istat
working
papers

N. 10
2011

Strumenti metodologici per l'audit della funzione informatica nelle organizzazioni complesse: “Alcune soluzioni adottate dall'Istituto nazionale di statistica nell'esperienza del processo di audit ICT”

Silvia Losco, Cecilia Colasanti

Istat
Istituto Nazionale
di Statistica

istat
working
papers

N. 10
2011

Strumenti metodologici per l'audit della funzione informatica nelle organizzazioni complesse: “Alcune soluzioni adottate dall'Istituto nazionale di statistica nell'esperienza del processo di audit ICT”

Silvia Losco, Cecilia Colasanti

Istat

Istat Working Papers

Strumenti metodologici per l'audit della funzione informatica nelle organizzazioni complesse: “Alcune soluzioni adottate dall'Istituto nazionale di statistica nell'esperienza del processo di audit ICT”

N. 10/2011

ISBN 88-458-1693-1

Istituto nazionale di statistica
Servizio Editoria
Via Cesare Balbo, 16 – Roma

Strumenti metodologici per l'audit della funzione informatica nelle organizzazioni complesse: "Alcune soluzioni adottate dall'Istituto nazionale di statistica nell'esperienza del processo di audit ICT"

Silvia Losco, Cecilia Colasanti

Sommario

La crescente complessità delle organizzazioni pubbliche e private ed il più stretto legame tra il core business aziendale ed i sistemi informativi impongono una gestione sempre più strutturata degli aspetti legati all'ICT. In questo documento viene preso in esame il processo di audit informatico, affrontando alcuni aspetti metodologici e descrivendo i principali framework di riferimento per la gestione dell'IT soprattutto nel settore pubblico. Sono evidenziati gli aspetti legati all'IT governance, all'analisi dei rischi, all'impatto sull'utenza avendo come riferimento l'approccio CobIT, il modello di maturità dei processi aziendali (CMMI), la matrice RACI per l'attribuzione dei ruoli e delle responsabilità. Viene poi descritta l'esperienza maturata dall'Istat nell'utilizzo di tali approcci metodologici nell'ambito del processo di audit ICT. L'Istat è tra le prime Pubbliche Amministrazioni italiane ad aver condotto un processo di audit informatico nell'ambito delle azioni intraprese per il miglioramento dell'efficienza ed efficacia delle proprie attività.

Parole chiave: audit, IT governance, rischio, maturity model.

Abstract

The increasing complexity of public and private organisations and the closer link between the enterprise's core business and information systems require a more and more structured ICT management. This paper examines the ICT audit process, facing some methodological issues and describing the main frameworks for IT management, particularly in the public sector. IT governance, risk analysis, user impacts are underlined, taking into consideration the CobIT approach, the processes maturity model (CMMI), the RACI matrix for separation of duty and responsibility. It is also described the Istat experience in using this kind of tools. Istat is one of the first Italian Public Administration to have conducted a similar process in connection with actions taken to improve efficiency and effectiveness of its activities.

Keywords: audit, IT governance, risk, maturity model.

1. Introduzione[1]

Il rapido progresso tecnologico avvenuto negli ultimi anni ha messo in discussione i tradizionali approcci adottati dalle aziende private e amministrazioni pubbliche per disegnare la struttura della funzione informatica e gestire in modo efficiente ed efficace i servizi dell'Information Technology (IT). Le nuove tecnologie hanno profondamente modificato il processo di produzione e di fruizione

[1] Il lavoro è il frutto della collaborazione degli autori. In particolare Silvia Losco ha curato i capitoli 1,2,4,6,7,8,9 e gli allegati 1,2,3 e Cecilia Colasanti i capitoli 3,5,10 e l'allegato 4.

dei prodotti dell'IT, ridisegnando le attribuzioni delle strutture sia dal lato utente sia dal lato tecnico. E' evidente la necessità di avviare tutte le misure che consentano di porre in sempre più stretta relazione l'IT e il core businesss dell'azienda, mettendo in atto soluzioni tecniche e organizzative che sappiano allineare la tecnologia alla strategia aziendale.

In tale panorama emerge in modo evidente l'esigenza di affrontare il tema della Corporate Governance e in particolare la Governance dell'IT e della funzione informatica attorno a cui ruotano soggetti e funzioni che, ognuna per la propria parte, contribuiscono alla conduzione dell'organizzazione in modo etico, corretto e coerente con gli obiettivi di business e di gestione dei propri rischi aziendali.

In tale ottica le organizzazioni complesse ed in particolare gli organismi pubblici avvertono la necessità di delineare con chiarezza i punti cardine del proprio sistema di governo al fine di garantire il conseguimento delle proprie finalità in ottica non solo di aderenza ai principi normativi ma anche di efficienza. Nelle amministrazioni pubbliche tale necessità è accelerata dall'esigenza di cambiamento delle PA evidenziata anche all'interno delle "Linee programmatiche sulla riforma della Pubblica Amministrazione" predisposte dal Ministro per la pubblica amministrazione e l'innovazione, che prevedono un programma di risanamento, ristrutturazione e rilancio del settore pubblico italiano.

Obiettivo del documento è fornire alcuni elementi chiave di carattere metodologico che consentono di effettuare l'analisi della funzione informatica in organizzazioni complesse, con particolare riferimento alle amministrazioni pubbliche. Vengono messe in luce metodologie e strumenti di riferimento per l'analisi del livello di governance adottato dalle organizzazioni in ambito IT, del livello raggiunto nel delivery dei servizi IT. Il documento fornisce inoltre l'approccio metodologico generale teso ad orientare l'analisi alla gestione dei rischi IT dell'organizzazione.

2. Aspetti di IT Governance

L'Enterprise governance consiste in un insieme di responsabilità e pratiche esercitate dall'alta direzione e dal management esecutivo dell'azienda con l'obiettivo di:

- definire gli indirizzi strategici;
- assicurare che gli obiettivi siano raggiunti;
- accertare che i rischi siano gestiti in modo appropriato;
- verificare che le risorse aziendali siano impiegate responsabilmente.

Con IT governance, o governo dei sistemi informativi, si intende quella parte della più ampia corporate governance che si occupa di dotare le organizzazioni aziendali di un corpo di regole volte a coniugare il raggiungimento degli obiettivi aziendali con le aspettative del mercato, fissando regole di governo e di controllo che favoriscano la creazione di valore per gli azionisti e la tutela degli interessi di tutti gli stakeholder.

Citando quanto definito dall'IT Governance Institute, "L'IT governance è responsabilità diretta del consiglio di amministrazione e del management esecutivo. È parte integrante della governance aziendale ed è costituita dalla direzione, dalla struttura organizzativa e dai processi in grado di assicurare che l'IT sostenga ed estenda gli obiettivi e le strategie dell'organizzazione".

Di fatto quindi l'IT governance è di responsabilità dell'alta direzione e del management esecutivo ed è una parte integrale del governo dell'organizzazione, consistente in leadership, strutture organizzative e processi al fine di assicurare che l'IT sostenga ed estenda le strategie e gli obiettivi dell'organizzazione.

L'IT governance consente la strutturazione di policy e di un sistema procedurale per indirizzare le attività di un'organizzazione al fine di fornire una ragionevole assicurazione che gli obiettivi siano conseguiti e che le operazioni siano eseguite in modo etico e responsabile. Nel contempo l'IT governance rende l'organizzazione più capace di prendere decisioni a fronte di cambiamenti strategici contribuendo sensibilmente ad incrementare le capacità di valutare i costi dei sistemi informatici e i ritorni degli investimenti.

L'IT governance ispira quindi un comportamento attivo e trasparente di chi gestisce i sistemi informatici e informativi dell'organizzazione, accompagnato dalla consapevolezza che gli strumenti

di informatizzazione adottati e adottabili possano incidere sulle scelte strategiche dell'organizzazione.

A tale aspetto fondamentale, connesso strettamente al concetto di allineamento strategico dell'IT al business, và inoltre aggiunta come finalità imprescindibile la gestione dei rischi informatici legati all'utilizzo degli strumenti.

Le aree focali su cui ruota l'IT governance sono.

Allineamento Strategico: Si focalizza sull'assicurare il collegamento del business e dei piani IT; sulla definizione, manutenzione e validazione delle IT value proposition;[2] e sull'allineamento delle operazioni IT con le attività dell'organizzazione.

Aggiunta di Valore: Riguarda l'esecuzione delle value proposition del ciclo di erogazione, garantendo che l'IT produca i benefici promessi nel rispetto della strategia, concentrandosi sull'ottimizzazione dei costi e dimostrando il valore intrinseco dell'IT.

Gestione delle Risorse: Riguarda l'investimento ottimale, e l'opportuna gestione, nelle risorse IT critiche: applicazioni, informazioni, infrastrutture e persone. I fattori chiave sono relativi all'ottimizzazione delle conoscenze e delle infrastrutture.

Gestione dei rischi: Registra e controlla l'implementazione della strategia, il completamento del progetto, l'impiego delle risorse, la performance del processo e l'erogazione del servizio, utilizzando, ad esempio, balanced scorecard che traducono strategia in azione per raggiungere obiettivi misurabili al di là dei metodi di contabilizzazione tradizionali.

Gli aspetti di IT governance sono strettamente correlati al tipo di organizzazione al suo mandato di business, al suo contesto organizzativo. Ovviamente nel settore privato la governance, pertanto, è correlata principalmente ai diritti degli stakeholders ed alla necessità di trasparenza/divulgazione e coinvolge significativamente il ruolo che il Consiglio di Amministrazione ed il Comitato di Controllo sono chiamati a svolgere. Di seguito si fornisce un'analisi del concetto di IT governance applicato alle organizzazioni pubbliche.

2.1 La Governance nel settore pubblico

L'IT governance concerne il modo in cui un'organizzazione assume e implementa le decisioni e in particolare i processi attraverso i quali le organizzazioni sono dirette, controllate e condotte responsabilmente. Le Pubbliche Amministrazioni hanno diversi mandati e diverse strutture organizzative pertanto non può essere unicamente individuabile il modello di IT governance da adottare comune a tutto il settore pubblico.

Nel contesto del settore pubblico il concetto di governance è principalmente collegato ad aspetti organizzativi che coinvolgono le responsabilità, i compiti e le deleghe del management. In altre parole dovrebbe definire "chi fa cosa". In questa ottica la governance dovrebbe includere il sistema procedurale finalizzato a fornire una ragionevole assicurazione che gli obiettivi siano conseguiti e che le operazioni siano eseguite in modo etico e responsabile, assicurando la credibilità dell'amministrazione pubblica ed un appropriato comportamento dei funzionari statali.

Si possono comunque identificare alcuni principi comuni che si affiancano alle peculiarità che caratterizzano l'obiettivo fondamentale del servizio pubblico da rendere al cittadino e alle altre istituzioni proprio di ogni singola PA.

Tali principi sono legati alla responsabilità nell'uso dei propri poteri e alla fornitura dei servizi attesi unitamente al ridurre il rischio di corruzione o uso illecito di poteri affidati.

I principi fondamentali si basano sulla responsabilità, trasparenza, integrità, equità e correttezza.

Responsabilità:[3] "L'accountability è il processo per mezzo del quale gli enti pubblici e gli individui che operano al loro interno, sono responsabilizzati per le loro decisioni ed azioni, inclusa l'amministrazione di fondi pubblici e tutti gli aspetti legati ai risultati della loro attività e sono sottoposte ad una adeguata valutazione esterna. Essa si ottiene attraverso una esatta cognizione da par-

[2] "Value proposition" riguarda tutto ciò che l'organizzazione si propone di dare ai propri utenti.
[3] Fonte: IFAC, Governance in the the Public Sector, a Governing Body Perspective, 2001.

te di tutte le parti in causa della chiara definizione di ruoli e responsabilità nella struttura. Pertanto l'accountability rappresenta il dovere di rispondere per la rappresentazione attribuita".

Trasparenza: Il principio di trasparenza riguarda i servizi erogati dall'amministrazione nei confronti dei propri stakeholders intesi come cittadini e altre istituzioni. La trasparenza prevede un'adeguata divulgazione delle informazioni di rilievo. Le decisioni, le azioni e le operazioni sono pertanto condotte in termini di piena apertura nei confronti di chi usufruisce dei servizi messi a disposizione. E' da notare che la trasparenza è fortemente connessa alla credibilità dell'amministrazione.

Integrità: Il principio di integrità richiede di agire con correttezza e onesta in modo che le informazioni e le azioni pubbliche siano effettivamente considerate affidabili.

Equità: Il principio di equità richiede all'amministrazione di esercitare il proprio mandato con imparzialità.

La governance applicata al mondo delle amministrazioni pubbliche, quindi, si dovrebbe tradurre nella costruzione di un sistema organico di regole in linea con i principi di responsabilità, trasparenza, integrità ed equità. La governance del settore pubblico assume aspetti distintivi rispetto al settore privato in quanto coinvolge processi particolari connessi a strategie, obiettivi, sistemi di gestione e controllo più numerosi, complicati, spesso rigidi e diversificati rispetto a quelli del settore privato.

2.2 Le aree focali per l'IT governance e i ruoli

Di seguito si riportano le aree focali di riferimento per l'IT governante così come definite dagli organismi di riferimento internazionali SACA - Information Systems Audit & Control Association e ITIG - IT Governance Institute che si occupano di governante e audit dei sistemi informativi.

Allineamento Strategico: Si focalizza sull'assicurare il collegamento del business e dei piani IT; sulla definizione, manutenzione e validazione delle IT value proposition e sull'allineamento delle operazioni IT con le attività aziendali.

Aggiunta di Valore: Riguarda l'esecuzione delle value proposition del ciclo di erogazione, garantendo che l'IT produca i benefici promessi nel rispetto della strategia, concentrandosi sull'ottimizzazione dei costi e dimostrando il valore intrinseco dell'IT.

Gestione delle Risorse: Riguarda l'investimento ottimale, e l'opportuna gestione, nelle risorse IT critiche: applicazioni, informazioni, infrastrutture e persone. I fattori chiave sono relativi all'ottimizzazione delle conoscenze e delle infrastrutture.

Risk Management: Richiede la consapevolezza del rischio dai membri della direzione aziendale, una chiara comprensione del "risk appetite" dell'azienda, dei requisiti di adeguamento a leggi e normative, trasparenza riguardo i rischi significativi per l'impresa, e l'inclusione delle responsabilità per il risk management nell'organizzazione.

Gestione delle Performance: Registra e controlla l'implementazione della strategia, il completamento del progetto, l'impiego delle risorse, la performance del processo e l'erogazione del servizio, utilizzando, ad esempio, balanced scorecard che traducono strategia in azione per raggiungere obiettivi misurabili al di là dei metodi di contabilizzazione tradizionali.

La figura 1 riportata a seguire sintetizza le aree focali dell'IT governance.

In merito agli attori e ai ruoli nella IT governante, di seguito si riporta l'articolazione di massima come definita da ISACA e ITGI.

Alta direzione e management esecutivo: Definisce la direzione per l'IT, registra i risultati e insiste sulle misure correttive.

Business management: Definisce i requisiti di business per l'IT e assicura che sia aggiunto valore e i rischi gestiti.

IT management: Eroga e migliora i servizi IT come richiesto dal business.

IT audit: Fornisce un'assicurazione indipendente finalizzata a dimostrare che l'IT eroghi quanto richiesto.

