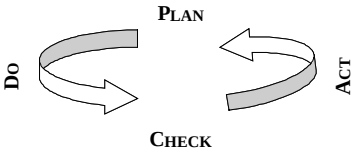
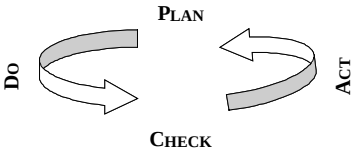


COBIT 4.1 E ISO 27001

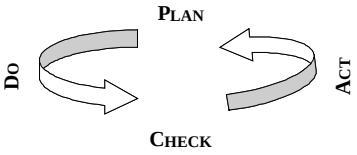
COBIT 4.1 E ISO 27001

CONFRONTO QUANTITATIVO E QUALITATIVO



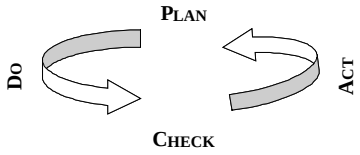
Contesto

- Proposta di metodologie e standard (ISO 27001, CobiT, ITIL/ISO20000, …)
- Elementi positivi: crescita competenza e convergenza su processi e tecniche di valutazione
- Elementi negativi: difficoltà di integrazione in un quadro coerente e di utilizzo sinergico
- Esigenza di armonizzazione e confronto già recepita da ISACA, ITGI, AIEA …
  - ITGI Mapping of ISO/IEC 17799:2005 With COBIT® 4.0
  - COBIT© - ITIL® : due framework complementari (AIEA, capitolo ISACA di Milano/ *itSMF Italia / SDA Bocconi) [novembre 2006]*
  - *Aligning Cobit, ITIL and ISO17799 for Business Benefit: Management Summary [The IT Governance Institute (ITGI), The Office of Government Commerce (OGC), itSMF The IT Service Management Forum]*
  - *An Introduction to CobiT 4.1 & Mapping CobiT to other Frameworks and Standards - Jimmy Heschl (ISACA e-Symposium)*
  - *ITGI Mapping of ISO/IEC 17799:2000 With COBIT, 2ndEdition*



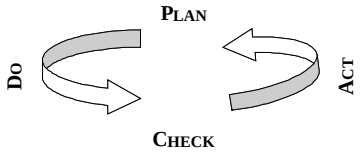
Obiettivi dello Studio

- Approccio di ricerca: è stato costituito un Gruppo di Ricerca AIEA
- Valorizzazione e crescita di competenze specifiche in AIEA
- Valutazione delle aree di sovrapposizione fra CobiT e ISO 27001 e delle relative specificità
- Con l'obiettivo di usarli al meglio entrambi
- NON una gara fra gli standard



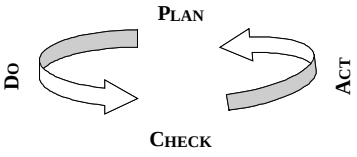
Cobit – Panoramica

- Il COBIT è uno schema di riferimento ed un insieme di strumenti di supporto che consentono al management di collegare requisiti di controllo, aspetti tecnici e rischi aziendali, e di comunicare tale livello di controllo a tutte le parti interessate.
- E' strutturato in
  - 4 Domini
  - 34 Processi



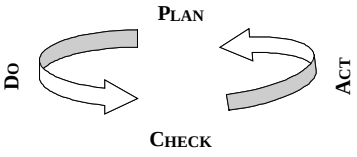
Cobit – Panoramica - Domini

- Pianificazione e Organizzazione (PO) - Si riferisce agli aspetti strategici e tattici, e riguarda l'identificazione del modo in cui l'IT può meglio contribuire al raggiungimento degli obiettivi aziendali.
- Acquisizione ed Implementazione (AI) - Per realizzare la strategia IT, le soluzioni IT devono essere identificate, sviluppate o acquistate, come pure realizzate ed integrate nei processi aziendali.
- Erogazione e Supporto (DS) - Si fa riferimento all'erogazione dei servizi richiesti, che includono l'erogazione del servizio vero e proprio, la gestione della sicurezza e della continuità, il servizio di assistenza agli utenti e la gestione dei dati e le infrastrutture operative.
- Monitoraggio e Valutazione (ME) - Tutti i processi IT devono essere regolarmente valutati nel tempo sotto l'aspetto della qualità e della conformità ai requisiti di controllo.



