

SCRAT è un prodotto di



info: [scrat@nispro.it](mailto:scrat@nispro.it)

Versione 1.0  
Maggio, 2011

The SCRAT logo consists of a green acorn icon positioned above the word 'SCRAT' in a large, bold, green, sans-serif font. Below 'SCRAT', the words 'Security Risk Assessment Tool' are written in a smaller, green, sans-serif font, enclosed within a green rounded rectangular border.

# SCRAT

Security Risk Assessment Tool

NETWORK INTEGRATION and SOLUTIONS srl – [www.nispro.it](http://www.nispro.it)

**MAIN OFFICE**

Via al Porto Antico 7 - Edificio Millo  
16128 GENOVA  
Phone. 010 5954946  
Fax. 010 8680159

**OPERATIONAL OFFICES**

GENOVA  
MILANO  
ROMA

Per maggiori informazioni  
contattare:  
[scrat@nispro.it](mailto:scrat@nispro.it)

Garantire la conformità dei servizi rispetto alle direttive ed alle disposizioni normative richiede un impegno costante nell'armonizzazione e nel governo della sicurezza tra i diversi ambiti aziendali.

Questi obblighi suggeriscono alle aziende di intraprendere un percorso per lo sviluppo e l'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni, nell'ambito delle proprie attività operative.

Considerando la complessità legata alla realizzazione ed all'esercizio del SGSI, il Tool si pone come parte integrante della metodologia per la analisi e gestione del rischio dei processi operativi interni allo stesso SGSI.

**ScRAT –Security Risk Assessment Tool** e la metodologia associata sono uno strumento per la valutazione dei rischi, tenendo conto degli asset aziendali, delle minacce e delle vulnerabilità identificate all'interno dell'Ambito di Applicazione e le risultanze ottenute in termini di report di rischio e di relativo piano di trattamento.

**ScRAT** è uno strumento di supporto all'Analisi, alla Valutazione e alla Gestione dei Rischi in relazione agli asset, alle vulnerabilità che li caratterizzano ed alle minacce cui sono sottoposte. Partendo dalla raccolta delle informazioni effettuata presso i siti operativi facenti parte del perimetro in oggetto, vengono applicati gli algoritmi di analisi che portano alla valutazione del rischio. In base alla logica di aggregazione, viene presentata la definizione del rischio accettabile, i report di valutazione del rischio con i risultati numerici da cui si può evincere il piano di trattamento comprendente le attività (controlli) volte alla mitigazione dei rischi identificati.



#### METODOLOGIA

La classificazione degli asset informativi riflette l'importanza ad essi attribuita dal management, in tal senso si può stabilire una diretta dipendenza fra i risultati dell'analisi del rischio e gli obiettivi di sicurezza stabiliti nelle politiche.

La corretta identificazione delle minacce è un elemento di basilare importanza in quanto il valore del rischio calcolato viene messo in relazione alla minaccia.

La valutazione dei rischi si applica a tutti gli asset del perimetro aziendale coinvolti nell'ambito di applicazione, con particolare riferimento agli asset tecnologici, informativi e infrastrutturali, nonché alle risorse umane a supporto dell'erogazione del servizio.

L'analisi dei rischi costituisce un elemento essenziale nell'ambito della componente di Governance relativa alla sicurezza.

L'approccio preventivo mira ad individuare anticipatamente le contromisure atte a ridurre la probabilità che gli incidenti si verifichino.

#### L'ANALISI DEL RISCHIO: PRINCIPI E METODI

A livello teorico, le metodologie per l'analisi e la gestione del rischio possono essere distinte in due principali categorie:

- Qualitativa: valutazione del rischio su base qualitativa. Essa risulta più semplice e veloce da implementare ma è fortemente condizionata da valutazioni soggettive;
- Quantitativa: le valutazioni sono ricondotte ad un valore numerico puntuale (solitamente inteso come la perdita economica derivante dal verificarsi di un evento dannoso). Risulta notevolmente più complessa da implementare e richiede una valorizzazione degli asset.

L'approccio di NIS è rappresentato nel seguente schema:



## ANALISI DEL RISCHIO

Una prima sezione consente di configurare e gestire l'asset management in base alle categorizzazioni definite per lo specifico ambiente.

