Information Risk Management

SAP Basis Components Controls

Giornata di studio AIEA

Torino, 02 Dicembre 2010

IT ADVISORY

Agenda

- IT Risk & Compliance: Requisiti Normativi Italiani
- IT Risk & Compliance: Requisiti Normativi Italiani - Impatti sul Sistema Informativo SAP
- SAP Basis Components: Definizione
- SAP Basis Components: Un unico approccio per la gestione delle SAP IT Operations
- Business Users e IT Users: Logiche di Controllo
  - SAP Programs Execution Controls
  - SAP Change Management Controls
  - SAP Logical Security
  - SAP Production Environment Security Management
    - Authorizations Monitoring Logics
    - Control Objectives

IT Risk & Compliance
Requisiti Normativi Italiani

Negli ultimi anni, un crescente numero di normative ha indirizzato le esigenze degli stakeholder verso una maggiore attenzione alla gestione del rischio e della compliance finanziaria.

In analogia con quanto introdotto dal *Sarbanes-Oxley Act negli US, la normativa 231/01 e successivamente la normativa 262, oltre che specifiche Normative di Settore, hanno introdotto in Italia l'obbligo per le società di adempiere alle leggi:*

- *231/01 - Corporate Governance Italiana: "Responsabilità amministrativa delle persone giuridiche, società e delle associazioni anche prive di personalità giuridica" Disposizione per prevenire i reati commessi all'interno della propria organizzazione nei rapporti con la pubblica amministrazione e con i privati; una particolare rilevanza è data alla prevenzione dei reati informatici;*
- *262/05 - Tutela del Risparmio: Disposizioni per la tutela del risparmio e la disciplina dei ercati finanziari;*
- *96 del 30/06/2003 - Privacy: Normative in materia di protezione dei dati personali;*
- *rmative di Settore: Requisiti richiesti da Enti/Funzioni di controllo o da altre leggi (Banca lia, ISVAP,…).*

IT Risk & Compliance
Requisiti Normativi Italiani

Le norme italiane sottolineano la centralità delle procedure amministrativo contabili, intese come l'insieme delle disposizioni interne e degli strumenti che consentono di ricostruire le modalità, i tempi e le responsabilità connesse allo svolgimento delle attività.

Le procedure incorporano anche i controlli che devono essere posti a presidio dei rischi assunti nell'operatività.

La predisposizione di adeguate procedure richiede:

- L'individuazione delle attività rilevanti ai fini della predisposizione dei documenti contabili societari;
- L'individuazione della strumentazione informatica a supporto;
- La predisposizione di un adeguato sistema di controllo interno;
- L'individuazione dei principali rischi e dei connessi controlli;
- La formalizzazione delle modalità di svolgimento delle attività, anche con riferimento alle attività di controllo e al funzionamento degli applicativi;
- La valutazione della documentazione prodotta in termini di completezza, coerenza, conformità alle normative di settore e di adeguatezza dei controlli previsti;
- Un continuo processo di monitoraggio, controllo e miglioramento.

IT Risk & Compliance
Requisiti Normativi Italiani: Impatti sul Sistema Informativo SAP

Le attuali normative e politiche societarie finalizzate alla gestione dei rischi determinano che le Società devono rispondere a nuove esigenze per soddisfare i diversi requisiti di Governance, Trasparenza e Responsabilità.

I sistemi ERP e in particolare SAP, consentono al management delle Società di rispondere a queste esigenze; tuttavia la relativa pervasività all'interno dei processi business e complessità dei processi di implementazione iniziale e di successiva manutenzione, hanno spesso indotto a sottovalutare l'importanza o sovrastimare l'effort necessario per l'adozione di un'adeguata applicazione di metodologie e strumenti di controllo e di governo delle operations IT.

L'adempimento delle normative e delle disposizioni di legge, determina la necessità di attivare controlli che riducano la probabilità di accadimenti che possano avere impatto su disponibilità integrità e riservatezza dei dati, attraverso:

- L'individuazione delle potenziali aree a rischio e miglioramento dei processi IT gestiti in SAP che potrebbero compromettere l'esattezza e veridicità del dato;
- Lo sviluppo di controlli sui privilegi di accesso IT che, essendo integrati nella configurazione di SAP, diventano automatici e non più quindi affidati unicamente al controllo umano.

SAP Basis Components

Definizione

SAP Basis Components, come evidenziato dal suo nome, è una parte fondamentale dei sistemi SAP. Tuttavia, è difficile rispondere alla domanda che cosa è esattamente il modulo SAP Basis Components in quanto comprende molteplici componenti:

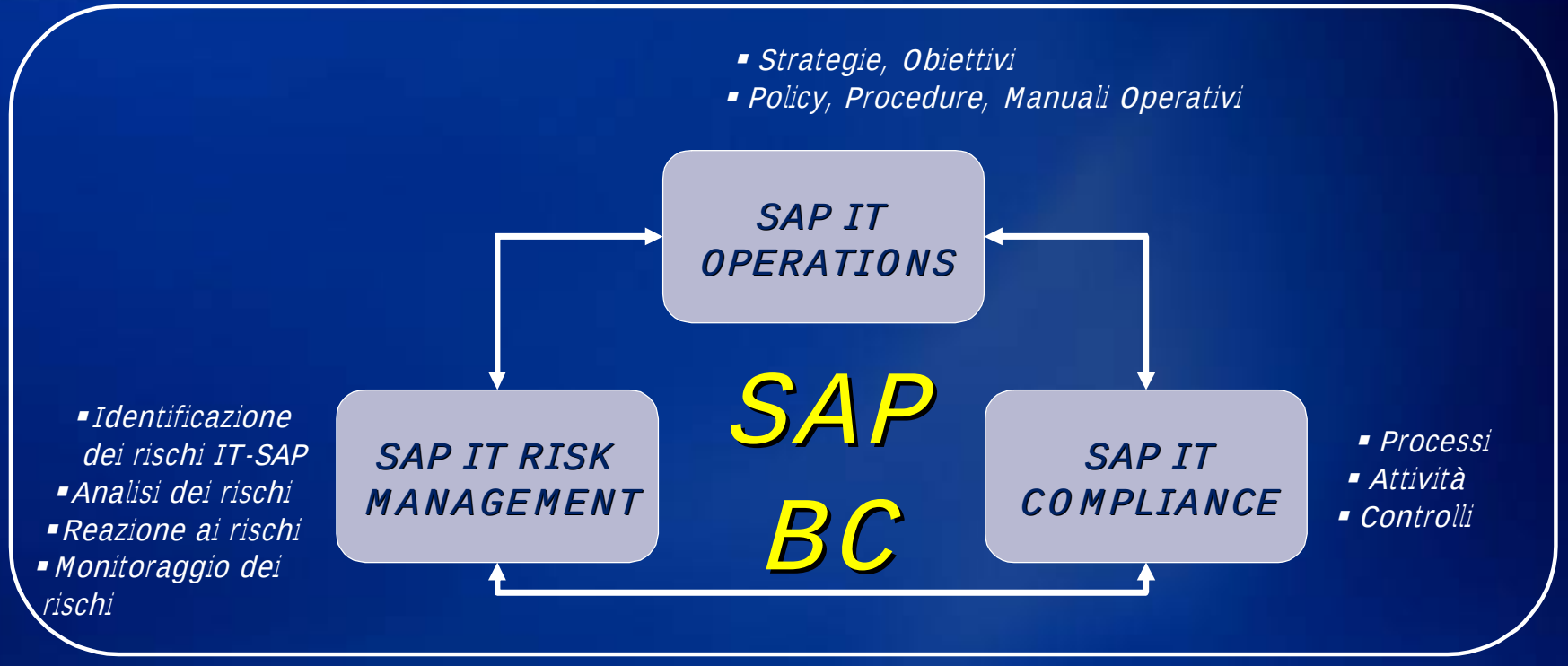
- Architettura e configurazione client / server : fondamento tecnico dei SAP Basis Components
- Database relazionali (RDBMS): gestisce molti aspetti della gestione di database tradizionali
- Graphical user interface (GUI): l'interfaccia attraverso la quale l'amministratore Basis interagisce con i sistemi SAP
- Ambiente di sviluppo: in questo sistema ha origine lo sviluppo dei Basis Components
- Data Dictionary: sono una parte indispensabile del processo di sviluppo.
- Amministrazione dell'utente e del sistema e strumenti di monitoraggio: consentono all'amministratore basis di mantenere e garantire l'integrità, la sicurezza e le prestazioni dei sistemi SAP.

KPMG IT Advisory, partendo dal Know How acquisito in molteplici progetti rivolti all'analisi e al miglioramento di queste componenti e delle relative attività a supporto, ha sviluppato una metodologia di gestione e controllo per quelle aree i cui rischi hanno un diretto impatto sull'ambiente di produzione SAP, sui dati gestiti (FRD, …) e sulle utenze e le relative autorizzazioni:

- SAP Programs Execution Controls
- SAP Change Management Controls
- SAP Logical Security
- SAP Production Environment Security Management

SAP Basis Components

Un unico approccio per la gestione della SAP IT Operations



✓ Integrare in un unico approccio la definizione delle strategie e degli obiettivi IT con la gestione dei rischi business

✓ Aiutare a pianificare e mantenere univocamente la compliance e la governance delle operations IT in SAP come un'estensione delle consuete attività svolte dalla società per la gestione dei controlli business (Internal Audit, Corporate Governance, …)

✓ Fornire in tempo reale ai "*business decision maker*" *informazioni sull'esistenza dei rischi IT in SAP e sulle relative strategie di risoluzione, di mitigazione e di controllo continuo.*

SAP Basis Components

Un unico approccio per la gestione della SAP IT Gove

APPROCCIO TOP-DOWN

SAP BASIS COMPONENTS

Aree Logistiche

MM
- Gestione contratti e offerte
- Gestione richieste / ordini d'acquisto
- Verifica fatture
- Gestione magazzini

SD
- Gestione contratti, offerte, ordini
- Consegne
- Fatturazione

PP
- Diverse tipologie di produzione
- Distinte base, cicli e centri di lavoro
- Pianificazione della produzione
- Controllo della produzione

QM
- Pianificazione qualità
- Controllo Qualità per produzione e approvvigionamenti e vendite

Aree Finanziarie

FI
- Contabilità generale
- Contabilità sezionale
- Tesoreria
- Consolidamento

CO
- Centri di costo
- Ordini interni
- Costo del prodotto
- Analisi di redditività
- Contabilità per centri di profitto
- Controlling aziendale

IM
- Controllo investimenti
- Contabilità cespiti

PS
- Gestione progetti
- Controllo flussi finanziari

Business Intelligence

- Business Workflow

Industry Solutions

- Automotive
- Eng. & Construction
- Retail
- Chemical
- IS-U
- Telecommunication
- ……..

Human Resources

- Pianificazione del personale
- Selezione e formazione
- Calcolo retributivo

"Business Application Controls may not operate effectively unless adequate IT Control program is in place to support them"

SAP Basis Components

SAP Programs Execution Controls

I seguenti obiettivi illustrano le prassi volte a garantire che tutti i programmi batch, le transazioni on-line e l'esecuzione delle relative attività siano eseguite tempestivamente fino a un corretto completamento. Inoltre si verifica l'appropriatezza delle autorizzazioni date agli utenti per l'esecuzione dei report e dei programmi.

Le aree considerate come High Risk sono relative, ma non limitate, alla gestione dei processi e delle abilitazioni per:

- Setup dei Batch Input
- Processo di schedulazione dei Job
- Monitoraggio dei Job
- Monitoraggio dei Batch Input
- Gestione dei Job "su Richiesta"
- Accesso ai programmi nell'ambiente di Produzione

SAP Basis Components

SAP Change Management Controls

SAP include una serie di strumenti per gestire i cambiamenti; questi strumenti sono comunemente denominati Change Transport System (CTS).

Il CTS è una componente integrante della gestione, del coordinamento, dello sviluppo e della specifiche metodologie di lavoro all'interno dell'area IT di SAP.

Il CTS ha due componenti dominanti:

- Change & Transport Organization (CTO)
- Transport Management Systems (TMS).

Il CTO è il punto centrale per l'organizzazione delle attività di sviluppo e aggiornamento.
La TMS è utilizzato per gestire, controllare, copiare o spostare gli oggetti o le impostazioni personalizzate tra i diversi sistemi SAP (sviluppo, test e produzione).

Questi strumenti hanno un ruolo fondamentale nel mantenere la coerenza dei cambiamenti nel corso dello sviluppo, del testing (garanzia di qualità) e il sistema SAP di produzione.

Le aree considerate come High Risk sono relative, ma non limitate, alla gestione dei processi e delle abilitazioni per:

- Autorizzazioni per gestire il Change Management utilizzando Tool interni a SAP (a livello di sviluppo, test, produzione)
- Livelli di approvazioni nel Change Management
- Esistenza e adeguatezza dei Test (Unit Test e User Acceptance Test)
- Monitoraggio e gestione degli errori nel Change Management
- Gestione delle Conversioni e dei progetti IT
- Gestione delle modifiche alla parametrizzazione del sistema svolte direttamente nell'ambiente di produzione

SAP Basis Components

SAP Logical Security

Le metodologie e gli strumenti di Logical Security sono configurati ed adottati per attivare e gestire i controlli e implementare le dovute restrizioni su accessi inappropriati ai dati e alla configurazione del sistema SAP.

Le aree considerate come High Risk sono relative, ma non limitate, alla gestione dei processi e delle abilitazioni per:

- Amministrazione delle autorizzazioni
- Documentazione delle autorizzazioni
- Utenze di default SAP (SAP*, DDIC, EarlyWatch, CPIC, SAPCPIC)
- Utenze generiche o condivise
- Autorizzazioni estese: assegnazione e utilizzo di "SAP_ALL" o "Z_SAP_ALL"
- Log delle tabelle critiche
- Accesso temporaneo alla produzione SAP
- Accesso Remoto al produzione SAP (OSS)
- Blocco delle transazioni critiche
- Parametri di sicurezza

SAP Basis Components

SAP Production Environment Security Management

Il management della Società è solitamente responsabile della definizione del piano generale di sicurezza SAP, delle politiche e dei requisiti che devono essere applicati in tale ambiente

L' IT aziendale ha solitamente la responsabilità di applicare le relative procedure operative e individuare un appropriato corredo autorizzativo per tutte le transazioni e funzionalità SAP e di come esse dovranno essere mantenute e gestite nel tempo.

In SAP, le User Master Record (UMR) contengono tutti i dati anagrafici di un utente nel sistema:
questo include informazioni quali l'indirizzo, password iniziale, gruppo di utenti, date di validità, autorizzazioni.

Le UMR sono specifiche per ogni mandante, pertanto, è necessario che l'IT mantenga le UMR individualmente per ogni mandante SAP presente all'interno del sistema SAP.

SAP Basis Components

SAP Production Environment Security Management

Le aree considerate come High Risk sono relative, ma non limitate, alla gestione dei processi e delle abilitazioni per:

- Amministrazione del ciclo di vita delle User
- Gestione e controllo delle abilitazioni delle User (IT e Business)
- Controlli di Sicurezza delle User
- Gestione degli accessi di Emergenza
- Gestione dei cambiamenti organizzativi
- Gestione dei parametri di sicurezza dell'ambiente di produzione
- Gestione degli Audit Log per il monitoraggio di utenti o funzionalità (transazioni o report) considerati critici

SAP Basis Components

SAP Production Environment Security Management

Authorizations Monitoring Logics

	BUSINESS USERS	IT USERS
AUTORIZZAZIONI USINESS	ASSEGNAZIONE DI AUTORIZZAZIONI BUSINESS SEGREGATE PER MANSIONE ORGANIZZATIVA	TUTTE LE AUTORIZZAZIONI BUSINESS PER MODULO SAP O PROCESSO* oppure NESSUNA AUTORIZZAZIONE BUSINESS*
TORIZZAZIONI IS COMPONENTS	NESSUNA ASSEGNAZIONE DI FUNZIONALITA' BC	ASSEGNAZIONE DI AUTORIZZAZIONI BC SEGREGATE PER MANSIONE ORGANIZZATIVA / TIPO CONTRATTO
DOLOGIE NTROLLO ZZATIVO	MATRICE DEI CONFLITTI BUSINESS CRITICAL ACCESS - BUSINESS CRITICAL ACCESS - BC	CRITICAL ACCESS BC CRITICAL ACCESS - BUSINESS

**** Dipende dalle decisioni del Management relativamente all'assegnazione delle abilitazioni di gestione delle Business Operations in SAP***

SAP Basis Components

SAP Production Environment Security Management Control Objectives

L'IT come funzione aziendale è solitamente incaricata di valutare e risolvere i problemi di sicurezza SAP relativi agli utenti e a sostenere le esigenze di auditing relativi alle autorizzazioni assegnate. Ogni sei mesi si dovrebbero verificare i seguenti controlli per verificare che i risultati siano in linea con le politiche di sicurezza previste dalla Società:

- Tutti gli utenti (interni, esterni e temporanei) e la loro attività sui sistemi IT (applicazioni di business, il funzionamento del sistema, sviluppo e manutenzione) sono univocamente identificabili. Non ci dovrebbero essere UMR generiche o condivisi
- I diritti di accesso degli utenti ai sistemi e ai dati sono in linea con le esigenze di business definite e documentate
- La manutenzione di ruoli e delle autorizzazioni è limitato alle persone autorizzate
- Le richieste di rimozione devono seguire la stessa procedura di sicurezza, ma la User deve essere rimosso da SAP entro un limitato periodo temporale
- L'accesso degli utenti per bloccare e sbloccare codici di transazione
- I ruoli non contengono autorizzazioni estese o non il linea con le regole autorizzative
- Verifica degli utenti di dialogo assegnati a profili e SAP_ALL o similari
- Verifica degli utenti standard SAP
- Verifica di assegnazione temporanea di profili o ruoli con autorizzazioni estese
- Gli utenti non hanno la capacità di aggiornare le tabelle personalizzate SAP o se non richiesto dalla loro lavoro
- Gli utenti non hanno la possibilità di eseguire tutti i programmi indipendenti del gruppo di autorizzazione assegnato
- Gli utenti non hanno accesso a sviluppare programmi nell'ambiente di produzione
- Gli utenti con accesso agli Audit Log sono esclusivamente quelli previsti
- Gli utenti che possono gestire i trasporti e le importazioni in produzione sono limitati
- Verifica delle abilitazioni per aggiornare le impostazioni del client di produzione
- Verifica delle abilitazioni per la configurazione delle connessioni RFC
- Verifica delle abilitazioni per eseguire comandi del sistema operativo

SAP Basis Components Controls Information Contact

KPMG IT-Advisory - Information Risk Management

m montixi@kpmg.it