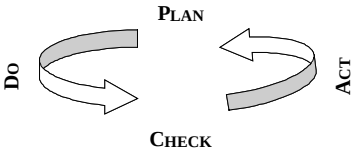
Cobit – Panoramica - Processi

PO1	Definire un Piano Strategico per l'IT
PO2	Definire l'architettura informatica
PO3	Definire gli indirizzi tecnologici
PO4	Definire i processi, l'organizzazione e le relazioni dell'IT
PO5	Gestire gli investimenti IT
PO6	Comunicare gli obiettivi e gli orientamenti della direzione
PO7	Gestire le risorse umane dell'IT
PO8	Gestire la Qualità
PO9	Valutare e Gestire i Rischi Informatici
PO10	Gestire i Progetti



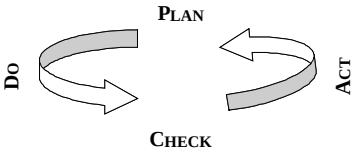
Cobit – Panoramica - Processi

AI1	Identificare soluzioni automatizzate
AI2	Acquisire e mantenere il software applicativo
AI3	Acquisire e mantenere l'infrastruttura tecnologica
AI4	Permettere il funzionamento e l'uso dei sistemi IT
AI5	Approvvigionamento delle risorse IT
AI6	Gestire le modifiche
AI7	Installare e certificare le soluzioni e le modifiche



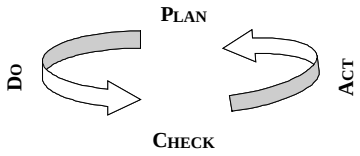
Cobit – Panoramica - Processi

DS1	Definire e gestire i livelli di servizio
DS2	Gestire i servizi di terze parti
DS3	Gestire le prestazioni e la capacità produttiva
DS4	Assicurare la continuità di servizio
DS5	Garantire la sicurezza dei sistemi
DS6	Identificare e attribuire i costi
DS7	Formare e addestrare gli utenti
DS8	Gestione del Service Desk e degli incidenti
DS9	Gestione della configurazione
DS10	Gestione dei problemi
DS11	Gestione dei dati
DS12	Gestione dell'ambiente fisico
DS13	Gestione delle operazioni



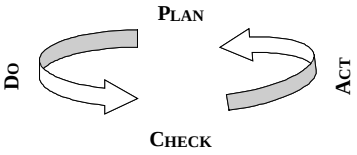
Cobit – Panoramica - Processi

ME1	Monitorare e valutare le prestazioni dell'IT
ME2	Monitare e valutare i controlli interni
ME3	Assicurare la conformità a leggi e a regolamenti
ME4	Istituzione dell'IT Governance



ISO 27001 - Panoramica

- Lo standard ISO 27001 descrive un modello per *definire, attuare, gestire, monitorare, rivedere, manutenere e migliorare* un Sistema di Gestione della Sicurezza dell'Informazione (SGSI)
- Lo standard è descritto in due manuali:
  - ISO/IEC 27001:2005 - Information security management systems - Requirements - Specifiche per la implementazione e gestione dell'ISMS
  - ISO/IEC 27002:2005 (già ISO/IEC 17799:2005) - Code of practice for information security management - Una guida implementativa che elenca, per ciascuno dei controlli definiti, un'ampia serie di misure e "best practice" della sicurezza dell'informazione
- Assumono valore normativo dal punto di vista dello standard unicamente i Cap. 4-8 di ISO/IEC 27001:2005 ed il relativo Allegato A che ne elenca Obiettivi di controllo e Controlli



ISO 27001 - Panoramica

ISO/IEC 27001:2005

Cap.1-3

Cap.4-8 → ISMS - Specifiche, Responsabilità della Direzione, Audit Interni, Riesame, Miglioramento

Annex A
11 Aree → 39+133 Obiettivi di Controllo e Controlli ⇨ ISO/IEC 27002:2005 (già ISO/IEC 17799:2005)

Annex B
Principi OECD

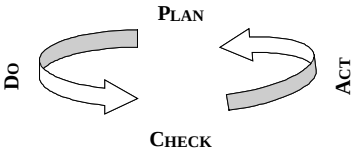
Annex C
Corrispondenza con ISO 9001 & 14001

Normativo

Informativo

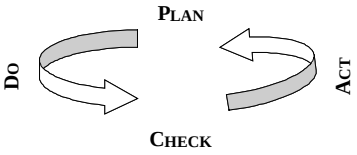
Code of practice

Elenca:
- Controlli
- Best practices
- Migliaia di Controlli e "Practices"



ISO 27001 - Panoramica

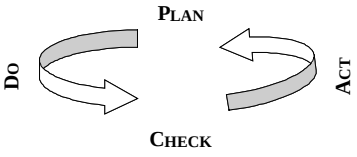
- L'Allegato A di ISO/IEC 27001:2005 è strutturato in:
  - AREE (11, da A.5 a A.15)
  - Obiettivi di controllo (39)
  - Controlli (133, definiti Information requirements nel citato documento dell'IT Governance Institute)



