

## Security Assessment

**Obiettivi:** Rilevare eventuali criticità tecnologiche, fisiche ed organizzative presenti nella struttura, al fine di valutare oggettivamente i principali rischi di sicurezza a cui risulta esposto il patrimonio informativo aziendale.

**Metodo:** Integrare l'approccio metodologico del Risk Assessment con quello del Penetration Test che, grazie all'uso di tecniche di attacco inferenziali, consente di accertare l'entità delle vulnerabilità presenti.

**Strumenti:** ISO/IEC 27005, OSSTMM, Penetration Test Tools.

## Risk Management

**Obiettivi:** Identificare e quantificare i rischi a cui l'organizzazione in esame è soggetta e guidare gli investimenti per la sicurezza, al fine di ridurli ad un livello accettabile.

**Metodo:** Condurre un ciclo completo di Analisi e Gestione dei Rischi di tipo qualitativo e/o quantitativo, seguendo standard internazionali riconosciuti, fino alla stesura del Piano di Trattamento dei Rischi (RTP) a copertura delle criticità riscontrate.

**Strumenti:** Risk Analysis Tools (Pilar, Cramm, Thor, ecc.); ISO/IEC 27005.

## Business Continuity

**Obiettivi:** Assicurare la continuità dei servizi di natura critica, anche in presenza di eventi indesiderati che possono causare il fermo prolungato dei sistemi e dei processi di elaborazione delle informazioni.

**Metodo:** Individuare il perimetro di applicazione, i ruoli e le relative responsabilità; condurre una Business Impact Analysis (BIA); definire ed attuare

strategie di continuità opportune; formalizzare un Piano di Continuità Operativa (BCP) e relative procedure; condurre una serie di esercitazioni e di verifiche al fine di validare le strategie di continuità scelte.

**Strumenti:** Risk Analysis Tools; BS 25999.

## Disaster Recovery

**Obiettivi:** Trasferire l'operatività e i dati di natura vitale da un centro primario a un centro secondario, nel caso in cui il primo sia coinvolto in una situazione di natura disastrosa (es. alluvione, black out, ecc.).

**Metodo:** Analizzare i processi e le soluzioni disponibili in base ai requisiti di business ed elaborare un Piano di Disaster Recovery (DRP) che riporti le procedure, ma anche le responsabilità ed il modus agendi in caso di "disastro"; assistere l'organizzazione durante la pianificazione e l'effettuazione dei necessari test di tale piano.

**Strumenti:** Normative nazionali ed internazionali.

## Solution Selection

**Obiettivi:** Individuare la migliore soluzione tecnologica ed organizzativa implementabile, finalizzata ad ottimizzare i flussi delle informazioni ed i processi aziendali che le governano.

**Metodo:** Analizzare i bisogni ed il work flow; identificare gli obiettivi di breve/medio/lungo periodo; stabilire i requisiti (capitolato tecnico); definire i parametri di valutazione e relativi pesi; ricercare le soluzioni ed i potenziali fornitori; analizzare le offerte e preparare la griglia di valutazione tecnico-economica; assistere l'organizzazione nella scelta, implementazione e validazione della soluzione.

**Strumenti:** BPI Matrix.

