Ridurre al minimo l'impatto dei rischi sull'organizzazione e fornire solide basi nel processo decisionale sono i motivi fondamentali per cui le organizzazioni sono chiamate a implementare un processo di gestione dei rischi per i loro sistemi IT.

Il Risk Assessment è uno strumento di analisi, semplice e accurato, che studia i rischi dell'organizzazione (operativi, strategici, finanziari ed esterni) al fine d'individuare successivamente le soluzioni e le misure più adeguate. I passi fondamentali del Risk Assessment possono riassumersi come segue:

- Identificazione dei rischi. Devono essere individuati i fattori di pericolo per l'organizzazione, evidenziando chi o cosa può essere danneggiato e in quale modo. Per ogni fattore di pericolo identificato, bisogna definire ciò che è esposto maggiormente al pericolo.
- Valutazione dei rischi e definizione delle le azioni di mitigazione. E' necessario valutare le azioni e le tecniche per ridurre il pericolo e portarlo a livelli accettabili.
- Annotazione dei risultati e attuazione del piano di mitigazione del rischio. La valutazione precedentemente effettuata va trasformata in un piano operativo, per ottenere una gestione consapevole dei rischi dell'organizzazione.
- Revisione periodica della valutazione e aggiornamenti. E' necessario rivedere periodicamente ciò che si sta facendo. Viene identificato il profilo di rischio e viene proposto un modello di gestione integrato dei pericoli, che evidenzia i singoli fattori di rischio. In seguito vengono valutate le varie misure preventive, agevolando la protezione del valore dell'ente.

Si riporta di seguito uno schema per il *Risk Assessment*:

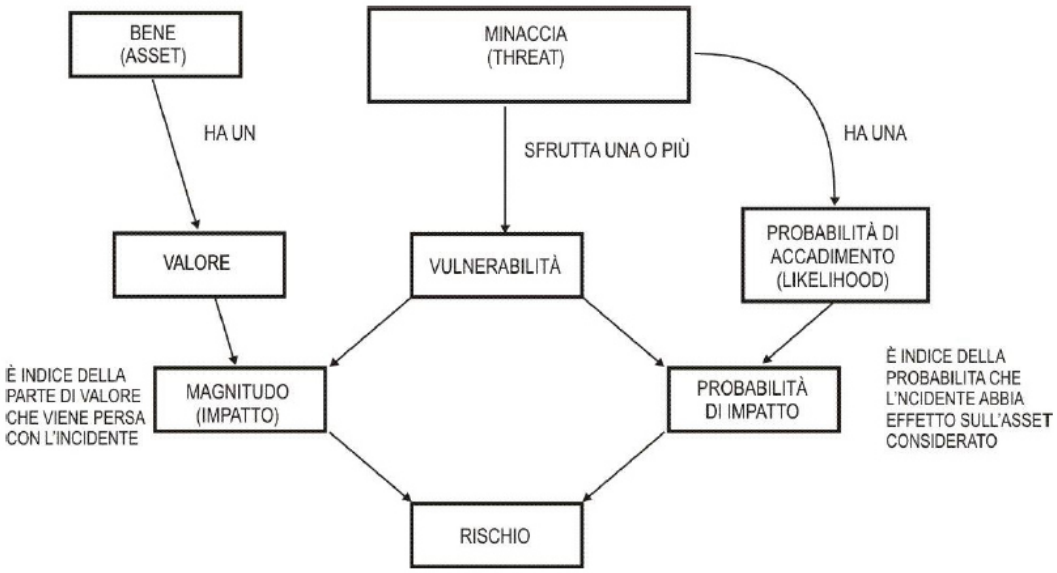

Figura 10 - Esempio di Schema di Risk Assessment

La gestione dei rischi per essere effettivamente efficace, deve essere totalmente integrata nell'SDLC: