L'evoluzione del modello dei controlli interni sull'Information Tecnology

L'esperienza Eurizon Financial Group

Bruno Ferrari

Indice

1. Esigenze normative

1.1 Sarbanes Oxley Act

Financial Group Eurizon

SEZIONE 302
Imposizione di un obbligo di attestazione dei bilanci societari a carico di CEO e CFO

SEZIONE 404
Attestazione del CEO e del CFO relativamente all'esistenza e adeguatezza degli Internal Control in merito al bilancio e alle altre informazioni finanziarie pubbliche

La società di revisione deve verificare le attestazioni del CEO e CFO, in accordo con gli standard emessi o adottati dal PCAOB (Public Company Accounting Oversight Board) ed emettere una propria relazione

Il principio di revisione AS2, nonché le interpretazioni operative del PCAOB, indicano le modalità operative e metodologie di riferimento che il Management deve utilizzare:
ad es.
CoSo Model come Framework di riferimento
attività specifiche e standard metodologici sui controlli generali IT (ad es Cobit)
specifica modalità per effettuare il test di operatività dei controlli

Auditing Standard No. 2 – *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements*

1. Esigenze normative

1.2 Legge 262 "decreto sul risparmio"

Art. 14 → Art. 154-bis comma 2 TUF

Attestazione da parte del Direttore Generale e del **Dirigente preposto** alla redazione dei documenti contabili societari e le informazioni e i dati contenuti negli atti e nelle comunicazioni previste dalla legge o diffuse al mercato **corrispondono al vero**.

Art. 14 → Art. 154-bis comma 3 TUF

Predisposizione di adeguate procedure amministrative e contabili per la **predisposizione del bilancio** e di ogn altra comunicazione finanziaria **da parte del Dirigente** preposto alla redazione dei documenti contabili societari.

Art. 14 → Art. 154-bis comma 5 TUF

Attestazione, con apposita relazione, **dell'adeguatezza e dell'effettiva applicazione delle procedure da parte degli organi amministrativi delegati e del Dirigente preposto** alla redazione dei documenti contabili societari **Attestazione della corrispondenza del bilancio** alle risultanze dei libri e delle scritture contabili **secondo regolamenti che saranno emanati dalla CONSOB.**

2. Modello emergente ed evoluzione del ruolo

Tratti del modello emergente:

Strategici

- **Gestione più consapevole** dei **legami tra orientamento strategico ed indirizzi operativi**
- **Crescente rilevanza** della **comunicazione finanziaria e dell'informativa societaria**

Organizzativi

- Necessità di **competenze evolute** per il **governo integrato dei progetti** (Basilea II, IAS, SOXA)
- Consolidamento di **principi di eccellenza nei modelli organizzativi di controllo**

Informativi

- Convergenza tra **logiche di valutazione gestionale** e regole di **rappresentazione contabile**
- **Evoluzione** dei **sistemi direzionali di sintesi** e delle **architetture informatiche a supporto**

Evoluzione del ruolo del Chief Financial Officer:

Strategici

- Definire **la struttura di relazioni tra financial reporting e processi organizzativi (driver risultati)**
- **Saldare** le attività di **financial planning** con la **valutazione delle implicazioni organizzative**

Organizzativi

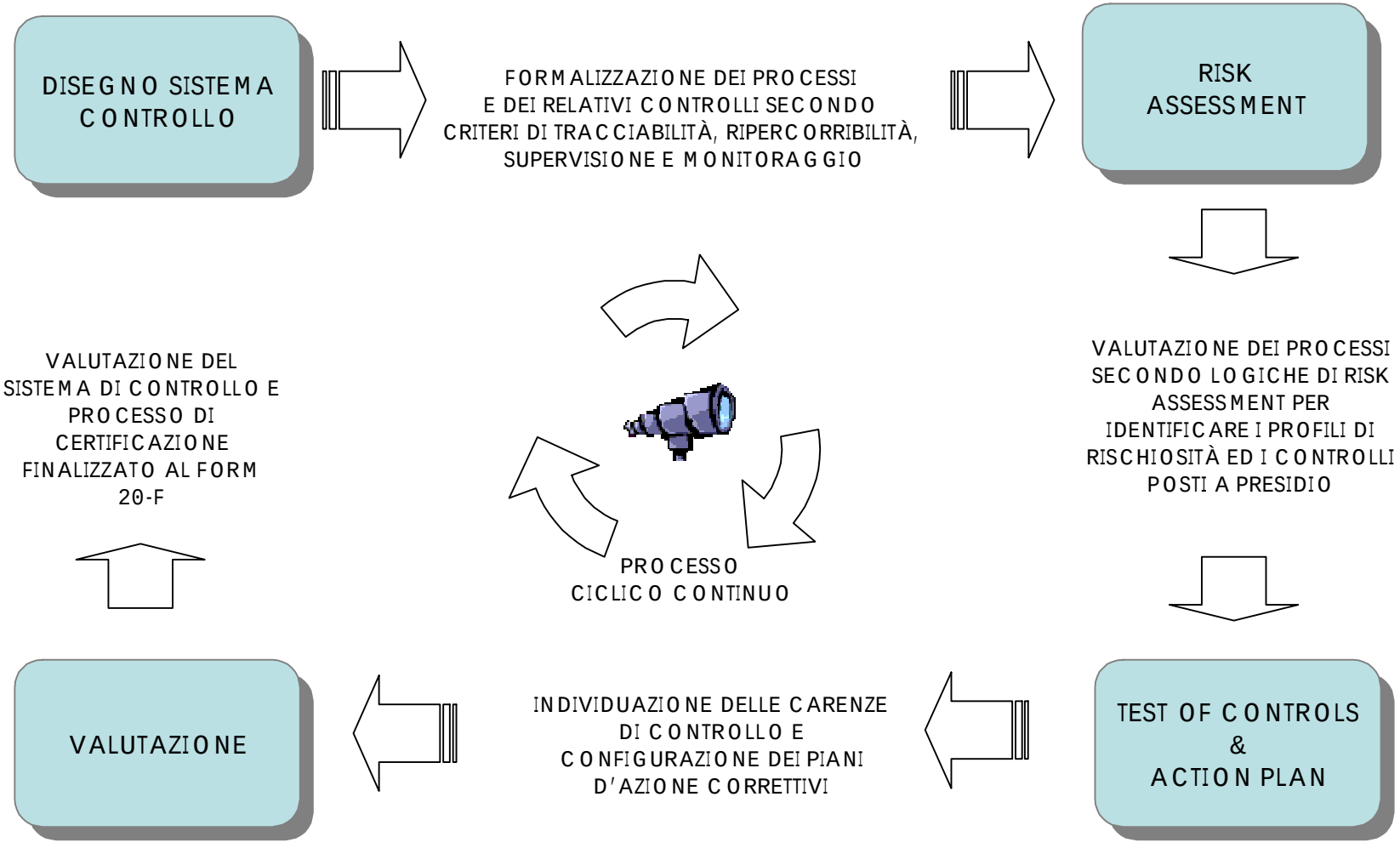
- **Presidiare** il **sistema di controllo sull'informativa societaria**
- **Gestire** unitariamente **i processi finalizzati alla produzione dei financial reporting di Gruppo**
- **Strutturare** e presidiare **il sistema di controllo** sull'informativa societaria

Informativi

- Adozione di **metriche consistenti tra i processi valutativi** (fair value, hedge accounting, ect.)
- **Armonizzare classificazioni gestionali e rappresentazioni di bilancio** (segment reporting)

3. Livello logico Assessment

Financial Group
Eurizon

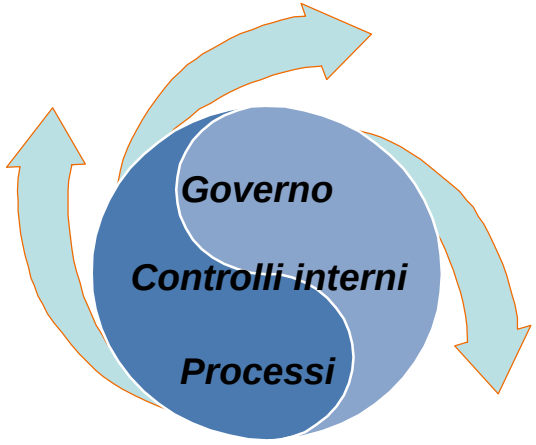


3. Livello logico Assessment

Financial Group Eurizon

Governo

- **Modifiche allo Statuto, nomina del dirigente preposto** (modalità di nomina e revoca del dirigente preposto)
- Conferimento al Dirigente preposto di **adeguati mezzi e poteri**
- Ridisegno del sistema delle **deleghe e dei poteri e delle responsabilità a livello Gruppo**
- **Disegno organizzativo della struttura dedicata** alla gestione nel continuo dell'adeguamento normativo



Sistema dei Controlli interni

- Individuazione di un **framework di riferimento per** la **valutazione** della **efficacia dei controlli sul sistema informativo e contabile**
- un sistema di **regole interne per** la **predisposizione** dei **documenti contabili**
- Sistema di **validazione** dei **dati contabili**
- Sistema di **monitoraggio che coinvolga** anche le **funzioni aziendali istituzionalmente preposte al controllo**

