Service Management per la compliance Sarbanes-Oxley

Un caso di studio

Roma, Palazzo dell'Informazione, 13 Marzo 2007

Domenico Raguseo
IBM Representative in itSMF Italy

Agenda

- I Requisiti di SOX
- Esigenze del Cliente
- Descrizione del Progetto
- Obiettivi Raggiunti

I Requisiti Sarbanes-Oxley

- ***a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;***
- ***a statement identifying the framework used by management to evaluate the effectiveness of this internal control;***
- ***management's assessment of the effectiveness of this internal control as of the end of the company's most recent fiscal year;***
- ***a statement that its auditor has issued an attestation report on management's assessment.***

Internal Control Framework

SEC requires the internal control *framework* to include:

- *systematic process methodology* **for evaluating internal control over financial reporting.**
- **evidence of this systemization in the form of** policy and procedure
- **guidelines, reports and process documentation including** audit logs
- reports **detailing conformance to the policies and procedures.**

Typical Auditor Findings for Change Management

- **Lack of a system change management process**
  - Develop and implement an organizational IT standard for application and system change control. Develop and implement a change control process for all computing platforms with segregation of duties to request and then approve changes to systems and applications across the organization.
- **Inadequate documentation of system configurations, policies and standards**
  - Implement an automated tool to collect and compare all system configurations to the organization's defined baseline for computer systems in specific security "zones" of control.
- **Inadequate audit logs for system change operations**
  - Implement an enterprise audit logging solution that captures all activity from users accessing and updating the financial data system. These audit logs are collected and correlated with other system logs to monitor systems and assess risks of confidentiality and integrity of financial data.

Obiettivi del progetto

- Stabilire un processo di change management auditabile:
  - **Identificare i sistemi critici su cui ci sono esigenze di complaine**
  - **Identificare i configuration item necessari ad affermare la compliance**
  - **Analizzare la configurazione dei sistemi in modo automatico**
  - **Paragonare la configurazione reale con quella definita come standard e detrminare eventuali deviazioni**
  - **Creare reports**
  - **Automatizzare le azioni di recovery**
- Definire l'implementazione di 11 controlli Cobit

Controlli Cobit richiesti

CobiT Domain	Check code	Target of check activity	Activity description
AI	3.06.01	**Check on changes performed on system software**	**Are changes to system software performed according to company procedures for change management?**
AI	3.06.02	**Check on changes performed on system software**	**Is there any control and supervision plan for the change process performed on system software?**
AI	5.04.02	**Systems conversion**	**Is systems conversion tested between origin and destination to confirm completion, accuracy and validity of required elements?**
AI	5.12.03	**Moving in production**	**Does test environment reflects production environment?**
AI	6.04.02	**Emergency changes**	**Are emergency patch installations performed according to simplified test procedures?**
AI	6.04.03	**Emergency changes**	**Is there any emergency rollback procedure?**
DS	9.01.01	**Registration of configuration**	**Is there any operative procedure to collect information about systems configuration?**
DS	9.01.02	**Registration of configuration**	**Is there any operative procedure to track changes occurred to systems configuration?**
DS	9.01.03	**Registration of configuration**	**Is there any operative procedure to control changes performed on systems configuration?**
DS	9.03.01	**Registration of state**	**Are configuration changes tracked?**
DS	9.04.01	**Control of configuration**	**Is there any procedure to periodically verify alignment between systems configuration?**

Macro-funzionalità richieste (1)

- Discovery

  Scoperta automatica dei sistemi, dei componenti applicativi con le relative dipendenze, e delle applicazioni di business

- CMDB

  Disponibilità di database centralizzato contenente la rappresentazione dei CI

- Change Tracking

  Tracciamento dei cambiamenti occorsi ai CI

- Configuration Comparison

  Comparazione live-to-live o con modello predefinito per le configurazioni dei CI

- Reports

  Disponibilità di reports che permettano di verificare la compliance Cobit

Macro-funzionalità richieste (2)

- Release Management

  Distribuzione centralizzata di software, patch e modifiche alle configurazioni

- Patch Management

  Gestione automatizzata di scaricamento, impacchettamento e distribuzione di patch di sistema

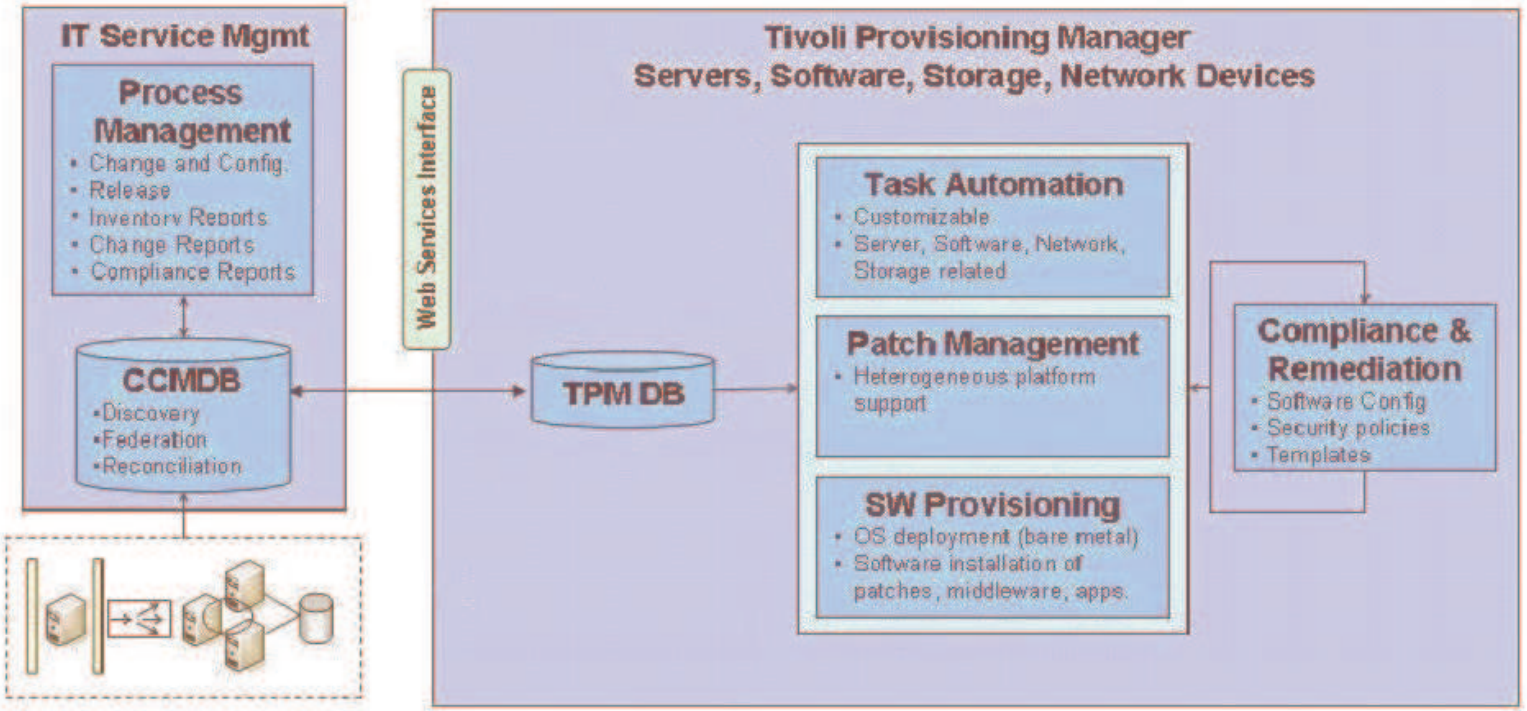
- Change & Configuration Management

  Disponibilità di uno strumento per la gestione dei processi di Change e Configuration

- Compliance & Remediation

  Automatizzazione dei controlli sulla corrispondenza delle configurazioni ai modelli definiti e delle eventuali azioni correttive

Soluzione proposta



- Change & Configuration Management Database (CMDB) fornisce un DB centralizzato per la raccolta dei dati sui CI:
  - **Configuration Discovery & Tracking (CDT) gestisce la discovery dei configuration item.**
  - **Process Management Integration Platform (PMIP) permette la gestione dei processi secondo ITIL e mette a disposizione i report per la compliance Cobit.**
- Tivoli Provisioning Manager (TPM), a partire dalle informazioni scoperte in CCMDB, gestisce i task di Release Management, Patch Management, Compliance e Remediation management.

Risultati raggiunti (1)

- **Discovery dei sistemi (circa 125) e delle componenti applicative dell'ambito SOA**
- **Discovery di una Business Application**
- **Funzionalità di Release Management (software & configuration deployment) disponibile in produzione sui sistemi dell'ambito SOA**
- **Funzionalità di Patch Management per Windows disponibile in produzione sui sistemi dell'ambito SOA**

Risultati raggiunti (2)

- **Processi di change management per le modifiche infrastrutturali disponibili in produzione**
- **Audit reports per Cobit disponibili in produzione**
- **Inventory reports per Cobit disponibili in produzione**
- **RFC related reports per Cobit disponibili in produzione**

Obiettivi Futuri

- **Estensione della discovery e gestione a tutto il parco applicativo**
- **Estensione dei processi di change management e di provisioning al network**
- **Discovery di tutte business application**
- **Rilascio della funzionalità di Patch Management per Solaris e AIX**
- **Rilascio funzionalità di release management per il deployment di una applicazione pilota e relativo training**
- **Rilascio di funzionalità di Compliance e Remediation per una applicazione pilota e relativo training**

Evoluzione Strategica

- **Implementazione Progressiva di tutta la framework COBIT**
- **Ridefinizione dei processi di IT Management per ottenere dei risparmi operativi grazie ad una maggiore automazione basata sul Tivoli Provisioning**
- **Integrazione dell' Help Desk**
- **Realizzazione di un cruscotto di business per integrazione con il service level management su tutte le business application critiche**