### Preparazione e Pianificazione

E' svolta mediante una preliminare serie di interviste ai vari responsabili di processo/funzione per la raccolta degli elementi atti ad identificare gli asset da proteggere, andando così a definire nel dettaglio il perimetro di analisi.

### Definizione delle categorie

E' la fase di definizione delle categorie e sottocategorie di appartenenza e attribuzione della relativa tipologia. Questo consente di raggruppare le tipologie di asset e informazioni al fine di poter associare successivamente le minacce e le vulnerabilità che su questi incombono.

### Classificazione degli asset

Tale fase prevede l'identificazione del valore degli asset rispetto all'impatto causato da un'eventuale perdita di riservatezza, disponibilità ed integrità degli stessi. Il valore dell'asset così determinato costituisce la prima variabile in input per la Matrice di Rischio.

Gli elementi atti ad identificare gli asset del perimetro sono suddivisi sulla base dei servizi supportati, andando così a definire il perimetro per ognuna delle funzioni all'interno dello scopo.

### Identificazione delle minacce

La corretta identificazione delle minacce è un elemento di basilare importanza in quanto il valore del rischio calcolato viene messo in relazione alla minaccia.

A ciascuna minaccia e in riferimento al tipo di asset (elemento desunto dalla precedente classificazione) sul quale la minaccia può ragionevolmente incombere, viene assegnata una terna di valori che, su base qualitativa, definisce la gravità degli impatti per ciascuno dei tre aspetti del RID. La terna ottenuta viene poi riconvertita in un valore unico che esprime l'impatto globale. Tale valore costituisce la seconda variabile in input per la Matrice di Rischio.

### Identificazione delle vulnerabilità

Come per la fase precedente, il processo adottato volto all'identificazione delle vulnerabilità prende in considerazione esclusivamente quelle riguardanti gli asset ed il contesto in cui esse operano. Nello specifico, le vulnerabilità identificate sono suddivise in categorie e relazionate ad un set di minacce in grado di sfruttarle. A ciascuna di esse viene attribuito un valore qualitativo che tiene conto delle eventuali contromisure già implementate. Tale valore costituisce la terza variabile in input per la Matrice di Rischio.

## IDENTIFICAZIONE DEL RISCHIO

### Popolamento del modello

Il modello viene popolato con l'inventario degli asset e l'attribuzione, a ciascuno di essi, della categoria di appartenenza e classe (con il relativo punteggio derivante dalla scala precedentemente definita).

### Identificazione del Rischio Accettabile

Con il termine rischio accettabile si intende il valore al di sotto del quale l'Azienda ritiene di non dover implementare contromisure di sicurezza volte alla riduzione del livello di rischio.

### Valutazione del Rischio

Il calcolo del Rischio viene effettuato mediante un algoritmo matematico che mette in relazione le tre variabili precedentemente definite.

Il valore di rischio è determinato come funzione del valore dell'asset, dell'impatto della minaccia su un determinato asset e della vulnerabilità intesa come grado di debolezza del sistema o asset alla specifica minaccia. E' una grandezza derivata dalle seguenti tre variabili:

- Livello di classificazione dell'asset.
- Impatto della minaccia.
- Vulnerabilità associata alla minaccia.

La valutazione dei rischi produce come risultato un valore che viene associato in maniera diretta all'asset preso in esame.

## TRATTAMENTO DEL RISCHIO

I risultati prodotti dalla valutazione del rischio vengono presentati sotto forma di report e di un template di piano di trattamento. Tale piano deve essere necessariamente completato attraverso la definizione di attività e fasi progettuali, che possono prevedere sia interventi di natura tecnico-operativa che di natura organizzativa. A fronte dell'applicazione del Piano di Trattamento, per ogni asset rimarrà associato un rischio residuo che tipicamente dovrà essere inferiore o uguale al rischio accettabile.

## ScRAT – SECURITY RISK ASSESSMENT TOOL

Il Security Risk Assessment Tool è uno strumento in grado di implementare la metodologia precedentemente descritta.

Il servizio viene erogato da NIS mediante una soluzione web che mette a disposizione del cliente tutte le funzionalità necessarie alla gestione del risk assessment sui propri sistemi.

