Consiglio Nazionale Forense

CONSIGLIO NAZIONALE DEGLI INGEGNERI

Fondazione Italiana per l'Innovazione Forense

Con il patrocinio del

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Corso DPO

Architetture IT e sicurezza dei dati

Ing. Giulio Destri

Dr. Ing. Giulio Destri, Ph.D.

ICT Business Advisor @ AREA Digital Solutions

Professore a contratto di Sistemi Informativi @ Università di Parma

Certificato ISO27001LA, COBIT-5, ITILv3, SCRUM Master

http://www.linkedin.com/giuliodestri

http://www.giuliodestri.it/

giulio.destri@unipr.it

twitter.com/GiulioDestri

Agenda (1/2)

- Il contesto: GDPR e IT
- Le qualità dell'accesso ai dati
- Le architetture IT per conservazione ed accesso ai dati
- Cosa è l'accesso sicuro ai dati
- Tecniche di pseudonimizzazione
- La cifratura la sua "forza"

Agenda (2/2)

- Tecniche per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- Il ripristino dei dati in caso di incidente fisico o tecnico
- Architetture e framework standard internazionali

Il contesto: GDPR e IT

Trattamenti dei dati

- Il GDPR definisce "**trattamento**" (**'processing'**) come: "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali*"

Gli articoli “principalmente” collegati

- Art. 24: Responsabilità del titolare del trattamento (in parte)
- Art. 25: Privacy e data protection by default & design
- Art. 28: Responsabile del trattamento (in parte)
- Art. 30: Registri delle attività di trattamento (in parte)
- Art. 32: Sicurezza del trattamento
- Art. 35: Valutazione d'impatto sulla protezione dei dati

GDPR: articolo 24

Responsabilità del titolare del trattamento

1.Tenuto conto della **natura**, dell'**ambito di applicazione**, del **contesto** e delle **finalità del trattamento**, nonché dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. […]

GDPR: articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. […] sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento il titolare del trattamento mette in **atto misure tecniche e organizzative adeguate**, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi e la protezione dei dati, quali la minimizzazione e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. […]

2. l titolare del trattamento mette in atto **misure tecniche e organizzative** adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.[…]

GDPR: articolo 28

Responsabile del trattamento

1.Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino **garanzie sufficienti** per **mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. […]

GDPR: articolo 30

Registri delle attività di trattamento

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

[…]

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1

GDPR: articolo 32 (1/2)

Sicurezza del trattamento

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

GDPR: articolo 32 (2/2)

Sicurezza del trattamento

b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico**;

d) una **procedura per testare**, **verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative** al fine di garantire la **sicurezza** del trattamento.

GDPR: articolo 35

Valutazione d'impatto sulla protezione dei dati

1.Quando un tipo di trattamento, allorché prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2.Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

Esempi di Trattamenti dei dati: interni

- **La raccolta,**
- **la registrazione,**
- **l'organizzazione e la strutturazione,**
- **la conservazione,**
- **l'adattamento,**
- **la modifica,**
- **l'estrazione e la consultazione**
- **l’uso (generico)**

- Anche il backup

Esempi di Trattamenti: comunicazione dei dati

- **la comunicazione mediante trasmissione,**
- **diffusione,**
- **qualsiasi altra forma di messa a disposizione,**

- Quindi ogni tipo di comunicazione

Esempi di Trattamenti: correlazione dei dati

- **il raffronto e/o l'interconnessione,**
- **la limitazione,**

- Quindi anche ogni correlazione (vedi Big Data)

Esempi di Trattamenti: cancellazione dei dati

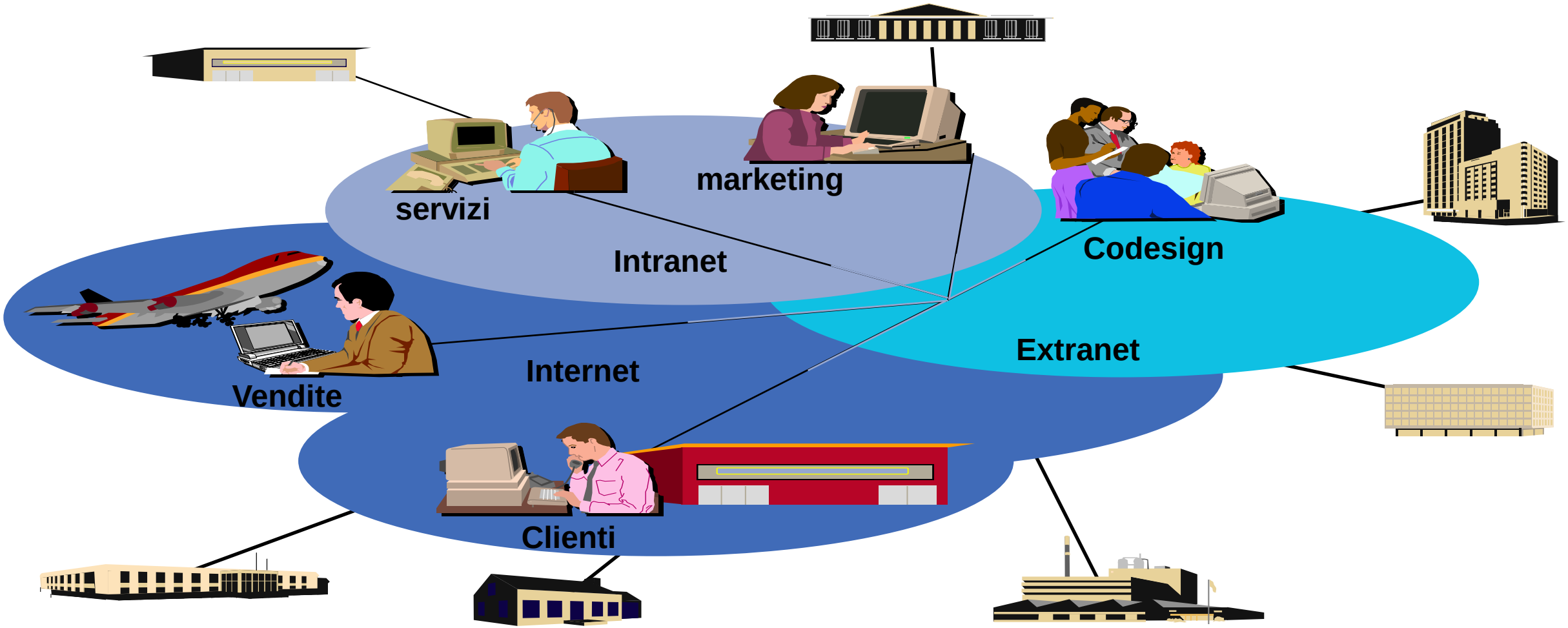
- **la cancellazione**
- **la distruzione**

- Quindi anche la distruzione (fisica) dei supporti

L’azienda/ente informatizzata/o

- Nell’azienda od ente pubblico odierno l’IT è pervasiva
- I dati sono trattati nella maggioranza dei casi tramite IT
- I sistemi informatici sono presenti in tutta l’azienda
- Le normali operazioni di lavoro sempre più sono basate sull’IT
- Anche le comunicazioni con l’esterno avvengono sempre più tramite strumenti IT/ICT

L’azienda/ente informatizzata/o



Il sistema informativo

"L'insieme di **persone**, **apparecchiature**, **procedure aziendali** il cui compito è quello di **produrre le informazioni** che servono per **operare** nell'impresa e **gestirla**".

(M. De Marco)

Corrisponde all'inglese "Information System"

Componenti dei sistemi informativi

Pertanto un sistema informativo si suddivide in:

- **Risorse umane** (con organizzazione, ruoli, esperienze, ecc…)
- **Risorse tecnologiche** (sistema **informatico**, inglese “IT System”)
- **Risorse organizzative** (procedure, regolamenti, workflow, ecc…)

Componenti del SI (secondo ITIL): le 4 P

- **P**ersone (People)
- **P**rocessi (Processes)
- **P**rodotti e tecnologia (Product & Technology)
- **P**artner e fornitori (Partner & suppliers)

Framework standard oggi molto usati

- COBIT (Control Objectives for Information and related Technology) – versione 5 – 2012: Governance e Audit Globale
- ITIL (Information Technology Infrastructure Library) – versione 3/2011 – 2011: Progettazione e Gestione dei servizi
- TOGAF (The Open Group Architecture Framework) – versione 9.1 – 2011: Architetture

Le qualità dell'accesso ai dati

Le 5 qualità dei dati per il GDPR

- Riservatezza
- Integrità
- Esattezza
- Disponibilità
- Conformità

In sostanza… è necessario

conoscere e poter dimostrare a richiesta:

- **quali dati** vengono trattati e in che modo sono rappresentati,
- per **quale finalità** sono trattati
- entro **quali processi aziendali** sono trattati
- con **quali strumenti**, informatici e non, sono trattati
- chi (**quali persone** entro l'organizzazione) li trattano, con **quale ruolo**
- **quali strumenti di sicurezza** sono posti a garantire la riservatezza, la esattezza e la disponibilità di tali dati

Focalizziamo l’attenzione su…

- con **quali strumenti**, *informatici,* i dati sono trattati

- **quali strumenti di sicurezza** (informatici e non) sono posti a garantire la riservatezza, la esattezza e la disponibilità di tali dati

Le architetture IT per conservazione ed accesso ai dati

L’architettura

“L’insieme dei ***concetti fondamentali*** e delle ***proprietà*** del sistema nel suo ambiente, contenuti nei **suoi elementi costitutivi**, nelle **relazioni che tra essi intercorrono**, e nei **principi del design** e nell'evoluzione di essi”

Definizione dallo standard ISO 42010, derivato dallo standard IEEE 1471

Architettura e sistema

Un sistema è un **insieme di elementi in relazione fra di loro** secondo **leggi ben precise**, che concorrono al raggiungimento di un obiettivo comune

L'architettura esprime la *descrizione formalizzata e completa di un sistema*

Architettura e sua descrizione

- L’architettura è intesa nel suo contesto di appartenenza

- E’ necessario sapere *dove il sistema si trova*
- ovvero *a quale ambiente appartiene*
- e *come interagisce con esso*.
- L’importanza delle proprietà dipende dal giudizio delle persone

Il componente base: il servizio IT

- L’architettura può essere scomposta in vari modi
- Da un punto di vista di componente logico, pensiamo allo scopo degli elementi componenti un’architettura, ossia alle funzionalità che essi offrono agli utilizzatori
- Ecco il concetto di servizio IT

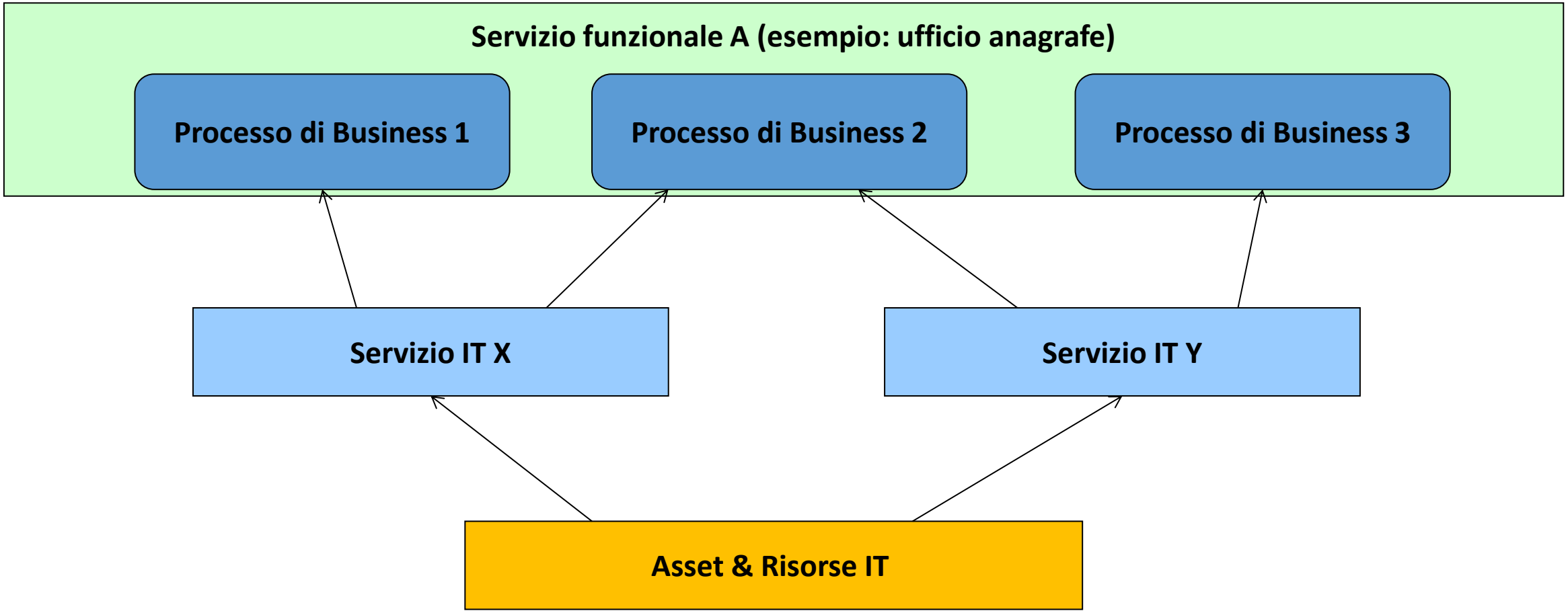
Servizi – IT come servizio (1/4)

Definizione di servizio:

- "I **Servizi** sono un mezzo per **fornire valore** ai clienti facilitando il conseguimento dei risultati che questi desiderano ottenere, senza la proprietà (diretta) dei **costi** e dei **rischi specifici**"

- *"People want a quarter-inch hole, not a quarter-inch drill" La gente vuole un foro da 4 pollici, non un trapano per fare un foro da 4 pollici (Prof. T. Levitt, Harward Business School)*

Servizi – IT come servizio (2/4)



Servizi – IT come servizio (3/4)

Definizione di **risultato** (**outcome**):

- Il risultato dell'esecuzione di un'attività, dello svolgimento di un processo o della erogazione di un servizio IT, ecc… Il termine viene utilizzato in riferimento ai risultati desiderati oltre che ai risultati effettivi
- Una definizione di servizio basata sui risultati porta le organizzazioni ad andare oltre l'allineamento tra Business e IT raggiungendo una effettiva **integrazione**
- Il dialogo e la discussione interna sul significato dei servizi è un passaggio elementare per giungere all'allineamento e alla integrazione con il Business del cliente

Servizi – IT come servizio (4/4)

- I clienti desiderano **ottenere i risultati** ma non assumersi la **responsabilità** o l'**ownership** di tutti i **costi** e **rischi** associati

Definizione di servizio IT

- Un SERVIZIO IT può essere definito come un insieme di funzioni fornite attraverso sistemi IT nel supportare uno o più aree dell'azienda (dipartimenti, agenzie, reparti, ecc.).

- Può essere costituito da software, hardware e mezzi di comunicazione, ma il cliente e utente lo percepisce come **una unica entità**.

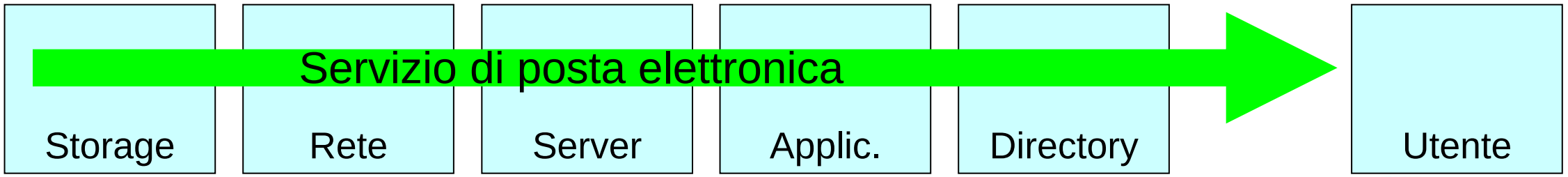
Definizione di sistema IT

- “Insieme di componenti di tipo hardware, software e mezzi di comunicazione che costituiscono, interamente o in parte, l’infrastruttura IT di un’Organizzazione”

- Può essere dedicato o condivisa fra Funzioni o Aziende/Clienti

L’interno del servizio IT

- Molti elementi contribuiscono al servizio
- Il cliente/utente lo percepisce come una sola entità
- In caso di problemi: “La posta non va!”
- Occorre conoscere e governare i componenti che contribuiscono al servizio



Configuration Item

- Nella terminologia del Configuration Management ITIL, i componenti IT ed i servizi con essi forniti sono noti come **Configuration Item** (CI).

- Tra i Configuration Item su cui si basa un servizio business sono presenti i servizi IT su cui si basa

- Lo stesso vale per i singoli servizi IT

Configuration Item

I Configuration Item possono includere

- l'hardware dei PC,
- i vari tipi di software,
- i componenti di rete sia attivi che passivi,
- i server,
- i processori,
- la documentazione,
- le procedure,
- i servizi (eventualmente di fornitori esterni)
- e tutti gli altri componenti IT che vanno controllati dall'Organizzazione IT.

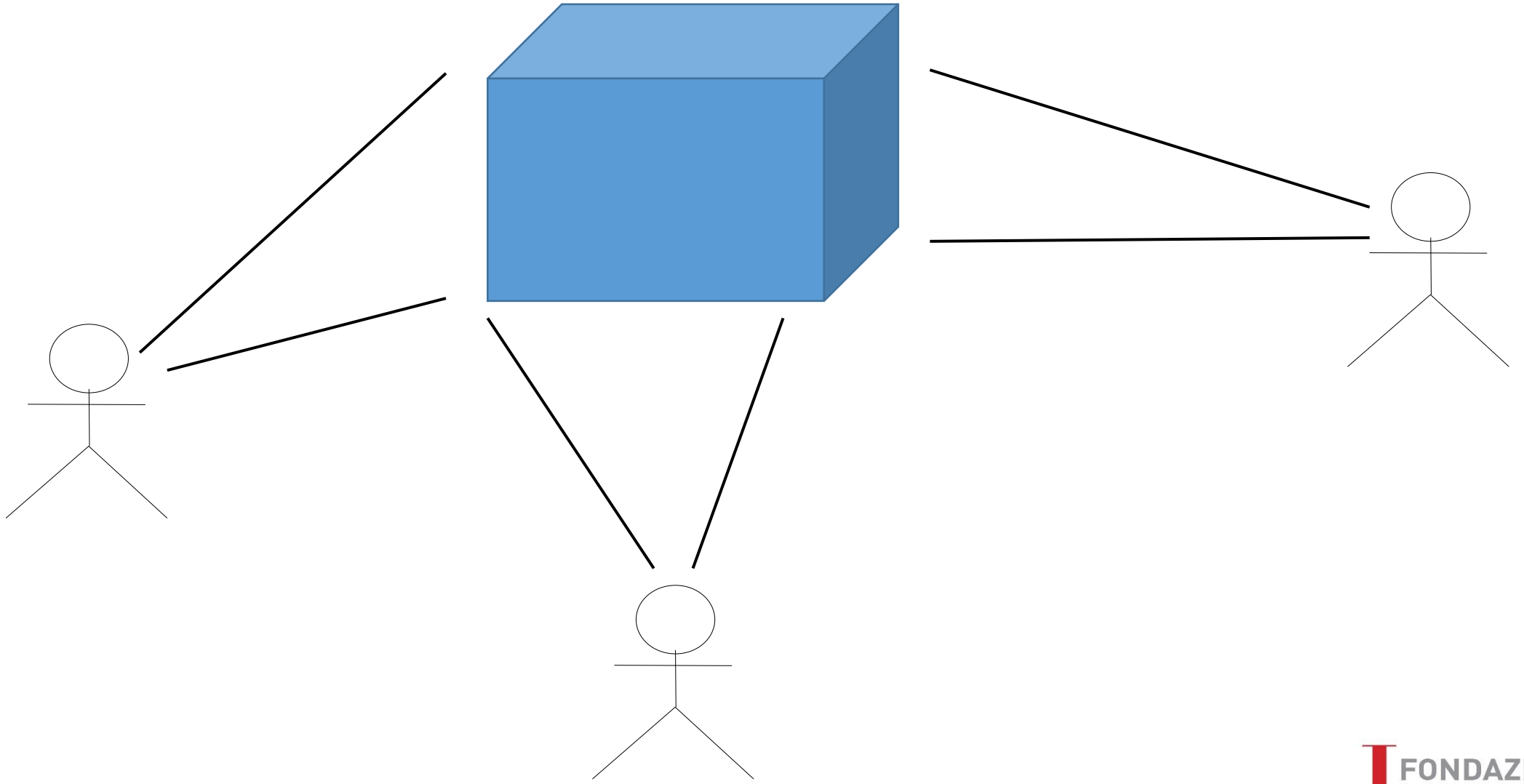
Livello di servizio e Accordi livello servizio (SLA)

