CONTROLLI E STRUMENTI DI PREVENZIONE

SISTEMI INFORMATIVI

Situazione di rischio	*Controllo*
Sicurezza informatica: presenza di segnali sulla incapacità di prevenire incidenti di sicurezza IT, quali ad es. l'accesso non autorizzato a dati e informazioni o la non Compliance normativa (Legge 262 del 2005; Decreto Legislativo 231 del 2001; Decreto Legislativo 196 del 2003). Perdita di controllo e integrità delle informazioni. Disservizi o ritardi nell'erogazione del servizio. Copia di dati, uso illegale di sistemi e informazioni, sottrazione/ diffusione di dati sensibili. Perdita di dati sensibili e critici per il business	• Valutazione del livello di sicurezza degli applicativi (sicurezza logica, modelli di autenticazione, accesso a data base, processo di change applicativo) e delle infrastrutture ICT (dispositivi di protezione perimetrale, apparati di interconnessione, rete locale, postazioni di lavoro, data center). • Comprensione e valutazione delle regole di gestione della sicurezza dei servizi erogati sia internamente (portali intranet, file server, user access) sia esternamente (portali web, portali mobile, app). • Rilevazione di eventuali vulnerabilità che possano consentire a soggetti non autorizzati di violare le politiche di sicurezza esistenti e accedere in modo non autorizzato agli ambienti informatici della società. • Analisi delle configurazioni ed esecuzione di test automatizzati e di controlli manuali, finalizzati all'individuazione della presenza di vulnerabilità dell'ambiente applicativo e sistemistico. • Rilevazione e valutazione dell'efficacia del sistema di gestione delle informazioni in termini di: Data Classification Policy & Process, Data Privacy e Data Quality, con particolare focus sui sistemi a supporto della gestione delle informazioni • Verifica della sicurezza fisica, logica e ambientale dei Data Center. • Verifica dell'architettura di sicurezza e delle procedure per la gestione della sicurezza dei Data Center (controlli degli accessi, gestione dei visitatori, identificazione e protezione degli asset) • Valutazione dell'efficacia dei controlli ambientali a prevenzione del rischio di interruzione a causa di eventi naturali (incendi, assenza di energia elettrica, condizioni atmosferiche)

Situazione di rischio	*Controllo*
Terziarizzazione servizi IT: supporto non adeguato alle esigenze di Business ed erogazione dei servizi non in linea con i livelli di servizio definiti. Erogazione non completa dei servizi	• Verifica dell'efficacia delle procedure esistenti per il governo degli outsourcer e la gestione dei relativi aspetti contrattuali • Verifica delle modalità di gestione dei servizi IT erogati dagli Outsourcer, con particolare focus su performance dei processi ICT e sull'operatività ricorrente, Service Desk, gestione delle Postazioni di Lavoro. • Verifica che i servizi forniti siano erogati in accordo con i livelli di servizio definiti (Service Level Agreement – SLA, Operational Level Agreement – OLA).
Dimensionamento: disservizi o degrado delle prestazioni. Incapacità di supportare picchi di utilizzo. Danni di immagine dovuti a interruzioni del servizio o altri disservizi Insoddisfazione del cliente	• Verifica dell'adeguatezza del dimensionamento e della capacità delle infrastrutture tecnologiche rispetto ai volumi e carichi da gestire entro i prefissati obiettivi di performance. • Verifica del livello di scalabilità delle infrastrutture e della conseguente capacità di adattarsi rapidamente e facilmente alle richieste del business.
Assenza o mancato aggiornamento di un disaster recovery plan	Verifica dell'efficacia del sistema di Disaster Recovery in essere, in termini di Piani di Recovery e di Gestione della Crisi, Procedure Operative, test delle soluzioni e awareness del personale, con particolare focus sui Data Center e sulle principali applicazioni amministrativo contabili (e.g. SAP), servizi infrastrutturali (e.g. Posta elettronica) e servizi di Business (e.g. Portali web, Siti mobile, APP).
Profili utente: incoerenza delle configurazioni dei sistemi e violazioni del principio di separazione dei compiti	• Verifica della presenza ed utilizzo di appositi strumenti informatici per la gestione dei profili utente. • Analisi dei profili di autorizzazione implementati a sistema al fine di evidenziare eventuali stratificazioni o incongruenze / verifica di violazioni SoD • Verifica dei controlli compensativi • Verifica dell'implementazione di una reportistica riepilogativa dei conflitti.