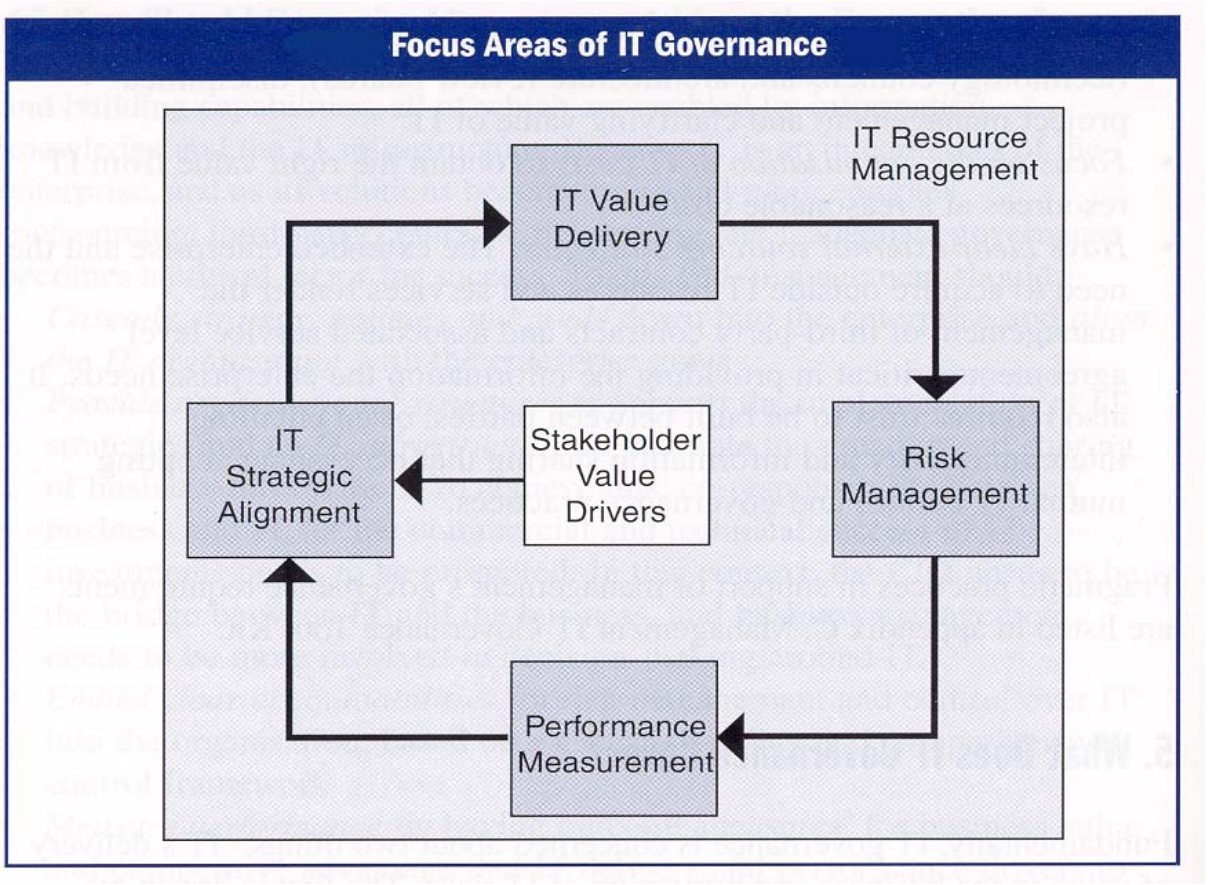
Rischio e adeguamento: Misura l'adeguamento alle politiche e si concentra sugli allarmi riguardo nuovi rischi.

E' da tener presente che ad oggi maggior evidenza viene richiesta per i ruoli riservati alle funzioni che tradizionalmente operavano nel sistema di controllo interno aziendale. In particolare nuo-

ve figure sono comparse e nuove funzioni si sono delineate in un panorama di orientamento generale verso la governance. I confini delle organizzazioni di oggi in ambito IT sono inoltre più flessibili e dinamici e, in alcuni casi, più ampi rispetto al passato. Le organizzazioni devono quindi focalizzarsi su interi processi, che spesso trascendono i limiti fisici della propria organizzazione IT. Devono raggiungere i *business partner*, i fornitori e i clienti fornendo informazioni accurate, appropriate e tempestive come una componente indispensabile di ciò che viene comunemente descritto come "*extended enterprise*".

Da ciò ne deriva che effettivamente non esiste un approccio valido per tutte le organizzazioni per massimizzare l'allineamento dell'IT con l'azienda e con tutte le sue componenti. Occorre considerare il tipo d'azienda, le dimensioni, il mercato, la dipendenza dal settore IT, lo stile di *leadership* e la cultura. Risulta comunque fondamentale fare in modo che ruoli e responsabilità di tutto il personale nell'organizzazione IT siano definiti e comunicati per permettere di esercitare il ruolo e le responsabilità assegnate con sufficiente autorità.

Figura 1 - Le aree focali dell'IT governance



Fonte: Board Briefing on IT Governance, 2nd Edition, IT Governance Institute, 2003

2.3 Le decisioni dell'IT e gli stili di governance

Nell'avviare un progetto finalizzato all'IT governance, le organizzazioni devono tener presente alcuni criteri fondamentali a garanzia di successo del progetto stesso. In primo luogo la soluzione di IT governance deve essere praticabile per l'organizzazione e in grado di confrontarsi con le sfide e i pericoli presentati dall'IT; un secondo importante elemento è costituito dalla necessità di focalizzarsi il più possibile sul miglioramento delle performance sui vantaggi competitivi e sulle facilitazioni possibili unitamente alla prevenzione dei problemi. Và inoltre tenuto presente che l'IT governance è di fatto una responsabilità condivisa tra il business (cliente) e il fornitore del servizio IT che deve avere il pieno commitment da parte del management in un quadro organico di allineamen-

to dell'IT governance all'interno dello schema più vasto dell'enterprise governance. L'alta direzione e il management esecutivo hanno bisogno di fatto di estendere l'enterprise governance per includere l'IT, fornendo le necessarie leadership e le adeguate strutture organizzative, unitamente a processi correttamente gestiti e adeguatamente controllati.

Per assicurare il governo dell'IT è necessario prendere decisioni in ambito IT seguendo due assi di riferimento:

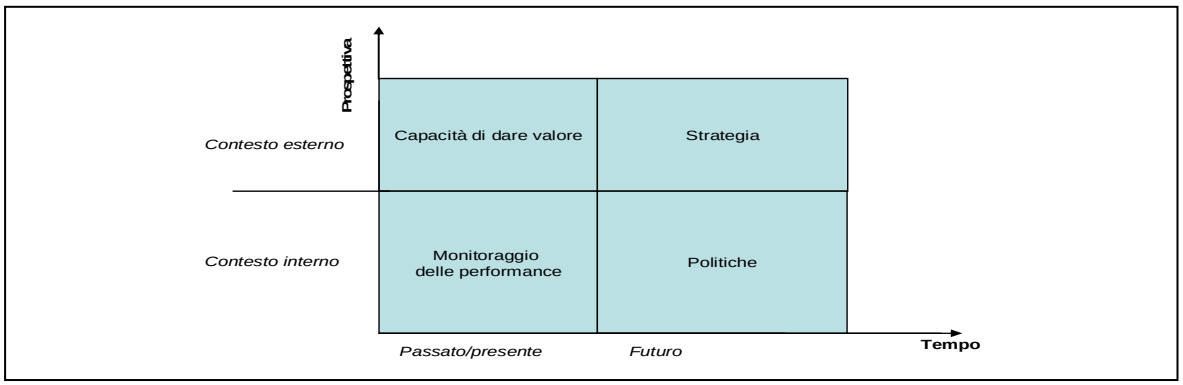
- le prospettive, interne ed esterne all'organizzazione;
- l'asse del tempo (passato/presente, futuro).

Secondo tali assi vanno inquadrati i seguenti parametri di riferimento dell'IT

- politiche dell'IT;
- strategia evolutiva dell'infrastruttura IT;
- capacità di dare valore;
- monitoraggio delle performance.

Lo schema riportato in figura 2 riporta i parametri di riferimento inquadrati secondo l'asse del tempo e l'asse di prospettiva.

Figura 2 - Parametri decisionali inquadrati secondo gli assi del tempo e di prospettiva



Le decisioni sull'IT riguardano essenzialmente quattro domini di riferimento:

- politiche IT;
- strategie evolutive dell'infrastruttura IT;
- architettura IT;
- investimenti IT e priorità.

A tali domini vanno comunque aggiunte le specifiche decisioni inerenti le esigenze di sviluppo di applicazioni per il business.

Esistono diversi stili di governance possibili in una organizzazione; tali stili riflettono l'obiettivo dell'organizzazione ma anche il clima organizzativo, il contesto in cui opera e il volume economico di riferimento del proprio business. Gli stili e i sistemi di governance noti in letteratura sono:

Sistema con stile di governance monarchico: è un sistema basato sulla leadership in cui le decisioni vengono prese unilateralmente dal manager responsabile dell'area. Tale sistema prevede:

- il sistema monarchico con la leadership del business, se a decidere sono i manager delle aree di business, includendo il Responsabile dei Sistemi Informativi, in modo unilaterale e indipendente l'uno dall'altro;
- il sistema monarchico con la leadership dell'IT, se a decidere è il Responsabile dei Sistemi Informativi con il proprio staff tecnico in modo unilaterale e indipendente dai manager del business;
- il sistema con stile di governance anarchico: tutti i manager, sia afferenti alle aree di business che alle aree IT, prendono le decisioni in merito all'IT;
- il sistema con stile di governance federata: se a decidere sono i manager di aree ben specifiche (per esempio l'IT e l'area economico/finanziaria).

Tali sistemi con stili di governance diversi possono anche essere coesistenti nella stessa organizzazione. Uno stile di governance si riferisce infatti alle modalità tramite le quali vengono prese le decisioni in merito all'IT. A seconda dell'ambito di riferimento possono essere adottati diversi stili applicati ai diversi domini di riferimento.

3. La gestione del rischio

Il rischio viene definito come il prodotto della probabilità che un evento negativo si verifichi per l'impatto che questo ha sull'organizzazione. La gestione del rischio è quel processo attraverso cui si misura o si stima il rischio e successivamente si sviluppano delle strategie per governarlo.

I principali approcci all'analisi del rischio sono:

approccio di baseline: consiste nell'applicare una protezione di base equivalente per tutti i sistemi. È questo il caso delle best practice, ossia dell'esperienza maturata positivamente da più gruppi di persone e di aziende;

approccio informale: consiste nel condurre un'analisi del rischio in modo informale, non strutturato, basato sull'esperienza;

analisi di rischio dettagliata: coinvolge un'analisi accurata degli asset, delle minacce e delle vulnerabilità;

approccio combinato: si identificano prima i sistemi ad alto rischio tramite un'analisi di alto livello, poi si dividono i sistemi in due categorie. Quelli per cui la protezione di base è sufficiente e quelli per cui deve essere fatta un'analisi di rischio dettagliata.

In Istat si è scelto di condurre un'analisi di rischio dettagliata che è cominciata da un'analisi dei processi aziendali su cui l'audit ICT ed il processo di risk management hanno trovato la loro area di convergenza.

L'analisi dei processi permette a sua volta di stabilire quali sono le risorse (hardware, software, persone, …) che rappresentano un valore per l'azienda e che la mettono in condizione di portare a termine con successo i propri obiettivi.

In generale i processi si possono suddividere in:

- processi strategici;
- processi operativi;
- processi di supporto.

I primi possono ancora essere suddivisi in processi competitivi, cioè quelli con cui l'organizzazione compete sul mercato e con i quali mira a superare la concorrenza (in Istat sono rappresentati dalla produzione statistica) e processi di innovazione e trasformazione, che riguardano investimenti su prodotti, servizi e tecnologie di avanguardia.

I secondi servono a realizzare i prodotti che l'organizzazione rilascia al mercato (in Istat i dati delle indagini).

Gli ultimi aggiungono efficienza ed efficacia ai primi due e sono rappresentati ad esempio dalla gestione delle risorse umane, finanziaria, amministrativa, etc, …

Il metodo di analisi dei processi implementato attraverso l'audit ICT ha permesso di raccogliere le seguenti informazioni:

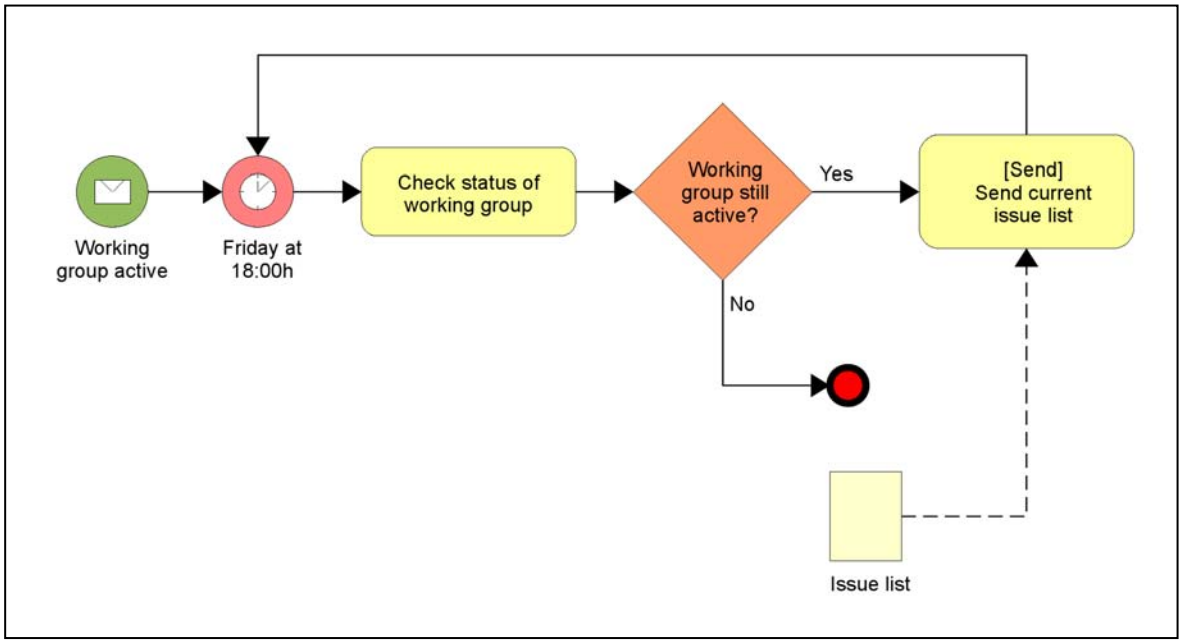
- definire lo scopo del processo;
- definire il responsabile del processo;
- delimitare il processo (stabilendone inizio e fine);
- identificare il cliente del processo;
- specificare l'output del processo;
- definire gli input del processo;
- definire i fornitori degli input;
- verificare i vincoli dati da leggi e regolamenti;
- stabilire i controlli da effettuare;
- identificare le infrastrutture necessarie a produrre l'output;

- identificare le risorse umane necessarie e i livelli di competenza richiesti;
- identificare i sottoprocessi;
- evidenziare le dipendenze tra processi (cioè se l'output di un processo costituisce l'input per un altro processo).

3.1 Il metodo BPMN (Business Process Modeling Notation) per l'analisi dei processi aziendali

Il metodo BPMN per l'analisi dei processi, sviluppato dalla BPMI (Business Process Management Inititiative), consiste nella rappresentazione grafica di specifici processi di business ed è basato sulla tecnica di flowcharting.

Figura 3 - Esempio di flow chart BPMN



L'obiettivo è quello di supportare gli utenti a tutti i livelli, dai manager agli operativi, nella gestione del processo di business fornendo una notazione intuitiva e comprensibile che rappresenti in modo semplice concetti semanticamente complessi.

Gli elementi che costituiscono questo modello sono quattro:

- Flow Object: sono gli oggetti base (events, activities, gateway);
- Connecting Object: connettono i flow object per rappresentare la struttura del processo (Sequence Flow, Message Flow, Association);
- Swimlane: possono essere considerati "raccoglitori" che permettono di raggruppare le attività in categorie visuali separate per mostrare diversi ambiti di responsabilità o funzioni (Pool, Lane);
- Artifact: forniscono informazioni su come documenti dati e altri oggetti sono usati in un processo (Data Object, Group, Annotation).

Queste quattro categorie danno l'opportunità di disegnare un business process diagram (BPD) personalizzato secondo le esigenze aziendali. Di seguito sono descritti gli elementi costitutivi di ciascun gruppo di oggetti.

Flow Object e Connecting Object

Un event è rappresentato da un cerchio ed è qualcosa che accade durante un processo di business (è diverso dall'attività che invece è qualcosa che è stato fatto). Ci sono tre tipi di evento a se-

conda del punto in cui intervengono sul processo: start, intermediate, end. Questi eventi modificano il flusso di processo e normalmente hanno una causa (trigger) ed un impatto (conseguenza).

Una activity è rappresentata da un rettangolo con i bordi arrotondati ed è genericamente un compito effettuato. Può essere atomica (semplice) o non-atomica (composta). I tipi di attività sono task e sottoprocesso. Il sottoprocesso è individuato da un "+" in basso nel rettagolo.

Un gateway è rappresentato da un rombo e caratterizza i punti di decisione dove il flusso si ramifica.

I Flow object sono connessi uno all'altro attraverso i Connecting object, che possono essere di tre tipi: Sequences, Messages, e Associations.

- Un Sequence Flow è una freccia che mostra in quale ordine vengono eseguite le attività;
- un Message Flow è una freccia tratteggiata, con un cerchio ad una estremità, che mostra il flusso di messaggi inviati o ricevuti tra due diversi partecipanti ad un processo (entità di business o ruoli di business);
- una Association è una freccia composta di punti, usata per associare dati, testo a artefatti a Flow Object. Mostra l'input e l'output delle attività.

Swimlane

Un pool rappresenta i principali partecipanti ad un processo, tipicamente di diverse organizzazioni e può contenere una o più linee (come una reale piscina), che rappresentano le attività.