ISO 27001 - Panoramica

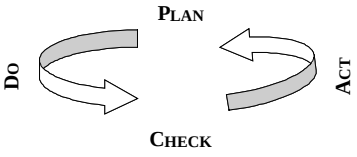
Aree

- A.5 POLITICA PER LA SICUREZZA
- A.6 ORGANIZZAZIONE DELLA SICUREZZA DELL'INFORMAZIONE
- A.7 GESTIONE DEGLI ASSET
- A.8 SICUREZZA DELLE RISORSE UMANE
- A.9 SICUREZZA FISICA ED AMBIENTALE
- A.10 GESTIONE DELLE OPERAZIONI E DELLE COMUNICAZIONI
- A.11 CONTROLLO DEGLI ACCESSI
- A.12 ACQUISIZIONE, SVILUPPO E GESTIONE DEI SISTEMI INFORMATIVI
- A.13 GESTIONE DEGLI INCIDENTI DI SICUREZZA
- A.14 GESTIONE DELLA CONTINUITA' OPERATIVA
- A.15 CONFORMITA'



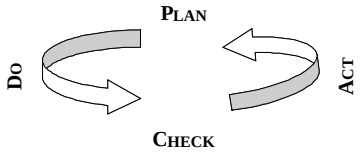
Metodologia di valutazione

- Un'attività di valutazione e confronto fra COBIT 4.1 ed ISO 27001 non può essere unicamente affidata a tecniche quantitative
- Ma occorre definire un modello condiviso, obiettivo e ripetibile di valutazione
- Tenendo conto dei Cap. 4-8 di ISO 27001 (questo motiva la scelta del Gruppo di Ricerca di proseguire nonostante la pubblicazione del documento ITGI)



Metodologia di valutazione

- E' stata definita la **Relazione** fra controlli ISO 27001 e CobiT, in generale esiste una relazione uno a molti fra i controlli, schematizzabile in una matrice
- La valutazione, è stata svolta – a cura dei partecipanti del Gruppo di Ricerca - in due passi:
  - **Valutazione di Pertinenza**: agli obiettivi CobiT associati ad uno specifico controllo ISO è stato attribuito un peso percentuale (la somma dei valori attribuiti deve valere 100). Tale scelta risponde all'esigenza di normalizzare le stime evitando errori di sovra/sotto-stima
  - **Valutazione di Merito**: per i controlli ISO associati ad uno specifico obiettivo CobiT è stata svolta una valutazione di merito, valutandone [in termini di Alto/Medio/Basso (0.8, 0.5, 0.2] la corrispondenza all'obiettivo CobiT
- La **VALUTAZIONE** per la specifica coppia di controlli CobiT/ISO deriva dalla moltiplicazione dei due valori

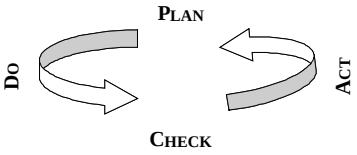


Metodologia di valutazione

A.9.1.2 CONTROLLI FISICI DI ACCESSO - Le aree sicure saranno protette da appropriati controlli di accesso per garantire che solo al personale autorizzato sia consentito l'accesso.

Il controllo A.9.1.2 CONTROLLI FISICI DI ACCESSO è in relazione con:

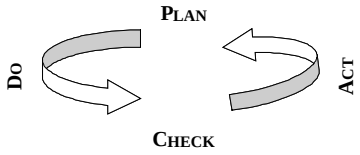
COBIT		Pert.
DS12.2	*Misure di sicurezza fisica - Definire e implementare misure di sicurezza fisica in linea con i fabbisogni di business. Le misure dovrebbero includere, ma non limitarsi a il layout del perimetro di sicurezza, zone di sicurezza, posizionamento di dispositivi critici, e aree di spedizione e di ricevimento. In particolare è necessario mantenere un basso profilo sulla presenza di operazioni IT critiche. Le responsabilità per il monitoraggio e le procedure per rendicontare e risolvere incidenti di sicurezza fisica devono essere stabilite.*	40
DS12.3	*Accesso fisico - Definire e implementare procedure per concedere, limitare e revocare gli accessi a locali, edifici ed aree secondo i fabbisogni di business incluse le emergenze. Gli accessi ai locali, edifici ed aree dovrebbero essere giustificati, autorizzati, registrati e monitorati. Questo si applica a tutte le persone che entrano nei locali di edifici, incluso personale, personale temporaneo, clienti, fornitori, visitatori od ogni altra terza parte.*	60