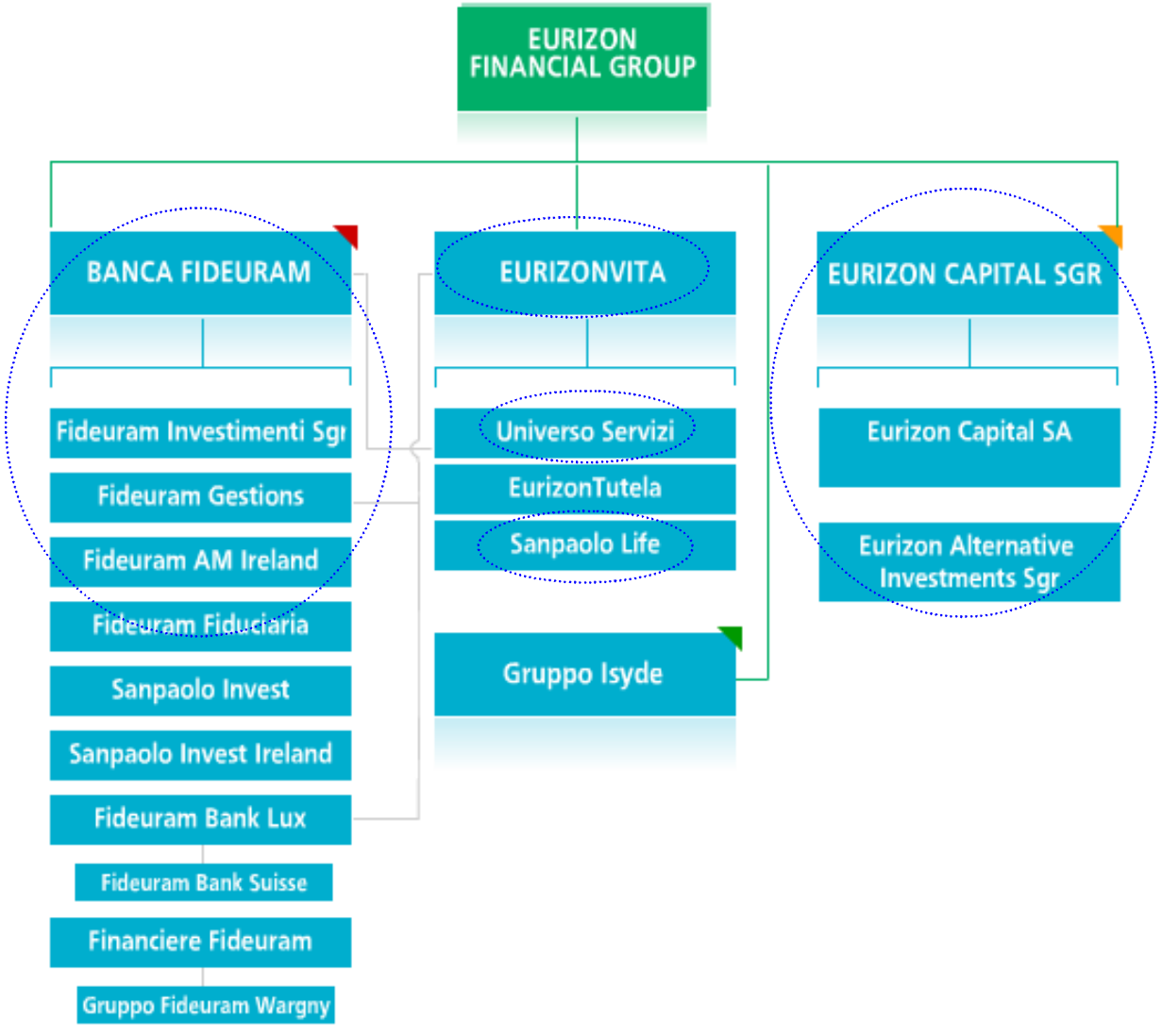
Processi

- **Individuazione delle entità societarie del Gruppo** rilevanti in termini quantitativi e qualitativi
- **Individuazione dei processi significativi** (in termini di rischi e di possibile impatto sulle voci di bilancio)
- **Documentazione dei processi e dei controlli significativi** per tutte le aree di intervento identificate
- Individuazione delle eventuali azioni di rimedio

4. Ambito d'intervento

Financial Group
Eurizon

Ambito



5. Framework IT – Cobit for SOA

Financial Group Eurizon

Control Objectives for Information and related Technologies (CobiT)

Domini	PO – AI – DS – M	PO – AI – DS – M
Processi	34	28
Obiettivi di controllo	318	123
	CobiT	*CobiT for SOA*

5. Framework IT – Cobit for SOA (segue)

Financial Group Eurizon

Ambito

L'ambito di azione della SOX ai fini IT prevede l' analisi dei quattro domini

- Organizzazione e Pianificazione
- Acquisizione/Sviluppo e Manutenzione
- Erogazione e Supporto
- Monitoraggio ed Auditing

Ogni dominio (4) - detto anche macroprocesso é articolato in processi (28)

Elementi di analisi

Per ciascun processo sono elencati

- Scenari di rischio
- Obiettivi di controllo che mitigano il rischio
- Fattori e misure di controllo e di sicurezza adottati

Ad ogni misura di controllo sono associati il relativo

- Process owner - responsabile del controllo riferito ai processi di propria competenza
- Control performer , ovvero il responsabile dell'attivitá di controllo

6. Information Technology in Eurizon

Financial Group Eurizon

Ambito

EurizonSolutions

Banca FIDEURAM

EurizonVita

EurizonCapital

Processi

ACQUISIZIONE E IMPLEMENTAZIONE

Identificare le soluzioni informatiche
Acquisire e manutenere le applicazioni
Acquisire e manutenere le infrastrutture tecnologiche
Sviluppare e manutenere le procedure
Installare e collaudare i sistemi
Gestione dei cambiamenti

EROGAZIONE E SUPPORTO

Definire e gestire i livelli di servizio
Gestire i servizi di terze parti
Gestire performance e capacity
Garantire la continuità del servizio
Garantire la sicurezza dei sistemi
Identificare e attribuire i costi
Formare e addestrare gli utenti
Assistere e dare consulenza ai clienti
Gestire la configurazione
Gestire i problemi e gli incidenti
Gestire i dati
Gestire le infrastrutture
Gestire le attività operative

PIANIFICAZIONE E ORGANIZZAZIONE

Definire un piano strategico per l'IT
Definire l'architettura dei dati
Determinare la direttrice tecnologica
Definire l'organizzazione IT e le sue relazioni
Gestione degli Economics ICT
Comunicare gli indirizzi e gli obiettivi del management
Gestire le risorse umane
Assicurare la conformità a leggi e norme esterne
Valutare i rischi
Gestire i progetti
Gestire la qualità

MONITORAGGIO

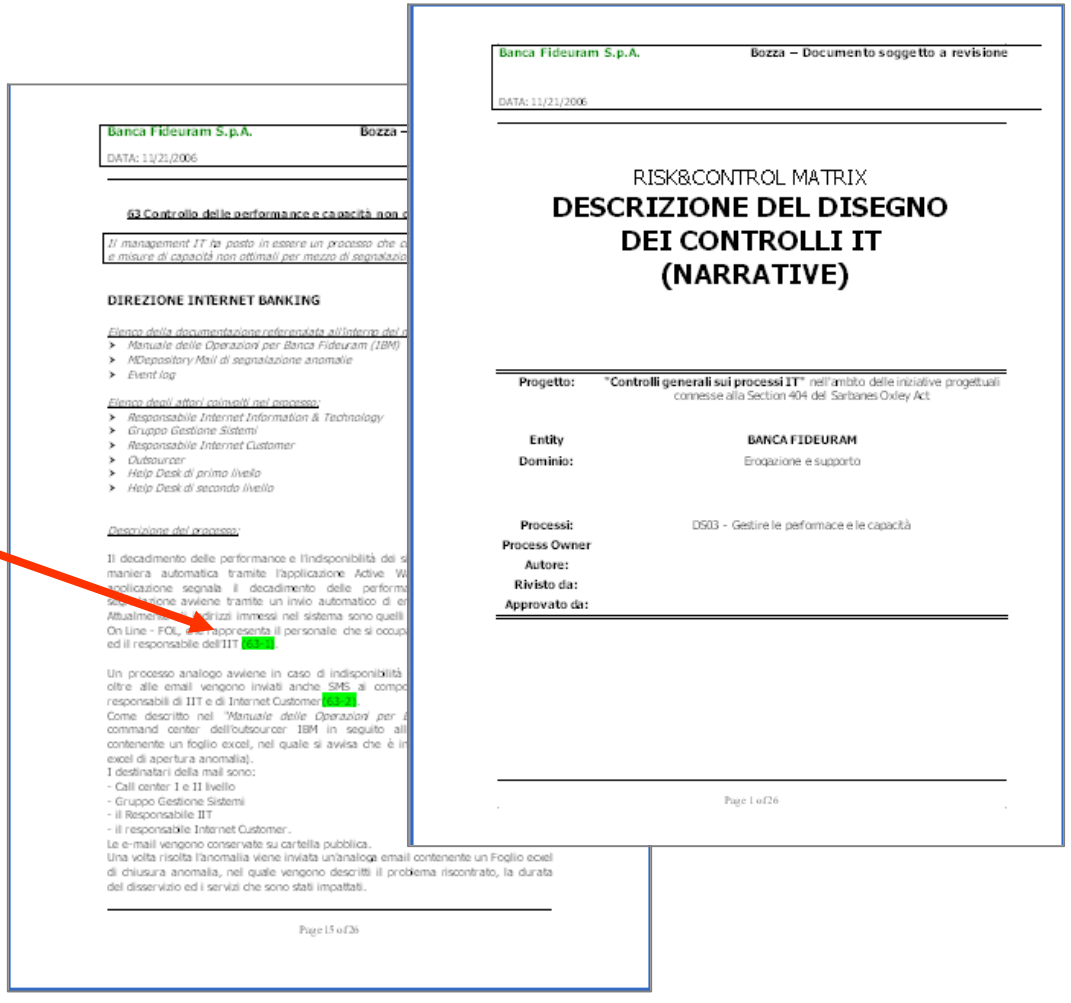
Monitorare i processi
Valutare l'adeguatezza del controllo interno
Ottenere certificazioni indipendenti
Provvedere alla revisione indipendente

- Altri servizi finanziari
- Asset management
- Assicurativo Vita
- IT

7. Attività effettuate

7.1. Assessment : Mappatura processo

Codice attività di controllo



Banca Fideuram S.p.A. Bozza – Documento soggetto a revisione

DATA: 11/21/2006

RISK&CONTROL MATRIX

DESCRIZIONE DEL DISEGNO DEI CONTROLLI IT (NARRATIVE)

Progetto: "Controlli generali sui processi IT" nell'ambito delle iniziative progettuali connesse alla Section 404 del Sarbanes Oxley Act

Entity BANCA FIDEURAM

Dominio: Erogazione e supporto

Processi: DS03 - Gestire le performace e le capacità

Process Owner

Autore:

Rivisto da:

Approvato da:

Page 1 of 26

7. Attività effettuate

7.2. Assessment : Analisi rischi

Financial Group Eurizon

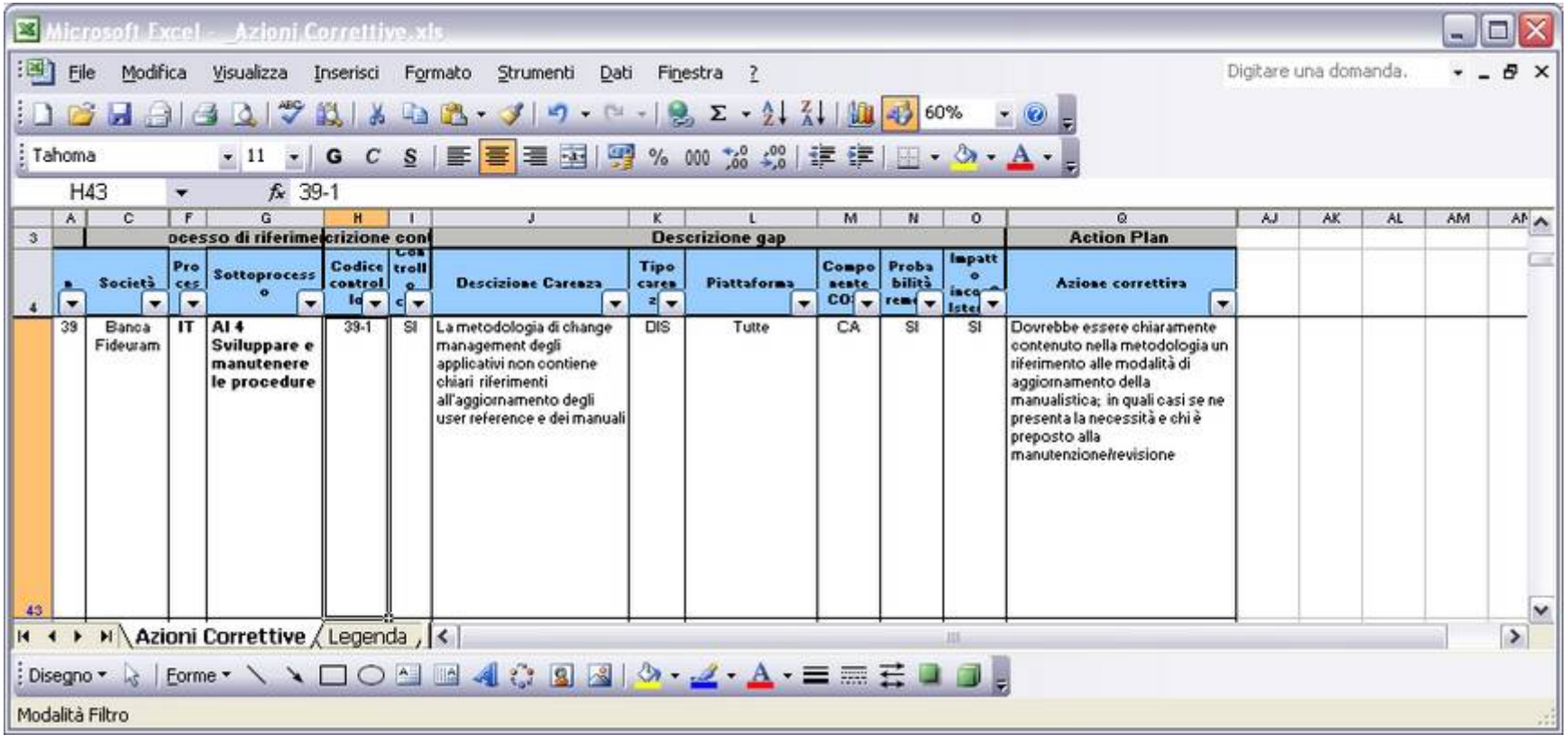
Cod Processo COBIT	Macro Obiettivo di Controllo	Rischio	Descrizione del rischio	N. O. C.	Key Control	Obiettivo di Controllo	Descrizione Controllo	COSO	Rif. Attività di Controllo	Descrizione Attività di Controllo	Piattaforma	Tipo di controllo	Frequenza del controllo	Documentazione del controllo	Strategia di controllo	Process Owner	Control Performer	Valutazione Efficacia Controllo	Check Evidence	Valutazione Complessiva Controllo	Riferimento Piano azioni correttive
PO 1	**Definire un piano strategico per l'IT**	Il piano Strategico per l'IT non è definito	Senza una adeguata pianificazione strategica l'organizzazione non riuscirebbe a raggiungere un equilibrio ottimale tra le opportunità fornite dall' IT e le esigenze aziendali di utilizzo dell' IT	1		Pianificazione obiettivi aziendali dell'IT	La Direzione IT utilizza politiche e procedure relative al processo di pianificazione, alle responsabilità della direzione, agli obiettivi aziendali dell'IT ed ai piani a lungo ed a breve termine	RA, IC, M	1-1	Gestione della strategia IT operata in accordo a logiche e direttive di Gruppo	MAINFRAME – DIPARTIMENTALE - AS/400 – RETE	P/M	On demand	SAL relativi ai progetti aziendali più significativi	Policy & Procedure	Direzione Generale di Banca Fideuram	Chief Operating Officer	E	NAD	3	1
PO 1				1					1-2	Definizione Piano Informatico di Direzione	MAINFRAME – DIPARTIMENTALE - AS/400 – RETE	P/M	Annuale	Piano informatico di Direzione	Check Evidence	Direzione DOS	Direzione DOS	E	AD	4	

Descrizione del controllo rilevato

7. *Attività effettuate*

7.3. Assessment : Identificazione azioni correttive

Financial Group
Eurizon

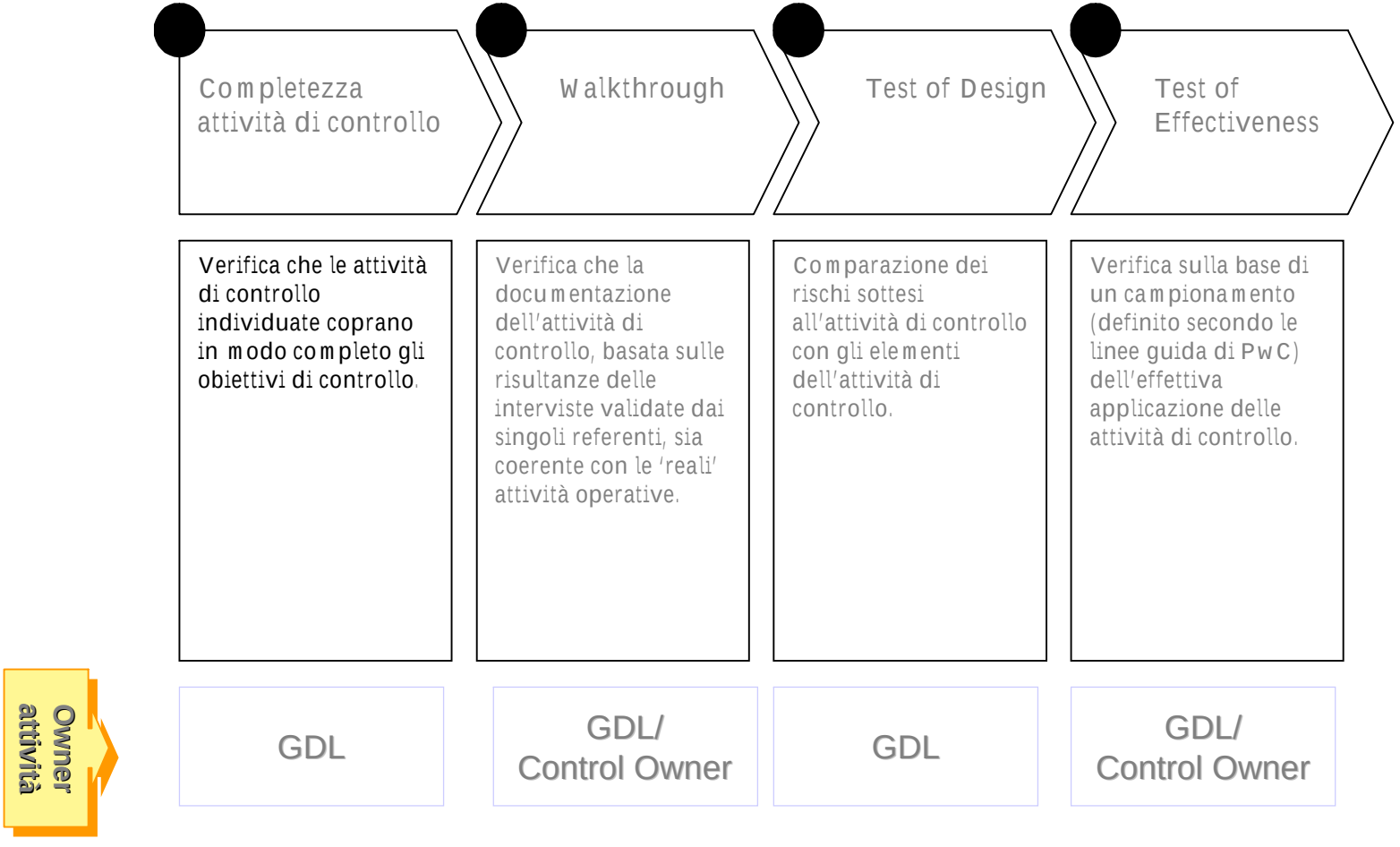


7. *Attività effettuate*

7.4. Test of Controls : ruoli ed attività

Financial Group
Eurizon

Piano di test (test planning)



7. *Attività effettuate*

7.5. Test of Controls : classificazione per difficoltà

Financial Group Eurizon

Sono stati identificati i seguenti li velli di diffcoltà nell'esecuzione dei ToC.

Test elementare che richiede solamente la presa visione della metodologia e la verifica della sua completezza.

Test elementare che richiede la verifica della metodologia e di evidenze documentali di facile campionamento e reperibilità.