- Il funzionamento normale di un servizio IT è definito da parametri (livelli di servizio)
- Di solito tali parametri sono oggetto di accordi formali (SLA)
- Esempi di parametri:
  - Tempo massimo di risposta di una interrogazione
  - Banda minima garantita in una connessione ADSL
  - Percentuale di tempo di disponibilità (es. 99,99%)
  - Tempo massimo di risoluzione di un guasto

Il concetto di vista (o prospettiva)

- Vista di un'architettura (o di un sistema)
- Formalizzato dallo standard ISO 42010
- Rappresenta il **punto di vista di uno stakeholder (parte interessata)**
- Da origine ad un modello "geometricamente" influenzato dal punto di vista

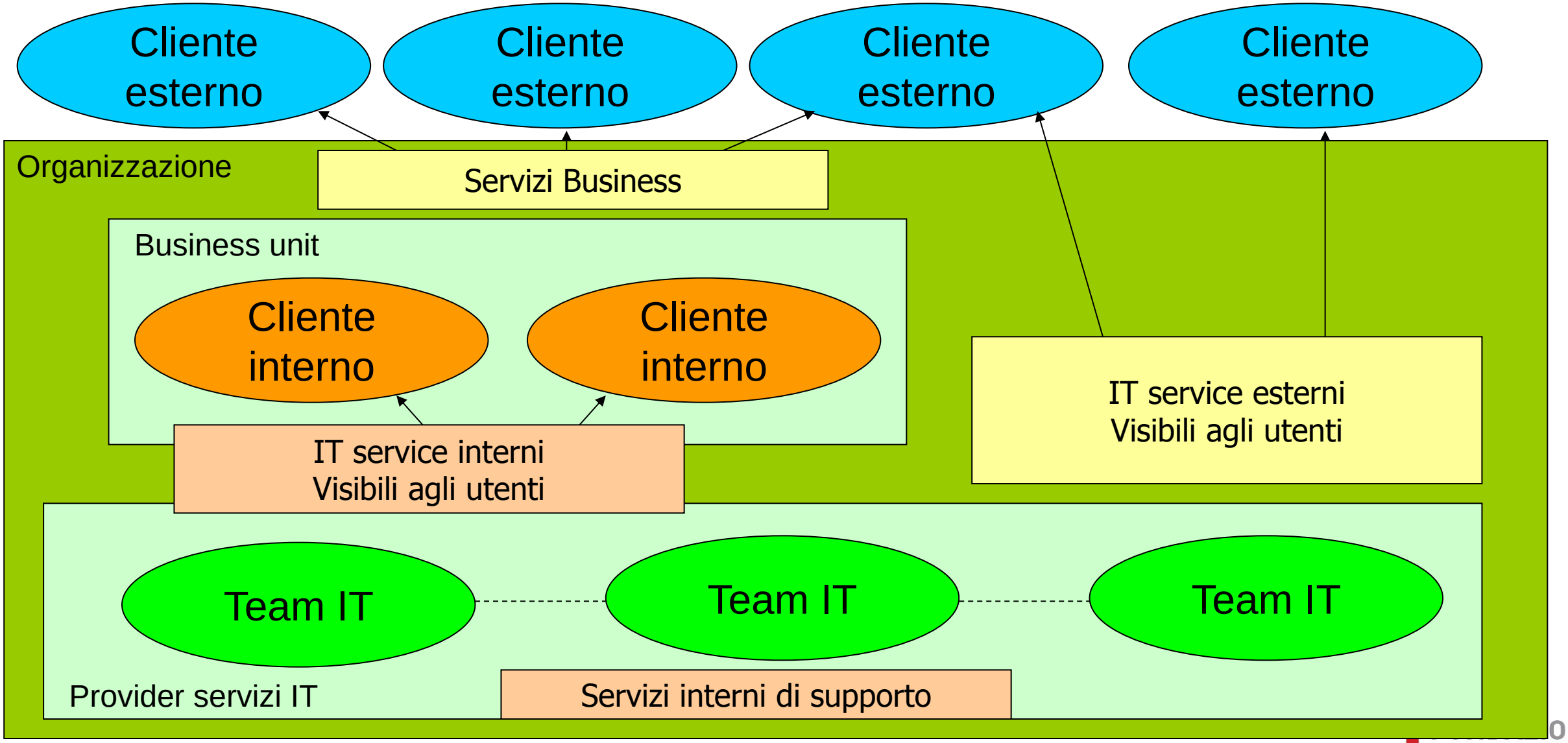
Il concetto di vista: esempio geometrico



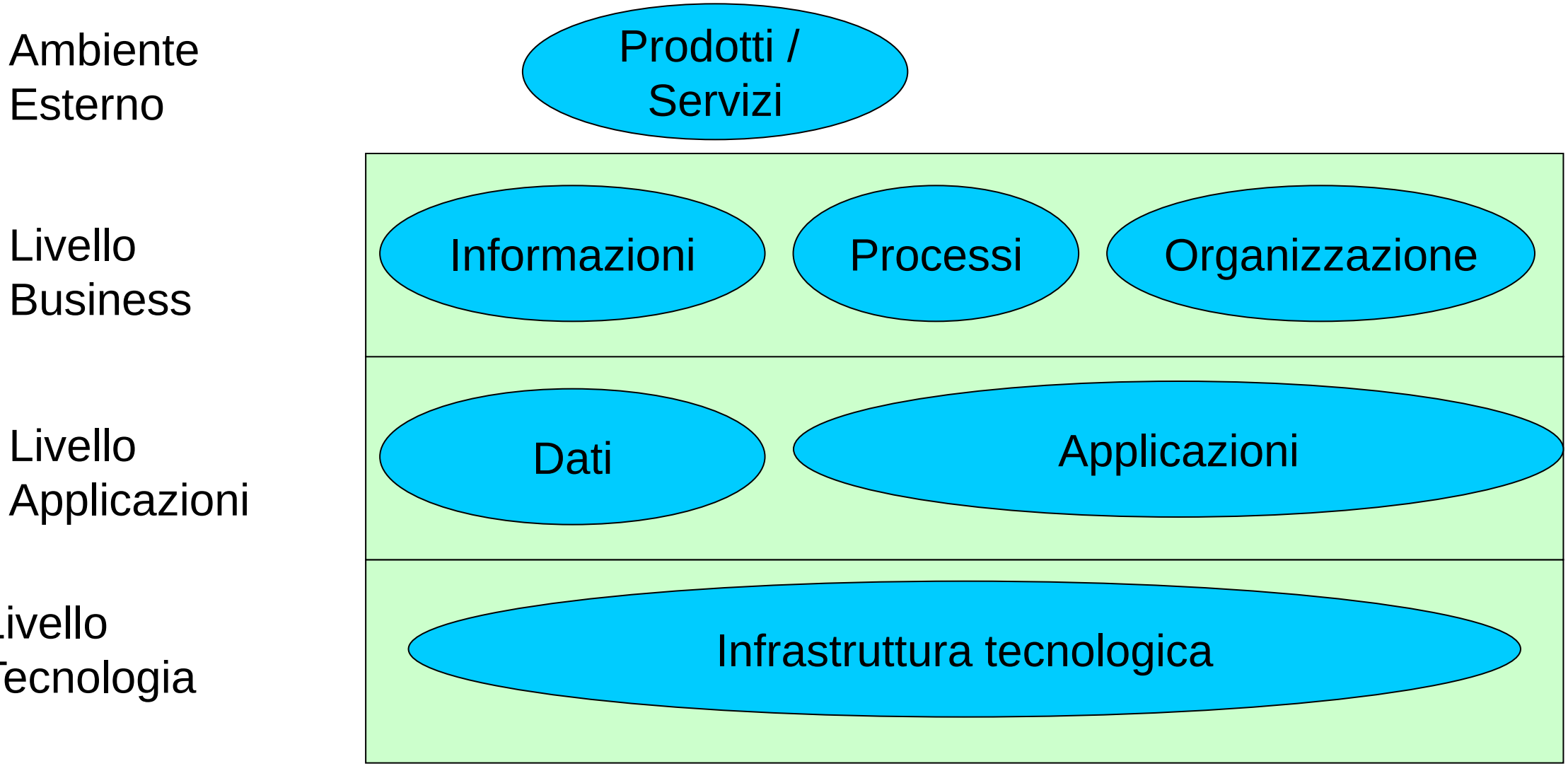
Le viste di Kruchten di un servizio IT

- *Vista logica* (logical view): che compito svolge
- *Vista dei casi d'uso* o *scenari* (scenarios): gli scenari di interazione utente-applicazione
- *Vista di processo* (process view): il processo gestionale cui appartiene
- *Vista di sviluppo* (development view): il codice sorgente che la genera
- *Vista fisica* (physical view): i componenti hardware e software che la formano

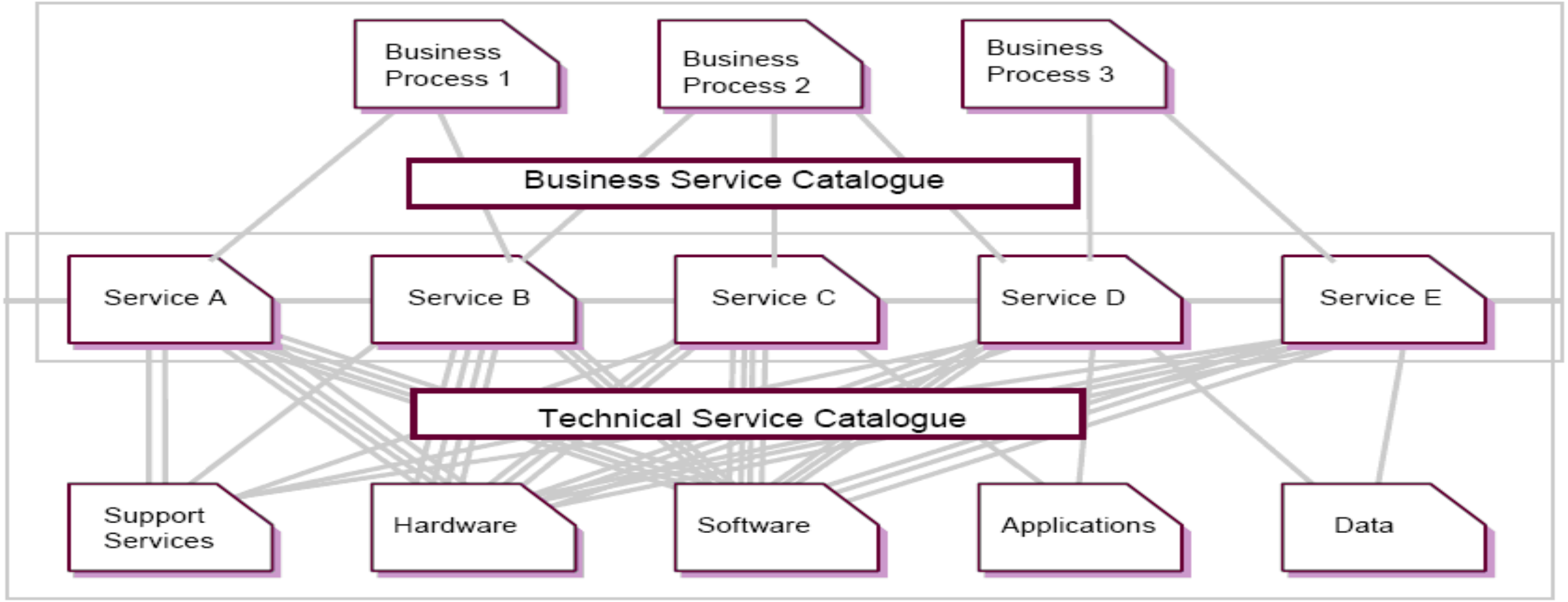
Insiemi di servizi



TOGAF/ArchiMate: lo schema dell'IT

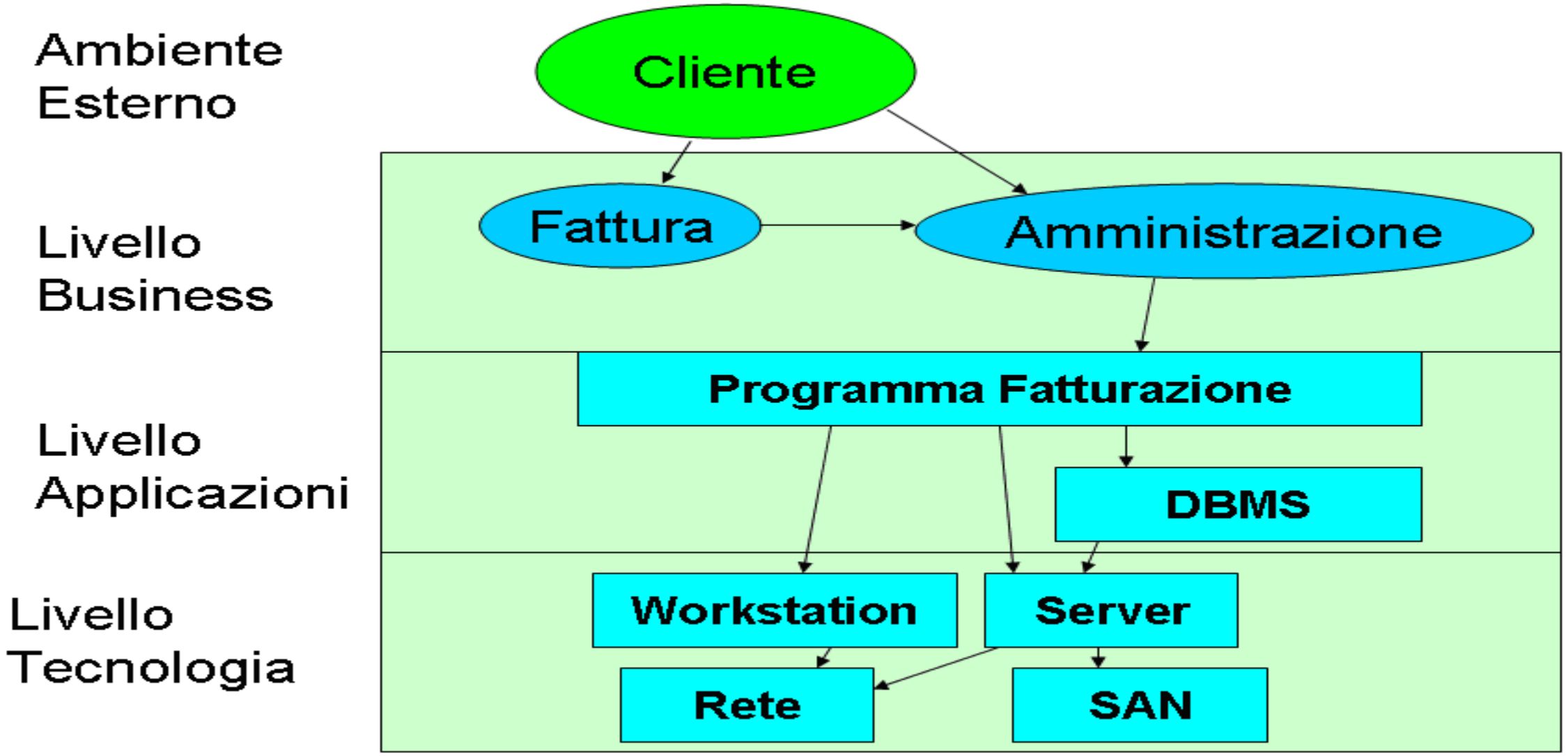


ITIL Service Catalogue (1/2)

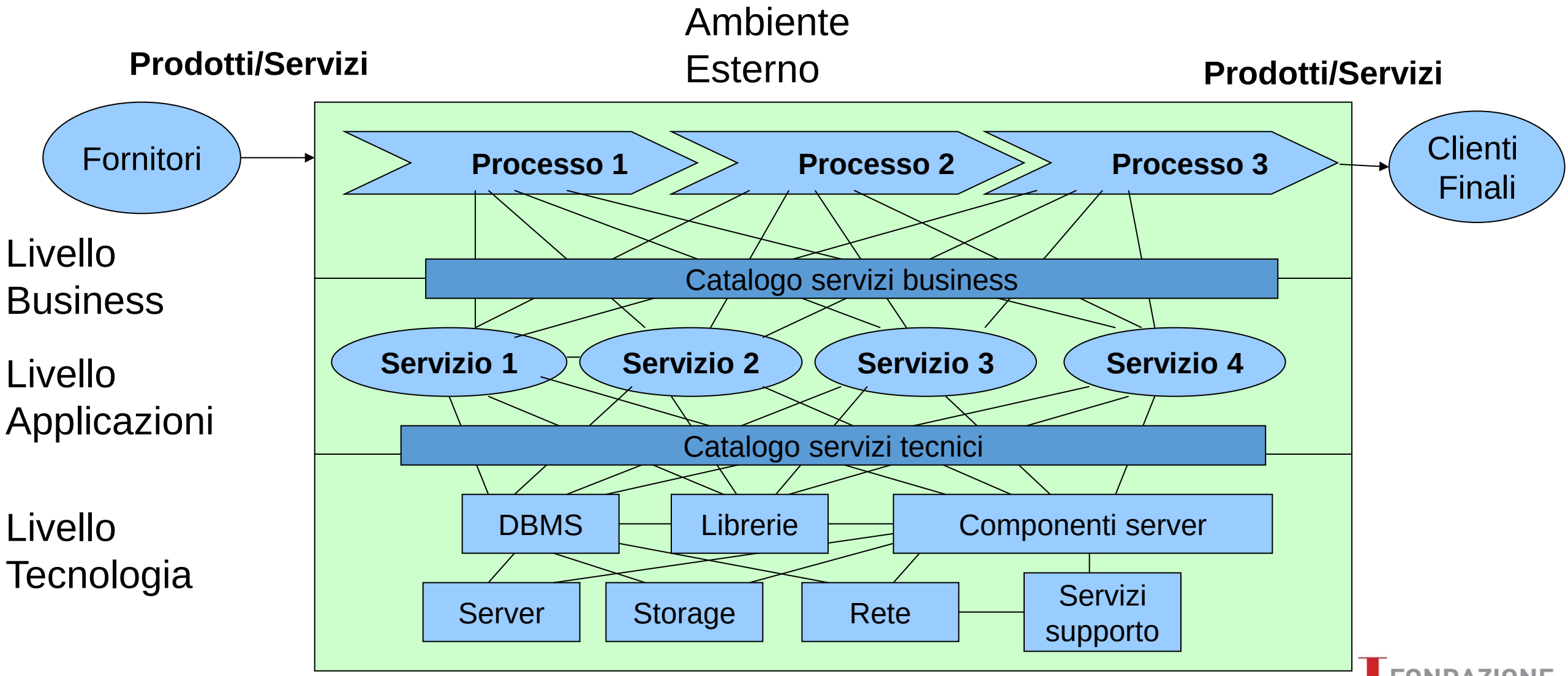


Fonte: ITIL – © Crown Copyright 2011 – Axelos 2014

ITIL Service Catalogue: applicazione



ITIL Service Catalogue (2/2)