Un lane è un elemento usato per organizzare le attività, funzioni o ruoli all'interno di un pool e può contenere Flow Objects, Connecting Objects e Artifact.

Artifact

Consentono di apportare alcune informazioni di dettaglio al diagramma per renderlo più leggibile. I principali elementi sono:

- Data Object mostra i dati richiesti o prodotti da un'attività;
- Group rappresentato da un rettangolo dai contorni tratteggiati, viene usato per raggruppare attività o per scopi di documentazione e analisi;
- Annotation fornisce testo informativo per il lettore ed è disegnata attraverso una parentesi quadrata aperta.

3.2 I processi critici e le loro interdipendenze

Il passo successivo è quello della determinazione dei cosiddetti processi critici. Rispetto all'azienda i processi critici sono quelli tali per cui:

1) l'output è utilizzato da più processi;
2) l'output ha valore per l'azienda;
3) il processo riceve molti input;
4) il numero dei sottoprocessi che lo compongono è elevato.

Considerando anche le variabili costo, tempo e qualità possiamo aggiungere che

5) l'output deve essere generato a partire dagli input in un tempo determinato;
6) l'output deve essere generato con una qualità definita;
7) l'output deve essere ottenuto entro un costo massimo per l'azienda.

Una volta individuati tali processi, bisogna considerare le dipendenze tra i processi stessi. Uno strumento utile all'analisi delle dipendenze è la Design Structure Matrix[4] che ha come righe e colonne tutti i processi aziendali. L'elemento Pij della matrice rappresenta il fatto che l'output del processo Pj della j-ma colonna è usato come input dal processo Pi della i-ma riga.

Alle colonne vengono aggiunte tante righe per quanti sono eventuali processi esterni al sistema, il cui output è usato da almeno un processo del sistema.

[4] http://www.dsmweb.org

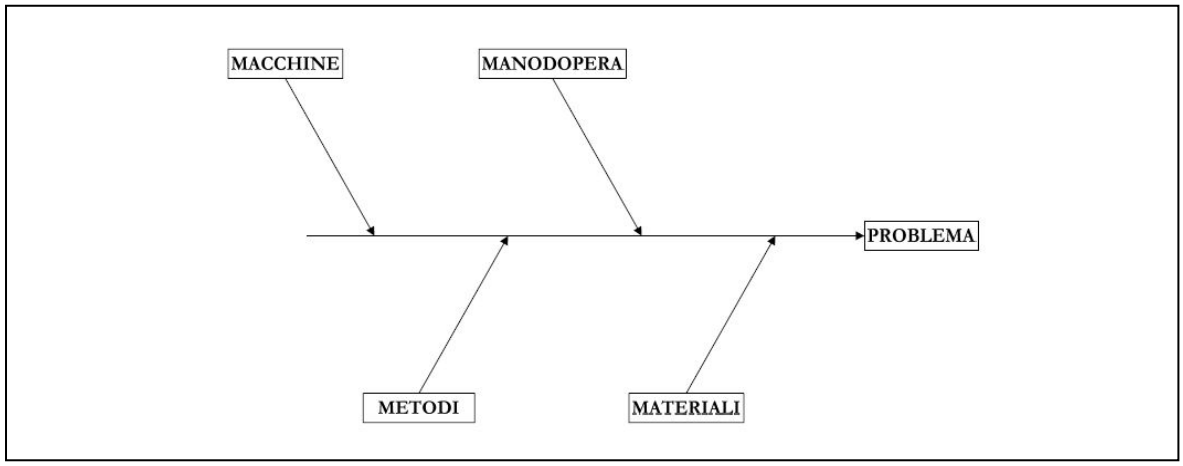
Esaminare le dipendenze tra processi comporta stabilirne anche una relazione di causa effetto.

Per questa ragione sono molto utili i diagrammi di Ishikawa, o diagrammi causa effetto o ancora a lisca di pesce, nati per

- studiare un problema determinandone le cause;
- studiare le motivazioni per cui un processo non funziona come dovrebbe;
- identificare le relazioni tra i dati;
- stabilire una relazione tra threat (albero di attacco).

Questo tipo di diagrammi vennero messi a punto in Giappone nel 1943 da Kaoru Ishikawa. Sostanzialmente si tratta di una rappresentazione grafica, che assume la forma di una lisca di pesce, di tutte le possibili cause relative ad un problema.

Figura 4 - Esempio di diagramma di Ishikawa



Le categorie principali usate per le cause più rilevanti sono (facendo riferimento alla lingua inglese):

- le 4 M che comprendono Method, Machine, Material, Manpower;
- le 4 P che comprendono Place, Procedure, People, Policy;
- le 4 S che comprendono Surrounding, Supplier, System, Skill.

Tali diagrammi possono contenere altre categorie in base al tipo di necessità.

4. Il processo di audit

Per proteggere l'interesse dell'organizzazione, sia essa pubblica che privata, ogni azienda e pubblica amministrazione può attivare un'attività di audit che fornisca una serie di servizi di assurance e consulenza che và dal contesto finanziario fino all'efficienza operativa e funzionale. Il processo di audit può essere attivato con servizi interni all'organizzazione ed esterni. Eventualmente le componenti interne ed esterne possono svolgere le proprie attività anche in modo congiunto.

L'esperienza maturata in Istat consente di dedurre che la funzione di audit deve essere estesa nell'ente per poter rispondere appieno alle esigenze delle attività di governo e deve essere organizzata in modo da avere garanzia di:

- una indipendenza organizzativa;
- un mandato formale;
- un accesso illimitato alle informazioni;
- risorse sufficienti;
- una leadership competente;
- un organico competente;
- il supporto degli Stakeholder;
- standard e metodologie di audit professionali.

Ovviamente l'organizzazione deve assicurare che la funzione di audit abbia i poteri necessari per riportare i problemi più significativi agli organi di governo. Al fine di preservare la propria indipendenza, la funzione di audit non deve mai assumere un ruolo di gestione.
Per superare le criticità del processo di audit può essere adottata una modalità di conduzione delle azioni che assicurino il coinvolgimento attivo dell'organizzazione, e che assicurino la trasparenza. E' questo il caso dell'Istat la cui esperienza verrà descritta nel dettaglio nei paragrafi successivi. Nel caso dell'Istituto, il processo è stato organizzato per fasi successive a livello di approfondimento diverso. Il coinvolgimento attivo dell'organizzazione è stato agevolato dalla nomina, da parte della Presidenza, della Commissione per il governo dell'Audit Informatico (CAI), a cui è stato affidato il compito di individuare le priorità dei temi da sottoporre ad audit, curare il coinvolgimento delle strutture sottoposte ad audit, effettuare la rilevazione validando gli output. Tale commissione è stata presieduta da due esperti nel settore ICT esterni all'Istituto.
In allegato (allegato 1) si riporta la descrizione del comitato in termini di ruoli, obiettivi, struttura e componenti.

4.1 Tipologia di audit

Il processo di audit fa riferimento a due tipologie di analisi diverse la prima volta alla valutazione della coerenza, della completezza e dell'equilibrio delle strutture organizzative esistenti (assessment) e l'altra orientata all'analisi degli strumenti in uso nell'organizzazione in ambito IT. Entrambi gli approcci possono trovare utilità nell'ottica di contribuire ad evidenziare le azioni possibili da intraprendere per aumentare il livello di governance e in generale le due tipologie possono essere sviluppate anche in modo integrato.

In realtà in letteratura non esiste una classificazione ufficiale dei tipi di audit, tuttavia sono individuati diversi tipi di audit in relazione alla specializzazione dell'ambito di riferimento. Si parla pertanto di audit finanziario, amministrativo, informatico proprio facendo riferimento alla specializzazione dell'ambito organizzativo oggetto d'analisi.

Nell'ambito dei sistemi informativi può essere individuata una classificazione di massima in relazione al campo di osservazione e alle modalità di conduzione del processo. Di seguito si riporta la classificazione di massima proposta da ISACA.

Audit around the computer

L'analisi prende in esame i dati di input e i dati di output del sistema informativo senza analizzare il processo che trasforma il dato di ingresso nel dato di uscita. La tecnica di audit prevede di confrontare l'output rilevato con un output generato da meccanismi diversi esterni all'organizzazione.

Audit through the computer

L'analisi prende in esame il processo di produzione degli output e le fasi intermedie del processo.

Audit by the computer

E' tipico dell'audit finanziario e prevede l'utilizzo di ulteriori strumenti di automazione per il controllo e l'analisi degli output.

4.2 Le fasi principali del processo

Il processo di audit si articola in diverse fasi strutturate. Di seguito si riportano le fasi principali tipiche del processo che sono sviluppate sia nel caso di analisi dell'assement dell'organizzazione sia nel caso di analisi degli strumenti e delle tecnologie in uso nell'organizzazione.

Audit charter

E' la fase di avvio dell'audit; in tale fase il top management dell'organizzazione individua gli obiettivi dell'audit attribuendo l'autorità a eseguire la funzione di analisi all'interno dell'organizzazione.

Approvazione dell' audit charter

In questa fase viene approvato da parte degli organi di governo dell'organizzazione l'audit charter ed assegnate le risorse idonee a svolgere le attività di analisi del processo di audit. L'incarico deve esplicitare gli obiettivi, i tempi, le priorità e le risorse.

Individuazione degli auditor e assegnazione di un audit staff

In questa fase vengono individuate gli esperti che si occuperanno di organizzare e condurre il processo. Gli esperti dovranno avere il giusto livello di competenza in relazione alla tipologia di organizzazione, alla sua finalità e obiettivo; devono inoltre avere competenza degli specifici ambiti rispetto ai quali è svolto l'audit. Agli esperti incaricati di svolgere l'audit può essere assegnato un audit staff interno all'organizzazione per agevolare le fasi di analisi interne all'organizzazione.

Audit Plan

E' la fase di pianificazione dell'audit. Deve includere la fase di *pianificazione strategica* in termini di strategia generale di analisi, e la *pianificazione tattica* intesa come definizione delle strutture organizzative da analizzare per l'ambito definito nel mandato. E' da tener presente che l'audit plan deve essere costruito analizzando la classificazione dei rischi dell'organizzazione e individuando come prioritarie le aree, inerenti il mandato, a più alto rischio per l'organizzazione. Devono quindi essere identificati i processi critici da analizzare e i livelli di controllo implementati dall'organizzazione per ridurre e gestire i rischi.

Determinare la compliance con i requisiti esterni

In questa fase è necessario identificare i requisiti in termini di leggi e normative esterne all'organizzazione che costituiscono vincolo per l'organizzazione.

Fase attiva di audit (verifiche e test)

E' la fase di effettuazione delle verifiche dei controlli adottati dall'organizzazione per raggiungere gli obiettivi prefissati nell'ambito di riferimento oggetto di audit. Sono propri di questa fase le verifiche attive in termini di eventuali test tecnici di verifica e la fase di raccolta di tutte le evidenze e i rilievi utili all'analisi.

Emissione del rapporto

E' la fase nella quale viene prodotto il rapporto di audit. Il rapporto deve raccoglie le evidenze, le carte di lavoro, i test e le verifiche effettuate. Il rapporto deve essere discusso con l'organizzazione che deve riconoscere come coerente e idonea l'analisi condotta e le evidenze individuate.

Valutazione e raccomandazioni

E' la fase in cui gli esperti riassumono le valutazioni e indicano le raccomandazioni e le eventuali azioni di recupero.

Follow up

E' la fase di chiusura del processo di audit che, in una ottica di miglioramento continuo, porta a ripetere ciclicamente il processo effettuando i controlli in merito alle attività di change management messe in atto dall'organizzazione per avviare e gestire le azioni di recupero e le raccomandazioni contenute nel rapporto.

5. L'impatto di un audit sull'organizzazione

L'introduzione di un qualsiasi meccanismo che abbia un forte impatto sui processi di un'organizzazione trova spesso l'opposizione da parte del personale, in quanto è percepito come un elemento che ne potrebbe minare l'equilibrio. In particolare un audit ICT viene essenzialmente considerato come un processo di controllo e verifica del settore informatico che ha come risultato la valutazione da parte dell'auditor dei processi e della struttura auditata. Nonostante le più moder-

ne e recenti interpretazioni, la percezione del giudizio associata all'audit e la conseguente chiusura da parte del personale, è un rischio che va attentamente considerato prima di predisporre l'audit stesso. Sempre più il settore ICT rappresenta un elemento chiave per il successo dell'azienda e dunque va evitata la possibilità che insorga un sentimento di sfiducia e di incertezza che possa avere ripercussioni negative sul business.

Vanno invece predisposte le condizioni per agevolare un confronto con gli auditor, al fine di rendere più semplice il loro lavoro, limitarne il costo e trarne i maggiori vantaggi.

Infatti, proprio in virtù delle molteplici esperienze maturate con la pratica professionale in svariati decenni (sopratutto negli Stati Uniti), questa funzione si è progressivamente trasformata da mero strumento di controllo interno, ad una vera e propria funzione aziendale che investe, in modo dinamico e trasversale, l'insieme dei sistemi e delle risorse dell'organizzazione che costituiscono la gestione globale dell'impresa. Essendo ormai giunta nella sua fase di piena maturità, l'auditing è oggi, per le aziende di medie e grandi dimensioni, una delle funzioni aziendali che più incisivamente possono contribuire, sotto determinate condizioni, ad un efficace controllo sull'integrità dell'impresa, alla salvaguardia del suo patrimonio, nonché alla razionalizzazione ed ottimizzazione delle attività di gestione.

L'obiettivo primario dell'audit è quello di assistere attivamente i membri dell'alta direzione nell'efficace adempimento delle loro funzioni aziendali, fornendo loro analisi, stime, raccomandazioni e commenti riguardanti le attività esaminate ed esercitando costantemente una funzione di monitoraggio del sistema.

Al perseguimento dell'obiettivo principale appena descritto concorrono anche altre finalità:

- favorire la velocità di circolazione delle informazioni. Il frapporsi di numerosi livelli intermedi nelle linea gerarchica ritarda molte volte l'informazione. Poiché la velocità di circolazione dell'informazione è un elemento determinante per poter prendere efficaci decisioni da parte del top management, l'agevolazione di tale processo porta evidenti benefici;
- promuovere uno spirito innovativo e di miglioramento volto ad evitare l'invecchiamento delle strutture: ciò avviene attuando una critica costruttiva nelle varie fasi che compongono un fenomeno aziendale, siano esse tanto di natura organizzativa che di natura operativa. In tal modo la direzione è costantemente stimolata a riesaminare i programmi formulati ed a verificare l'efficienza della propria struttura;
- agevolare l'attività svolta dal settore ICT per creare le premesse per un lavoro più proceduralizzato e standardizzato in cui la gestione di un qualsiasi incidente sia facilitata e i tempi di risoluzione siano ottimizzati;
- istruire il personale destinato ai quadri della società: il processo di audit ha anche come scopo quello di contribuire alla formazione delle risorse umane personale da destinare a particolari incarichi presso i vari settori aziendali.

Si tratta, come risulta evidente, di un complesso di obiettivi piuttosto articolati, ma complementari fra loro, che caratterizzano e valorizzano il ruolo dell'auditing nel contesto dell'intera struttura organizzativa aziendale, la cui attività è diretta al supporto del management e delle altre funzioni aziendali.

Per evitare i rischi evidenziati sopra e favorire invece una visione costruttiva della funzione di audit, le responsabilità dell'auditor devono essere chiaramente stabilite dall'alta direzione e attribuite con incarichi formali e vanno opportunamente rese note a tutte le parti interessate.

L'autorità aziendale competente deve preliminarmente autorizzare l'auditor ad avere libero accesso alle informazioni di qualunque genere che lo stesso ritenga utile per lo svolgimento del proprio incarico presenti nell'azienda.

5.1 Le responsabilità dell'auditor

Le responsabilità di un auditor sono quelle di informare e consigliare l'alta direzione; coordinare le proprie attività con le altre dell'azienda, in modo da conseguire al meglio sia gli obiettivi nell'ambito del suo incarico. E' opportuno sottolineare che, nell'adempiere a questa funzione, l' auditor non ha una diretta autorità e responsabilità sulle attività che sottopone a verifica. Pertanto la funzione di controllo che espleta non solleva in alcun modo dalle loro responsabilità le altre persone che operano nell'impresa.

5.2 L'indipendenza dell'auditor

L'indipendenza, che è un elemento assolutamente cruciale nella funzione di auditing, può essere effettivamente ottenuta solo in presenza di due situazioni concomitanti, l'una di carattere oggettivo e l'altra di natura soggettiva.

Gli elementi oggettivi a fondamento dell'indipendenza consistono:

- nell'assegnare l'incarico di audit ad una persona esterna all'azienda;
- nel sostegno concreto da parte dell'alta direzione all'auditor.

