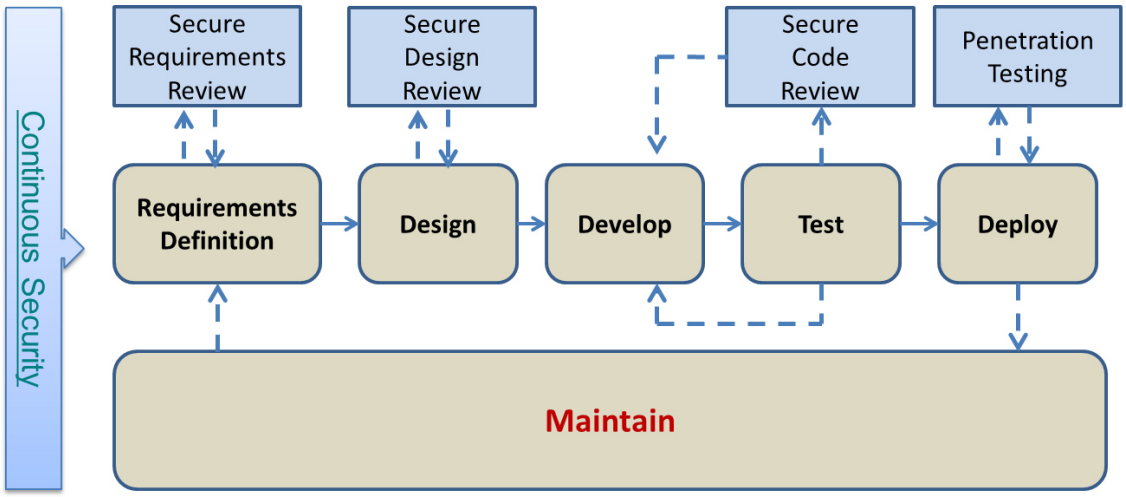

Figura 26 - Continuous Security

Qualsiasi modifica a un sistema ha il potenziale per ridurre l'efficacia dei controlli esistenti o per avere in qualche modo un impatto sulla riservatezza, sulla disponibilità o sull'integrità dello stesso. La soluzione è garantire che nella valutazione delle modifiche del sistema sia inclusa una fase di valutazione del rischio (paragrafo 6.2). Sfortunatamente, non solo i sistemi, ma anche le minacce possono cambiare. Quando vengono identificate nuove minacce, potrebbero essere necessari nuovi controlli per portare il rischio a un livello accettabile. Questo è il motivo per cui le valutazioni periodiche del rischio sono importanti, anche quando un sistema cambia raramente. La valutazione del rischio può fornire un ulteriore vantaggio in per migliorare l'efficacia di politiche, procedure e formazione.

9.5.1 Identificazione degli strumenti a supporto

In ottica di un processo di 'Continuous Security', in questa fase vengono attuate di nuovo le azioni afferenti alle diverse fasi di: Revisione dei requisiti di sicurezza, revisione dei risultati di progettazione, revisione degli aspetti di sicurezza del codice sorgente implementato, penetration test del codice rilasciato.

Gli strumenti per le fasi sopra menzionati sono stati già identificati e indicati nei precedenti paragrafi:

- Definizione dei requisiti di sicurezza [Par. 9.1.1];
- Progettazione di applicazioni sicure [Par. 9.2.1];
- Implementazione di applicazioni sicure [Par. 9.3.1];
- Verifica della sicurezza delle applicazioni [Par. 9.4.1].