Architettura (tecnica) delle applicazioni

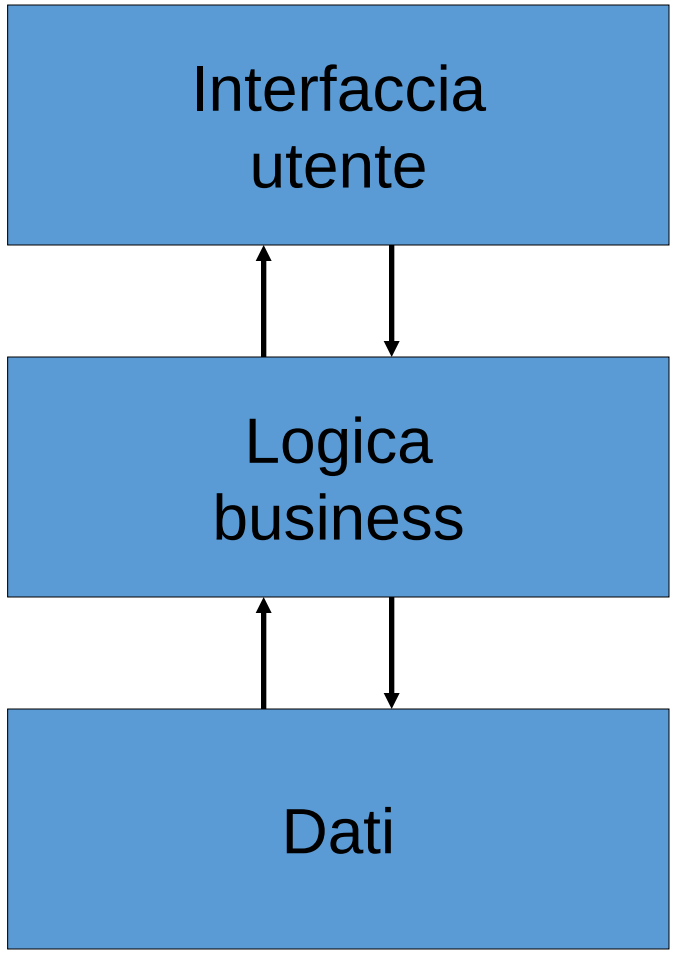
- Le applicazioni con interfaccia utente hanno un'architettura riconducibile a un modello comune

- Sono presenti alcuni componenti logici comuni
- Le tecnologie che li implementano possono essere diverse

Struttura base di un'applicazione

- **Interfaccia utente** (grafica): presentazione dei dati e interazione con l'utente
- **Regole funzionali** (logica business): le procedure che compiono le operazioni in base ai comandi ricevuti dal livello precedente
- **Dati**: su cui si deve agire e che devono essere memorizzati (durano oltre i programmi)

La struttura di un’applicazione interattiva



Le reti in azienda

Il termine rete è nato per indicare in modo generico

- un collegamento tra due apparecchiature (sorgente e destinazione)
- attraverso un mezzo trasmissivo
- per effettuare una trasmissione di informazioni

Le reti in azienda: oggi

- Attualmente per rete di calcolatori si intende un insieme di computer indipendenti,
- cioè che possono anche lavorare autonomamente
- ma collegati tra loro in modo da potersi scambiare informazioni (architettura distribuita)

Il modello client-server

- Un **programma server** opera su un **computer server** (server o host)
- Un **programma client** opera su una **postazione client** (postazione di lavoro o workstation, anche mobile)
- L'utente interagisce col programma client sulla postazione client
- Il programma client dialoga col server **via rete**

Il DBMS (1/2)

- Database Management System (Sistema di Gestione di Basi di Dati)
- Applicazione tecnica che gestisce insiemi di archivi strutturati di dati (basi di dati)
- Rende indipendente la rappresentazione tecnica dei dati dalle applicazioni con interfaccia utente che vi accedono
- Gestisce accessi simultanei in lettura e scrittura ai dati (accodamento)
- Rende le operazioni transazionali

Transazioni

- Operazioni di lettura o modifica dei dati nel DBMS
- Godono delle proprietà “ACID”
  - Atomicità: la transazione viene completata (commit) o annullata (rollback) tutta insieme
  - Consistenza: il DBMS passa da uno stato consistente ad uno stato consistente (es. Bonifico fra conti correnti)
  - Isolamento: ogni transazione deve essere eseguita in modo isolato e indipendente dalle altre transazioni
  - Durabilità o persistenza: una volta completata del programma i cambiamenti apportati non devono essere persi

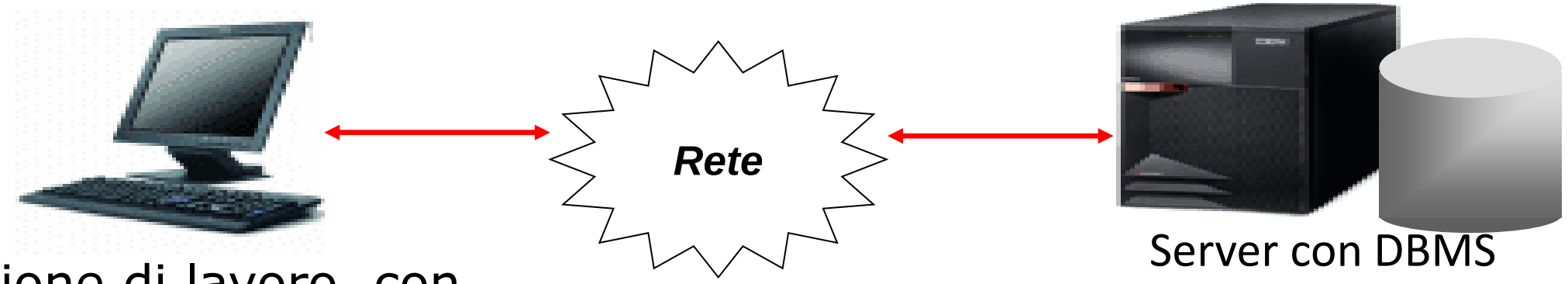
Il DBMS (2/2)

- Diverse tecnologie “storiche” (reticolari, gerarchici…)
- Tecnologia più diffusa: Relazionale, i dati sono organizzati a tabelle (RDBMS), l’accesso avviene attraverso il linguaggio SQL
- Nuova generazione: DB NoSQL, usati anche nei Big Data
- Diritti di accesso ai dati contenuti legati alle credenziali di accesso al DBMS
- I dati vengono salvati attraverso il backup

Big Data

- Grandi raccolte di dati, di solito presenti in cloud
- Indica anche tecnologie e metodologie per gestire questi dati
- Sono caratterizzate dalle proprietà 5 V
  - Volume
  - Velocità
  - Varietà
  - Veridicità
  - Valore

Client-server a 2 livelli

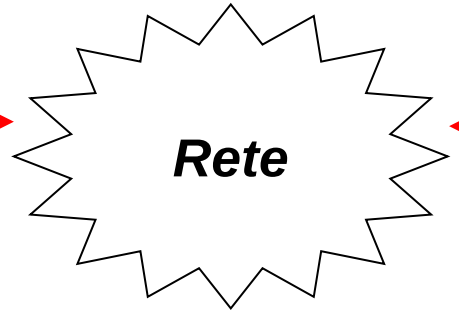


Postazione di lavoro, con applicazione client dotata di interfaccia utente

Server con DBMS

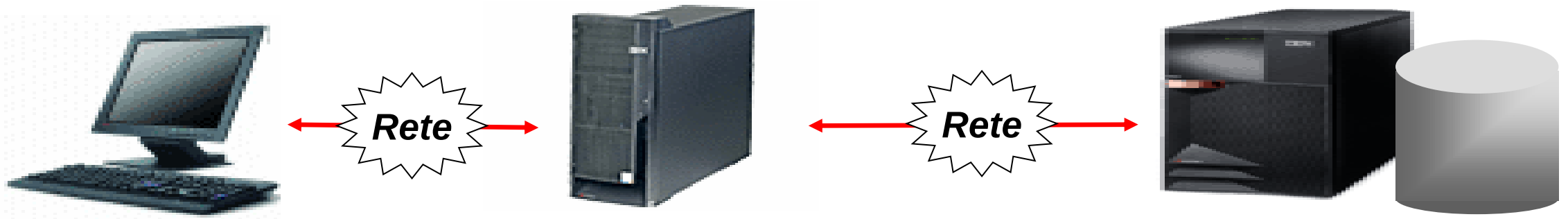
Terminale-Host (Mainframe)

Postazione di lavoro, con terminale 3270/5250



Mainframe con DBMS

Client-server a 3 livelli



Postazione di lavoro, con applicazione client dotata di interfaccia utente

Server con applicazione server

Server con DBMS

Client-server Web

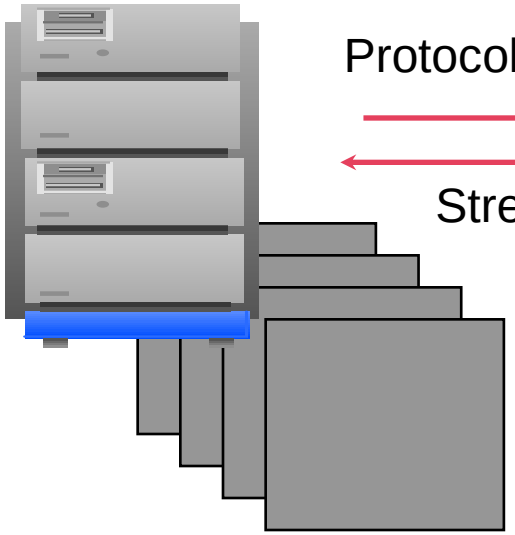
Postazione di lavoro
con Web Client
(browser)

HTTP request

HTTP response

Rete TCP/IP

Web Server

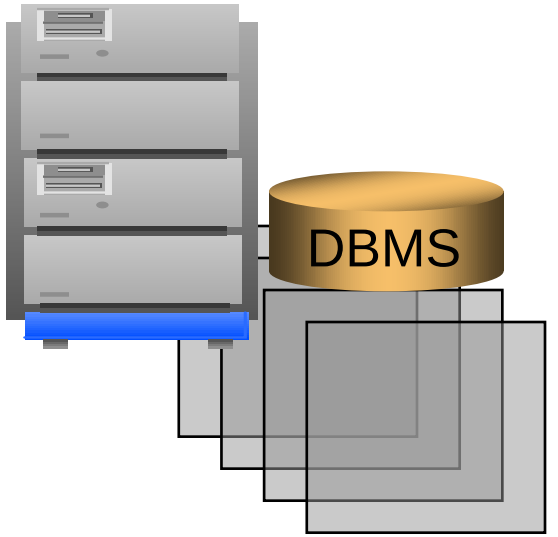


Documenti HTML e
immagini

Protocolli specifici

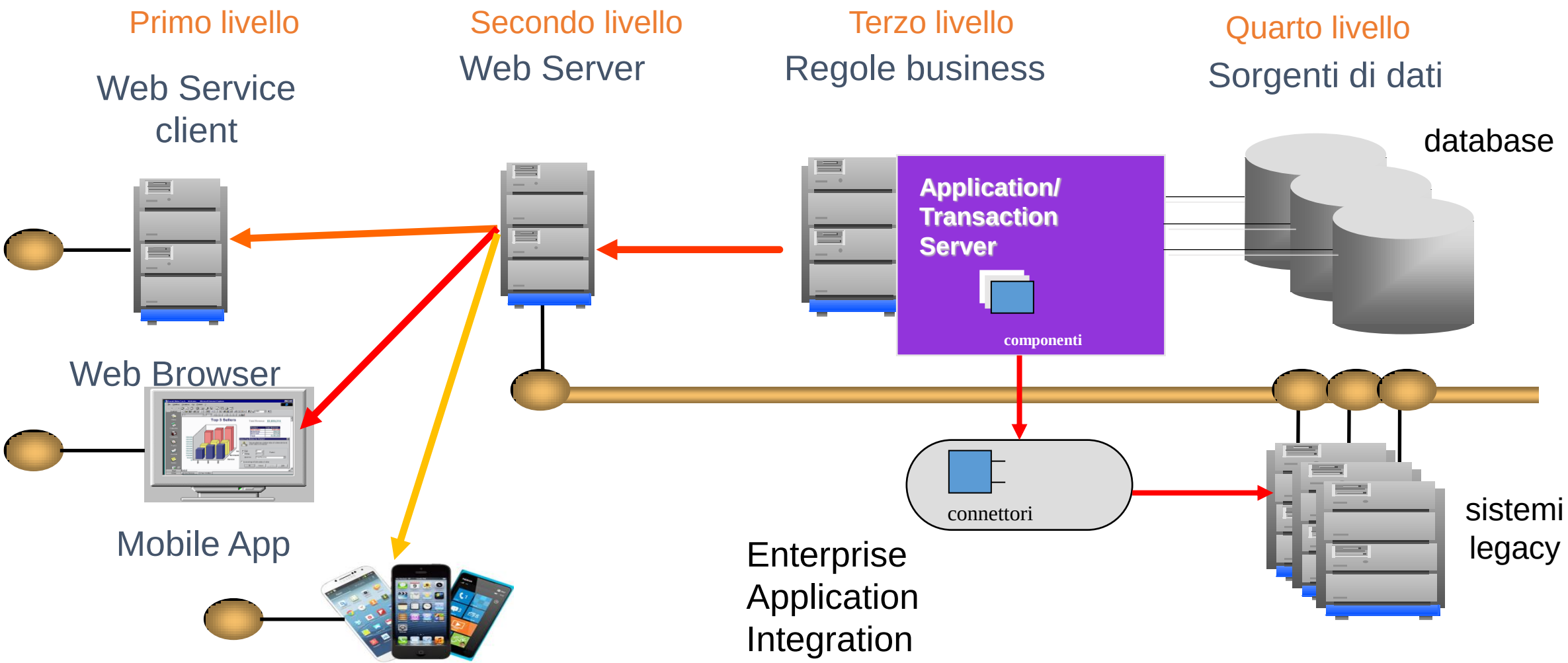
Stream dinamico
HTML

Application
Server con DBMS

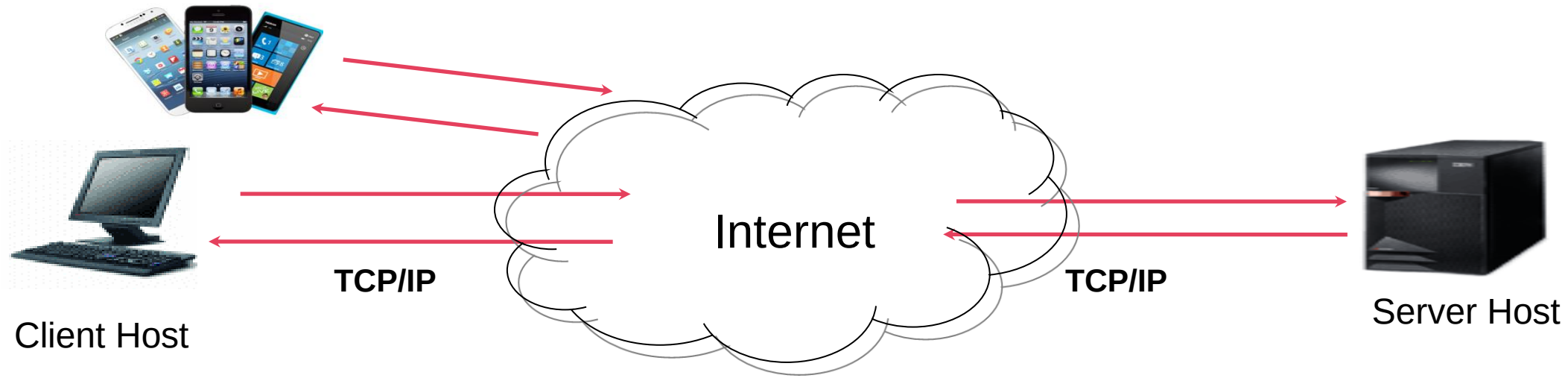


Template HTML
+ Contenuti HTML
generati dinamicamente

Client-server Web multilivello



Tipiche connessioni interattive



- **Desktop**: interazione tipica con applicazioni Windows e Mac
- **RDP**: terminale grafico/desktop remoto (teleamminnistrazione, postazioni di lavoro virtuali)
- **telnet**: terminale a caratteri (teleammnistrazione)
- **tn3270/tn5250**: terminale a caratteri (banca, gestionali)
- **Web Browser**: terminale HTML (siti web, applicazioni web)
- **Mobile/App**: App su tablet o smartphone (tantissime applicazioni)

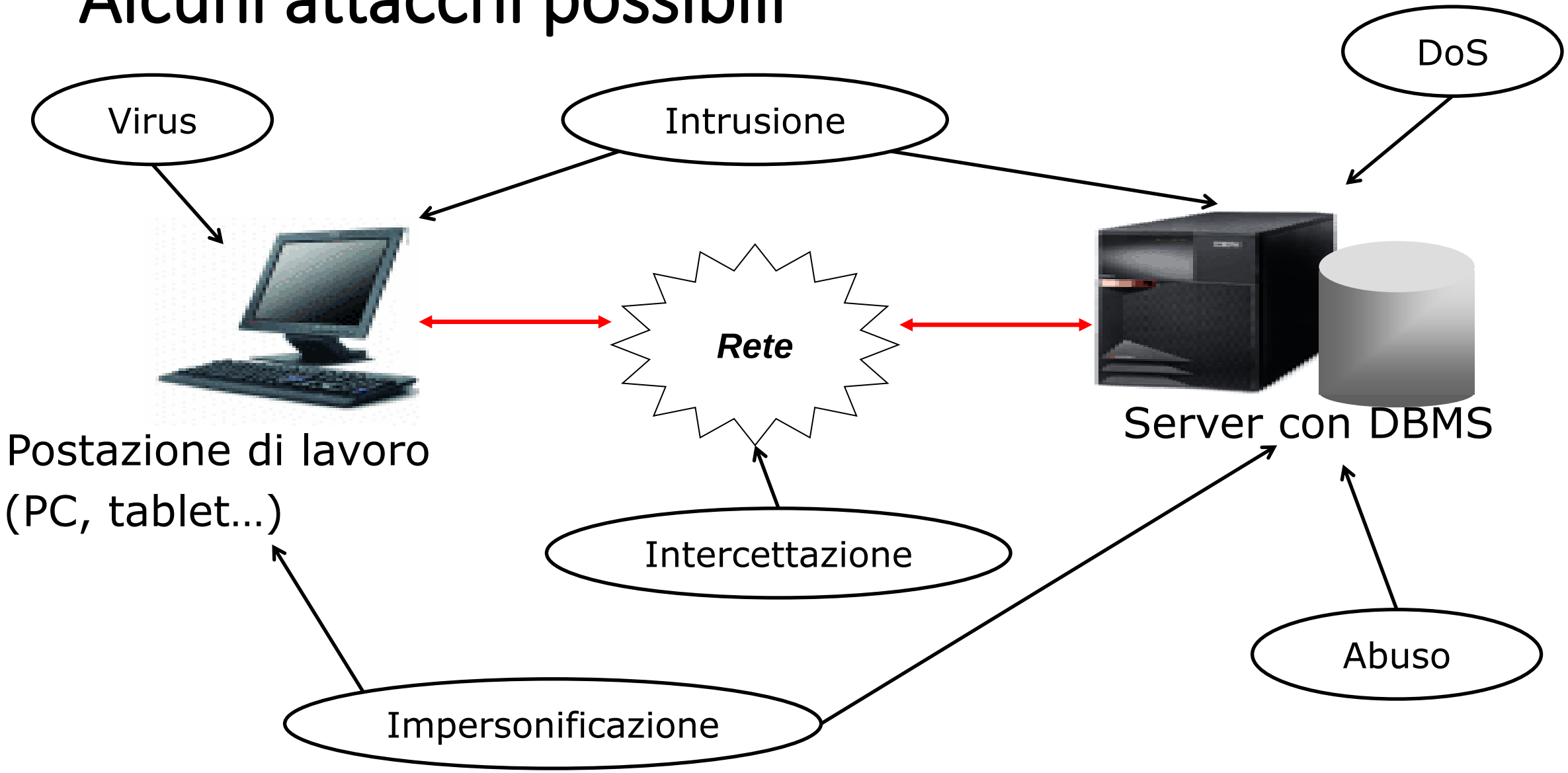
L’accesso sicuro ai dati

Obiettivi di sicurezza IT, ovvero riduzione impatti

Valutazione Impatto in termini di mancanza di:

- Riservatezza
- Integrità
- Esattezza
- Disponibilità
- Conformità

Alcuni attacchi possibili



Protezione dei dati (personali): riservatezza

- Quali sono i dati?
- Dove sono i dati?
- Come si accede ai dati?
- Come si interpretano i dati?