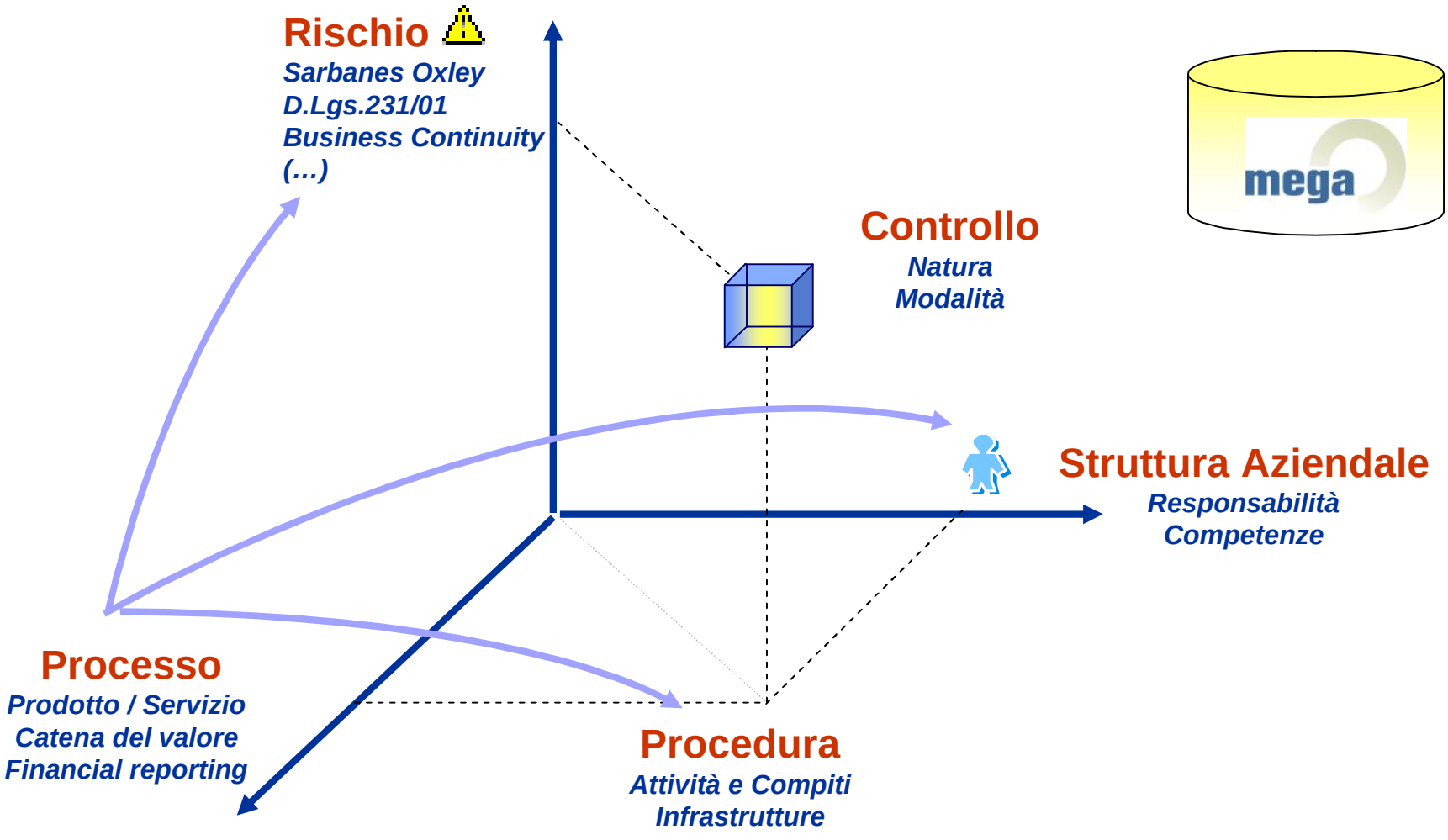
Test che richiede la verifica della metodologia e di evidenze documentali che non sono di immediato campionamento o reperibilità, o comporta estrazioni di dati dai sistemi.

Test strutturato con conseguente dilatamento dei tempi di esecuzione del walkthrough; il walkthrough potrebbe richiedere il coinvolgimento di diversi attori e/o il test potrebbe richiedere la riperformance del controllo

Test estremamente strutturato che, rispetto al caso 4, comporta una attività complessa per l'effettuazione di walkthrough e valutazione del design

10. I "plus" ottenuti

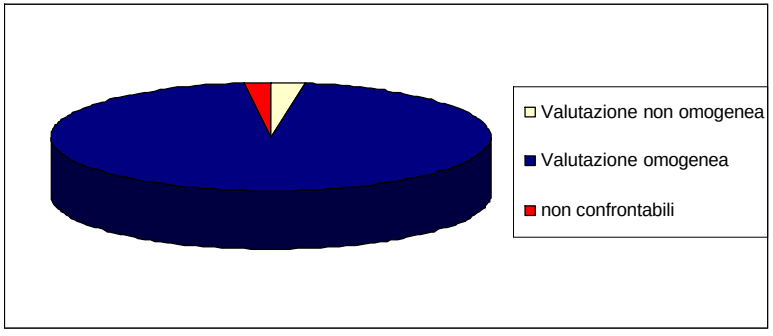
10.1. Gestione integrata processi, controlli e rischi



10. I “plus” ottenuti
10.2. Razionalizzazione processi IT dell'outsourcers

- Omogeneità rispetto a modello CobiT

Valutazione non omogenea	10
Valutazione Omogenea	391
Non possibile giudizio	8
Totale	409



10. I “plus” ottenuti
10.2. Razionalizzazione processi IT dell'outsourcers

Financial Group
Eurizon

E' stata effettuata una attività di aggregazione delle attività di controllo sulla base dei seguenti parametri:

- Piattaforma tecnologica
- Tipologia di attività
- Process Owner

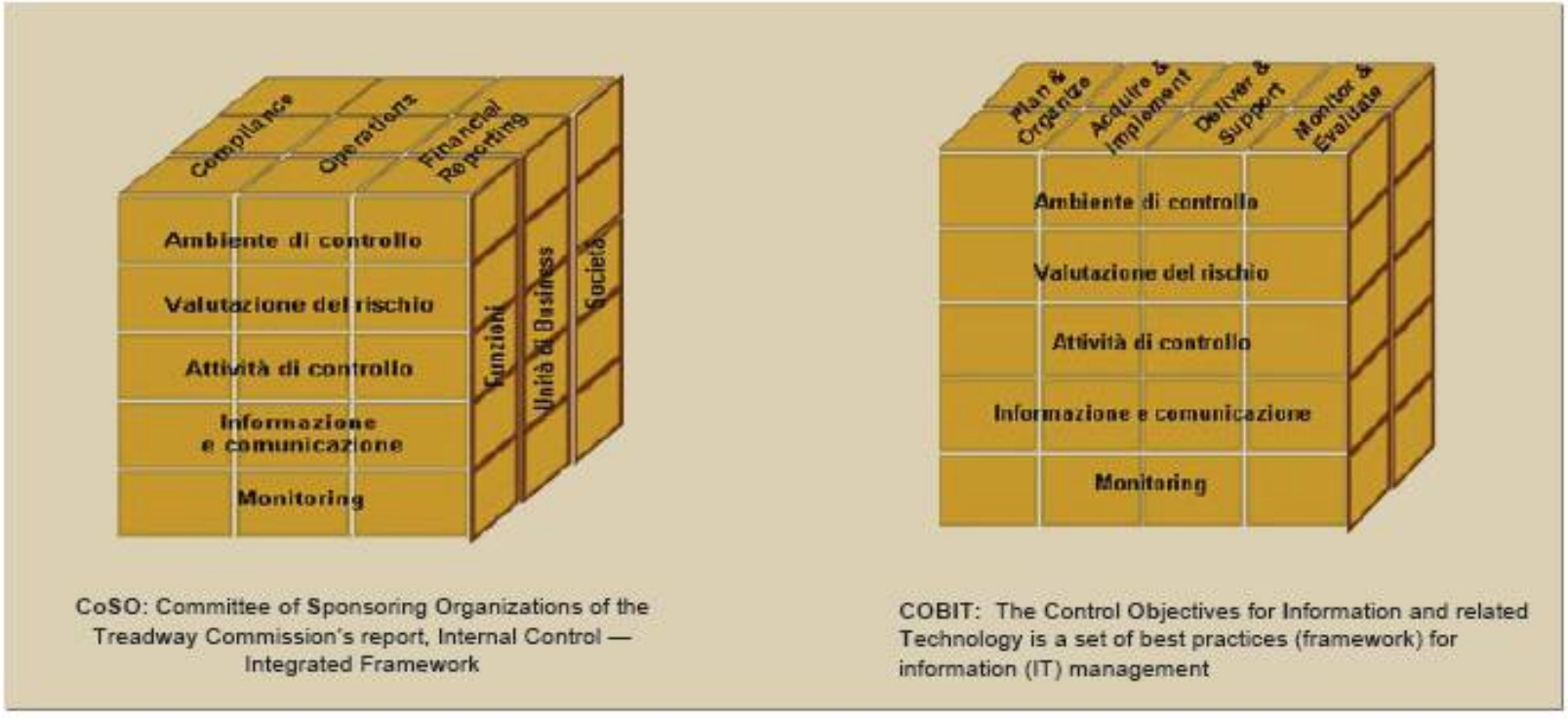
Sono state individuate 193 aggregazioni per le 409 attività.
Le aggregazioni più significative sono:
- N° 1 aggregazione che raggruppa 11 attività (sicurezza logica);
- N° 2 aggregazioni (Config. Sistemi e gestione problemi incidenti) che raggruppano 10 attività ciascuna;
- N° 7 aggregazioni che raggruppano 6 attività ciascuna.

Sono state comunque rilevate:
- N° 42 aggregazioni che raggruppano 2 attività ciascuna;
- N° 99 attività non raggruppabili.

11. Normativa 262/05
11.1. Contestualizzazione del Framework

Financial Group
Eurizon

•La **Legge 262/2005** non fa riferimento a standard per la valutazione dell'efficacia dei processi.
•Il **benchmark** comunemente utilizzato a livello internazionale per la valutazione dell'efficacia dei processi è rappresentato dal **Coso (**Committee of Sponsoring Organizations of the Treadway Commission's Report, Internal Control) **Integrated Framework** e, per la componente IT, dal **COBIT** (The Control Objectives for Information and related Technology) **Framework.**



CoSO: Committee of Sponsoring Organizations of the Treadway Commission's report, Internal Control — Integrated Framework

COBIT: The Control Objectives for Information and related Technology is a set of best practices (framework) for information (IT) management

11. Normativa 262/05
11.1. Contestualizzazione del Framework

•Il COBIT Framework si pone l'obiettivo di fornire le linee guida per la strutturazione e la manutenzione di un adeguato Sistema dei Controlli Interni sui processi IT, sulla base di un approccio strutturato definito dall'Associazione Internazionale I.S.A.C.F. (InformationSystems Audit and Control Foundation) .
•Caratteristica principale del COBIT è l'orientamento al business: è stato disegnato non solo per essere utilizzato dai fornitori di servizi IT, utenti e audit ma soprattutto per fornire una guida comprensiva per il management e gli owner dei processi di Business