Tale sostegno si esplica nel fatto che l'audit manager riferisca direttamente all'Amministratore Delegato o al Direttore Generale, la cui autorità gli assicuri un vasto campo di attività di revisione, una considerazione adeguata della funzione ed un'azione efficace secondo i risultati della revisione e delle sue raccomandazioni.

L'indipendenza è senz'altro favorita da numerosi altri fattori concomitanti, quali il grado di professionalità e le specifiche attitudini degli addetti a questa funzione.

L'elemento soggettivo che determina l'indipendenza è senz'altro l'obiettività. L'auditor pertanto non dovrebbe sviluppare ed instaurare procedure, predisporre registrazioni o impegnarsi in qualsiasi altra attività all'interno dell'azienda che possa essere successivamente oggetto di un suo esame e valutazione. E evidente che un'eventuale partecipazione a queste attività può risultare controproducente per la sua indipendenza ed in ogni caso può prestare il fianco a critiche da parte di altri soggetti sottoposti a controllo. Un secondo aspetto dell'obiettività, altrettanto importante, è direttamente riconducibile alla sfera della personalità dell'individuo e consiste nell'atteggiamento psicologico in cui si pone l'auditor nell'esecuzione del suo lavoro. Un approccio professionale eccessivamente condiscendente, costantemente orientato a sottovalutare i problemi, a sminuire la portata degli errori rinvenuti ed a compiacere le aspettative altrui, privo di autentico spirito critico e non orientato al "problem solving", svuota di reale efficacia l'attività di controllo esercitata.

Per contro anche l'atteggiamento eccessivamente rigido, che trae la sua soddisfazione professionale dall'enfatizzare le piccole mancanze altrui e che è sempre alla ricerca di reprimende da impartire per affermare la propria personalità, non è senz'altro quello ottimale che risulti utile ad analizzare con obiettività i problemi ed a fornire ai vertici aziendali dei suggerimenti equilibrati. L'obiettività di natura soggettiva si ritrova normalmente in una personalità forte ma equilibrata, capace di lucidità di analisi e di indipendenza di giudizio, dotata di sufficiente rigore morale ed intellettuale, che sia costantemente orientata ad un atteggiamento costruttivo nei confronti dell'azienda e degli altri. E' opportuno pertanto tenere conto di queste importanti caratteristiche intrinseche in sede di selezione del personale da destinare a questa funzione per poter ottenere delle prestazioni professionali di qualità adeguata.

6. I Framework di riferimento e l'approccio metodologico di COBIT per il governo dell'IT

Le organizzazioni complesse richiedono un approccio strutturato per gestire le attività tese alla governante dell'IT. In particolare l'utilizzo di standard e framework riconosciuti assicurerà che ci sia allineamento tra gli obiettivi per l'IT, che vengano messe in atto buone pratiche di controllo manageriale e un efficace monitoraggio delle performance. Tali elementi contribuiscono a rendere l'organizzazione competitiva gestendo i rischi e contenendo la spesa.

In particolare l'uso di tali strumenti consentirà di rispondere ai seguenti quesiti principali:

Allineamento strategico

Quanto bene sono allineati gli obiettivi dell'impresa e dell'IT? Cosa succede se non lo sono?
Cosa accade se la strategia di business è inesistente o insufficiente?
Il business sa sempre cosa è meglio?
C'è spazio per l'audit?

Aggiunta di valore

Gli utenti finali sono soddisfatti della qualità dei servizi IT?

Come si determina e valuta il valore trasferito dall'IT ai clienti, sia interni che esterni?
Perché i progetti spesso falliscono nel produrre ciò che avevano promesso?

Misura delle performance

*Qu*ali sono gli ostacoli per determinare efficacemente e con precisione il ROI di ogni principale progetto o investimento IT?
Come si può misurare le performance e collegarle efficacemente alla strategia IT?
Come può un'organizzazione valutare efficacemente il bilanciamento tra risorse proprie e servizi/risorse ottenuti dall'esterno, tra cui l'outsourcing?

Risk management

Come può un'organizzazione sviluppare una definizione dei rischi che efficacemente includa quelli IT?
I rischi IT sono efficacemente comunicati e compresi dal senior management?
La direzione è regolarmente informata sui rischi cui l'organizzazione è esposta?
Quale è la persona più indicata a fare ciò?

Gli standard, le linee guida e i framework di riferimento per l'IT governance tentano di dare riferimenti metodologici e best practices per fornire risposte in termini tecnico-organizzativi a tali quesiti. Nel paragrafo che segue si fornisce una sintetica descrizione dei principali framework di riferimento in uso presso organizzazioni pubbliche e private.

6.1 Standard, linee guida e framework di riferimento per l'IT governance

L'IT governance e le attività di audit vengono svolte in contesti giuridici e culturali diversi all'interno di organizzazioni che variano per finalità, dimensioni, complessità e struttura organizzativa. Tipicamente sono svolte da esperti interni o/e esterni all'organizzazione pertanto è opportuno operare in conformità con gli standard, le linee guida e i framework di riferimento del settore. Effettivamente le metodologie proposte possono essere utilizzate dai manager che organizzano piani di attività finalizzati all'IT governance ma anche da esperti a cui vengano affidate attività di audit dei sistemi informativi. Il manager dell'IT e l'auditor sono chiamati infatti ad operare sugli stessi ambiti seguendo solo due punti di vista differenti, *(i)* organizzare i sistemi informativi in ottica di governance, *(ii)* valutare l'adeguatezza dei sistemi informativi adottati dall'organizzazione in ottica di governance. Entrambe le figure, il manager e l'auditor, operano stabilendo quanto vale un sistema informativo e che ritorno può fornire agli investimenti sostenuti dall'organizzazione.

Scopo degli *standard* è quello di delineare i principi base che guidano le attività IT in ottica di governance. Forniscono un quadro di riferimento per lo sviluppo e l'effettuazione di una vasta gamma di interventi di miglioramento a valore aggiunto e definiscono nel contempo i parametri per la valutazione delle prestazioni, promuovendo il miglioramento dei processi organizzativi e degli ambienti di gestione operativa. Gli standard fissano requisiti vincolanti basati su principi, pertanto l'osservanza potrà essere soggetta a giudizi professionali che ne giustifichino eventualmente l'inosservanza.

Le *linee guida* sono essenzialmente standard di prestazione che descrivono la natura dell'attività e forniscono criteri qualitativi per valutarne l'effettuazione. Nell'impostare un programma di IT governance e nell'eseguire attività di audit sull'IT possono essere prese in considerazione in relazione al contesto organizzativo in cui si opera. Ovviamente l'utilizzo di linee guida è fortemente consigliato ma non ha carattere di obbligatorietà. Un auditor può eventualmente scegliere anche solo in relazione a specifici ambiti tecnici di riferimento.

I *framework* di riferimento per la governance dell'IT forniscono un quadro di regole che rispondono a determinati requisiti sulla base di una raccolta organizzata di raccomandazioni derivanti dalla selezione delle pratiche migliori per l'erogazione dei servizi. Forniscono uno schema sistematico e strutturato sulle modalità per organizzare le attività in ambito IT e le attività di audit per l'IT. Sono in generale definiti, aggiornati e promossi da organizzazioni di professionisti che operano al livello mondiale sull'IT organizzati in steering committee internazionali. La formulazione dei framework parte dall'analisi di best practices diffuse nel settore di riferimento e

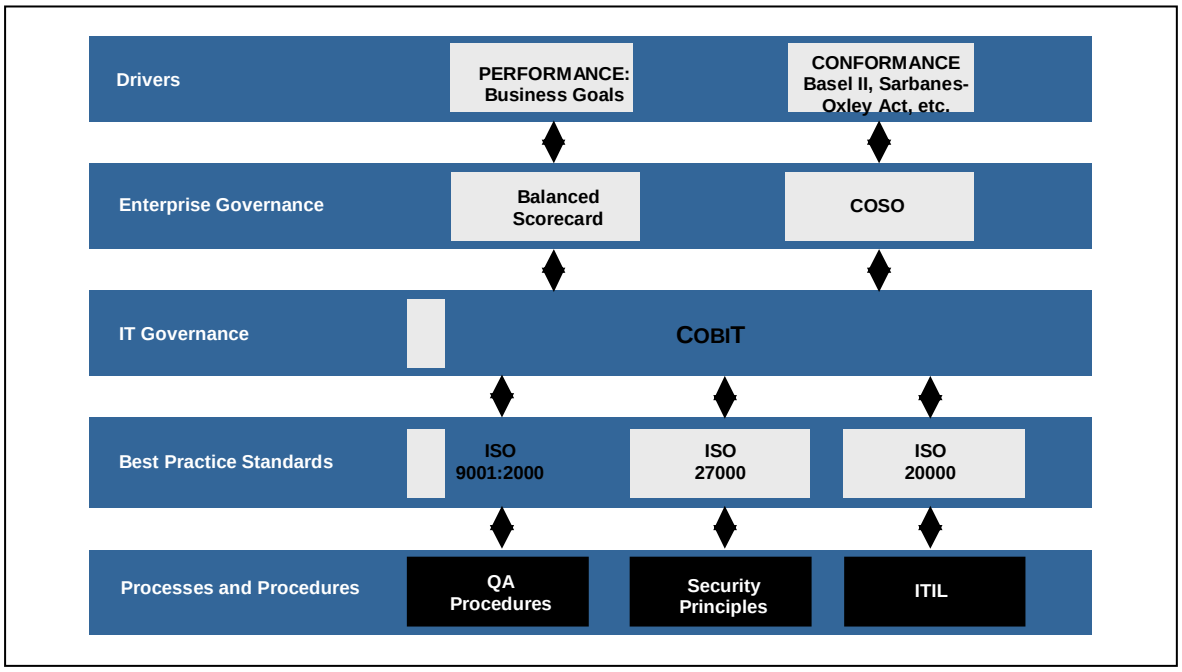
formulano, provvedendo a periodica revisione, linee guida professionali che consentono di fornire schemi ai professionisti dell'IT.[5]

6.2 Alcuni framework di riferimento

Le organizzazioni considerano e utilizzano una varietà di modelli IT, standard e best practice spesso combinati ed integrati tra loro nei vari ambiti di riferimento. La scelta è legata principalmente alle finalità e alla tipologia di organizzazione. E' da considerare che l'utilizzo dei framework comuni facilita la comunicazione tra settori diversi di una stessa organizzazione e tra organizzazioni diverse, contribuendo a definire un gergo comune e uniforme individuando i termini critici delle organizzazioni. Il coordinamento tra i vari gruppi di progetto e tra le diverse organizzazioni gioca un ruolo chiave per un efficace utilizzo dei framework. Il linguaggio comune, inoltre, aiuta a costruire fiducia e confidenza. Nella figura 5 vengono riportati i framework di più diffuso uso ripartiti per ambito di utilizzo e il loro rapporto di interdipendenza.

E' da mettere in evidenza il framework COBIT progettato esplicitamente per la governance dell'IT e costituisce un insieme consolidato di processi e controlli IT utilizzati anche dal punto di vista dell'*information risk management*. COBIT è internazionalmente riconosciuto come una *global best practice*; ha una ampia versatilità unita ad una semplicità di utilizzo pertanto la sua implementazione è largamente diffusa in organizzazioni complesse; ruotano attorno al COBIT processi aggiuntivi e iniziative di miglioramento continuo che contribuiscono a favorire COBIT rispetto ad altri framework anche nelle organizzazioni pubbliche.

Figura 5 - Framework e loro collocazione negli ambiti di riferimento



Il paragrafo 6.2 fornirà una descrizione dei principi fondamentali e degli strumenti proposti dal framework COBIT. E' inoltre da segnalare ITIL V3 nell'ambito generale del "Process and Proce-

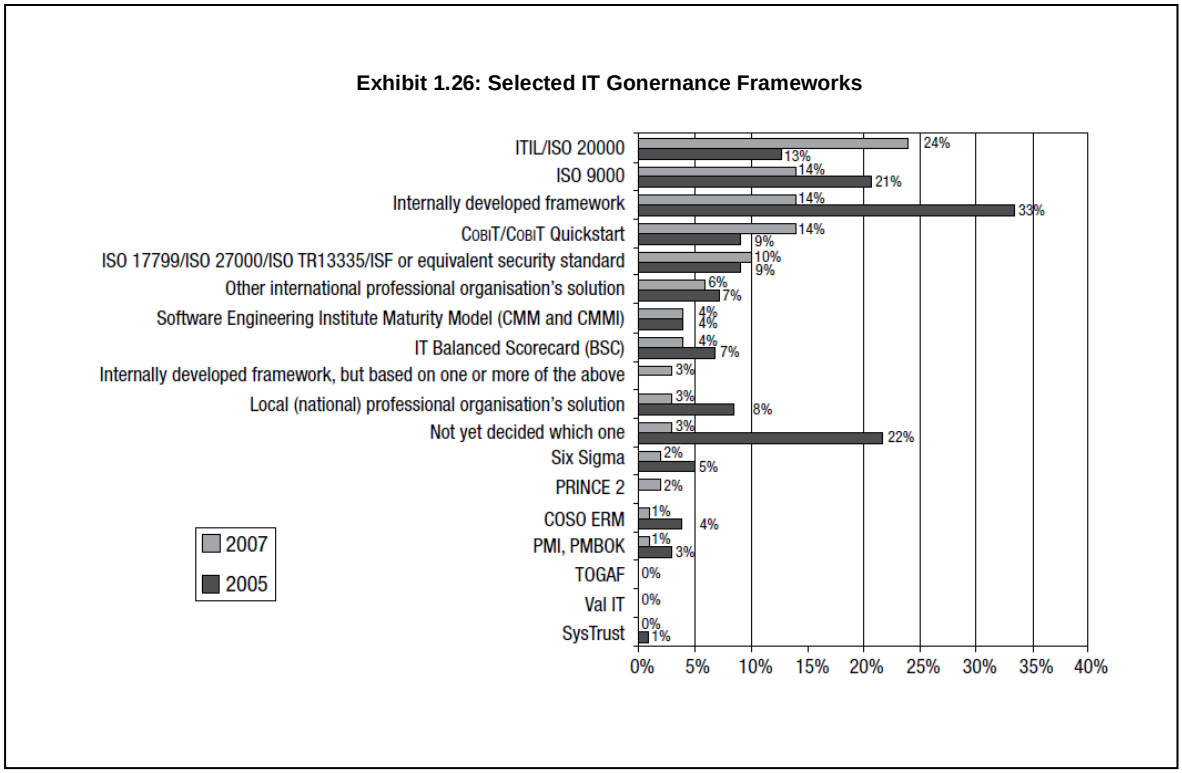
[5] Organizzazioni di riferimento
ISACA - Information Systems Audit & Control Association
CISA - Control Asscіation and Information System Audit
IIA - The Institute of Internal Auditors
ISACF - Information Systems Audit & Control Foundation.
ITIG - IT Governance Institute
AICPA - American Institute of Certified Public Accountants
AIEA - capitolo di Milano di ISACA

dures" come framework di riferimento nel *delivery and support* e nell'organizzazione dei servizi e nei rapporti con l'utenza. I due framework citati, COBIT e ITIL, possono essere visti anche in chiave di supporto alla gestione dei rischi rispondendo ai quesiti che seguono:

- Come può un'organizzazione sviluppare una definizione dei rischi che efficacemente includa quelli IT?
- I rischi IT sono efficacemente comunicati e compresi dal senior management?
- I livelli più operativi sono regolarmente informati sui rischi cui l'organizzazione è esposta?

La figura seguente (figura 6) sintetizza il livello di utilizzo dei diversi framework in organizzazioni a livello mondiale; la rilevazione, condotta dall'IT Governance Institute, prende come riferimento gli anni 2005 e 2007 evidenziando l'incremento nell'utilizzo in termini percentuali dei diversi framework.

Figura 6 - Framework di IT governante e percentuale di utilizzo



Source: IT Governance Institute, *IT Governance Global Status Report – 2008*, ISACA, USA, 2008, figure 67 (*www.isaca.org*)

6.3 Il framework COBIT per l'IT governance

La metodologia COBIT (*Control Objectives for Information and related Technology*) è un insieme di *best practices* (*framework*) per il governo dell'Information Technology creato dall'*Information Systems Audit and Control Association* (ISACA) e dall'*IT governance Institute* (ITGI) nel 1996. La missione del COBIT è quella di pubblicare promuovere e autorizzare le prassi, generalmente accettate, rendendo pubblico un set di obiettivi di controllo accettati a livello internazionale per il controllo e governo l'IT.

Il framework è stato creato per fornire un modello dettagliato e specifico per l'IT Governance ed è oggi costantemente aggiornato a partire dagli ISACA Control Objectives pubblicati nel 1992. Include standard e regolamenti provenienti da ISO, EDIFACT, da *Codes of Conduct* pubblicato dalla Comunità Europea, dagli Standard professionali dell'Auditing: quali COSO, IFAC, IIA, ISACA, AICPA standards, ecc.