Il formato dei dati

- Formato testo
- Pagine Web/HTML
- Formato documenti (es. MS-Office)
- Tabelle all'interno di DBMS
- Export/dump DB
- Formati proprietari di applicativi
- Immagini fisse
- File audio
- Filmati
- …

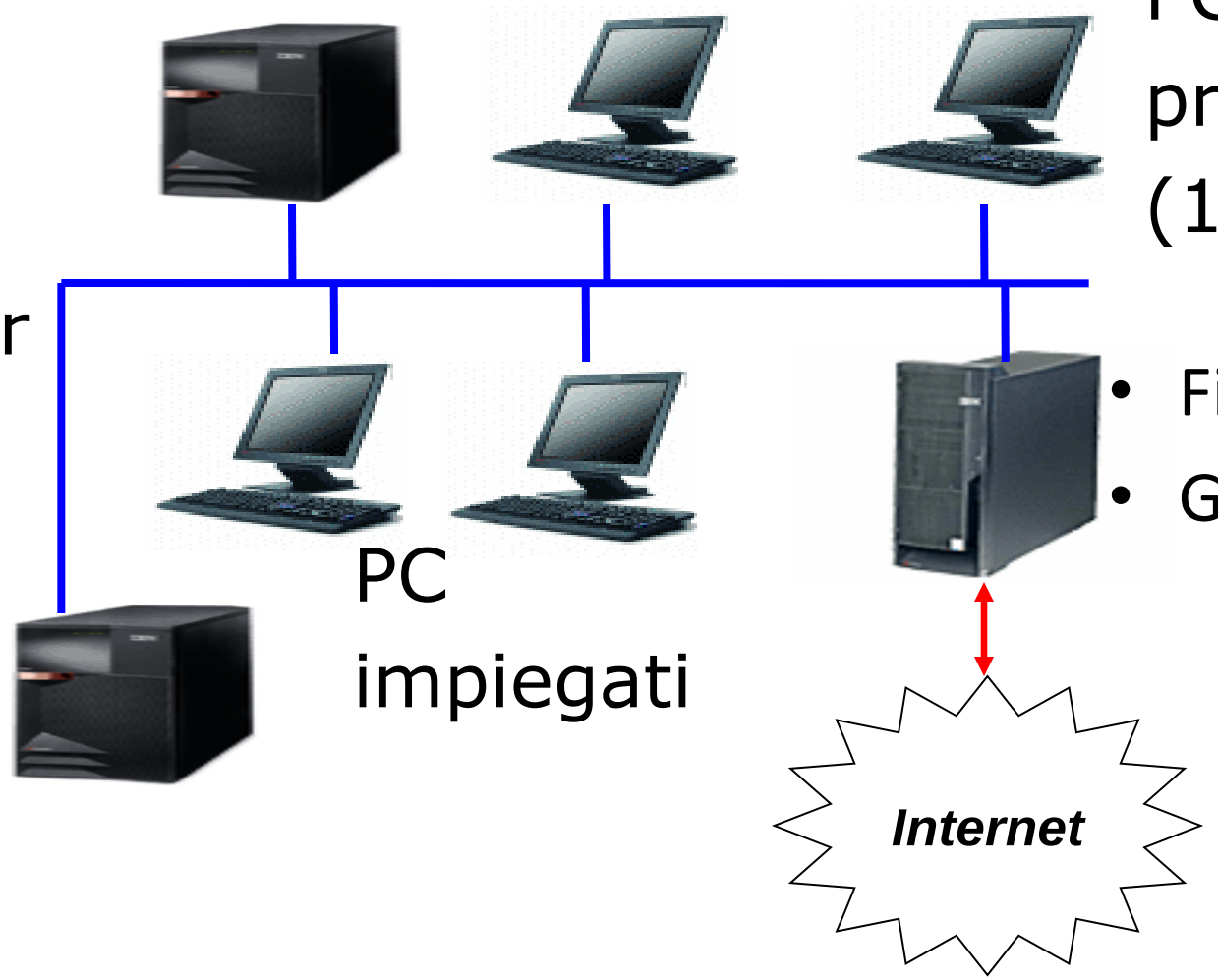
Sicurezza dei formati

- Anche nel caso di formati binari proprietari la sicurezza non è garantita
- Un abile hacker, se accede ai file, è in grado di ricostruirne i tracciati
- L'unica garanzia è la **cifratura** o **crittografia** dei dati

Studio di professionisti associati

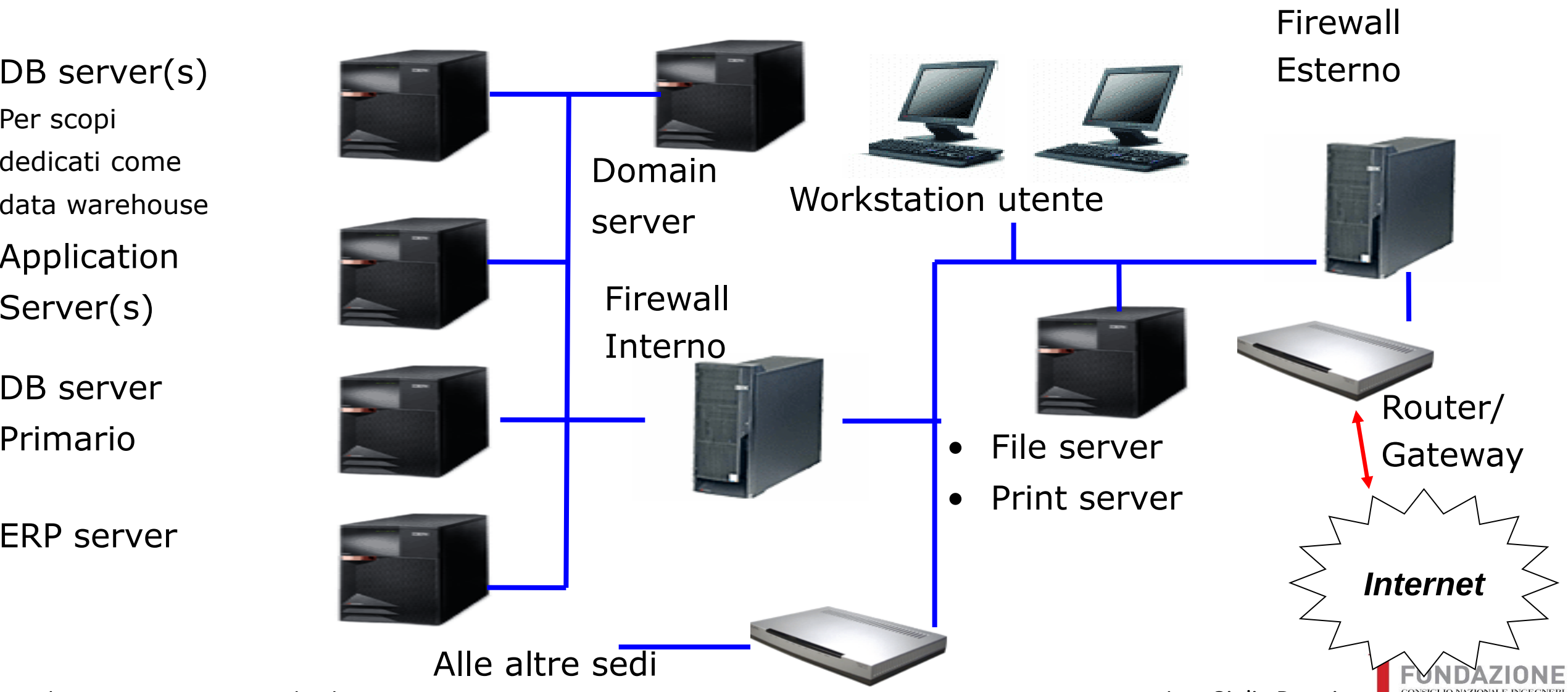
- File server
- Print server
- DB server
- Domain server

- Mail server



- Firewall
- Gateway

Media azienda Italiana



Banca (centro EDP)

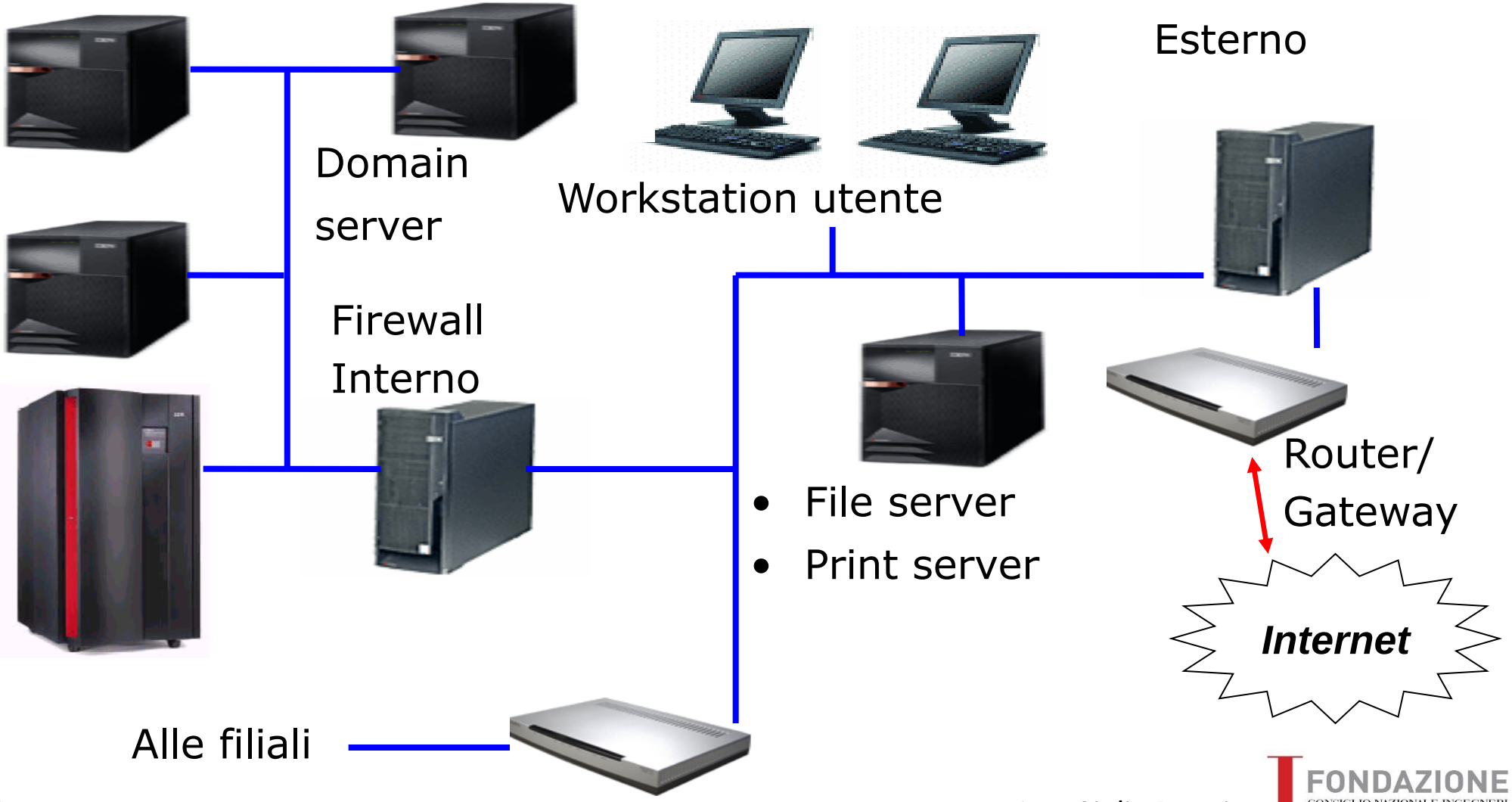
DB server(s)

Per scopi dedicati come data warehouse

Application Server(s)

Mainframe(s)

- DB primario
- Applicazioni legacy



Tecniche di pseudonimizzazione

Pseudonimizzazione (da art. 4 GDPR)

Il trattamento dei dati personali in modo tale che i dati personali **non possano più essere attribuiti a un interessato specifico** senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Pseudonimizzazione con Mascheramento

I dati personali sono mascherati (es cifrati)

Gli altri dati, utili per i trattamenti, sono in chiaro

Cognome	**Nome**	**Indirizzo**	**CAP**	**Città**	**Prodotto**	**Data Acquisto prodotto**
HozeRE	AAnXerz	ZAE	00XXX	Roma	TV	22/11/2018

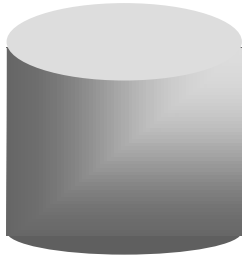
Pseudonimizzazione con Token/ID

I dati personali sono separati e conservati in un archivio separato

Esiste una tabella di congiunzione che permette il collegamento

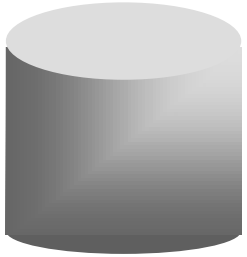
L'accesso ai dati e alla tabella di congiunzione è limitato solo ai ruoli effettivamente aventi diritto

DB dati personali



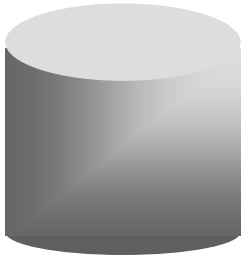
ID_Persona	Cognome	Nome
10	Destri	Giulio

DB congiunzione



ID_Persona	Token
10	3090

DB prodotti acquistati



ID_Prodotto	Prodotto	Token
123	TV	3090

La cifratura e la sua «forza»

Crittografia o cifratura

Operazione di traduzione di un dato dallo status di leggibile a tutti (dato «in chiaro») a quello di leggibile solo ai possessori di uno strumento chiamato **chiave** (dato cifrato)

I termini

- Testo in chiaro = testo originale
- Testo cifrato o codificato = testo crittografato
- Cifratura o codifica = operazione di “traduzione” del testo da “chiaro” a “cifrato”
- Decifratura o decodifica = operazione inversa
- Chiave = entità usata per la codifica

Un esempio “classico”: l’algoritmo di Cesare

- Si basa sullo scorrimento (rotatorio) dell’alfabeto dei caratteri
- Si dice ordine dell’algoritmo il numero di posizioni di cui viene ruotato l’alfabeto durante l’operazione

Esempio di algoritmo di Cesare

- Sia 4 l'ordine
- Si suppone che lo spazio sia il carattere avente indice zero
- La frase "Se magna" diventa "Widqekre"

Crittoanalisi

- Scienza che studia la decifratura di dati senza conoscere la chiave con cui sono stati cifrati
- Usa diversi approcci

- L'approccio di tentativi esaustivi è detto «a forza bruta»

Limiti dell'algoritmo di Cesare

- Studiando la frequenza dei caratteri del testo cifrato si può intuire come funziona
- E' quindi facile indovinare che si tratta di uno scorrimento
- E' sensibile ad un attacco a "forza bruta" ossia per prove esaustive delle combinazioni possibili dello scorrimento

Evoluzione: scorrimento con chiave

- In questa variante lo scorrimento dei singoli caratteri del messaggio avviene in base ai valori dei caratteri di una “parola chiave”
- Pertanto ogni carattere del messaggio risulta traslato in modo diverso rispetto agli altri
- E’ evidente la maggiore robustezza

Esempio di scorrimento con chiave

- Testo in chiaro: “fido”
- Parola chiave: “abcd”
- Testo cifrato: “gkgs”

- Più lunga è la chiave, più sicura è la protezione rispetto ad attacchi a “forza bruta”

Applicazione della crittoanalisi all'algoritmo di Cesare con chiave

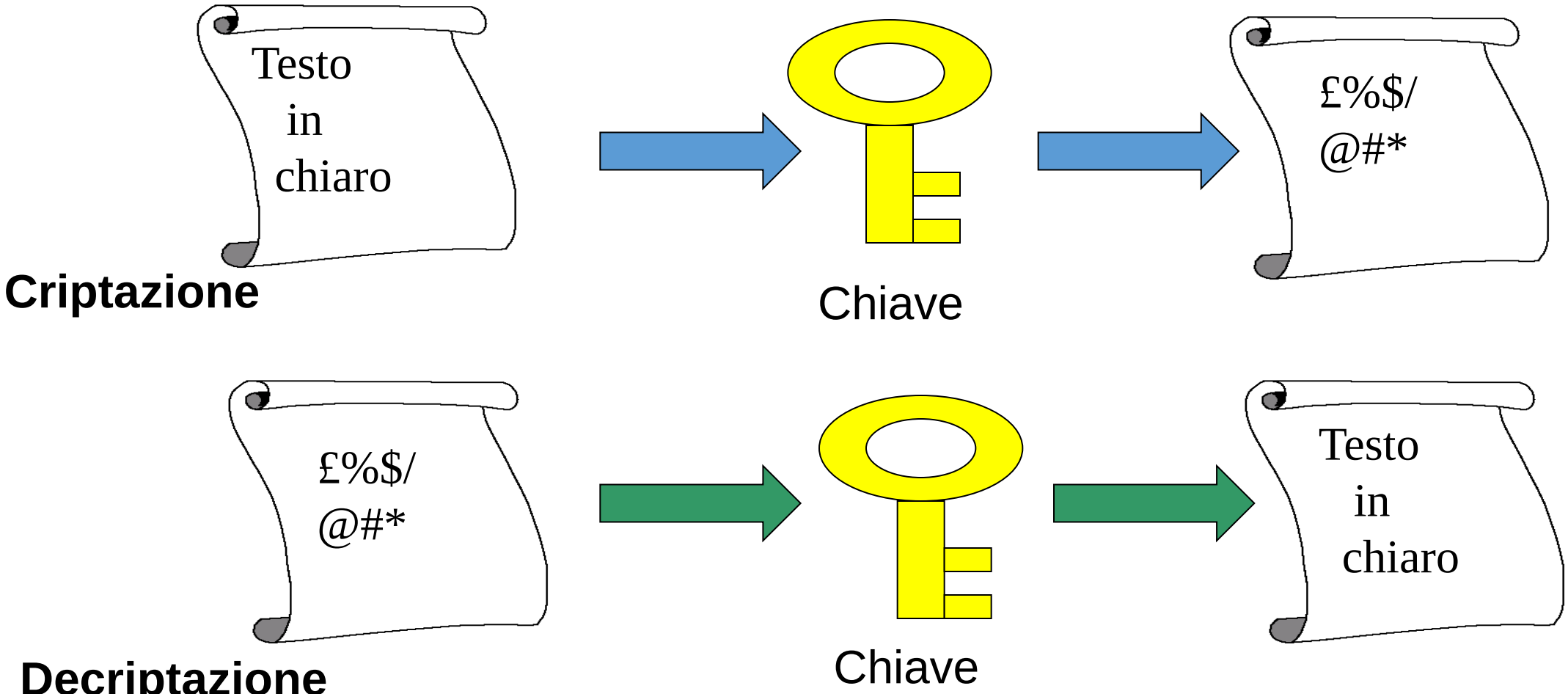
- Con l'uso dell'algoritmo di Cesare a chiave è più difficile applicare l'analisi basata sulla frequenza di occorrenza dei caratteri

- E la difficoltà è maggiore tanto maggiore è la lunghezza della chiave

Attacchi possibili ad un metodo crittografico

- Confronto fra testo in chiaro e testo crittografato
- Individuazione del metodo
- Individuazione della chiave

Chiave simmetrica: lo scenario



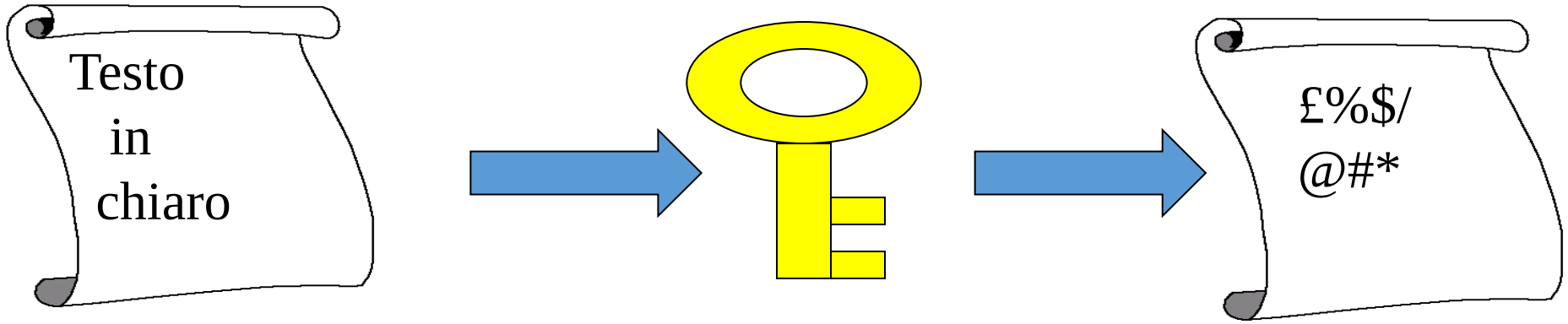
Chiave simmetrica

- La stessa chiave viene usata sia per la criptazione sia per la decriptazione
- Con lunghezza delle chiavi >= 128 bit il sistema è al sicuro da attacchi a forza bruta
- Se la chiave viene intercettata i messaggi non sono più sicuri
- Non garantisce l'autenticazione del mittente

