution" that impacts the achievement of business objectives. This requirement highlights the importance of identifying new, emerging and changing risk. Examples would include a change in business objectives, a change in business context, and a change that was previously unknown or was previously unidentified. The new COSO guidance also cautions against bias in assessment, in which one's personal point of view plays an unproportioned role in the evaluation of risk.

Enterprise risk management requires the organization to consider the potential implications of a risk profile from an entity-wide perspective. This requires the completion of a final executive level report, which presents and categorizes residual risks. Often a "heat map" is used to display the severity of one risk to another, and categorize and identify key obstacles to the achievement of objectives.