In particolare la metodologia è finalizzata a dare un aiuto alle organizzazioni anche nel gestire i rischi dell'IT, assicurare che i processi IT siano coerenti con gli obiettivi di Business dell'azienda,

avviare l'organizzazione e i processi verso una sempre più rigorosa aderenza alle migliori pratiche internazionali e in ultimo garantire una valutazione dei costi in funzione degli obiettivi.

La metodologia COBIT fornisce una serie di misure, indicatori, processi e *best practices*, che consentono ai manager e ai responsabili dei processi aziendali di governare l'IT sfruttando appieno le potenzialità dell'*Information Technology*. COBIT costituisce un frame work di riferimento, modello per il governo dell'IT. In particolare il frame work supporta l'IT governance assicurando che l'IT sia allineata al business, che l'IT abiliti il business aziendali rendendo massimi i benefici, che le risorse IT siano usate in maniera responsabile e ottimizzata.

Al fine di fornire l'informazione di cui l'organizzazione necessita per conseguire i suoi obiettivi, le risorse IT devono essere gestite da un set di processi naturalmente raggruppati.

COBIT è diventato lo standard de facto per l'IT Governance nel mondo ed ha come principali valori di essere:

- "Business-focused" → si basa sui requisiti del Business;
- "Process-oriented" → orientato ai processi;
- "Controls-based" → identifica le risorse principali e gli obiettivi di controllo manageriale;
- "Measurement-driven" → è basato su parametri misurabili.

L'implementazione di COBIT permette la mutua interazione ed interoperabilità, all'interno di un sistema di Governance IT, con i principali standard e best practices, quali ISO 27001, ISO 9000, ITIL (ISO 20000).

La metodologia COBIT indica best practices da tenere presente nel disegno di una struttura organizzativa del settore IT . Il frame work è costituito da 34 obiettivi di controllo di alto livello, e una loro classificazione composta da 4 domini. I 34 obiettivi di controllo sono normalmente visti come processi di un'azienda, e ad ogni processo è associata una serie di attività e compiti. Attraverso i 34 Obiettivi di Controllo di alto livello, e la loro classificazione composta da 4 Domini l'adozione di COBIT porta come risultato:

- che i servizi saranno allineati con gli obiettivi del cliente;
- che i servizi saranno allineati con gli standard di qualità e di sicurezza;
- che i servizi supporteranno l'organizzazione e massimizzeranno i benefici;
- che le risorse saranno usate responsabilmente;
- che i rischi saranno gestiti opportunamente.

I domini del COBIT consistono di:

- **Pianificazione e Organizzazione:**
  questo dominio copre la strategia e la tattica, riguarda come l'IT può meglio identificare il modo con cui contribuire al raggiungimento degli obiettivi dell'organizzazione, realizzare una visione strategica con la pianificazione da parte del management, che deve comunicare e gestire.
- **Acquisizione e Realizzazione:**
  per poter realizzare una strategia è necessario individuare delle soluzioni, da Sviluppare o Acquisire, gestione delle modifiche e loro manutenzione.
- **Erogazione e Assistenza:**
  erogazione servizi richiesti, operazioni tradizionali "Sistemistiche", alla sicurezza e continuità del servizio, elaborazione di dati, e controlli delle applicazioni.
- **Monitoraggio e Valutazione:**
  tutti i processi devono essere valutati nel tempo, sotto l'aspetto qualità e conformità ai requisiti di controllo, il management deve eseguire la supervisione dei processi di controllo, compresa la valutazione indipendente fornita dall'Audit sia interno che esterno.

6.4 I criteri di controllo e le risorse

L'informazione deve rispondere a criteri di controllo specifici. Di seguito si indicano i controlli imprescindibili che devono essere applicati in ottica di governance del sistema informativo:

- *Efficacia*: Le informazioni debbono essere rilevanti e pertinenti ai processi aziendali.
- *Efficienza*: Riguarda l'uso ottimale delle risorse, (Produttività ed Economicità).
- *Riservatezza*: La protezione delle informazioni da accessi non autorizzati.
- *Integrità:* Riguarda la Accuratezza e Completezza delle informazioni.
- *Disponibilità*: L'informazione deve essere disponibile quando richiesto dai processi aziendali.
- *Conformità*: Rispetto di leggi e regolamenti, accordi contrattuali, cui è soggetta l'azienda.
- *Affidabilità*: Riguarda la fornitura di appropriate informazioni alla Direzione, per far fronte alle proprie responsabilità e a obblighi di bilancio.

Con il termine *risorse* devono essere inteso il complesso sistema costituito dalle applicazioni del sistema informativo unitamente alle informazioni, dall'infrastruttura tecnologica di riferimento e dalle risorse umane. In particolare:

- le applicazioni rappresentano i sistemi automatizzati e le procedure manuali che processano l'informazione;
- l'informazione rappresenta il dato in input processato in tutte le sue forme, e come output dei sistemi informativi, in qualsiasi forma sia utilizzato per il business aziendale;
- l'infrastruttura: è la tecnologia e le caratteristiche dell'installazione (hardware, sistemi operativi, database management system, networking);
- le risorse umane: sono le persone richieste per pianificare, organizzare, acquisire, implementare, consegnare, assistere, monitorare e valutare i sistemi informativi. Posso essere interne, in outsourcing o reclutate a contratto all'occorrenza.

6.5 La determinazione dell'ambito di riferimento e la descrizione dei processi IT

Per determinare l'ambito abbiamo bisogno di investigare, analizzare e definire:

- i processi di business;
- le piattaforme e i sistemi informativi che supportano i processi di business e le interconnessioni con altre piattaforme o sistemi;
- la definizione dei ruoli e delle responsabilità dei processi IT includendo anche ciò che è in outsourcing;
- i rischi di business associati e le scelte strategiche.

Determinare l'ambito vuol dire selezionare quali parti della metodologia COBIT sono applicabili. L'ambito può essere determinato identificando i processi IT oppure partendo dai processi di business e successivamente individuando i processi IT ad essi collegati.

I processi IT devono essere descritti evidenziando per ciascuno di essi le risorse IT associate in termini di risorse umane, applicazioni, tecnologia, infrastruttura, dati trattati.

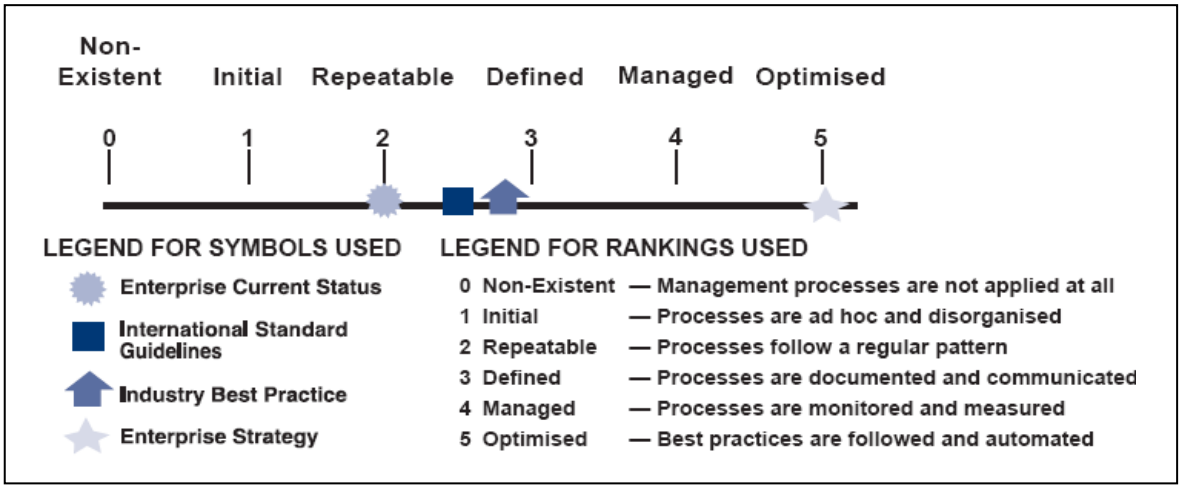
7. Strumenti di analisi e progettazione organizzativa

7.1 Il modello di maturità

Il modello di Maturità dei processi del COBIT è uno strumento dell'IT Governance che consente di misurare il livello di evoluzione dei processi dell'IT dell'organizzazione.

Il modello di maturità consente alle organizzazioni di rilevare il proprio grado di maturità in una scala da "Non esistente" a "Ottimizzato" (5). Nella successiva figura x è rappresentata la scala a cinque valori proposta dall'IT *Governance Institute.*

Figura 7 - La scala di maturità



Fonte: Board Briefing on IT Governance, IT Governance Institute

Di seguito si riporta il significato dei sei livelli di maturità:

1. inesistente – nessun processo riconoscibile – questione non nota;
2. iniziale – questione nota, nessun approccio riconoscibile – approccio caso per caso;
3. ripetibile – attività svolte di norma allo stesso modo anche da persone diverse;
4. definito – processo documentato e comunicato;
5. gestito – elementi di misurazione e contromisure in caso di scostamenti o inefficacia;
6. ottimizzato – applicazione delle migliori pratiche di interventi di ottimizzazione.

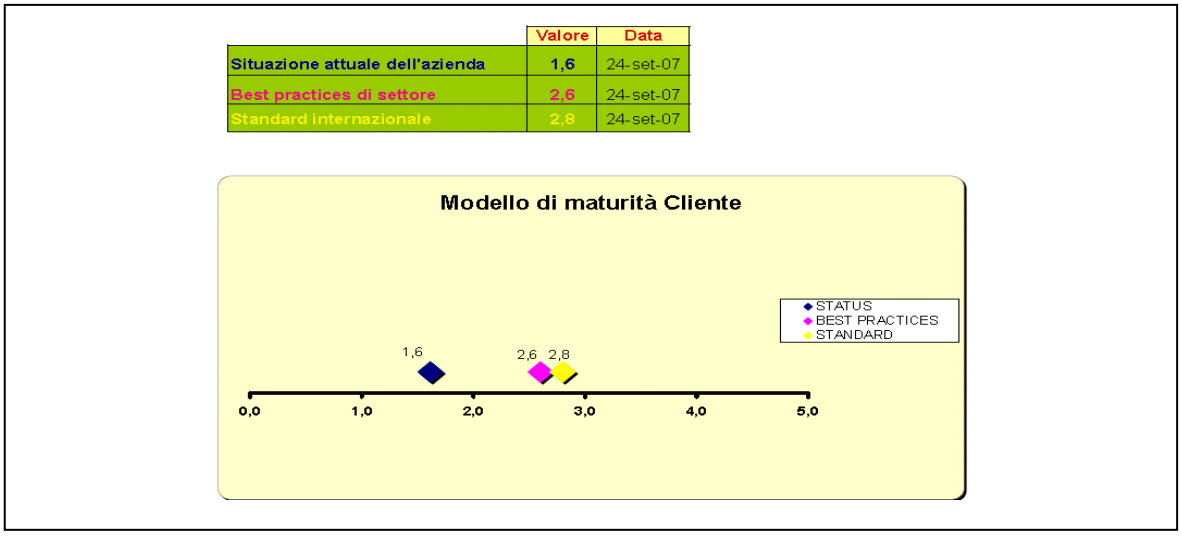
L'utilizzo del Maturity Model può essere importante per supportare il Management nel governo dell'IT e dei suoi servizi soprattutto quando lo schema e i sui valori vengono messi in relazione alle medie dei livelli raggiunti su base nazionale o mondiale per situazioni analoghe. Il modello di maturità consente alle organizzazioni di rilevare il proprio grado di maturità generale o su singoli servizi.

Tramite questi punteggi (livelli) sviluppati per ognuno dei 34 obiettivi di controllo del COBIT, è possibile misurare:

– lo status corrente dell'organizzazione – dove si trova "oggi" l'organizzazione;
– lo status delle organizzazioni dello stesso settore – il paragone;
– lo status corrente rispetto agli standard internazionali;
– la strategia dell'organizzazione per il miglioramento – dove l'organizzazione vorrebbe posizionarsi.

La scala sintetica del Maturity Model e la tabella di esempio riportate in figura 8 rendono esplicativa la modalità di possibile utilizzo e di come può essere confrontato lo stato rilevato ad una certa data con gli standard internazionali e le best practices di settore.

Figura 8 - Esempio di scala sintetica del Maturità Model e di confronto con best practices e standard



Applicando il Maturity Model è possibile rilevare una visione d'insieme del posizionamento del Sistema Informativo dell'azienda rispetto ai 34 processi di COBIT che deve essere confrontata con la situazione internazionale (europea e mondiale).

Lo scopo è quello di evidenziare i gap per ogni processo e conseguentemente individuare i pending issues di ogni processo che consentiranno la realizzazione di futuri piani generali di miglioramento.

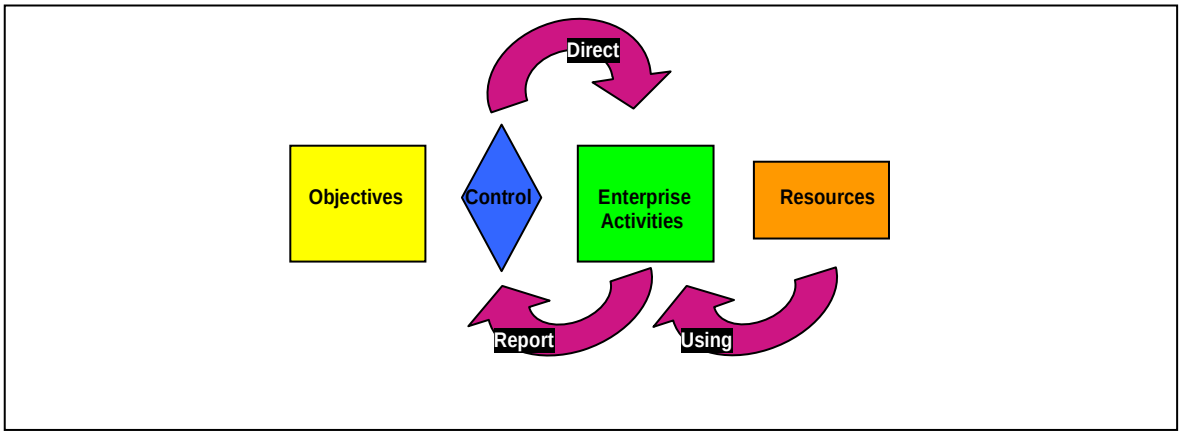
Per ogni singolo processo oggetto di miglioramento verrà:

- descritta la situazione attuale (AS-IS);
- indicato l'obiettivo a tendere (TO-BE);
- esposte le macro attività da svolgere (TO-DO);
- indicati i benefici che se ne otterranno (VALUE DRIVERS);
- analizzati i rischi in caso di non esecuzione (RISK DRIVERS).

7.2 Implementare la metodologia COBIT in organizzazione complesse

La figura seguente (Figura 9) indica il flusso delle attività previste dalla metodologia. Il flusso prevede che le attività debbano essere dirette sulla base degli obiettivi di controllo evidenziati dalla metodologia e dal framework. Nel contempo le attività devono poter essere monitorate in termini di effettivi risultati ottenuti in relazione agli obiettivi di controllo applicati. Tale procedimento è ciclico e si avvale delle risorse messe a disposizione dal sistema in termine di applicazioni, informazioni, architetture tecnologiche di supporto e risorse umane.

Figura 9 - Il flusso delle fasi della metodologia COBIT



La metodologia si articola in tre fasi principali distinte:

- applicazione del COBIT Maturity Model estendendolo dai processi ai controlli;
- definizione dei fattori critici di successo che potenziano i controlli e li rendono efficaci;
- valutazione dei controlli al fine di determinare le conseguenze e la probabilità di un loro eventuale fallimento.

I controlli identificati sono valutati mediante una scala a cinque valori come nella figura seguente.

Figura 10 - La scala dei valori da attribuire ai controlli nella metodologia COBIT

Code	Name	Control Eff.	Description
0	Non-Existent	Weak	Control not available or ineffective
1	Initial		Control ad hoc with minimal effectiveness
2	Repeatable	Moderate	Control follows a regular pattern
3	Defined		Control are documented and communicated
4	Managed	Strong	Processes are monitored and measured
5	Optimized		Best practices are followed and automated

Fonte: ISACA- Cobit 4.1

La tabella seguente riporta fedelmente la descrizione dettagliata afferibile a diversi livelli di maturità diffusa da ISACA.