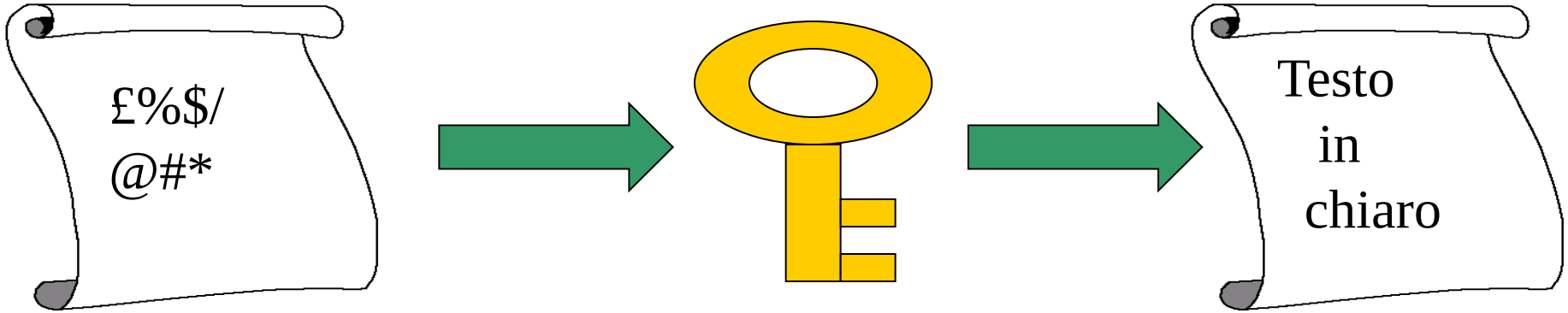
Alcuni standard di crittografia simmetrica

- DES (Data Encryption Standard), obsoleto
- 3-DES
- Blowfish
- IDEA

Chiavi asimmetriche: lo scenario



Codifica



Decodifica

Chiave asimmetrica

- Il ruolo delle chiavi è duale: ciò che viene crittografato con una può essere decrittato solo con l'altra
- Si deve conoscere solo una chiave (pubblica)
- Usando la mia chiave privata e quella pubblica del destinatario, garantisco contemporaneamente autenticazione e sicurezza
- Numero di bit elevato (>= 1024)

La funzione della crittografia asimmetrica

- E = azione di crittografia
- D = azione di decrittografia
- M = messaggio originale

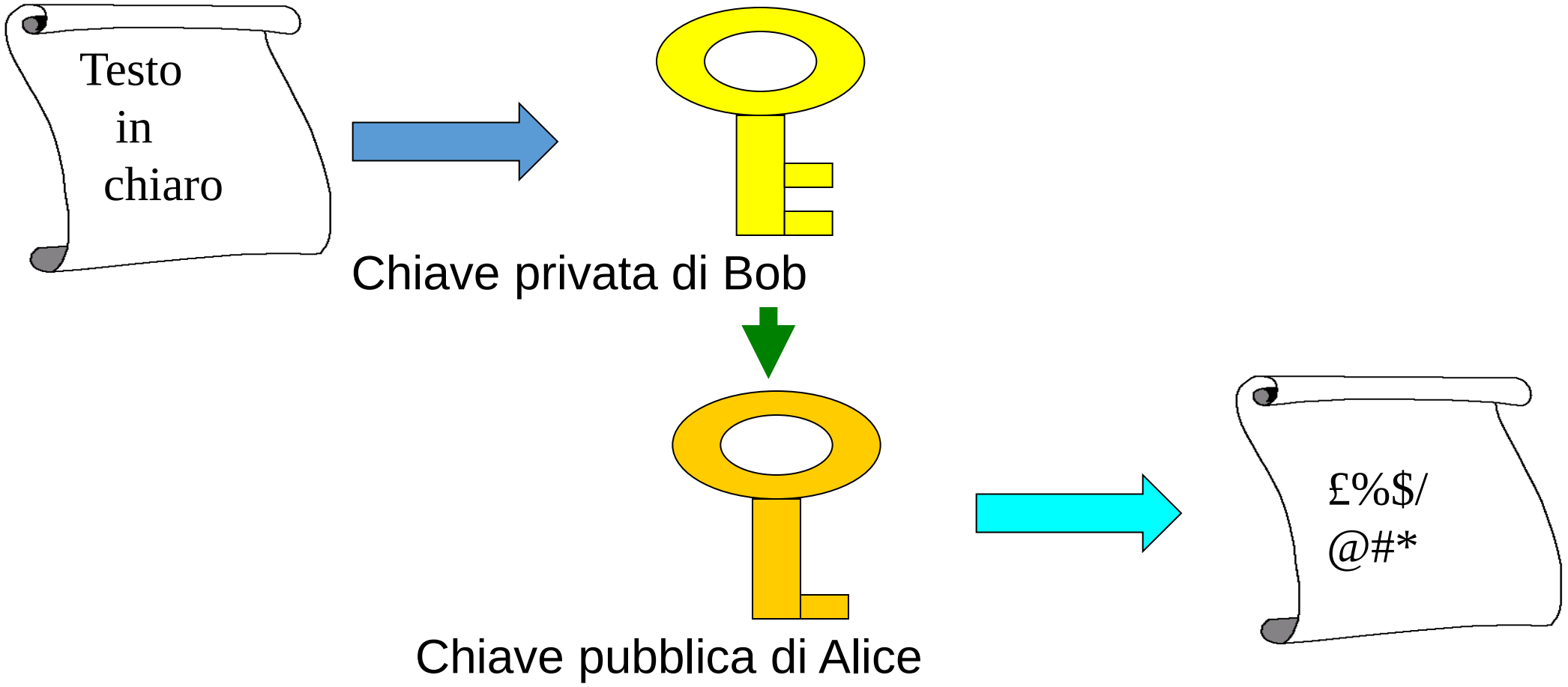
- D(E(M)) = M
- E(D(M)) = M

Elenchi pubblici garantiti

- Le chiavi pubbliche possono essere raccolte in opportuni siti, gestiti da Autorità di Certificazione, a disposizione degli utenti

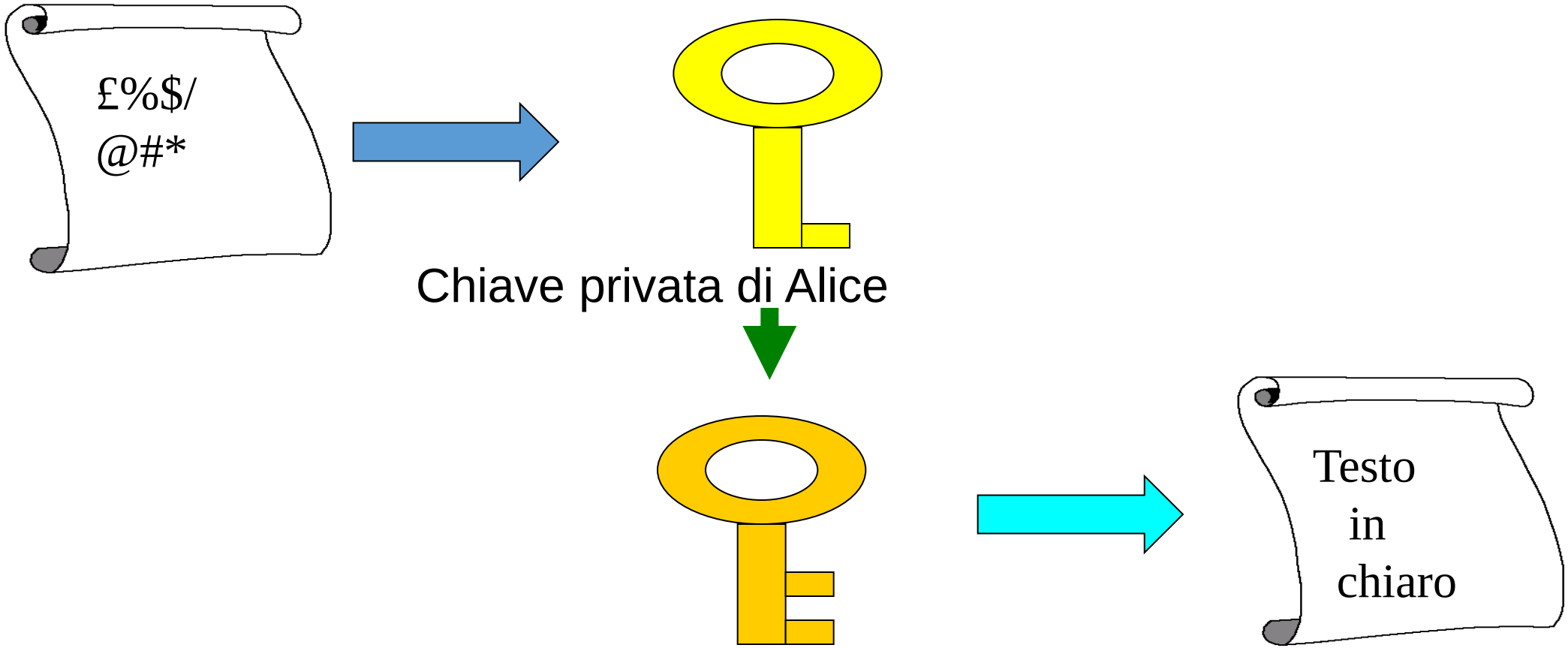
- Si deve conoscere solo una chiave (pubblica)

Doppia chiave - codifica



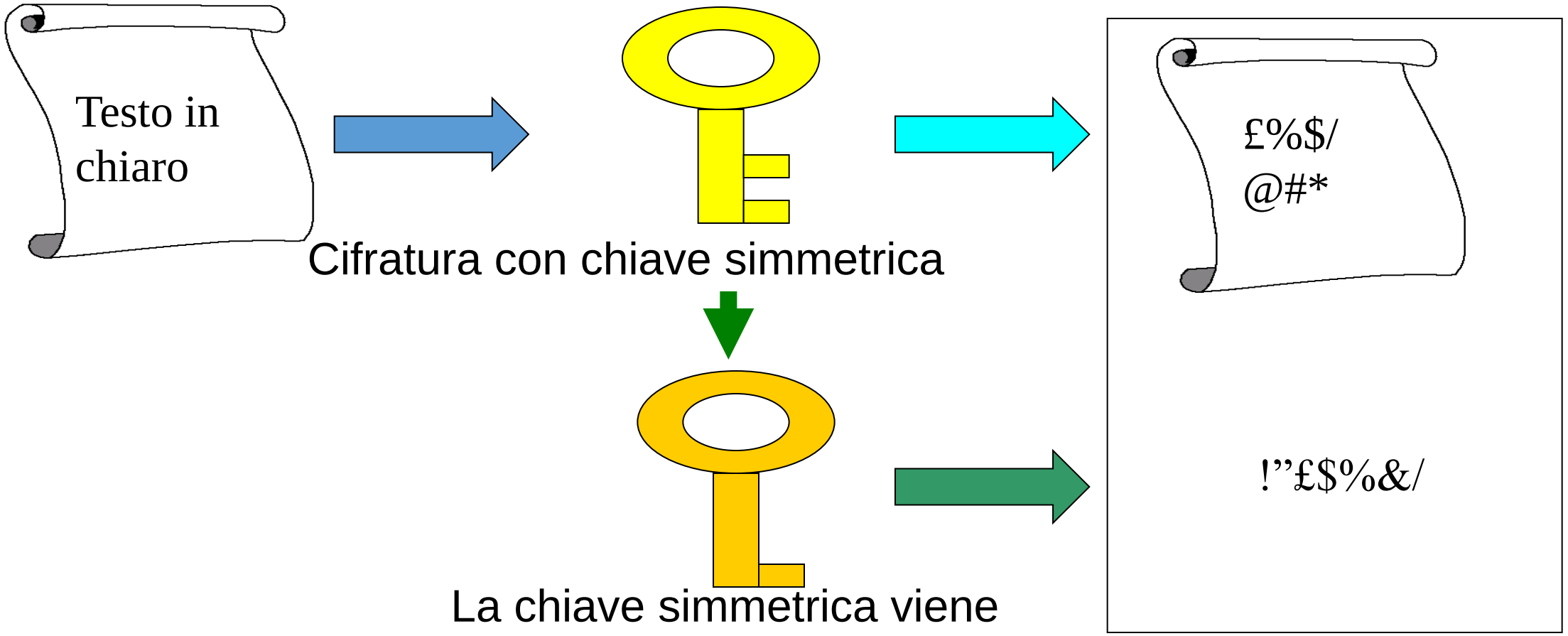
Codifica da parte di Bob

Doppia chiave - decodifica



Decodifica da parte di Alice

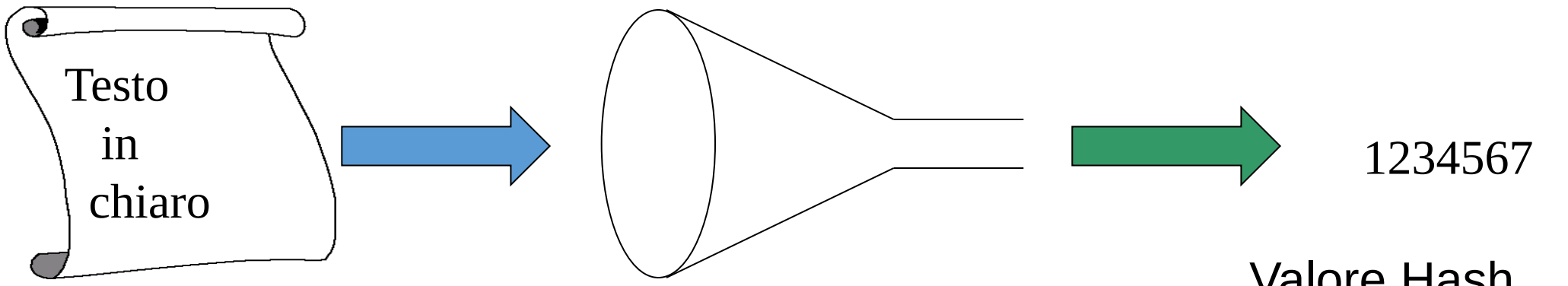
Message Enveloping



Funzione di Hash

Dato un documento in forma digitale, la funzione di hash produce in uscita un numero binario in corrispondenza pressochè biunivoca con esso (impronta del documento)

Applicazione della funzione di Hash

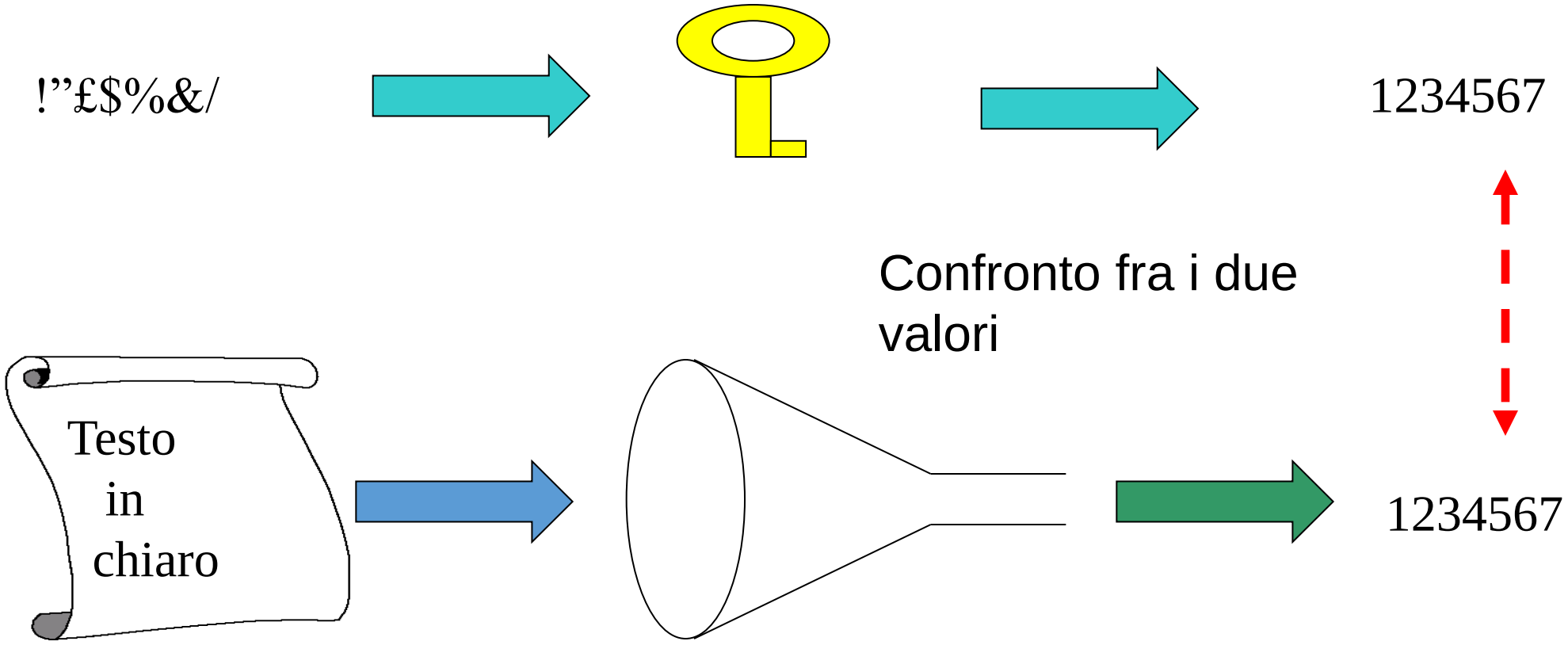


Messaggio

Funzione Hash
monodirezionale

Valore Hash
Univocamente
Associato al
Messaggio

Applicazione della funzione di Hash -verifica

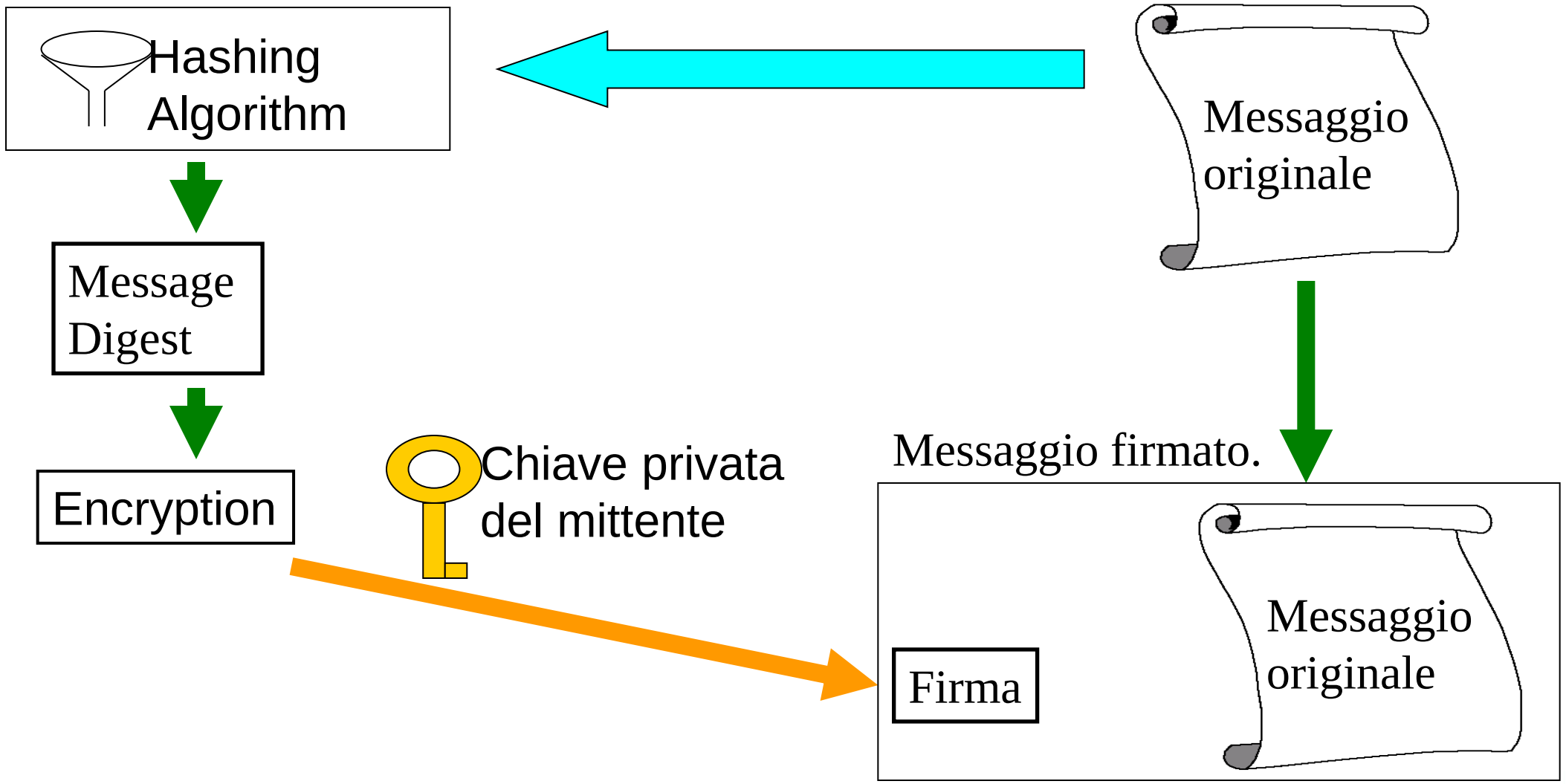


Nonce

- Protezione contro gli attacchi a replica

- Basato su una informazione usata una sola volta
  - Interi sempre crescenti (non ciclici)
  - Timestamp
  - Timestamp+numero casuale

Firma di un messaggio



Caratteristiche da mantenere

Riservatezza del messaggio

Integrità del messaggio

Disponibilità del messaggio

Identità del mittente

Timestamping

Non ripudiabilità

Nodi della rete coinvolti nella transazione

Tecniche per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

Definizione di Vulnerabilità

- **Debolezza di una risorsa (asset) o di un gruppo di asset che può essere sfruttato da una o più minacce.**

- **MINACCIA:** la possibilità di verificarsi di un evento negativo che fa leva su una vulnerabilità del sistema.
- **IMPATTO:** danno potenziale derivante dall'accadimento di un evento negativo.

