

Enterprise Risk Management Framework

The Enterprise Risk Management (ERM) framework includes four steps: identify the risks, determine the probability and impact of each one, identify controls that are already in place that mitigate that risk, and propose additional controls if needed.

Step 1: Identify Risks – What can go wrong? This step should identify the negative outcomes that could result from an action or decision. It is important to consider a wide range of risks, and so the Department's ERM framework includes five broad categories:

- (1) Mission – can a system, action, or decision hinder accomplishment of the mission?
- (2) People – will a failure impact the well-being of an employee or the public?
- (3) Physical Assets – could there be loss or damage to a physical asset (e.g., property)?
- (4) Financial – could there be loss of funds or unavailability of funds?
- (5) Reputation and Trust – will the Department suffer damage to its credibility with the public or other stakeholders?

Step 2: Determine the probability and impact. Through either a quantitative or qualitative analysis, this step captures the probability of the risk occurring and the impact to the Department if it does. For this step, it is important to assume that no controls are in place or mitigating actions are taken. Probability and impact are then combined, using the table below, to arrive at an overall risk level. Common definitions help ensure consistency.

Impact:

Negligible – impact is easily and quickly corrected with little effort or time

Low – short-term impact, easily corrected without long-term consequences

Medium – significant short-term impacts, significant time and resources to recover

High – impacts are catastrophic and long-term, significantly affecting the mission

		Impact			
Probability		Negligible	Low	Medium	High
	Certain	Minor	Moderate	Extreme	Extreme
	Likely	Minor	Moderate	Significant	Extreme
	Possible	Minor	Moderate	Significant	Extreme
	Unlikely	Minor	Minor	Moderate	Significant
	Rare	Minor	Minor	Minor	Moderate

Probability:

Rare – probability is incredible during the time period of interest

Unlikely – unlikely to occur to during the time period of interest

Possible – an even possibility of occurrence exists during the time period of interest

Likely – more likely than not during the time period of interest

Certain – nearly certain in the time period of interest

Step 3: Identify the risk-mitigating controls that already exist. For each identified risk, actions can be taken to reduce that risk's probability and/or impact. First, any existing external requirements or standards that are applicable to address the risk should be identified. Next, identify any existing DOE directives that address the risk. These steps identify existing controls.

Step 4: If unacceptable risks remain, identify additional controls. In this step, the remaining risks in Step 3 are considered and each one is either accepted (i.e., the risk level does not warrant further action) or mitigated by making a different decision or developing an additional control. Additional controls can include things like a mandatory process, a required report, or a specified DOE approval.