Il tool integra i vantaggi del metodo semi-quantitativo, garantendo al tempo stesso:

- **Semplicità e rapidità di configurazione e utilizzo** – capacità di delineare le fasi di sviluppo dell'analisi dei rischi in tempi rapidi e con semplicità di utilizzo.
- **Flessibilità** – possibilità di effettuare analisi a diversi livelli di dettaglio, partendo dalle risorse principali, fino a scendere a tutti gli asset del servizio; capacità di effettuare valutazioni a livello di sottosistemi e aggregazioni di fattori di rischio.
- **Produzione di risultati consistenti e ripetibili** – lo strumento deve essere in grado di poter ripetere ad intervalli regolari o ad occorrenza la valutazione al fine di ottenere risultati confrontabili, ripetibili e oggettivi.
- **Scalabilità** – la metodologia deve potersi adattare in relazione alla evoluzione del business o alle dimensioni dell'organizzazione per la quale viene applicata

Lo strumento utilizzato per il calcolo del rischio viene alimentato in input dai dati raccolti attraverso interviste mirate al personale aziendale, riguardanti l'esistenza e il livello di applicazione dei pertinenti controlli sicurezza.



Altre informazioni possono essere reperite da altre analisi condotte in materia di Sicurezza delle Informazioni all'interno dell'azienda. Pertanto, il processo di analisi e gestione dei rischi diventa parte integrante della gestione aziendale.

Al fine di automatizzare quanto più possibile tale processo e di standardizzare la tipologia dei dati in ingresso, il tool presenta una checklist in forma di questionario che, attraverso l'utilizzo di domande ad hoc, mappa i controlli ISO/IEC 27001:2005, ma potenzialmente è applicabile ai controlli di altre normative (tra cui il DPS ai sensi del D.Lgs 196/03).

Il risultato di tale check list viene automaticamente fornito in input agli algoritmi di calcolo del rischio, consentendo al tempo stesso di popolare il modello in modo ripetibile nel tempo e standardizzato.

Le vulnerabilità caratteristiche di ciascun ambiente considerato possono quindi facilmente emergere come mancata applicazione di uno o più controlli previsti dallo schema di riferimento.

## Anagrafica

Il tool mette a disposizione un'ampia sezione di anagrafica in grado di gestire contemporaneamente diverse utenze e molteplici profili autorizzativi di accesso alle sue funzionalità.



## Definizione degli asset

In prima istanza il tool consente la definizione delle categorie degli asset in maniera gerarchica in modo da poter effettuare una corretta mappatura degli asset istanziati all'interno delle aree operative.

Category	Sub-Category	Asset Type	Typology
ASSET FISICI	EQUIPMENT	Equipment ambientali e tecnologici	Asset
		Equipment di Rete	Asset
		Media	Asset
		Sistemi di alimentazione	Asset
	HARDWARE	Client	Asset
		Server	Asset
		Storage (SAN, Tape Libran)	Asset
	LOCATION	Area Operativa	Asset
		Building	Asset
		CDN	Asset

## Classificazione degli asset

La scala di punteggi che determina il valore dell'asset in termini qualitativi (in base all'impatto) è definita su una scala a n livelli, derivante dall'applicazione di criticità in termini di Riservatezza, Integrità e Disponibilità, poi convertita numericamente.

## Popolamento del modello

Il modello è quindi popolato con tutti gli asset del perimetro a partire dagli asset fisici fino alle risorse umane e alle informazioni.

Ad ogni asset è assegnato un valore secondo la scala di punteggi di cui sopra e un insieme di metadati che li caratterizzano.

Tramite questa relazione è possibile periodicamente ridefinire gli asset e la loro criticità all'interno del perimetro preso in considerazione.

Ad ogni asset è associato l'owner di riferimento, con indicazione sia del centro di competenza, sia delle persone direttamente responsabili dell'asset.

E' poi prevista una breve descrizione dell'asset, in termini di informazioni dettagliate, posizionamento, relazione con altri asset.

Le informazioni relative agli asset possono essere inserite a partire da sorgenti esterne in vari formati e gestite internamente al tool, tenendo traccia delle loro interdipendenze.