Definizione di Vulnerabilità IT

- **Debolezza intrinseca del sistema informativo** o del **sistema informatico** tale che, qualora avesse luogo una minaccia che la sfrutti, condurrebbe ad una **violazione di uno degli obiettivi di sicurezza** (Riservatezza, Integrità, Disponibilità…)

Vulnerabilità IT: esempi

- Vulnerabilità dovute alla collocazione geografica del sistema informatico (es: terremoti, inondazioni…)
- vulnerabilità dovute a errori sistematici presenti nell'hardware o nel software (errori di progettazione)
- vulnerabilità dovute a possibili malfunzionamenti accidentali dell'hardware,
- vulnerabilità dovute a deficienze nelle procedure di utilizzo da parte degli utenti.

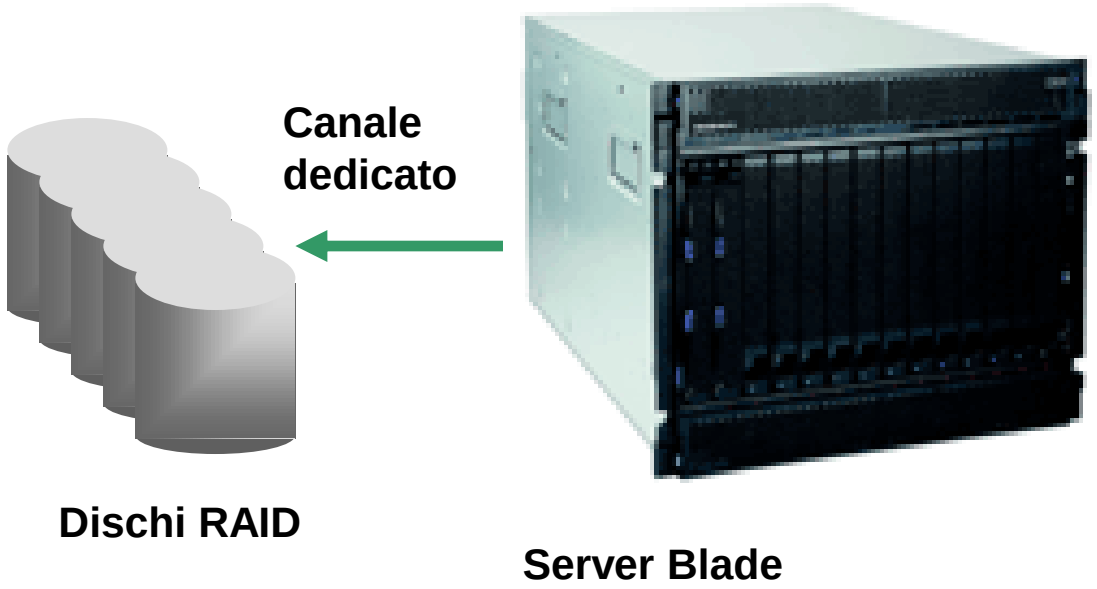
Vulnerabilità IT: gruppi

- Ambientali e geografiche (eventi naturali)
- Da progettazione
- Da realizzazione
- Da mancato test / mancati controlli
- Da errori / debolezze in componenti software
- Da errori / malfunzionamenti hardware
- Da malfunzionamenti infrastruttura
- Da attacchi deliberati (virus compresi)

Vulnerabilità IT: le cause

- Le caratteristiche del sistema, la sua collocazione, il livello di competenza degli utenti concorrono a determinare un elenco di vulnerabilità.

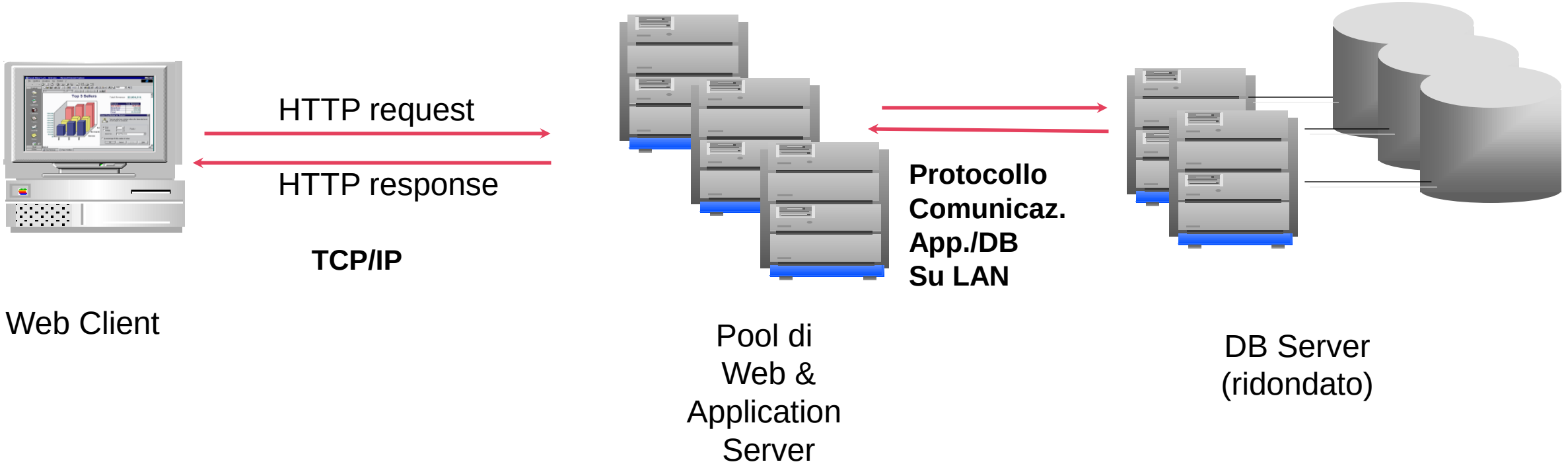
Componenti ridondati



Elementi da ridondare:

- **Alimentatori**
- **Ventole**
- **Dischi**
- **CPU**
- **RAM**
- **Schede di rete**
- **…**

Architettura ridondata



Disaster recovery site

Le soluzioni

- **Gli strumenti tecnici da soli non bastano**
- **Occorrono le competenze delle persone**
- **Occorrono le procedure appropriate (e verificate) per procedere**

Il ripristino dei dati in caso di incidente fisico o tecnico

I dati: l'anima dei sistemi

Cosa si intende per "dati"?

- Contenuto di DB relazionali
- Archivi documentali/multimediali
- Micro applicativi (es. generatori report)
- DB personali (es. elenco indirizzi)
- Archivi di Directory Service
- Configurazioni dei programmi e delle postazioni di lavoro

I dati: l'anima dei sistemi - 2

- In un sistema fortemente centralizzato tutti i dati risiedono o nel DB o, comunque, entro file sui dischi del server
- In un sistema distribuito i dati sono ripartiti su più server e hanno una forma molto varia
- Spesso poi ci sono dati importanti "sparsi in giro" per i client

Salvaguardia dei dati: il backup

- Per la conservazione dei dati è necessario centralizzare la raccolta dei file almeno su server dipartimentali
- Un backup automatico dei dischi dei client (es. sfruttando le condivisioni di dominio) diventa rapidamente ingestibile
- Gli utenti devono procedere alla salvaguardia dei propri dati

Il backup (1/2)

- Cosa si deve salvare?
- Quanto è grande la mole di dati?
- Con che frequenza?

Il backup (2/2)

- Incrementale o alle differenze
- Totale
- Politica di salvataggio (es. giorno/settimana/mese)

Il backup: i supporti

- Nastri singoli
- Librerie di nastri e robotape
- Altri nastri
- CD, DVD ROM
- Disco trasportabile
- SSD
- Dischi distribuiti (es. disaster recovery)

Archiviazione dei dati

- Riordino dei dati secondo schemi prestabliti
- Suddivisione su più supporti
- Conservazione dei supporti

Il backup dell'Immagine (1/2)

- La fase di installazione e configurazione di un sistema assorbe molto tempo
- Client: installazione OS, MS-Office, Client prog. Contabilità, client tn5250…

- Server: installazione di tutte le parti
- In funzione dello scopo del sistema (es. piattaforma di amministrazione)

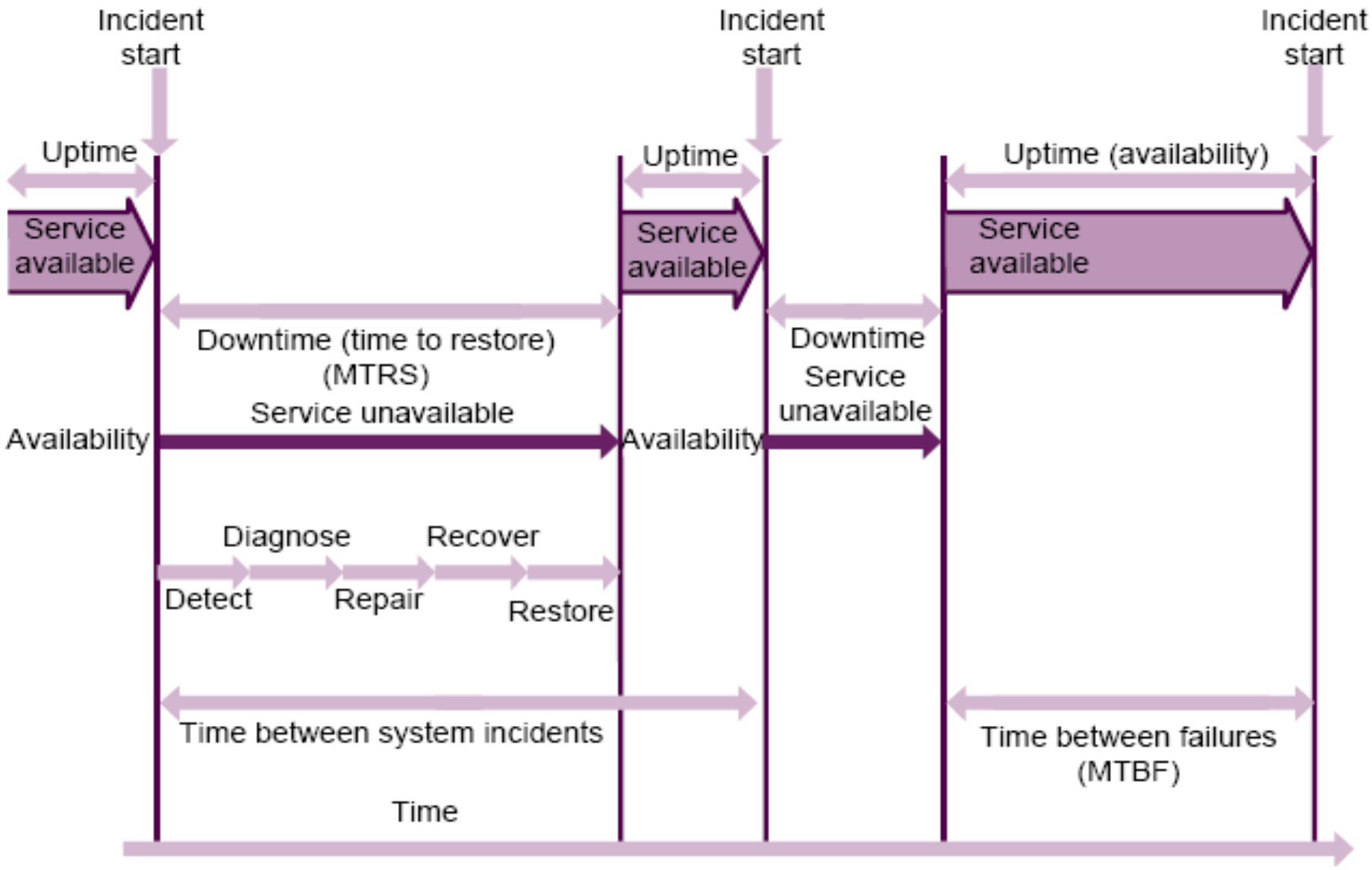
Il backup dell'Immagine (2/2)

- In funzione dello scopo del sistema (es. piattaforma di amministrazione) si definiscono tutti i componenti software della dotazione base
- Con un programma con Norton Ghost o DiskImage si crea una "immagine" dell'installazione
- In caso di problemi si ripristina la configurazione base

Procedure di restore

- Il restore è l'operazione di ripristino dei dati, a partire da un backup
- I dati vengono ripristinati entro un sistema IT, non necessariamente quello originario
- I dati devono essere ripristinati integri, senza perdite
- Il restore non garantisce ancora la disponibilità

Dall'incidente al ritorno alla piena operatività



Fonte: Manuali ITIL - © Crown copyright 2011 – Axelos 2014

Architetture e framework standard internazionali

Alcuni standard rilevanti per l'IT (1/2)

- ISO/IEC 9001, il «famoso» standard «generale» della qualità;
- ISO/IEC 15504, processi business;
- ISO/IEC 20000, IT Service Management;
- ISO/IEC 22031, Business Continuity;
- ISO/IEC 25000, Qualità del Software;
- ISO/IEC 27000, Sicurezza delle informazioni;
- ISO/IEC 42000, Architetture Business ed IT;
- Capability Maturity Model Integration (CMMI®), IT Governance;
- Information Technology Infrastructure Library (ITIL®), IT Service Management;
- Control OBjectives for Information and related Technology (COBIT®), IT Governance;

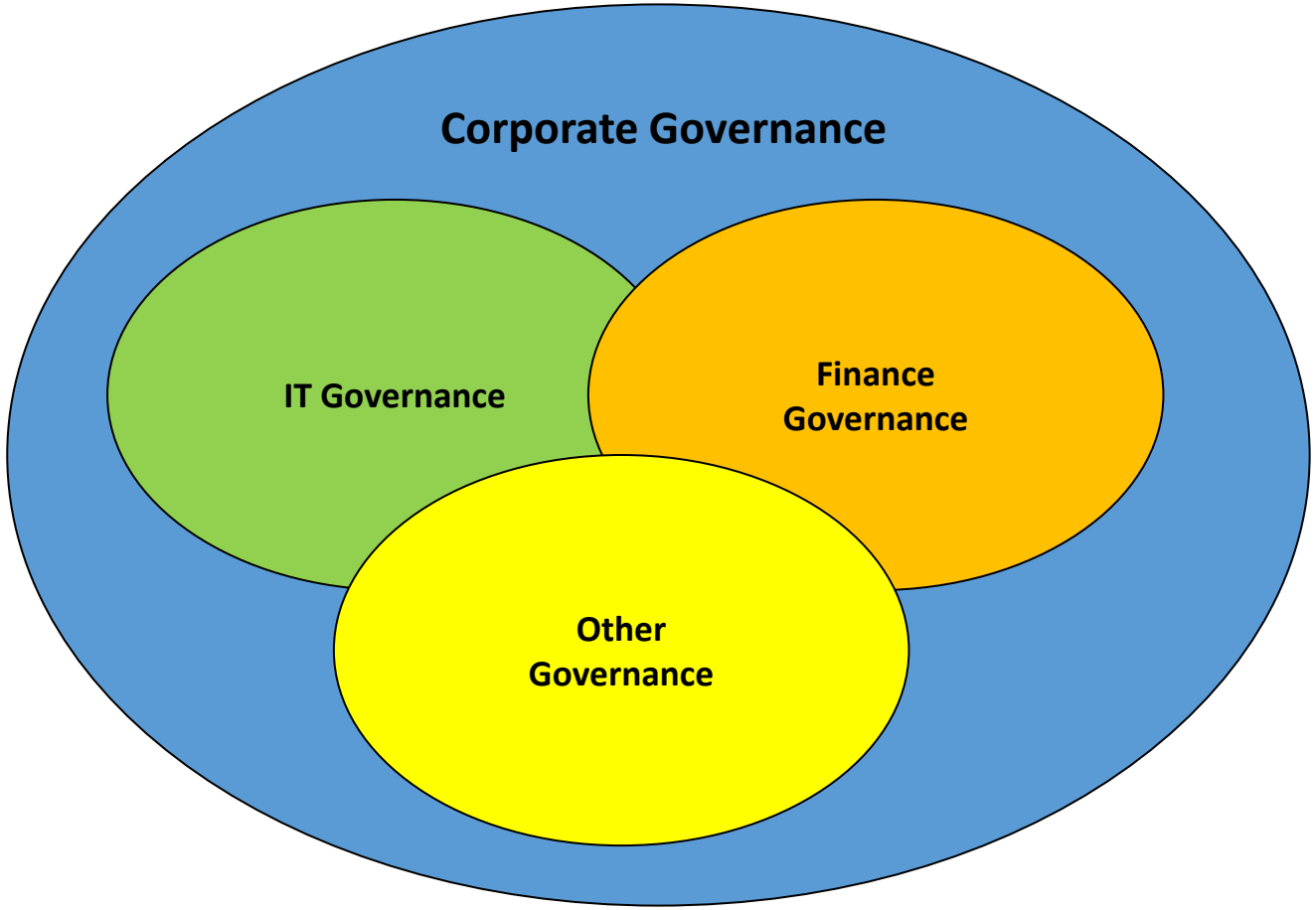
Alcuni standard rilevanti per l'IT (2/2)

- Projects in Controlled Environments (PRINCE2™), Project Management;
- Project Management Body of Knowledge (PMBoK®), Project Management;
- The Open Group Architecture Framework (TOGAF), Architetture e IT Governance;
- TOGAF/Archimate, linguaggio semigrafico per la descrizione delle architetture;
- Six Sigma™, qualità dei prodotti e dei processi;
- UML, linguaggio semigrafico di analisi e progettazione IT e Business;
- BPMN, linguaggio semigrafico di modellazione processi business;
- Unified Process (UP) e Rational Unified Process (RUP), sviluppo software
- SCRUM e altri standard Agile.

