- A completamento di questa fase è necessario produrre la Reportistica/documentazione completa che sintetizza i risultati per ogni punto precedente.

Figura 18 - Input e Output della fase Risk Assessment

Si evidenzia che in questa fase devono essere tenuti in considerazione anche gli aspetti di integrazione e di interfaccia con eventuali altri moduli dell'ecosistema software. Inoltre vanno considerati i requisiti di sicurezza applicativa di carattere generale: Performance, Password nel codice sorgente, Privilegi esecutivi minimi, Fattore di integrità, Input data validation, Gestione dell'output, etc. (per ulteriori dettagli si rinvia al al paragrafo 4.1 "Progettazione e sviluppo dell'Applicazione: direttive standard" del documento ***Allegato 2 - Linee Guida per lo sviluppo sicuro di codice***). Tali requisiti di sicurezza applicativa devono essere mutuati in questa fase sulla base dei requisiti, funzionali e non funzionali, individuati.

9.1.1 Identificazione degli strumenti a supporto

Nel paragrafo 6.3.2 è stato presentato lo stato dell'arte dei tool a supporto di questa fase. Di seguito viene fornito un esempio di approccio metodologico per la valutazione dei tool.

La baseline comparativa è costituita da 8 parametri (Software Security Requirements). I tool vengono analizzati sulla base di questi parametri. Il risultato è illustrato nella tabella che segue:

Tools	Fair Exchange	Non-repudiation	Rbac	Secrecy & Integrity	Authenticity	Secure Informat. Flow	Guarded Access	Freshness
RequisitePro	√	X	X	X	X	X	X	√
CaseComplete	√	X	X	X	X	X	X	√
Analyst Pro	√	X	√	X	√	X	X	X
DOORS	√	X	√	X	√	X	√	√
Objectiver	X	X	X	X	X	X	X	√
RDT	X	X	X	X	X	X	X	√
RDD-100	√	X	X	X	X	X	X	√
RTM	X	X	√	√	√	X	√	√
Reqtify	√	X	X	X	X	X	X	√
TcSE	X	√	√	√	√	√	√	√
Atlas	X	√	√	√	√	√	√	√
Visure RMT	X	X	√	X	X	X	X	X