MATURITA LIVELLO	Descrizione
0	Non-Esistente • Il risk assessment non viene effettuato per i processi e le decisioni di business. L'organizzazione non considera gli impatti sul business associati alle vulnerabilità di sicurezza e alle incertezze dei progetti in sviluppo. Il risk management non è stato ritenuto fattore rilevante nell'acquisto di soluzioni IT e nella fornitura dei servizi. • L'organizzazione non riconosce la necessità dell'IT security. Le responsabilità e le capacità finanziarie per garantire la sicurezza non sono assegnate. Non sono implementate misure che supportano la gestione della sicurezza IT. Non esiste alcuna linea di riporto per la sicurezza IT e nessuna procedura di risposta contro le violazioni della sicurezza. C'è una completa mancanza di processi amministrativi riconoscibili per la gestione della sicurezza. • Non c'è consapevolezza dei rischi, dovuti a vulnerabilità o minacce alle attività IT o dell'impatto sul business dovuto alla perdita dei servizi IT. La continuità del servizio non è ritenuta meritevole di attenzione da parte del management.
1	Iniziale/Ad-Hoc • L'organizzazione considera il rischio sull'IT in modo estemporaneo, senza seguire processi o politiche definiti. Sono effettuate valutazioni informali del rischio di progetto, specifiche per ognuno di essi. • L'organizzazione riconosce la necessità della sicurezza IT, ma la consapevolezza dipende dall'individuo. La sicurezza IT è valutata su base reattiva e non misurata. Le violazioni della sicurezza presuppongono uno stile "dito puntato" se scoperte, poiché le responsabilità non sono chiare. Le reazioni alle violazioni della sicurezza IT sono imprevedibili. • Le responsabilità per la continuità del servizio sono informali, limitata autorità. Il management sta diventando consapevole dei rischi correlati e della necessità di garantire la continuità del servizio.

2	Ripetibile ma intuitivo • C'è un'emergente presa di coscienza del fatto che I rischi IT sono importanti e del bisogno di considerarli. Esiste un qualche approccio al risk assessment, ma il processo è ancora immature e in sviluppo. • Responsabilità e risorse per la sicurezza IT sono assegnate a un coordinatore per la sicurezza IT, senza tuttavia autorità manageriale. La consapevolezza della sicurezza è frammentata e limitata. L'informazione sulla sicurezza IT è prodotta, ma non analizzata. La sicurezza tende a rispondere in modo reattivo agli incidenti, adottando soluzioni e servizi di terze parti, senza considerare i bisogni specifici dell'organizzazione. Le politiche di sicurezza sono in via di sviluppo, ma sono ancora utilizzati competenze e strumenti inadeguati. Il reporting della sicurezza IT sè incomplete, fuorviante o non pertinente. • E' assegnata la responsabilità per la continuità del servizio. Gli approcci sono tuttavia frammentari. Il reporting sulla disponibilità dei sistemi è incomplete e non tiene in conto dell'impatto sul business.
3	Processo definito • Una politica globale di risk management stabilisce quando e in che modo effettuare i risk assessment. Il risk assessment segue un processo definito documentato e disponibile a tutto lo staff tramite il training.. • Esiste la consapevolezza della sicurezza ed è promossa dal management. Le riunioni per la consapevolezza della sicurezza sono state standardizzate e formalizzate. Le procedure per la sicurezza IT sono definite e si inseriscono in una struttura per tutte le politiche e procedure di sicurezza. Le responsabilità per la sicurezza IT sono assegnate, ma non riaffermate costantemente. Esiste un piano per la sicurezza IT, che conduce all'analisi del rischio e alle soluzioni. Il reporting sulla sicurezza IT è focalizzato all'IT, piuttosto che al business. Sono effettuati dei test di intrusione ad hoc. • Il management comunica costantemente la necessità di assicurare la continuità del servizio. Componenti ad alta disponibilità e sistemi ridondanti sono applicati pezzo per pezzo, un po' alla volta. E' rigorosamente mantenuto un inventario dei sistemi e dei componenti critici.
4	Gestito e misurabile • La valutazione del rischio è una procedura standard e le eccezioni nel seguirla sono evidenziate dal management IT. E' probabile che l'IT risk management è una funzione definita del management di alto livello di responsabilità. Il senior management e l'IT management hanno determinato i livelli di rischio che l'organizzazione può tollerare e dispongono di misure standard per i rapporti rischi/ritorni. • Le responsabilità per la sicurezza IT sono chiaramente assegnate, gestite e fatte rispettare. L'analisi sulla sicurezza IT e dell'impatto sono effettuate costantemente. Le politiche di sicurezza e le prassi sono completate da specifiche linee guida. Riunioni sulla consapevolezza della sicurezza sono divenute obbligatorie. L'identificazione degli utenti, autenticazione e autorizzazione sono standardizzati. E' stabilita la certificazione sulla sicurezza per il personale addetto. Il test di intrusione è un processo standard e formalizzato che porta a miglioramenti. L'analisi costi/benefici, a supporto dell'implementazione delle misure di sicurezza è sempre più utilizzata. I processi di IT security sono coordinate con l'intera funzione di sicurezza dell'organizzazione. Il reporting sulla sicurezza IT è legato agli obiettivi di business. • Responsabilità e standard per la continuità del servizio sono fatti rispettare. Le pratiche per la ridondanza dei sistemi, incluso l'impiego di componenti ad alta disponibilità, sono costantemente impiegate.
5	Ottimizzato • Il risk assessment si è sviluppato al livello in cui è costantemente applicato un processo strutturato, esteso a tutta l'organizzazione, sorvegliato costantemente e ben gestito. • La sicurezza IT è una responsabilità congiunta del business e dell'IT management ed è integrata con gli obiettivi globali di sicurezza del business dell'intera organizzazione. I requisiti per la sicurezza IT sono definiti con chiarezza, ottimizzati e compresi in un piano verificato di sicurezza. Le funzioni di sicurezza sono integrate con le applicazioni durante la fase di progettazione, e gli utenti sono costantemente responsabili per la gestione della sicurezza. Il reporting sulla sicurezza IT fornisce un'informazione anticipata sui rischi di cambiamento ed emergenti, utilizzando approcci attivi al monitoraggio per i sistemi critici. Gli incidenti sono prontamente affrontati con procedure di notifica formalizzate supportate da strumenti automatizzati. Verifiche periodiche sulla sicurezza valutano l'efficacia dell'implementazione del piano di sicurezza. L'informazione su nuove minacce e vulnerabilità è raccolta sistematicamente ed analizzata, e gli opportuni controlli per ridurre l'impatto sono prontamente comunicati e implementati. L'Intrusion test, radice principale per l'analisi degli incidenti di sicurezza e l'identificazione proattiva del rischio è la base per il miglioramento continuo. I processi di sicurezza e le tecnologie sono integrate a livello dell'intera organizzazione. • I piani per la continuità del servizio e i business continuity plan sono integrati, allineati e mantenuti routinariamente. L'acquisizione di beni per le necessità della continuità del servizio è garantita dai maggiori fornitori.

La definizione dei fattori critici di successo si ottiene analizzando due aspetti:

- revisione e analisi dei controlli attualmente presenti al fine di determinare le eventuali debolezze;
- determinazione dei fattori di miglioramento che consentono di ottenere l'ottimizzazione del rischio.

La valutazione dei controlli si ottiene mediante:

- valutazione dell'efficacia dei controlli utilizzando il COBIT Maturity Model;
- valutazione dell'efficacia dei controlli assumendo che i Fattori Critici di Successo siano stati individuati e ottenuti;
- rivalutazione dell'impatto (rischio) e probabilità.

Di seguito si forniscono alcuni esempi di valutazione dell'efficacia di un controllo:

- incapacità di effettuare il recovery di un sistema in un tempo ragionevole che non crei perdite economiche all'organizzazione;
- ritardi dovuti all'inadeguatezza e inaffidabilità del Piano Tecnico di Disaster Recovery;
- impiegati che mantengono i diritti di accesso al sistema dopo aver lasciato l'azienda;
- il progetto eccede i limiti del budget in termini di costo e tempo di completamento.

7.3 Le matrici RACI

Un contributo all'analisi delle organizzazioni è costituito dalle **matrici RACI** (note anche come *Responsibility Assignment Matrix* - RAM, *Linear Responsibility Chart* - LRC) descrivono i diversi ruoli svolti delle strutture organizzative nello svolgimento dei processi e possono essere utilizzate sia per analizzare una struttura esistente sia per indirizzare la progettazione di strutture nuove.

La matrice ha un asse verticale che contiene le attività (tipicamente derivate da un'analisi WBS - *Work Breakdown Structure*) e un'asse orizzontale nel quale sono inserite le unità organizzative (derivati dall'organigramma). RACI è un acronimo che deriva dalle iniziali dai quattro tipici ruoli che le unità organizzative posso svolgere nei processi.

***Responsible* (Responsabile)**

Chi ha la responsabilità dell'esecuzione del processo e della realizzazione del prodotto finale. Normalmente il ruolo di Responsabile è unico.

***Accountable* (anche *Approver* – organo decisionale)**

Chi è responsabile, in ultima istanza, del completo e corretto svolgimento del compito e/o della consegna del prodotto. L'*Accountable*, a cui il *Responsible* deve rendere conto, approva il lavoro svolto dal *Responsible*. Deve esserci un unico *Accountable* per ogni compito.

***Consulted* (consultato)**

Chi fornisce consulenze e/o pareri e collabora con i Responsabili allo svolgimento del compito.

***Informed* (informato)**

Chi riceve informazioni sullo svolgimento del compito senza essere direttamente coinvolto nelle attività. Spesso l'informazione avviene solo a conclusione dei lavori.

Talvolta il ruolo di Accountable può combinarsi al ruolo di Responsible (in questi casi la matrice RACI contiene l'indicazione di un Accountable senza un Responsible: la duplice funzione è implicita). A parte questa eccezione, viene generalmente raccomandato che ciascuna unità organizzativa ricopra un solo ruolo.

Secondo la Structural Cybernetics Theory di Dean Meyer una organizzazione efficiente dell'IT deve basarsi su alcuni principi organizzativi fondamentali tra cui i seguenti:

- ognuno ha un'unica responsabilità funzionale;
- solo un'unità organizzativa offre un certo prodotto o servizio; ovvero, non ci deve essere competizione interna per i servizi;
- le unità responsabili per le operazioni giornaliere sono chiaramente separate da quelle che lavorano sulle nuove tecnologie.

Il modello di Meyer classifica le unità organizzative in quattro tipologie principali:

Tecnici: queste unità promuovono l'uso delle nuove tecnologie e curano la progettazione dei sistemi hardware e software.

Bureau di servizi: queste unità si dedicano a fornire servizi operativi affidabili ed efficienti. Ci sono due tipi di *bureau* di servizi: quelli che offrono servizi prodotti da sistemi automatici, quelli che forniscono servizi prodotti dalle persone, come l'*help desk* di supporto e la formazione.

Architetti: l'unita di architettura ha la responsabilità di mettere assieme i *decision-maker* interni e di definire un'architettura informatica per l'impresa. Questa piccola unità deve creare il consenso sugli standard, le linee-guida e le direttive che vincolano i progetti.

Consulenti: i consulenti sono responsabili del rapporto con i clienti interni ed esterni.

Meyer raccomanda che le unità organizzative siano sempre ortogonali rispetto ai gruppi.

Chiama "*rainbows*" le unità organizzative che forniscono più di una delle funzioni descritte sopra (ad es. un'unità responsabile per la progettazione, l'installazione e l'amministrazione quotidiana di una LAN: essa presenta un conflitto fra l'innovazione e un'affidabile operatività quotidiana).

8. L'assessment della struttura organizzativa e dello stato dei rapporti IT-utenti

La rilevazione dello stato dei rapporti tra IT e utenti viene condotta tipicamente tramite interviste individuali e workshop collettivi con un campione di referenti delle aree di business. L'intervista è finalizzata ad ottenere tutte le informazioni non direttamente presenti tra le evidenze che emergono dalla documentazione ufficiale dell'organizzazione.

Devono essere considerate e incluse nell'intervista alcune variabili su cui l'utente intervistato può pronunciarsi attraverso la sua esperienza di settore dell'organizzazione aziendale e di ruolo; riguardano in particolare i rapporti con l'IT nei diversi processi contemplati dall'analisi.

Di seguito si riportano alcune variabili ritenute chiave.

- *Importanza del fattore di analisi*: deve essere esplicitato il livello di importanza del fattore rispetto all'attività di business del referente (vincolante / importante / bassa importanza).
- *Trasparenza*: devono essere evidenziate da parte dell'utente le caratteristiche, la composizione, le modalità di erogazione, ecc. del fattore oggetto di rilevazione.
- *Tempestività*: tempi, disponibilità e capacità di messa a punto.
- *Qualità percepita*: deve essere specificata la rispondenza del servizio "day-by-day" alle esigenze del business.
- *Costi rispetto alla qualità percepita*: deve essere esplicitata la percezione del livello di costo rispetto alla rispondenza alle esigenze.

Per ogni intervista devono essere realizzate schede riepilogative di valutazione che, oltre a permettere di tracciare quanto descritto dall'intervistato sia in termini descrittivi sia in termini valutativi rispetto alle variabili sopra elencate, permettono di descrivere ulteriori argomenti e indicazioni ritenuti importanti dal referente ai fini dell'analisi e dei successivi sviluppi nei rapporti tra la Funzione IT e il business.

Tipicamente le interviste devono essere strumenti aperti che non inducano gli interlocutori a mentire. Le domande pertanto non devono essere chiuse ma devono essere organizzate in modo da fornire e consentire di raccogliere tutti gli elementi di completamento del quadro e delle pratiche in uso nell'organizzazione.

La rilevazione deve basarsi su un framework di riferimento in modo da consentire il confronto con altre realtà organizzative analoghe all'oggetto di osservazione.

Partendo dal frame work ITIL V3, è possibile costruire una rilevazione dello stato dei rapporti IT-utenti focalizzato sul delivery and support e sulla governance.

Di seguito si riporta una selezione dei processi considerati più significativi a descrivere lo stato dei rapporti IT-utenti. Tale selezione ha guidato le interviste condotte nel processo di audit svolto in Istat descritto nei paragrafi a seguire e in appendice (appendice 2).

Il modello di riferimento che focalizza l'attenzione sull'IT governance è articolato in cinque macroprocessi:

"Rilevazione e gestione della domanda - Demand management"
"Pianificazione e gestione del portafoglio - Portfolio management"
"Gestione dei progetti - Project management"
"Gestione del rapporto con l'utente - Customer Service"
"Esercizio - Operations".

Di seguito sono riportate brevi definizioni di ciascun macro processo dedotte dalla metodologia ITIL V3.

La "Rilevazione e gestione della domanda - Demand management" è il processo che, a partire dalla generale strategia dell'azienda e dalle linee di evoluzione di ciascun settore di business, individua le esigenze degli utenti che possono dar luogo a iniziative progettuali IT.

In tale fase è indispensabile il contributo del settore IT in termini di proposizione dell'offerta tecnologica (che può costituire il fattore abilitante di nuovi processi).

La "Pianificazione e gestione del portafoglio - Portfolio management" è il processo che a partire dall'analisi della domanda rilevata, sulla base della generale strategia dell'azienda e dello sviluppo del business case effettuato dal proponente, porta alla definizione del portafoglio dei progetti e, conseguentemente, delle priorità realizzative.

La "Gestione dei progetti - Project management" è il processo di realizzazione e controllo dei progetti IT dalla fase di analisi funzionali fino al collaudo e alla messa in esercizio. Include anche la fase di scelta dei fornitore (sourcing) e di acquisizione delle risorse (procurement).

La "Gestione del rapporto con l'utente – Customer Service" è l'insieme di tutte le attività di contatto con gli utenti, inclusa la fornitura delle dotazioni individuali, di gestione e risoluzione dei problemi, di rilevazione del livello di soddisfazione rispetto ai servizi IT forniti.

L'"Esercizio - Operations" è l'insieme delle attività operative che portano all'erogazione di servizi infrastrutturali o applicativi.

I temi trattati nelle interviste riguardano essenzialmente i seguenti ambiti di riferimento:

Demand Management: Business Requirements, Fattibilità, Processo Innovazione, Catalogo servizi

Portfolio Management: Gestione delle priorità, Pianificazione, Project Portfolio

Project Management: Progettazione funzionale, Project Management, Processo di realizzazione, test e collaudi, Formazione

Customer Service: Postazioni di lavoro e dotazioni individuali; Help Desk / Assistenza all'utente negli interventi, Customer Relationship

Operations: Servizio di esercizio dei sistemi informativi, Performance management

L'appendice 2 riporta lo schema di riferimento delle interviste condotte in Istat con i responsabili dei settori di produzione statistica dell'Istituto.

Ciascuna intervista ha avuto una durata di circa 2 ore. Al termine dell'intervista gli intervistatori hanno riempito una scheda con la sintesi delle valutazioni in termini qualitativi e quantitativi con riferimento ai 5 processi identificati. Le valutazioni sono state poi riscontrate dall'utente intervistato per eventuali feedback e/o correzioni.

