Progettazione: in questa fase si esamina il sistema in divenire con l'ausilio di tecniche di analisi e modellazione delle minacce. Requisiti di sicurezza di maggior dettaglio si aggiungono quindi a quelli prodotti nella precedente fase.

Implementazione: in questa fase si realizza il sistema attraverso la stesura di codice sicuro. Seguono l'esecuzione di test di sicurezza basati sull'analisi delle minacce e l'analisi statica del codice sorgente. Quest'ultima può produrre nuovi requisiti di sicurezza, che possono portare alla revisione del codice.

Verifica: in questa fase si analizzano gli aspetti di sicurezza del sistema in esecuzione in un ambiente controllato impiegando tecniche e strumenti di analisi dinamica;

Validazione: è la fase immediatamente prima del rilascio, nella quale viene effettuata una final security review per la verifica del rispetto dei requisiti.

Supporto: in questa fase si esamina il sistema in essere con l'ausilio di tecniche di: analisi e modellazione delle minacce e/o verifica statica/dinamica del codice applicativo, al fine di produrre nuovi requisiti di sicurezza di dettaglio per indirizzare un'eventuale fase di reingegnerizzazione e/o di patching del sistema in oggetto.

6.2 Risk Assessment

L'obiettivo dell'analisi del rischio è da una parte identificare, valutare e misurare la probabilità e la gravità dei rischi (ciò che viene generalmente indicato con il nome di *Risk Assessment*) nei diversi processi dell'organizzazione e, dall'altra decidere come comportarsi a fronte dei rischi identificati (ciò che viene generalmente indicato con il nome di *Risk Management*) al fine di minimizzarli o eliminarli.

Si fornisce di seguito, una classificazione dei principali rischi:

- Rischio strategico, derivante dall'incompatibilità tra due o più dei seguenti fattori:
  - obiettivi strategici,
  - strategie di business,
  - mezzi utilizzati per raggiungere gli obiettivi,
  - quadro macroeconomico nel quale opera l'organizzazione.
- Rischio reputazionale, che può manifestarsi in molteplici situazioni, per esempio in caso di mancato soddisfacimento della clientela.
- Rischio finanziario, derivante dall'incapacità di assolvere gli oneri finanziari assunti.
- Rischio operativo, che è connesso ai processi utilizzati per definire le strategie.
- Rischi di compliance, derivanti da inadempienze legislative (normative e regolamenti).
- Rischi di gestione delle informazioni, derivanti da un insufficiente livello di sicurezza dei sistemi informatici.
- Rischi emergenti e/o potenziali che potrebbero danneggiare il business dell'organizzazione e/o le persone che vi operano.

La gestione del rischio comprende tre attività principali:

- Risk Assessment che include l'identificazione e la valutazione dei rischi e degli impatti; le raccomandazioni e le misure per la riduzione del rischio;
- Mitigazione del rischio, che si riferisce alla prioritizzazione, implementazione e mantenimento delle misure appropriate per la riduzione del rischio raccomandate dal processo di Risk Assessment;
- Valutazione e analisi dei processi e delle misure per l'implementazione di un programma di gestione del rischio di successo (vedi paragrafo 6.2.1).

Una metodologia di gestione del rischio ben strutturata, se utilizzata in modo efficace, può aiutare l'organizzazione a identificare i controlli adeguati per garantire le capacità di sicurezza essenziali.