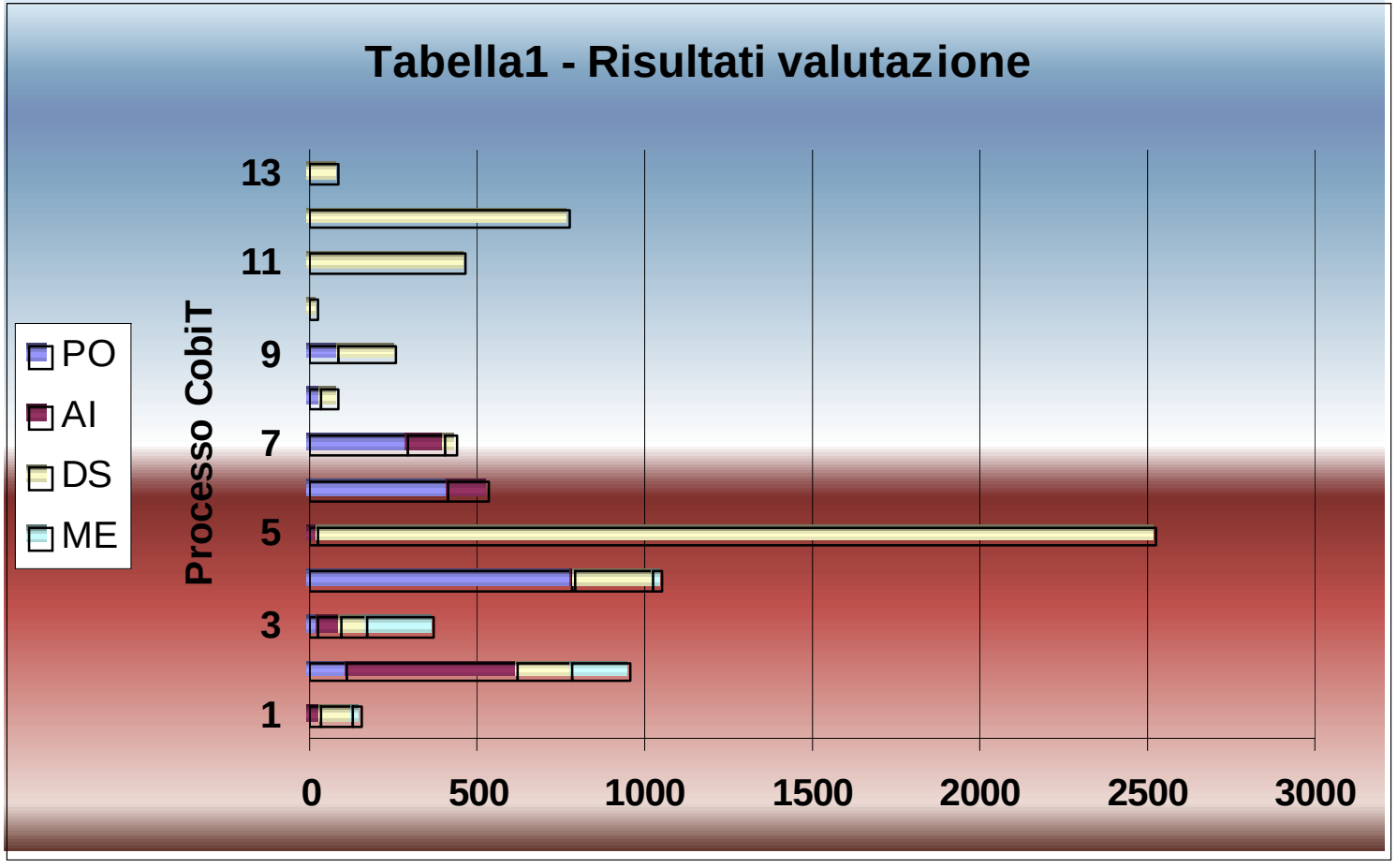
Metodologia di valutazione

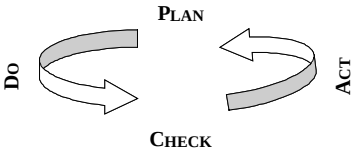
L'obiettivo DS12.3 – ACCESSO FISICO è in relazione con i controlli ISO 27001:

ISO	Pert.	Mer.	Ris.
A.6.2.1 IDENTIFICAZIONE DEL RISCHIO ASSOCIATO A TERZE PARTI - *I rischi per l'organizzazione e le relative risorse elaborative derivanti da processi di business che coinvolgono terze parti devono essere identificati ed appropriati controlli attuati prima di consentirne l'accesso.*	5	A	4
A.9.1.2 CONTROLLI FISICI DI ACCESSO - *Le aree sicure saranno protette da appropriati controlli di accesso per garantire che solo al personale autorizzato sia consentito l'accesso.*	60	A	48
A.9.1.5 LAVORARE IN AREE SICURE - *Saranno progettate e rese operative protezioni fisiche e definite linee-guida per il lavoro in aree sicure.*	45	A	36
A.9.1.6 AREE PUBBLICHE, E PER IL CARICO E LO SCARICO DEI MATERIALI - *I punti di accesso come le aree di carico e scarico ed altri punti in cui personale non autorizzato può accedere ai locali dell'organizzazione saranno controllate e, se possibile, isolate dalle risorse elaborative per evitare accessi non autorizzati.*	40	A	32
A.9.2.5 SICUREZZA DELLE APPARECCHIATURE FUORI SEDE - *Si deve garantire la sicurezza degli apparati fuori sede tenendo in considerazione i rischi derivanti dallo svolgimento di attività svolte all'esterno dell'organizzazione.*	48	A	38,4

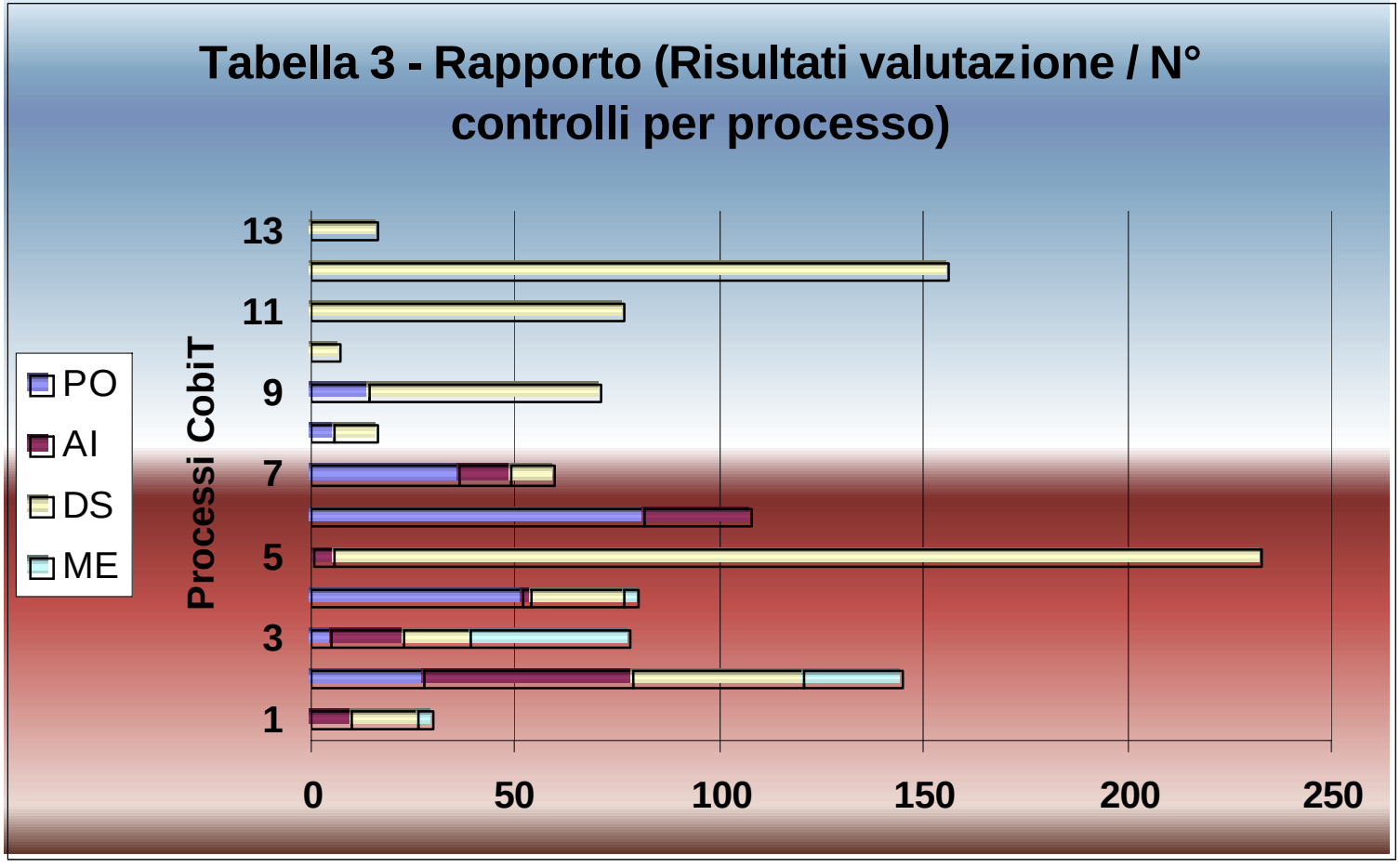


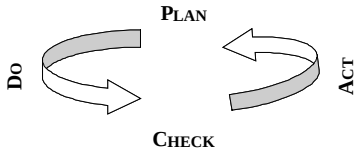
Risultati valutazione (Solo Controlli)