9. Il processo di audit informatico condotto in Istat

9.1 Il contesto di riferimento

La necessità di aggiornare le proprie piattaforme di elaborazione, di introdurre le nuove tecnologiche affermatesi sul mercato ICT e di rendere l'Istituto quanto più possibile indipendente dai fornitori, ha spinto l'Istituto negli ultimi anni a una profonda revisione della propria architettura di elaborazione e dei software utilizzati.

Il contesto informatico dell'Istituto, le scelte e gli standard adottati in questi ultimi anni hanno reso l'ICT dell'Istituto sempre più articolato e complesso. Le scelte tecnologiche hanno assunto un peso sempre più crescente e strategico spesso influenzando e condizionando i processi di produzione dell'Istituto.

Tenendo conto di tale complessità, al fine di inquadrare l'audit nel contesto d'Istituto, si è ritenuto utile avviare un'analisi preliminare tesa a definire gli assi di riferimento nei quali potranno essere inquadrate le tematiche sottoposte ad audit. Il contesto generale di riferimento dell'Istituto può essere inquadrato secondo 3 assi fondamentali:

Il contesto normativo ed evolutivo. Questo aspetto comprende la normativa vigente e il complesso quadro istituzionale che, a livello nazionale, coinvolge l'insieme degli altri enti della Pubblica Amministrazione (PA) Italiana e, a livello internazionale, comporta rapporti con l'Eurostat e l'insieme degli altri Istituti Nazionali di Statistica (INS).

Il contesto organizzativo. Rientrano in questo ambito gli aspetti legati all'organizzazione informatica dell'Istituto e alle funzioni svolte dalle strutture centrali della DCMT e dalle strutture delle direzioni di produzione statistica e della direzione generale.

Il contesto infrastrutturale e tecnologico. Rientrano in questo settore le scelte e gli standard tecnologici adottati, le strategie in atto per la messa in sicurezza dell'infrastruttura e delle strutture di elaborazione e di rete, le procedure di continuità operativa, ecc.

9.2 La struttura organizzativa di supporto al processo

Per condurre l'audit della funzione informatica, l'Istat ha definito una struttura di audit committee costituito da una Commissione per l'audit informatico (CAI). La commissione è stata nominanata dal Presidente dell'Istituto il 19 Agosto 2010 con fine mandato previsto per Marzo 2011.

Di seguito si descrive brevemente il ruolo, la sua composizione e il piano di massima dei lavori eseguiti.

Ruolo della Commissione CAI

La Commissione ha il compito di effettuare la rilevazione e l'analisi sulle varie strutture informatiche dell'Istat sullo stato di automazione dell'Istituto, mettendo in evidenza la qualità, l'efficienza e l'efficacia al fine di migliorare i servizi informatici offerti.

Coordinamento della commissione

La Commissione è presieduta da due esperti esterni scelti dall'amministrazione in qualità di esperti esterni in organizzazione e funzionamento dei sistemi informativi e di esperti in direzione e gestione di sistemi di Information and Comunication Technology.

Membri e segreteria tecnica

La Commissione è costituita da un membro esterno dirigente della Banca d'Italia e cinque membri interni, 4 direttori dei settori di produzione statistica e un rappresentante delegato dalla Presidenza. La Commissione si è avvalsa di una segreteria tecnica costituita da 3 dirigenti di strutture tecnico-informatiche dell'istituto.

Piano di massima dei lavori

Coerentemente con il mandato affidatole, la Commissione ha espleta la propria attività attraverso due principali fasi di lavoro:

- una fase di rilevazione;
- una fase di valutazione.

Il lavoro di rilevazione e valutazione è stato inquadrato in quello che è il contesto normativo, nazionale ed internazionale delle attività ICT.

9.3 La fase di rilevazione delle evidenze

La fase di Rilevazione delle evidenze è stata articolata su due indagini distinte finalizzate a raccogliere informazioni rispettivamente all'interno ed all'esterno dell'Istituto.

Al fine di validare e monitorare il lavoro di rilevazione, durante lo svolgimento della fase in oggetto, sono state effettuate 5 riunioni della Commissione in modalità plenaria.

Sono stati quindi presentati risultati preliminari della fase di rilevazione al Comitato di Direzione.

Rilevazione interna

La rilevazione è stata rivolta ad analizzare sia le strutture centrali (con particolare attenzione alla Direzione DCMT- Direzione Centrale delle metodologie e del supporto tecnologico) che le strutture di produzione statistica.

Per quanto riguarda la DCMT, la rilevazione approfondisce gli aspetti di seguito elencati:

- la struttura organizzativa;
- i sistemi di pianificazione e controllo dei progetti;
- le infrastrutture tecnologiche;
- il software di base e di ambiente;
- i pacchetti applicativi;
- i sistemi informativi gestiti direttamente dalla DCMT;
- i siti Web gestiti dalla DCMT;
- i livelli di servizio e i processi di produzione;
- la business continuity e la sicurezza.

Per quanto riguarda le Direzioni di produzione statistica , per ciascuna di esse l'analisi è stata su:

- la Struttura e le funzioni della Direzione;
- i sistemi informativi governati dalla Direzione e/o condivisi con la DCMT;
- i siti Web gestiti dalla Direzione.

Le informazioni sono state raccolte attraverso colloqui e la compilazione di tabelle strutturate a vario livello di approfondimento. L'esecuzione è risultata relativamente rapida per la DCMT, mentre per le singole Direzioni di produzione statistica richiede un impegno più significativo e la convinta collaborazione del personale addetto alle stesse. Al fine di assicurare la buona condotta della rilevazione, le Direzioni i cui Direttori partecipano alla Commissione sono state le prime ad essere esaminate. Tale fase è stata anche l'occasione per raccogliere, a tutti i livelli di responsabilità, opinioni e suggerimenti preziosi per la successiva fase di valutazione.

Rilevazione esterna

La rilevazione esterna è stata rivolta agli istituti di statistica dei paesi esteri ed è stata finalizzata a raccogliere dati per definire un benchmark con la situazione dell'Istituto. Il questionario di rilevazione ha raccolto informazioni sui seguenti aspetti: le strutture organizzative con cui è articolata la funzione ICT e i costi. Si prevede anche di approfondire, mediante apposite visite, la specifica realtà di uno o più Istituti esteri considerati come virtuosi.

9.4 La fase di valutazione

La fase di valutazione ha riguardato gli aspetti specifici di seguito elencati:

- i costi dell'ICT ripartiti nelle diverse componenti e rielaborati per Direzione ed ove possibile per prodotto;
- il confronto dei costi suddetti con indicatori disponibili e con quelli di analoghi Istituti esteri;
- l'analisi dei rischi operativi;
- la qualità dei processi (operativi, di supporto, di sviluppo, di governo e controllo, di pianificazione,etc.);
- l'organizzazione del processo di produzione dei servizi ICT.

La valutazione ha riguardato i due macro aspetti analizzati nel lo svolgimento del processo di audit.

1. *Il contesto organizzativo* rilevato attraverso l'analisi dei documenti ufficiali dell'Istituto e tramite i seguenti strumenti ausiliari:
   - indagine sul clima organizzativo rivolta al Board dei Direttori e ai Dirigenti ICT;
   - indagine sulla maturità della governance rivolta al Board;
   - matrice RACI dei Processi (Board);
   - analisi con i responsabili ICT delle varie Direzioni dei processi di sviluppo.

2. *L'asset patrimoniale rilevato attraverso*:
   - ricostruzione del valore del patrimonio software e hardware;
   - indagine di benchmark rivolta ai Direttori ICT degli Istituti Nazionali di Statistica.

9.5 Le modalità di conduzione del lavoro

Al fine di rendere lo svolgimento della attività il più efficace possibile è stato articolato il lavoro della Commissione su due livelli:

- un nucleo operativo costituito dai membri esterni, dal Direttore della DCMT, dai componenti della segreteria tecnica;
- la Commissione nella sua interezza.

Il nucleo di valutazione costituito dagli esperti esterni all'Istituto ha proposto l'approccio metodologico, di rilevazione e di analisi ed elaborazione dei risultati. La Commissione ha effettuato la valutazione ed approvazione del procedimento metodologico proposto, delle valutazioni dei risultati ed il monitoraggio sullo stato di attuazione delle attività previste.

E' stata condotta una intervista tesa ad individuare il livello di maturità della governante dei servizi IT erogati dall'Istituto all'utenza interna e all'utenza esterna.

L'intervista ha curato i seguenti processi specifici selezionati come critici per l'ente:

1. Gestione della domanda.
2. Relazioni con gli utenti (CRM).
3. Gestione infrastrutture.
4. Gestione SLA.
5. Architettura tecnica (Enterprise Architecture).
6. Sviluppo soluzioni software.
7. Gestione delle reti e dei sistemi di telecomunicazione.
8. Supporto strumenti individuali.
9. IT Procurement.
10 Ricerca.
11 Gestione sicurezza.

L'intervista è stata rivolta ai direttori dei settori di produzione statistica dell'Istat. Il campione di riferimento è stato costruito selezionando i dirigenti della DCMT e i Direttori centrali che rappresentano l'utenza d'Istituto e i principali utilizzatori di servizi ICT. L'intervista è stata condotta al fine di analizzare il possibile stato di non completa soddisfazione chiamando gli intervistati a individuare l'ambito a maggiore criticità.

Le valutazioni sono state analizzate in relazione al modello federato della funzione IT adottato dall'Istituto: la presenza di nuclei tecnici presso le Direzioni in alcuni casi ha portato ad influenzare positivamente le valutazioni degli utenti

Gli intervistati sono stati chiamati a classificare i temi secondo due criteri di riferimento:

- l'importanza del tema (inquadrato secondo una scala a 3 livelli con 0 - poco importante, 1- importante, 2- vincolante;
- la qualità percepita (inquadrata secondo una scala a 5 livelli con 0 – assente, 1 - molto inferiore alle esigenze, 2 - inferiore alle esigenze, 3 - in linea con le esigenze, 4 - superiore alle esigenze, 5 - molto superiore alle esigenze.

Le appendici 2 e 3 riportano gli schemi utilizzati per l'intervista sulla governance e il questionario per rilevare il livello percepito dai direttori di produzione in merito agli aspetti di governance dell'IT dell'Istituto.

9.6 Considerazioni in merito all'approccio utilizzato

L'approccio utilizzato in Istat è stato basato essenzialmente sull'analisi organizzativa. Tale approccio è risultato in generale meno costoso e impegnativo, gli strumenti adottati sono risultati poco invasivi e snelli ed hanno permesso di individuare con immediatezza i problemi macroscopici e le criticità rilevanti su cui intervenire.

L'analisi tecnico/economica di dettaglio è in generale molto onerosa da condurre ma l'approccio adottato ha consentito di individuare le criticità più evidenti quantificando l'impatto sull'organizzazione. E' stato raggiunto un livello di conoscenza relativamente all'architettura tecnologica, alla consistenza del patrimonio applicativo, all'utilizzo delle risorse umane e ai costi complessivi dell'IT dell'Istituto. La conduzione del lavoro con personale interno risulta critica per il carico di lavoro aggiuntivo richiesto, ma diminuisce i timori dell'organizzazione e i rischi di rigetto delle strutture che devono fornire i dati se i lavori vengono condotti con il pieno coinvolgimento dei manager dell'IT dell'Istituto e del personale informatico.

10. Rilevazione web sull'audit informatico nei paesi esteri

Al fine di raccogliere elementi il più possibile esaustivi su un tema così delicato quale è un audit, si è ritenuto opportuno avviare anche una fase di confronto con gli Istituti di statistica di Paesi europei ed extraeuropei e con alcuni organismi internazionali con ad esempio Eurostat, OCSE, FMI, ecc. A tale proposito, è stata realizzata una rilevazione on-line orientata ai Direttori del settore IT attraverso un questionario, finalizzato a raccogliere alcune informazioni sia di tipo organizzativo, sia di tipo più propriamente tecnico sull'IT dell'ente di riferimento. Tale rilevazione, indicata nel seguito come Lime Survey sull'Audit Informatico (LSAI), è finalizzata a conoscere se gli istituti coinvolti hanno effettuato un audit, quali tipi di processi sono eventualmente monitorati, quali attori sono coinvolti, se il lavoro è certificato. I risultati ottenuti dall'indagine e successivamente elaborati costituiscono un forte motivo di riflessione sia nel caso in cui emerga che l'audit è un processo consolidato nell'organizzazione, sia quando non lo è. Infatti, nel primo caso l'Istat acquisisce utili informazioni dall'esperienza degli altri, nel secondo propone un modello per gli altri paesi coinvolti nella rilevazione. I dati quantitativi forniscono invece un *benchmarching* ed un termine di confronto per l'Istat.

10.1 I quesiti e la modalità di conduzione dell'indagine

Il questionario è stato strutturato secondo i seguenti quesiti:

1. Di quale budget annuale dispone l'Istituto e quante persone vi lavorano?
2. Quale è il costo totale del personale?
3. Dov'è posizionato il Servizio ICT nell'organigramma? Se possibile descrivere brevemente le funzionalità e inviare il diagramma organizzativo al seguente indirizzo mail survey@istat.it
4. Qual è il budget per i servizi ICT e quante persone vi lavorano?
5. Qual è il costo totale del personale ICT?
6. I processi ICT sono gestiti in full outsourcing? Si/No
   Se si: qual è il costo del servizio di outsourcing?
   Se no: Qual è il costo dei servizi esterni, con riferimento alle voci di:
   - sistemi hardware e software;
   - telecomunicazioni;
   - servizi di sviluppo software;
   - software statistico (specificando il prodotto);
   - altro.
7. E' mai stato condotto nell'Istituto un Audit ICT? Si/No
   Se si: Il processo di valutazione ha creato problemi all'interno dell'organizzazione? Se si, spieghi brevemente quali.
   Dopo il processo di valutazione c'è stato un cambiamento nell'organizzazione? Se si, spieghi brevemente quali.
   Se no: L'Istituto per cui lavora è interessato ad introdurre un processo di audit ICT? Si/No
8. Eventuali commenti.

L'idea di questa survey è quella di catturare informazioni di tipo quantitativo relativamente agli aspetti ICT degli altri Istituti per "misurare" i vari elementi in gioco. Di qui le informazioni sul budget totale e relativo all'ICT, sul numero di persone impiegate nell'organizzazione e nell'area informatica e sul tipo di servizi dati eventualmente in outsourcing. L'ultima parte è stata invece dedicata all'impatto del processo di audit sull'organizzazione.

In Istat, parte della rilevazione, è consistita nella ricognizione di tutti prodotti software dell'Istituto, spesso realizzati *in house*. Ciò ne ha permesso una quantificazione in termini di numero, di linee di codice (LOC) e quindi economica.

La sponsorship di questa iniziativa è direttamente legata alla Presidenza Istat. Il questionario viene somministrato a 30 utenti che rappresentano i CIO delle organizzazioni considerate. L'indagine è stata lasciata attiva per due settimane ed i risultati raccolti, e successivamente rielaborati, sono resi noti in forma aggregata agli Istituti che hanno deciso di rispondere (cfr Appendice 4).

Allegato 1: La Commissione CAI per l'audit informatico in Istat

Per condurre l'audi della funzione informatica, l'Istat ha definito una struttura di audit committee costituito da una Commissione per l'audit informatico (CAI). La commissione è stata nominanata dal Presidente dell'Istituto il 19 Agosto 2010 con fine mandato previsto per Marzo 2011.

Di seguito si descrive brevemente il ruolo, la sua composizione e il piano di massima dei lavori eseguiti.

Ruolo della Commissione CAI

La Commissione ha il compito di effettuare la rilevazione e l'analisi sulle varie strutture informatiche dell'Istat sullo stato di automazione dell'Istituto, mettendo in evidenza la qualità, l'efficienza e l'efficacia al fine di migliorare i servizi informatici offerti.

Coordinamento della commissione

La Commissione è presieduta da due esperti esterni scelti dall'amministrazione in qualità di esperti esterni in organizzazione e funzionamento dei sistemi informativi e di esperti in direzione e gestione di sistemi di Information and Comunication Technology.

Membri e segreteria tecnica

La Commissione è costituita da un membro esterno dirigente della Banca d'Italia e cinque membri interni, 4 direttori dei settori di produzione statistica e un rappresentante delegato dalla Presidenza. La Commissione si è avvalsa di una segreteria tecnica costituita da 3 dirigenti di strutture tecnico-informatiche dell'Istituto.

Piano di massima dei lavori

Coerentemente con il mandato affidatole, la Commissione espleta la sua attività attraverso due principali fasi di lavoro:

- una fase di rilevazione;
- una fase di valutazione.