Framework e standard molto importanti

- COBIT (Control Objectives for Information and related Technology) – versione 5 - 2012
- ITIL (Information Technology Infrastructure Library) – versione 3/2011 - 2011
- TOGAF (The Open Group Architecture Framework) – versione 9.1 – 2011
- Famiglia delle norme ISO27000 – in divenire

Governance e IT Governance



Corporate Governannce

"Il comportamento etico di dirigenti o altri soggetti nella creazione e conservazione di ricchezza per tutti gli stakeholder"

(IT Governance Institute)

IT Governance

"Parte integrante della Corporate Governance che garantisce che l'IT dell'organizzazione ne sostenga ed estenda strategie ed obiettivi"

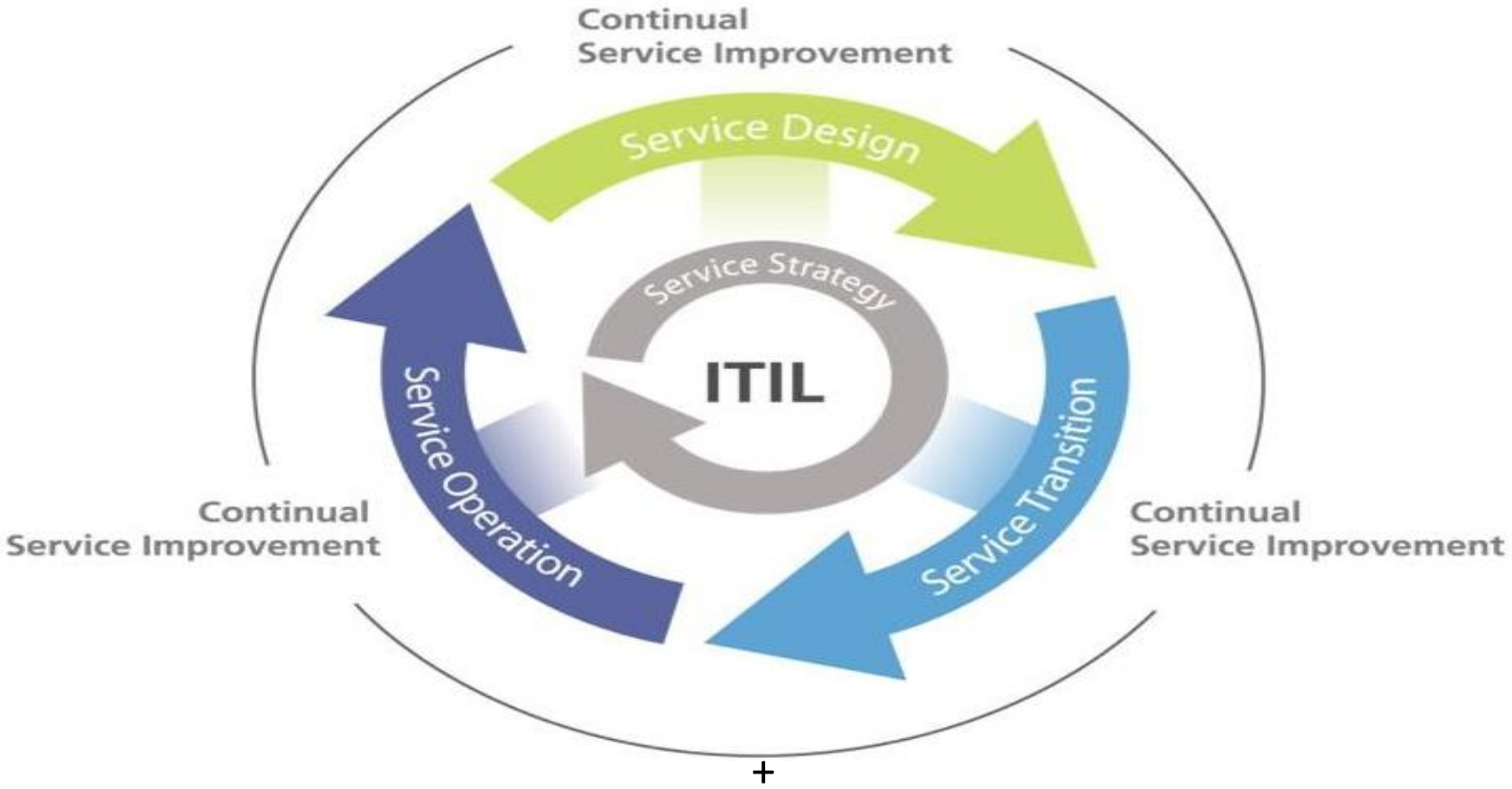
IT Service Management

- **IT Service Management (ITSM)**: l'implementazione e la gestione della qualità dei servizi IT in grado di soddisfare le esigenze del Business. L'IT Service Management viene svolto dai fornitori di Servizi IT attraverso una giusta combinazione di persone, processi e tecnologia informatica
- **Fornitore di Servizi IT**: un Fornitore di Servizi che fornisce servizi IT a clienti esterni o interni

Introduzione a ITIL

- ITIL è l'acronimo di IT Infrastructure Library
- Cronologia
  - Formulazione negli anni '80
  - ITIL v2 nel 2001
  - ITIL v3 nel 2007
  - ITIL v3/2011 o 2011 edition nel 2011
- Soggetto a © di Axelos, società del governo britannico
- Si basa sulle best practice del settore
- User group internazionale: ItSMF

Libreria ITIL



+

- Complementary Publications
  - Web Support Services

Focus sul ciclo di vita dei servizi

- Il ciclo di vita dei servizi è fondamentale nell'aggiornamento ITIL 2011 edition

- In precedenza ITIL si concentrava sulla fornitura ed il supporto di processi di IT Service Management

- Oggi ITIL si allinea con la strategia di business

Azioni nel ciclo di vita dei servizi (1/2)

- Service strategies: definizione della strategia per ITSM e per il servizio specifico
- Service Design: progettazione dei servizi a support della strategia
- Service Transition: implementazione dei servizi a soddisfare i requisiti di progettazione

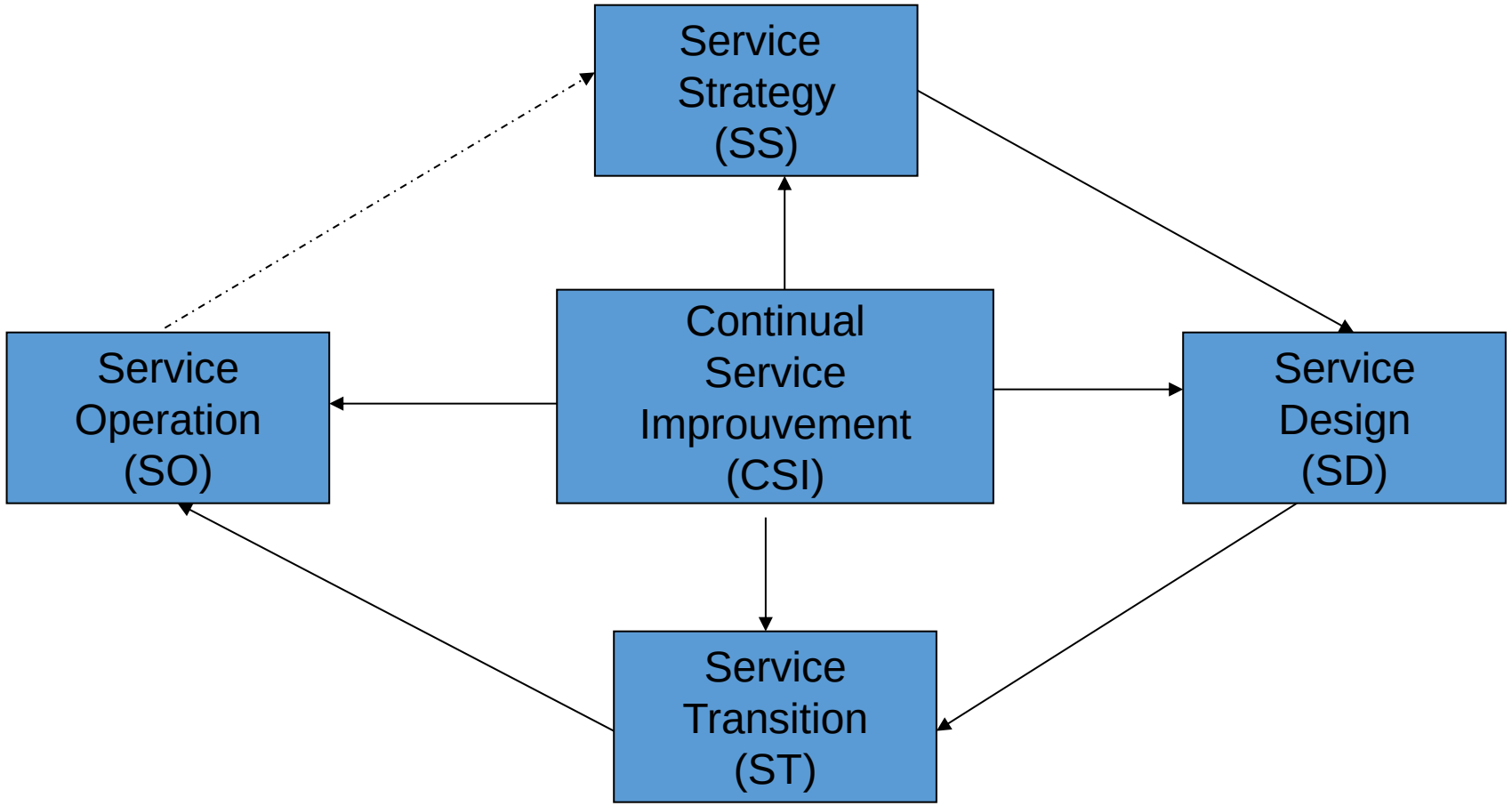
Azioni nel ciclo di vita dei servizi (2/2)

- Service Operation: supporto dei servizi tramite le attività operative
- Continual Service Improvement: interazione tra le fasi e miglioramento continuo

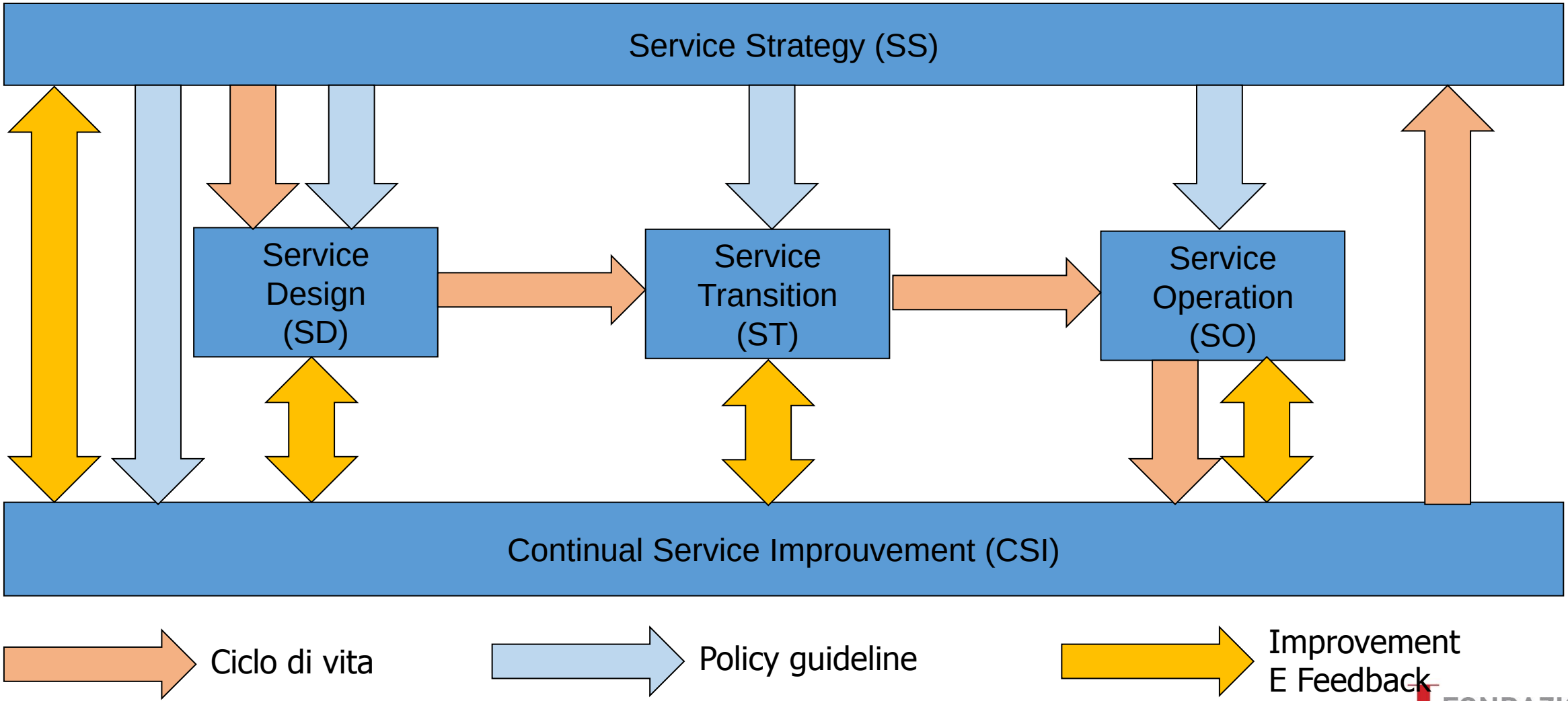
La sequenza dei macro processi ITIL

5 macro processi fondamentali:

- Service strategies
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement



Il clclo di vita dei servizi ITIL

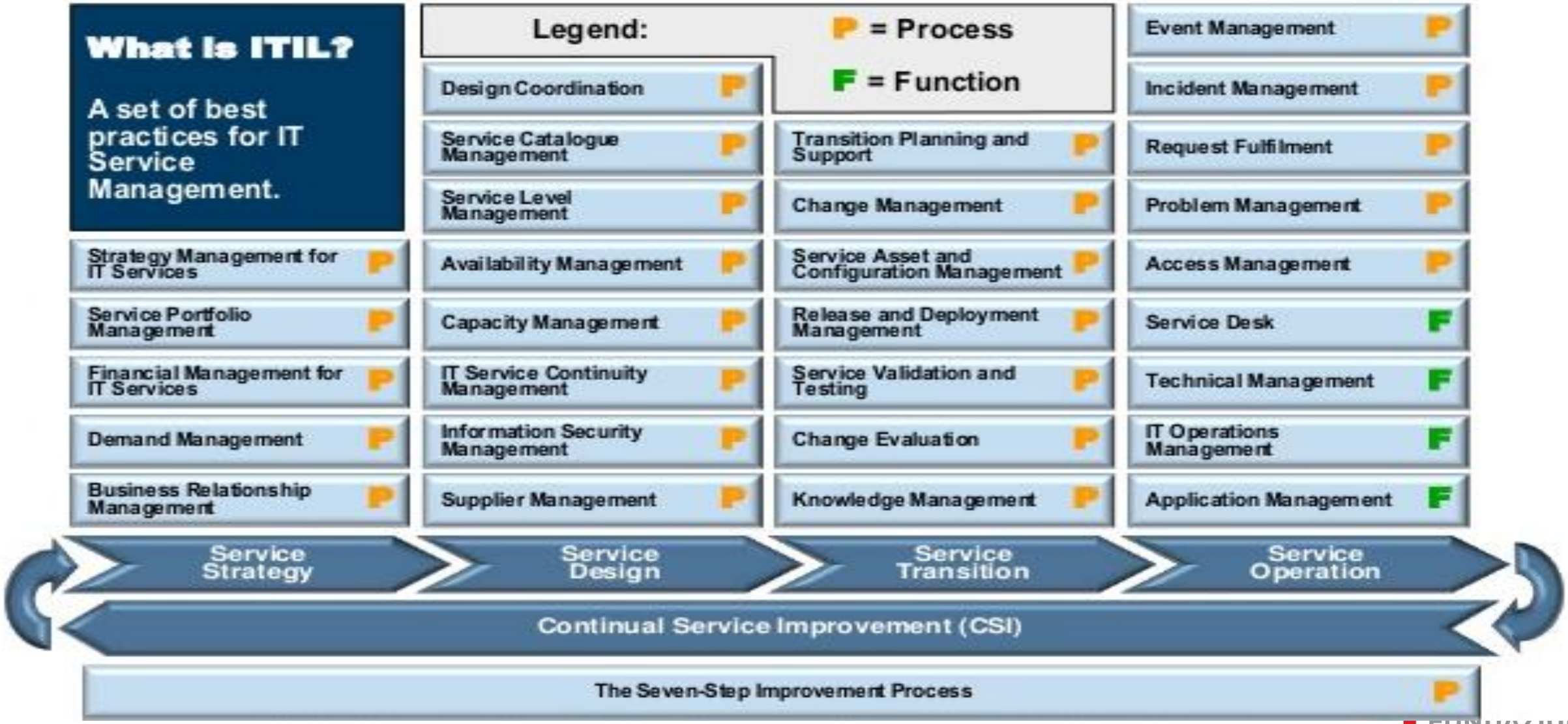


ITIL v3/2011:
ITSM lungo tutto il ciclo di vita di un servizio

Coprire tutto il ciclo di vita:

- Pianificazione
- Analisi funzionale
- Progettazione tecnica
- Organizzazione e gestione
- Cura del funzionamento
- Ritiro

ITIL: macro processi e sotto-processi



Il framework TOGAF

- The Open Group Architecture Framework
- E’ un framework che prevede un approccio globale alla progettazione, pianificazione, attuazione, e la governance di un'architettura delle informazioni entro tutta un’azienda.
- Creato nel 1995 e mantenuto da The Open Group, consorzio di aziende IT e non per la definizione di standard aperti

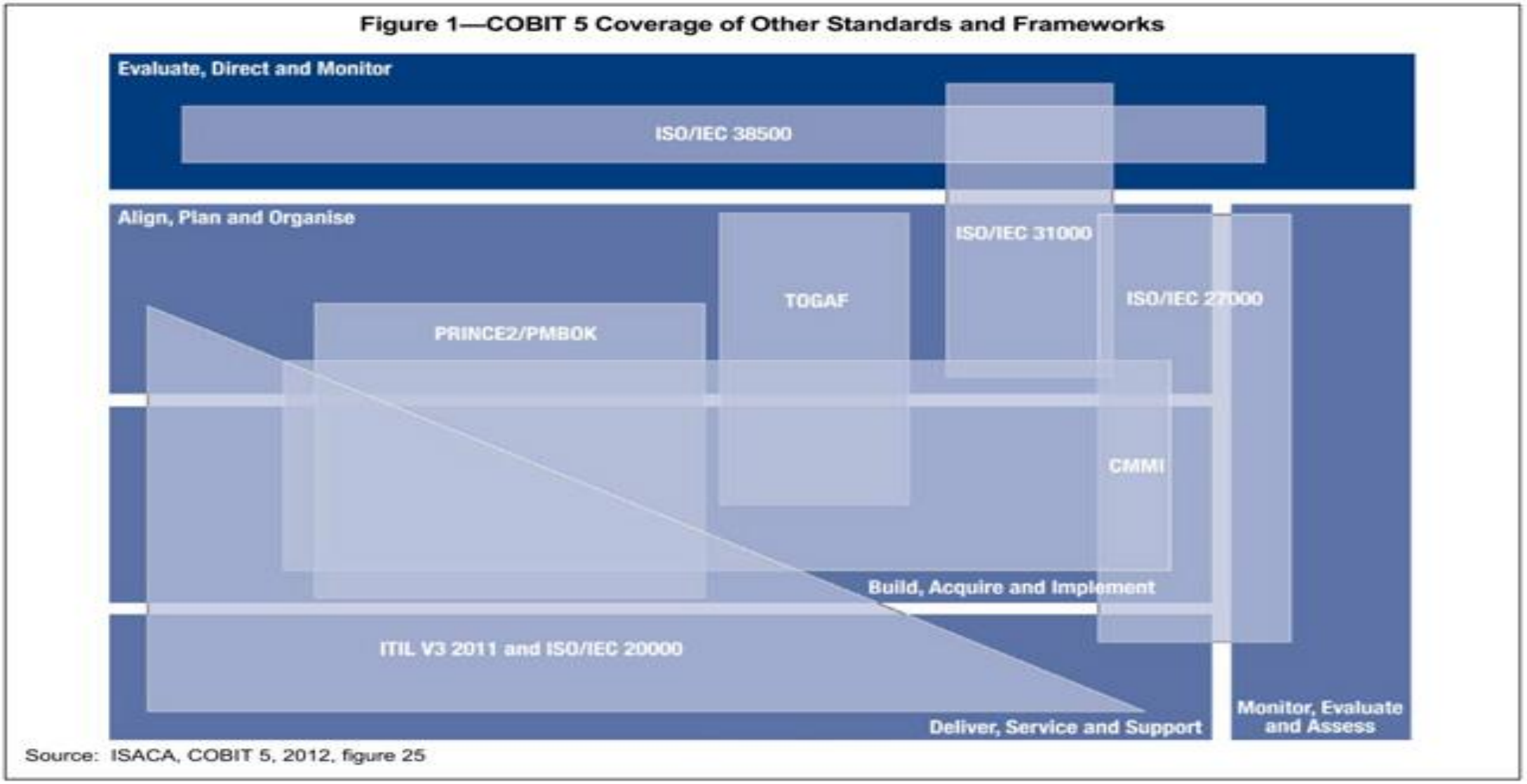
Il framework COBIT (1/2)