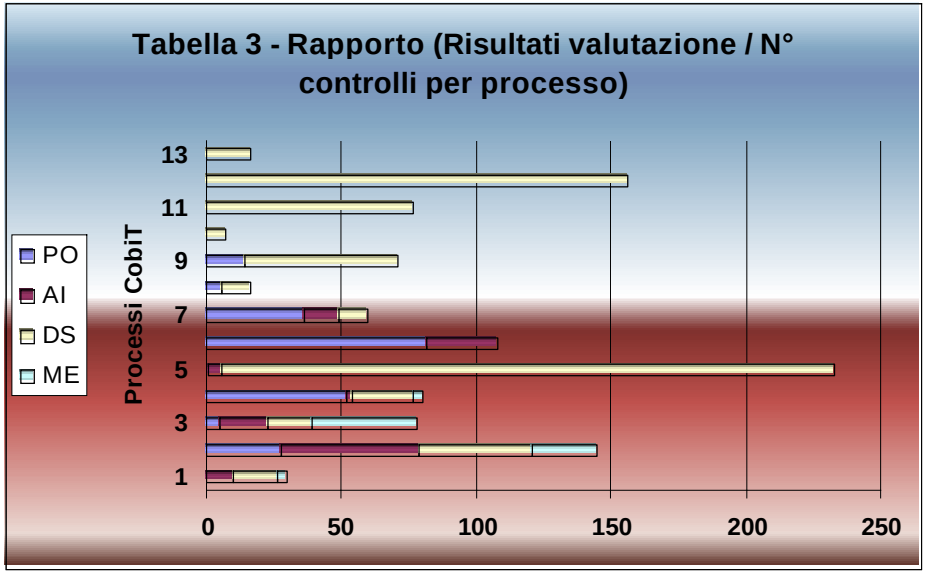
Risultati valutazione (Solo Controlli)

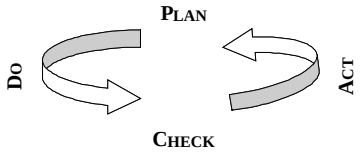




Risultati valutazione (Solo Controlli)

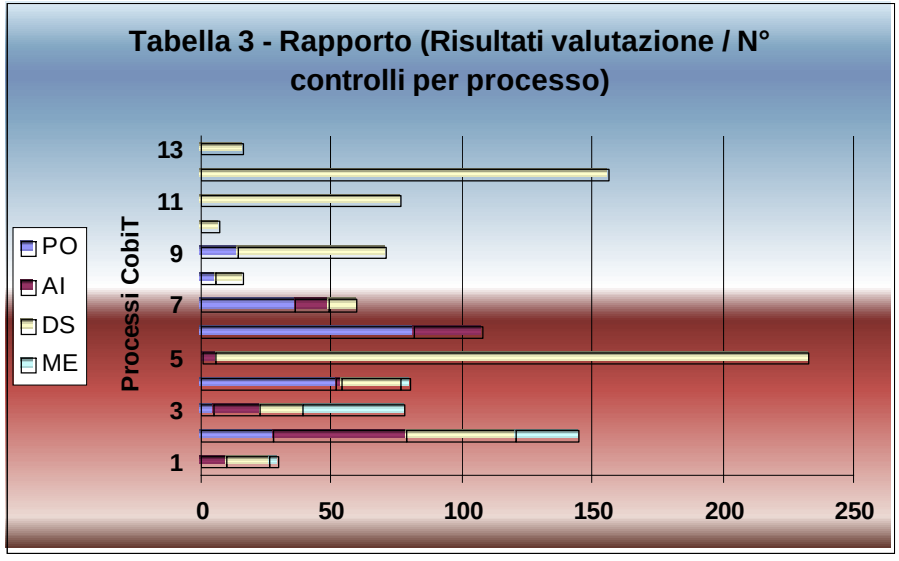
DS5	Garantire la sicurezza dei sistemi
DS12	Gestione dell'ambiente fisico
PO6	Comunicare gli obiettivi e gli orientamenti della direzione
DS11	Gestione dei dati
DS9	Gestione della configurazione
PO4	Definire i processi, l'organizzazione e le relazioni dell'IT

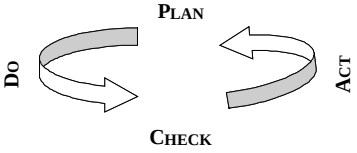




Risultati valutazione (Solo Controlli)