Attraverso l'utilizzo di template predefiniti, è possibile estrarre ed utilizzare la configurazione più appropriata per l'ambiente oggetto dell'analisi, definendo in maniera rapida ed efficace il perimetro.

## Identificazione delle minacce

L'apposita sezione consente di identificare le minacce all'interno della metodologia di analisi dei rischi, raggruppandole secondo macro categorie.

Per ogni macro categoria sono configurabili le minacce corrispondenti ed possibile descrivere il tipo di danno che quella determinata minaccia provoca.

A partire da questa analisi, sarà possibile definire le contromisure da intraprendere, in relazione all'impatto della minaccia sullo specifico asset.

E' possibile aggiornare il set di minacce e vulnerabilità in relazione all'evolversi del contesto tecnologico e dei requisiti di business aziendali.

## Identificazione delle vulnerabilità

La sezione di identificazione delle vulnerabilità consente di evidenziare quali sono gli elementi di criticità specifici, sui quali si può verificare una situazione di rischio.

Le vulnerabilità si possono pertanto considerare come degli elementi caratteristici degli asset del servizio considerato, suddivisibili in categorie.

Per ogni categoria vengono definite le vulnerabilità relative ai servizi e una breve descrizione.

Le vulnerabilità sono quindi messe in relazione al tipo di asset attraverso la relazione con le minacce.



## Valutazione del rischio

La sezione di calcolo del rischio, in funzione delle variabili impatto/minaccia/vulnerabilità calcola il risultato dell'analisi per ogni tipo di asset.

Le tre variabili di ingresso sono:

- Impatto Globale della Minaccia
- Vulnerabilità associata alla minaccia
- Valore relativo all'impatto sull'asset

Il calcolo del rischio viene effettuato mediante un algoritmo matematico che mette in relazione le tre variabili precedentemente definite. Vengono evidenziati i livelli di rischio uguali o superiori a quello accettabile, al fine di individuare qualitativamente l'esposizione al rischio del sistema o asset.

I risultati del calcolo del rischio possono essere aggregati sulla base delle minacce identificate. Per ciascuna di esse vengono quindi riportati i valori di rischio associati a ciascun asset, in relazione ad ognuna delle vulnerabilità che può essere sfruttata dalla minaccia in esame.

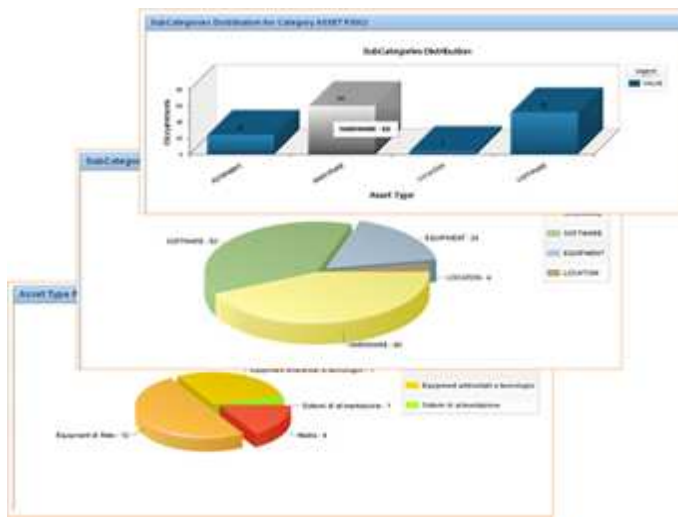
Il risultato è ricalcolabile a distanza di tempo, garantendo la ripetibilità della valutazione dei rischi, nonché la sua oggettività in base ai valori di ingresso.

Ogni valutazione è associata ad un ciclo di raccolta (in termini asset, minacce, vulnerabilità) rendendo così possibile seguire i risultati dell'analisi nel corso del tempo a fronte dei piani di trattamento svolti.

E' possibile inoltre ottenere una valutazione del rischio associata ad una specifica applicazione o processo come il risultato della valutazione effettuata su tutti gli asset che la compongono (informazioni, hardware, software, reti, risorse umane, ecc.).