FASE DI RILEVAZIONE

La fase di Rilevazione è articolata su due indagini distinte finalizzate a raccogliere informazioni rispettivamente all'interno ed all'esterno dell'Istituto.

Rilevazione interna

La rilevazione viene rivolta ad indagare sia le strutture centrali (con particolare attenzione alla Direzione DCMT) che le strutture di produzione.

Rilevazione esterna

La rilevazione esterna è rivolta agli istituti di statistica dei paesi esteri ed è finalizzata a raccogliere dati per definire un benchmark con la situazione dell'Istituto. Il questionario di rilevazione raccoglie informazioni sugli seguenti aspetti: le strutture organizzative con cui è articolata la funzione ICT e i costi. Si prevede anche di approfondire, mediante apposite visite, la specifica realtà di uno o più Istituti esteri considerati come virtuosi.

FASE DI VALUTAZIONE

La fase di valutazione riguarda gli aspetti di seguito elencati:

- i costi dell'ICT ripartiti nelle diverse componenti e rielaborati per Direzione ed ove possibile per prodotto;
- il confronto dei costi suddetti con indicatori disponibili e con quelli di analoghi Istituti esteri. L'analisi dei rischi operativi;
- la qualità dei processi (operativi, di supporto, di sviluppo, di governo e controllo, di pianificazione, etc.);
- l'organizzazione del processo di produzione dei servizi ICT.

Allegato 2: Lo schema di intervista sulla Governance adottato in Istat

INTERVISTA SULLA GOVERNANCE

Dati intervistato
nome:_ _____ struttura: __ _____
data intervista: _____ intervistatore: _____ durata (media 1 ora) ___

processo		Attività	Valutazione/giudizio		
			Scala_ 0/2 0 - poco importante 1- importante 2- vincolante	**Scala 0/5** 0 – assente 1 - molto inferiore alle esigenze 2 - inferiore alle esigenze 3 - in linea con le esigenze 4 - superiore alle esigenze 5 - molto superiore alle esigenze	
			Importanz fattore	***Qualità percepita***	***note***
Progettualità	**1. Demand management / gestione della domanda**	***Requisiti utente***			
		Fattibilità			
		Processo innovazione			
	2. Planning / pianificazione	***Catalogo dei servizi*** *(infrastrutture)*			
		Gestione priorità			
		Gestione del portafoglio (piano) dei progetti			
	3. Gestione progetti	***Progettazione funzionale***			
		Project management			
		Processo di realizzazione test e collaudi formazione			
erogazione dei servizi IT	**4. Esercizio**	***Servizio esercizio applicativi*** *(server e rete - incluso SLA)*			
		Performance management			
	5. Customer service	***Postazioni di lavoro e dotazioni individuali***			
		Help desk e assistenza utenti negli interventi			
	6. Customer relationship				

Note di carattere generale:

Allegato 3: Il questionario sul livello di maturità della Governance percepita in Istat

Istat.it

IT Governance Healthcheck Tool

Questionnaire

Nome dell'Istituto:	ISTAT
Consistenza del personale dell'Istituto:	1250
Consistenza personale centrale ICT:	225
Consistenza personale ICT esterno:	«Number of external IT staff»
Numero di procedure ICT in produzione:	20
Numero di progetti ICT in corso:	109
Budget ICT centrale annuale, in Euro:	15,000,000

Data della compilazione: Luglio 2010

Effettuata da: Gruppo di lavoro Commissione Audit

Contrassegnare con una 'X' la colonna che meglio risponde ad ogni domanda

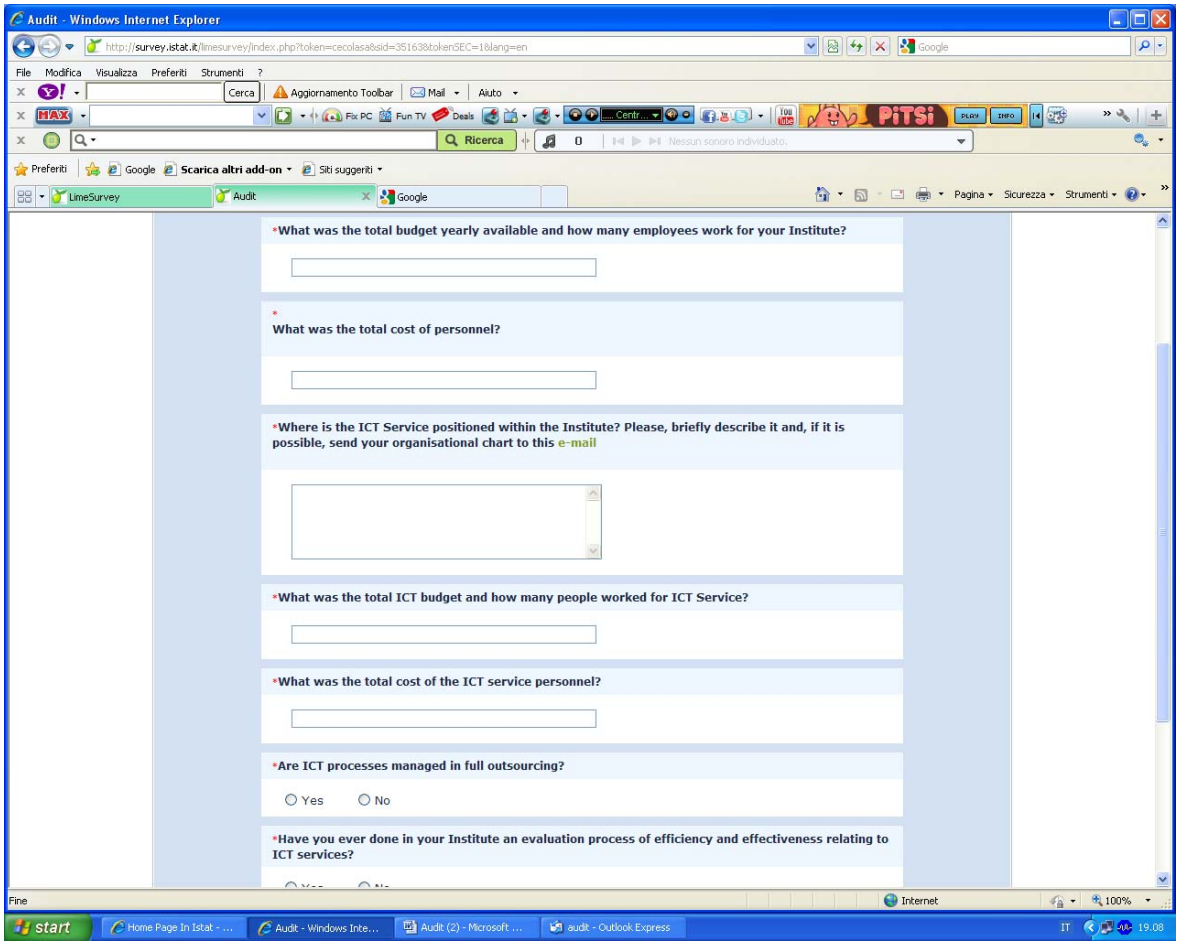
Rif	IT Governance: Contesto, Struttura Organizzativa e Processi	Sì, Sempre	In gran misura	In parte	Di rado	Molto di rado	No, mai	Non so	Commenti
1	L'Istituzione si avvale di processi di governance ICT ben definiti e stabili								
2	I Comitati/Commissioni che guidano importanti decisioni informatiche hanno una composizione stabile ed il loro lavoro è ben conosciuto ed accettato								
3	Questi Comitati/Commissioni Informatiche condotano in misura eguale di responsabili della produzione e dei loro servizi informatici								
4	I processi decisionali ICT a livello istituzionale funzionano bene, sono ben strutturati, le priorità sono chiare, i cambiamenti ai calendari di lavoro e le eccezioni si decidono rapidamente, ecc.								
5	Anche i processi decisionali ICT a livello divisionale funzionano bene, sono ben strutturati e si integrano bene, le priorità sono chiare, i cambiamenti ai calendari di lavoro e le eccezioni si decidono rapidamente, ecc.								
6	I Direttori hanno familiarità con la Governance IT; possono spiegarne il funzionamento e come essa è organizzata; sanno chi guida importanti decisioni ICT come queste decisioni vengono prese.								
7	I Direttori sono coinvolti nelle decisioni ICT e sostengono la Governance IT tramite il loro coinvolgimento nelle strutture di Governance; sono membri attivi dei comitati informatici, sostengono e rafforzano le politiche informatiche, ecc...								
8	I Capi Servizio sanno spiegare la Governance IT; possono descriverne i concetti, o fornire un'accurata descrizione di come la Governance IT funziona; sanno chi prende le decisioni informatiche importanti, e come queste decisioni vengono formulate.								
9	I Capi Servizio sono impegnati in decisioni che riguardano l'informatica e appoggiano la Governance IT con il loro coinvolgimento personale; sono membri attivi di comitati informatici, sostengono e rafforzano le strutture e gli standard della governance IT, ecc.								
10	Esistono canali efficaci di comunicazione tra i diversi livelli gerarchici - tra Direttori, Capi Servizio, Capi Unità ed il loro personale. Strategie, decisioni, rischi, opportunità, ecc.. sono esposti chiaramente.								
11	Esiste un'entità nell'Istituto dedicata al sostegno della Governance IT e facilmente raggiungibile per fornire spiegazioni, raccogliere idee, ecc..								
	Rapporto tra il Business e l'Informatica								
12	Le strutture di produzione conoscono come funzionano le strutture informatiche, o cosa l'IT può e non può fare entro certi termini.								
13	I settori di produzione e l'IT si capiscono a vicenda su: - i bisogni IT della produzione - le possibilità IT per la produzione								
14	I rapporti tra la produzione e l'IT sono collaborativi, essi lavorano assieme per il raggiungimento degli obiettivi principali dell'Istituto								
15	Esistono canali ben definiti che permettono all'IT di comunicare attraverso l'organizzazione								

Rif	Allineamento Strategico dell'ICT al Business	Sì, Sempre	In gran misura	In parte	Di rado	Molto di rado	No, mai	Non so	Commenti
16	La strategia dell'Istituto a livello istituzionale è ben definita ponendo come obiettivo l'eccellenza operativa oppure l'innovazione oppure il rapporto con le parti interessate, ecc... Questa strategia e le sue implicazioni sono ben comunicate all'IT e alle sue strutture.								
17	La strategia dell'Istituto è ben definita anche per la Direzione Generale ponendo come obiettivo l'innovazione oppure il rapporto con le parti interessate, ecc... Questa strategia e le sue implicazioni sono ben comunicate all'IT e alle sue strutture.								
18	I Direttori hanno una visione chiara e ben articolata sul ruolo dell'IT.								
19	La strategia di produzione statistica include o tiene conto del fattore IT.								
20	Esistono meccanismi per assicurare l'allineamento tra IST e gli obiettivi strategici della produzione; questi meccanismi possono includere opportuni comitati e procedure, il coinvolgimento formale della produzione nell'approvazione di nuovi programmi e progetti IT, ecc..								
21	I rapporti tra gli obiettivi istituzionali e gli obiettivi dell'IT e viceversa, sono chiari.								
22	L'IT non è vista solamente come funzione operativa e di supporto. La produzione si interessa delle opportunità presentate dall'IT su come le nuove tecnologie potrebbero beneficiare l'organizzazione.								
23	Le analisi d'impatto dell'IT sulle decisioni della produzione vengono fatte regolarmente. Le decisioni della produzione vengono prese solo dopo aver considerato il loro impatto sull'IT, la fattibilità della messa in opera, i tempi di realizzazione, le risorse necessarie, ecc..								
24	Esiste una strategia IT per il medio-lungo termine, con obiettivi strategici che vanno ben oltre le funzioni operative IT.								
25	La Strategia IT a medio-lungo termine è costruita con il contributo delle Direzioni di Produzione								
26	In aggiunta alla Direzione DGMT, altri dirigenti partecipano all'elaborazione della Strategia IT e dei suoi obiettivi strategici.								

Rif	Valore Aggiunto dell'Automazione	Sì, Sempre	In gran misura	In parte	Di rado	Molto di rado	No, mai	Non so	Commenti
27	Gli investimenti IT e relativi servizi, risorse ed investimenti sono gestiti in modo strutturato, si mantiene il piano degli investimenti, esiste un catalogo dei servizi, ecc..								
28	La dirigenza fornisce linee guida strategiche per gli investimenti IT (non solo per ragioni di bilancio, ma anche sulle specificità della produzione).								
29	Chiari e precisi obiettivi esistono per gli investimenti IT in termini di riduzione dei costi, miglior servizio alla clientela, migliore qualità del prodotto, sostegno alle iniziative del business, ecc..								
30	Progetti IT vengono valutati e prioritizzati normalmente sulla base delle risorse e fondi disponibili.								
31	Il "valore" del prodotto IT è ben definito: è chiaro ciò che l'IT fornirà in termini di funzionalità, attese e livelli di servizio; allo stesso tempo l'Istituzione verifica in che misura tale valore viene realizzato.								

Allegato 4: L'indagine LSAI

L'indagine descritta nel capitolo 10, fruibile via web, è stata realizzata attraverso l'applicativo Limesurvey e si presenta all'utente come riportato nella figura che segue.



Riferimenti bibliografici

Associazione Italiana Internal Auditors. Aprile 2008. *Il Ruolo dell'Auditing nella Governance del Settore Pubblico*. Milano. AIIA.

Colasanti, C., Murgia, M., 2011. *Innovative solutions for data capturing strategies*. Bruxelles: Eurostat NTTS 2011 http://www.ntts2011.eu

Falorsi, P.D., Losco, S., 2009. *Audit sull'attuale dotazione e direzione della strategia informatica* . Azioni a breve termine per il miglioramento dell'efficienza e l'efficacia dell'attività dell'Istat. http//www.istat.it/wiki (novembre 2009, accesso disponibile su richiesta).

Guldentops E., 2003, *Maturity Measurement—First the Purpose,Then the Method*, Information System Audit and Control Journal, Volume 4 , 2003.

International Organization for Standardization (ISO), ISO 27001 *Information Security Management Systems - Code of Practice***,** 2006.

International Register of Certificated Auditors (IRCA). http://www.irca.org

Information System Audit and Control Association (ISACA). http://www.isaca.org

IT Governance Institute, *IT Governance Implementation Guide: Using COBIT® and Val IT* TM, *2nd Edition,* United States of America, ITGI.

IT Governance Institute, *COBIT Mapping, Overview of International IT Guidance, 2ndEdition,* United States of America, 2007, ITGI.

IT Governance Institute, *COBIT 4.1Control Objectives Management Guidelines maturity Models,* United States of America, 2007, ITGI.

IT Governance Institute, *IT assurance guide using COBIT,* United States of America, 2007, ITGI.

IT Governance Institute, The Risk IT framework, Principles Process Details Management Guidelines Maturity Models United States of America, 2009, ITGI.

Office of Government Commerce (OGC), *IT Infrastructure Library® (ITIL),* UK.

Sinibaldi, A., 2007. *Risk Management*: Milano: Hoepli Editore.

Informazioni per gli autori

La collana è aperta ad autori dell'Istat e del Sistema statistico nazionale, e ad altri studiosi che abbiano partecipato ad attività promosse dal Sistan (convegni, seminari, gruppi di lavoro, ecc.). Da gennaio 2011 essa sostituirà Documenti Istat e Contributi Istat.

Coloro che desiderano pubblicare sulla nuova collana dovranno sottoporre il proprio contributo alla redazione degli Istat Working Papers inviandolo per posta elettronica all'indirizzo iwp@istat.it. Il saggio deve essere redatto seguendo gli standard editoriali previsti, corredato di un sommario in italiano e in inglese; deve, altresì, essere accompagnato da una dichiarazione di paternità dell'opera. Per la stesura del testo occorre seguire le indicazioni presenti nel foglio di stile, con le citazioni e i riferimenti bibliografici redatti secondo il protocollo internazionale 'Autore-Data' del *Chicago Manual of Style*.

Per gli autori Istat, la sottomissione dei lavori deve essere accompagnata da una mail del proprio dirigente di Servizio/Struttura, che ne assicura la presa visione. Per gli autori degli altri enti del Sistan la trasmissione avviene attraverso il responsabile dell'ufficio di statistica, che ne prende visione. Per tutti gli altri autori, esterni all'Istat e al Sistan, non è necessaria alcuna presa visione. Tutti i lavori saranno sottoposti al Comitato di redazione, che valuterà la significatività del lavoro per il progresso dell'attività statistica istituzionale. La pubblicazione sarà disponibile su formato digitale e sarà consultabile on line.

Gli articoli pubblicati impegnano esclusivamente gli autori, le opinioni espresse non implicano alcuna responsabilità da parte dell'Istat. Si autorizza la riproduzione a fini non commerciali e con citazione della fonte.