AI2	Acquisire e mantenere il software applicativo
DS2	Gestire i servizi di terze parti
ME3	Assicurare la conformità a leggi e a regolamenti
PO7	Gestire le risorse umane dell'IT
PO2	Definire l'architettura informatica
ME2	Monitorare e valutare I controlli interni





Risultati valutazione (Solo Controlli)

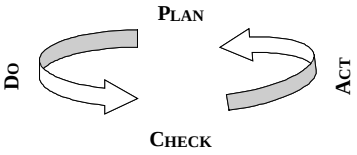
Processi con punteggio "basso"

- PO1 Definire un Piano Strategico per l'IT
- PO3 Definire gli indirizzi tecnologici
- PO5 Gestire gli investimenti IT
- PO8 Gestire la Qualità
- PO9 Valutare e Gestire i Rischi Informatici
- PO10 Gestire i Progetti

- AI1 Identificare soluzioni automatizzate
- AI3 Acquisire e mantenere l'infrastruttura tecnologica
- AI4 Permettere il funzionamento e l'uso dei sistemi IT
- AI5 Approvvigionamento delle risorse IT
- AI6 Gestire le modifiche
- AI7 Installare e certificare le soluzioni e le modifiche

- DS1 Definire e gestire i livelli di servizio
- DS3 Gestire le prestazioni e la capacità produttiva
- DS4 Assicurare la continuità di servizio
- DS6 Identificare e attribuire i costi
- DS7 Formare e addestrare gli utenti
- DS8 Gestione del Service Desk e degli incidenti
- DS10 Gestione dei problemi
- DS13 Gestione delle operazioni

- ME1 Monitorare e valutare le prestazioni dell'IT
- ME4 Istituzione dell'IT Governance



Risultati valutazione (Solo Controlli)

Confronto con valutazione ITGI

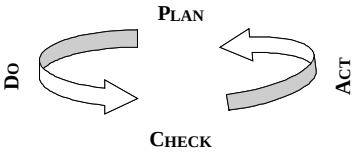
Tabella 4 - Relazione con valutazione ITGI

	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	o	-	o	-	+	o	-	-	-			
AI	-	o	-	-	-	o	-						
DS	-	o	-	o	+	-	-	-	o	-	+	+	-
ME	-	o	o	-									

Valutazione ITGI

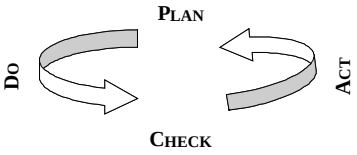
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	o	o	o	-	+	+	-	+	-			
AI	o	o	o	-	-	o	o						
DS	-	o	-	+	+	-	-	o	o	-	+	+	o
ME	-	+	+	-									

+	Significant match
o	Minor match
-	Unrelated focus



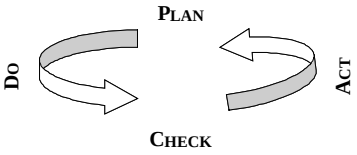
Risultati valutazione (Cap. 4-8)

Processo COBIT		Implicazioni ISO/IEC 27001:05 - Cap. 4-8
PO2	Definire l'architettura informatica	Copertura limitata agli obiettivi di controllo: - PO2.3 Schema di Classificazione dei Dati - PO2.4 Gestione dell'Integrità
PO6	Comunicare gli obiettivi e gli orientamenti della direzione	Copertura ALTA LIMITATAMENTE AL PERIMETRO DELLA SICUREZZA, per il Processo e specificamente per l'obiettivo di controllo: - PO6.5 Comunicazione degli Obiettivi e gli Indirizzi dell'IT
PO7	Gestire le risorse umane dell'IT	Copertura ALTA LIMITATAMENTE AL PERIMETRO DELLA SICUREZZA, per gli obiettivi di controllo: - PO7.1 Assunzione e Ritenzione del Personale - PO7.2 Competenze del Personale - PO7.4 Formazione del Personale - PO7.7 Valutazione della Performance del Personale



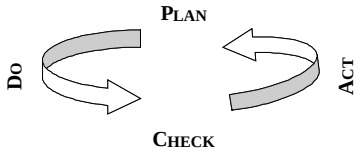
Risultati valutazione (Cap. 4-8)

Processo COBIT		Implicazioni ISO/IEC 27001:05 - Cap. 4-8
PO9	Valutare e Gestire i Rischi Informatici	Copertura COMPLETA per gli obiettivi di controllo: - PO9.1 Allineamento della Gestione dei Rischi Aziendali ed Informatici - PO9.2 Definizione del contesto di Rischio - PO9.4 Valutazione dei Rischi - PO9.6 Mantenimento e Monitoraggio di un Piano d'Azione per la Gestione dei Rischi (Risk Action Plan)
AI1	Identificare soluzioni automatizzate	Copertura COMPLETA per l'obiettivo di controllo: - AI1.2 Riferire sull'analisi dei rischi