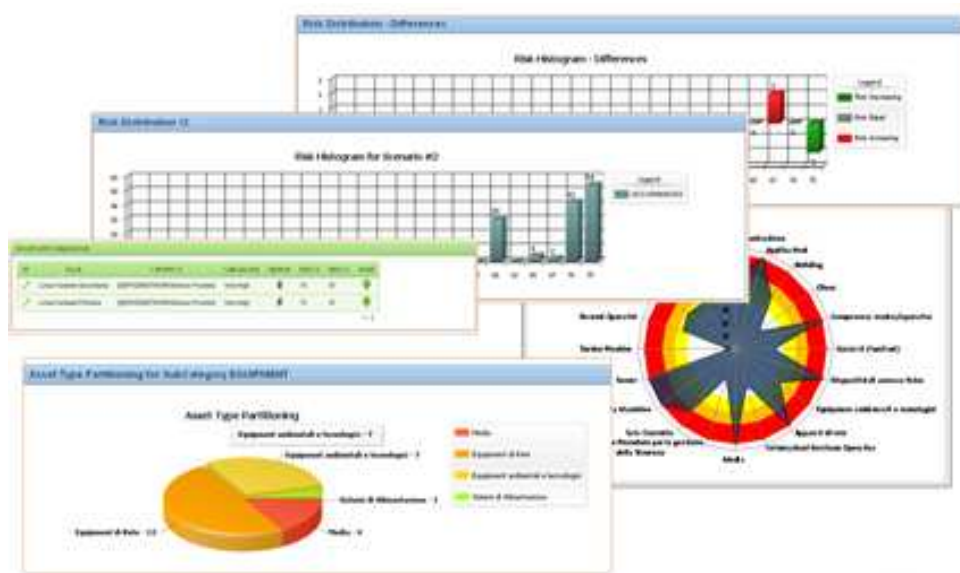
## Definizione del piano di trattamento

Il tool fornisce infine una sezione con una serie di report volti ad evidenziare i valori di rischio associati a ciascuna minaccia ed a fornire le indicazioni atte a pianificare gli interventi e le contromisure di sicurezza necessarie alla riduzione dello stesso a livelli ritenuti accettabili per l'organizzazione.



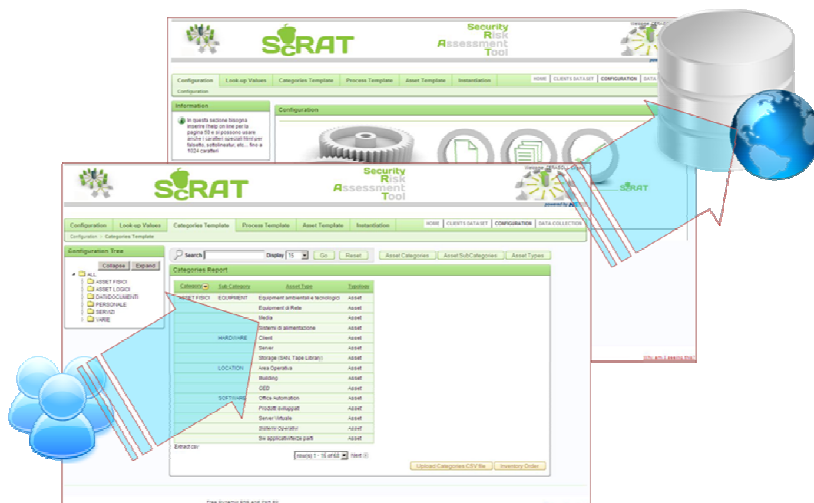
**Simulazione con differenti scenari**

La possibilità di eseguire cicli differenti e ripetuti di valutazione del rischio, in funzione di vari cicli di raccolta in termini di asset, minacce e vulnerabilità consente di creare diversi scenari in cui i parametri di input possono essere variati al fine di osservare il comportamento del sistema in output.



**ScRAT – L'ARCHITETTURA**

Il tool è stato implementato sfruttando una tecnologia web oriented per garantire la massima accessibilità e flessibilità ed un'architettura basata su database Oracle per fornire i requisiti di sicurezza e protezione del dato indispensabili al trattamento di dati sensibili.



Browser: Internet Explorer 8 o superiore, Mozilla Firefox 3 o superiore  
 Web Server / Application Server: Oracle 10G o superiore  
 Print Server: Oracle OC4J – Oracle BI Publisher