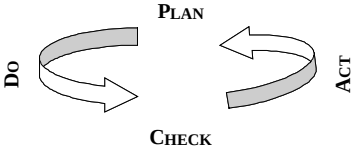
Risultati valutazione (Cap. 4-8)

Processo COBIT		Implicazioni ISO/IEC 27001:05 - Cap. 4-8
DS5	Garantire la sicurezza dei sistemi	Copertura COMPLETA per gli obiettivi di controllo: - DS5.1 Gestione della sicurezza IT - DS5.2 Piano di sicurezza IT
DS7	Formare e addestrare gli utenti	Copertura ALTA LIMITATAMENTE AL PERIMETRO DELLA SICUREZZA, per gli obiettivi di controllo: - DS7.1 Identificazione della formazione e dell'addestramento necessario - DS7.2 Erogazione della formazione e dell'addestramento - DS7.3 Valutazione dell'addestramento ricevuto



Risultati valutazione (Cap. 4-8)

Processo COBIT		Implicazioni ISO/IEC 27001:05 - Cap. 4-8
ME1	Monitorare e valutare le prestazioni dell'IT	Copertura ALTA LIMITATAMENTE AL PERIMETRO DELLA SICUREZZA, per il Processo.
ME2	Monitorare e valutare i controlli interni	Copertura ALTA LIMITATAMENTE AL PERIMETRO DELLA SICUREZZA, per il Processo.
ME4	Istituzione dell'IT Governance	Copertura COMPLETA per gli obiettivi di controllo: - ME4.5 Gestione del rischio - ME4.7 Certificazione indipendente

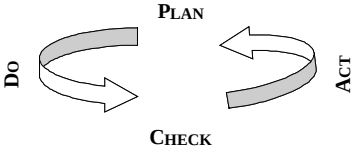


Risultati valutazione (Cap. 4-8)

PO9 (Valutare e Gestire i Rischi Informatici)

Dettaglio Riferimenti ISO/IEC 27001:05 - Cap. 4-8

PO9.1	Allineamento della Gestione dei Rischi Aziendali ed Informatici	Cap. 4.2.1 Istituire il SGSI [da c) a j)] Cap. 4.2.3 [d) Rivedere le valutazioni dei rischi a intervalli prestabiliti, ed i rischi residui e i livelli di rischio accettabile già identificati] Cap. 5.1 [f) Decidendo i criteri per l'accettazione dei rischio]
PO9.2	Definizione del contesto di Rischio	Cap. 4.2.1 [a) Istituire il SGSI, b) Definire la politica del SGSI, c) Definire l'approccio al Risk Assessment dell'organizzazione]
PO9.3	Identificazione dell'Evento	Cap. 4.2.1 [d) Identificare i rischi, e) Analizzare e valutare i rischi]

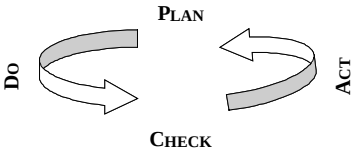


Risultati valutazione (Cap. 4-8)

PO9 (Valutare e Gestire i Rischi Informatici)

Dettaglio Riferimenti ISO/IEC 27001:05 - Cap. 4-8

PO9.4	Valutazione dei Rischi	Cap. 4.2.1 [d) Identificare i rischi, e) Analizzare e valutare i rischi, f) Identificare e valutare le opzioni per il trattamento dei rischi] Cap. 4.2.3 [d) Rivedere ad intervalli regolari Analisi dei Rischi, Rischio residuo e Livello accettabile di risc
PO9.6	Mantenimento e Monitoraggio di un Piano d'Azione per la Gestione dei Rischi (Risk Action Plan)	Cap. 4.2.2 [a) Formulare un piano di trattamento dei rischi (azioni, risorse, responsabilità e priorità)] Cap. 4.2.2. [b) Realizzare il piano di trattamento dei rischi, c) Implementare i controlli, c) Definire come misurare l'efficacia dei controlli]



Risultati valutazione

Tabella 5 - Valutazione complessiva

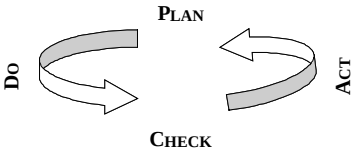
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	N	P	N	P	N	S	P	N	C	N			
AI	P	P	P	N	N	P	P						
DS	P	P	P	P	C	N	P	P	P	P	P	C	P
ME	S	S	P	S									

C Completo

S Completo per gli aspetti di sicurezza

P Parziale

N Nullo



Risultati valutazione