- Control Objectives for Information and related Technology
- Dalla versione 5 del 2012 è un framework per la governance e management dell'ICT e per il suo allineamento con le esigenze di business
- Nato nel 1992, inizialmente come modello per l'audit dei sistemi informativi
- Creato e mantenuto da Associazione americana degli auditor dei sistemi informativi (Information Systems Audit and Control Association - ISACA), e dal IT Governance Institute (ITGI)

Il framework COBIT (2/2)

- Fornisce ai manager, agli auditor e agli utenti dei sistemi IT una griglia di riferimento costituita da:
  - una struttura dei processi della funzione IT, rispetto alla quale si è venuto formando il consenso degli esperti del settore
  - una serie di strumenti teorici e pratici collegati ai processi
- con l'obiettivo di valutare se è in atto un efficace governo della funzione IT (IT governance) o di fornire una guida per instaurarlo.
- E’ allineato con gli standard ISO e i framework ITIL e TOGAF

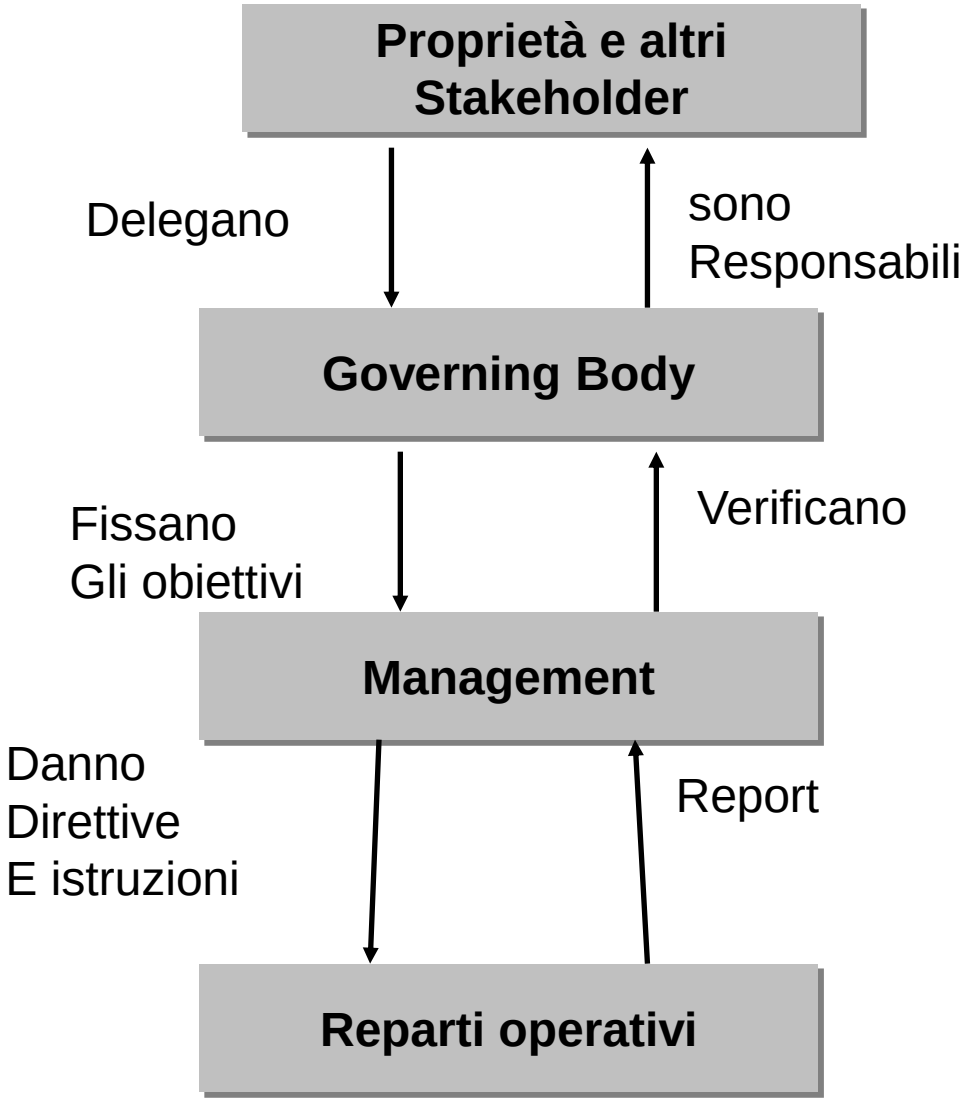
COBIT e gli altri standard



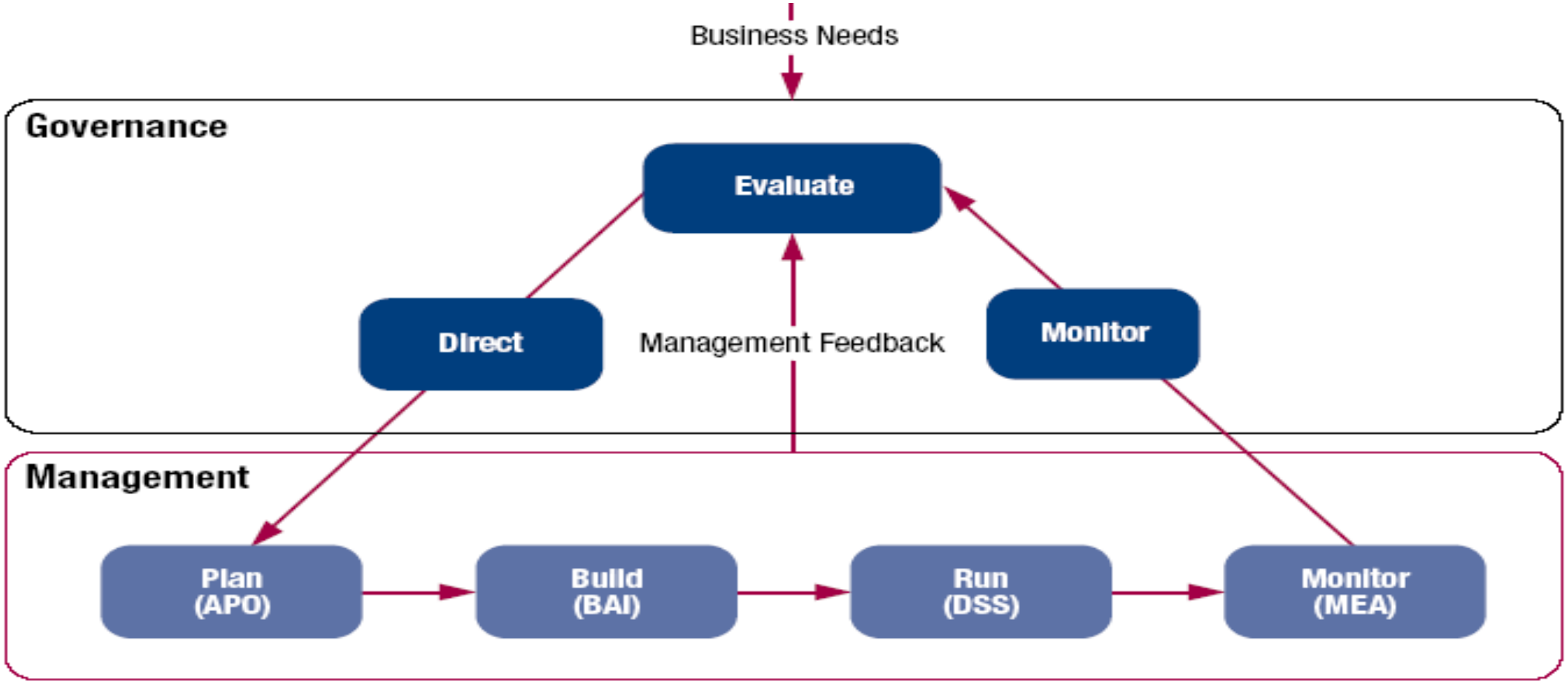
Obiettivi di COBIT

- Mette insieme **5 principi fondamentali**
- per permettere all'azienda o all'organizzazione di costruire
- sia **una effettiva IT governance**
- sia **un effettivo IT management**
- attraverso **l'uso pragmatico di 7 fattori abilitanti**
- che possono **ottimizzare** gli investimenti **in tecnologie ed informazione** per usarli **a beneficio** degli stakeholder

Le relazioni in COBIT

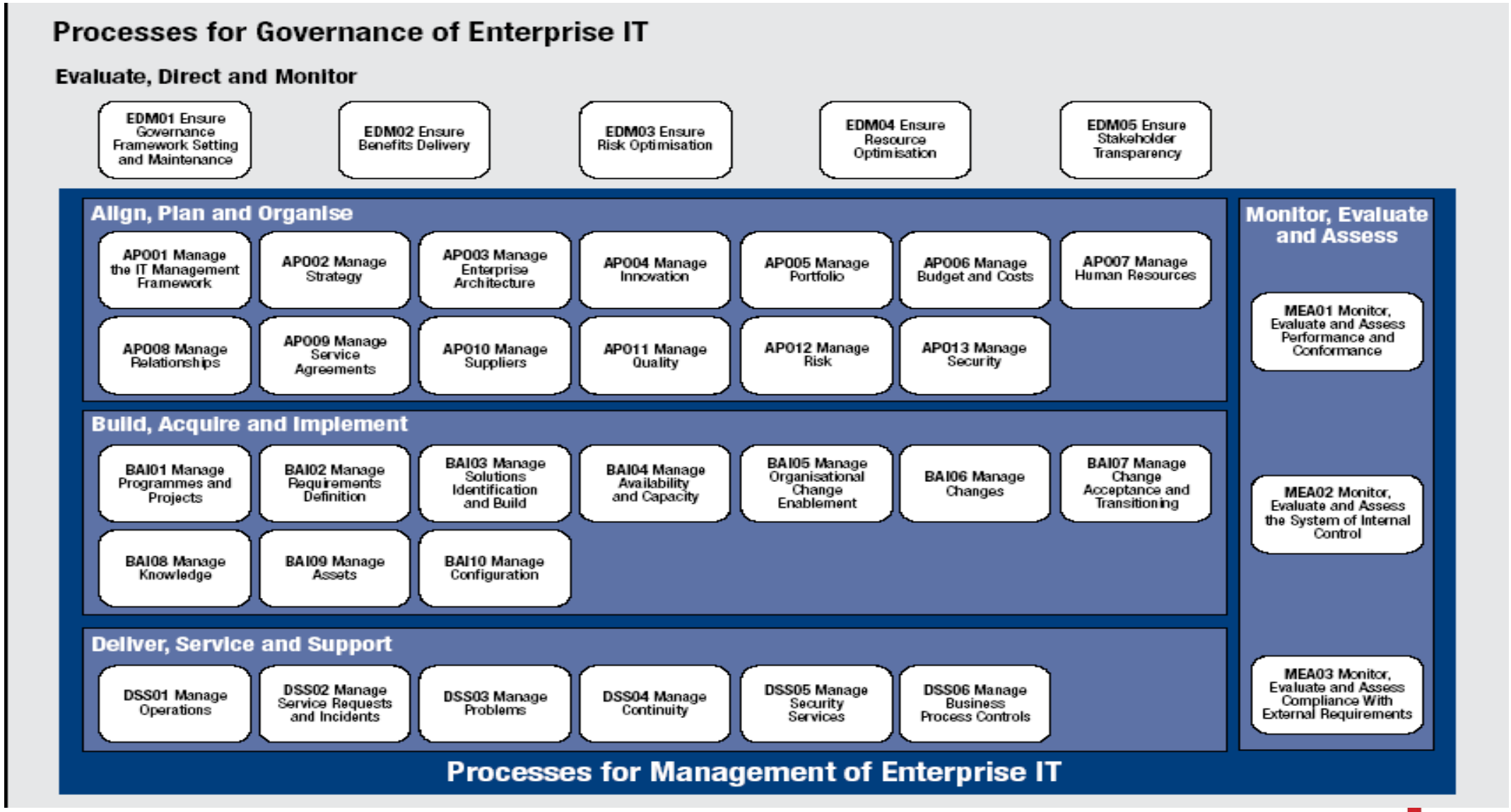


Governance e Management in COBIT



Fonte: COBIT 5 – © ISACA 2012

I processi di COBIT



Fonte: COBIT 5 – © ISACA 2012

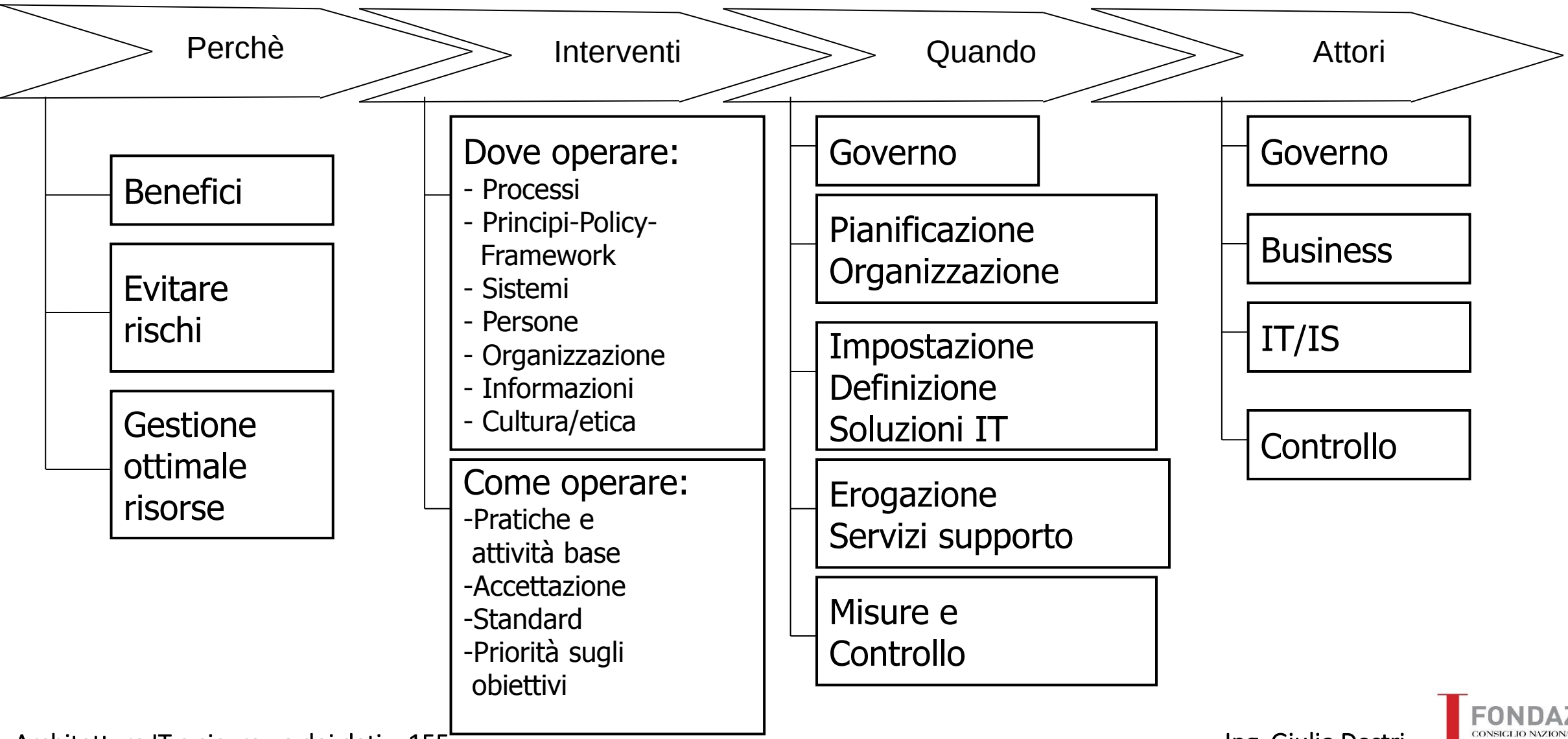
I 5 principi di COBIT

- Andare incontro ai **bisogni degli stakeholder**
- Coprire l'impresa in modo **end-to-end**
- Applicare un **singolo framework integrato**
- Rendere possible un **approccio olistico (sistemico integrato)**
- Separare la **Governance dal Management**

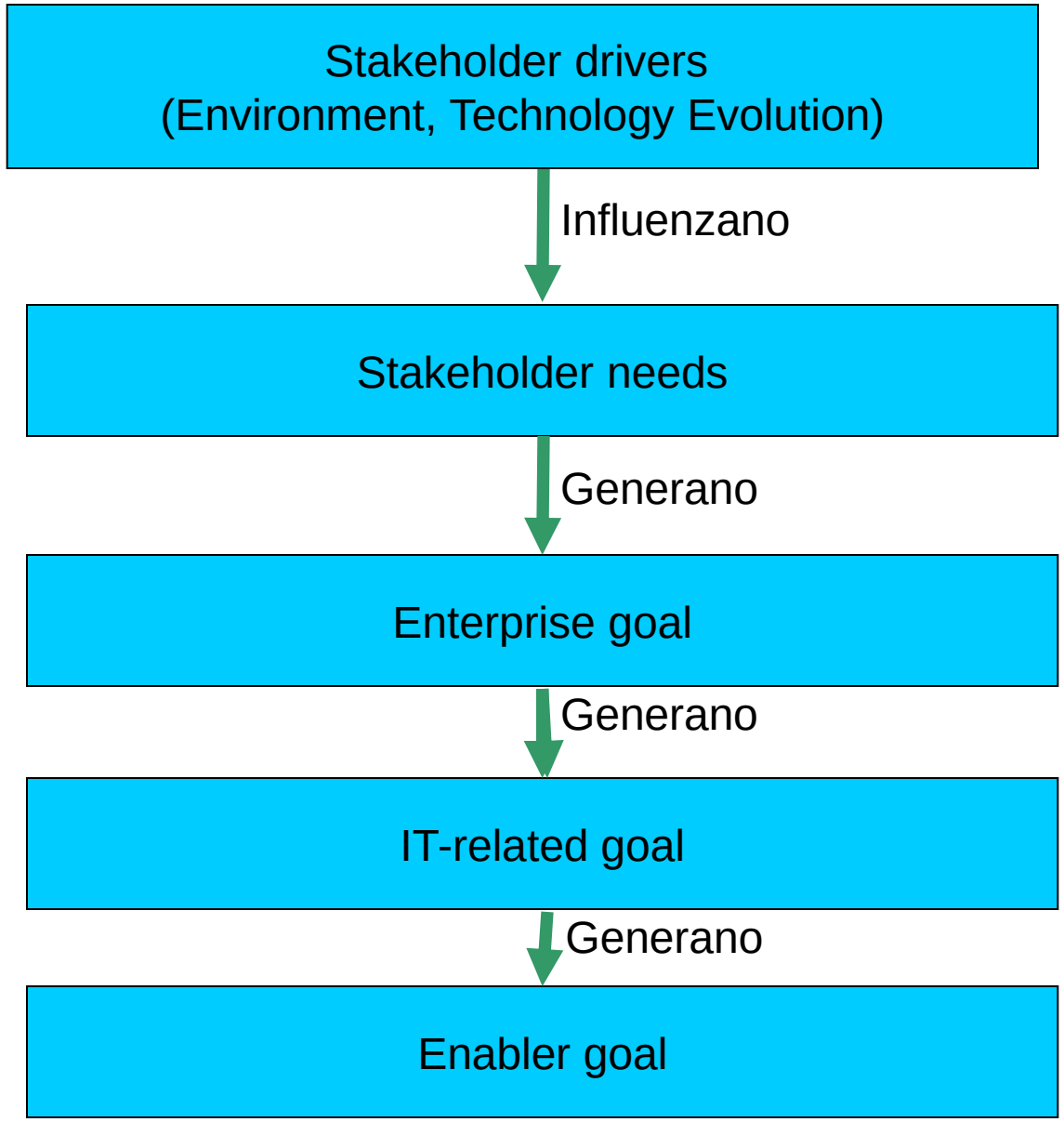
I 7 fattori abilitanti di COBIT

- Principi, politiche e framework
- I processi
- Le strutture organizzative
- Cultura, etica e conoscenza
- L'informazione
- Servizi, infrastrutture ed applicazioni
- Le persone, i loro skill e le competenze

Applicazione operativa dell'IT Governance secondo COBIT



La cascata degli obiettivi in COBIT



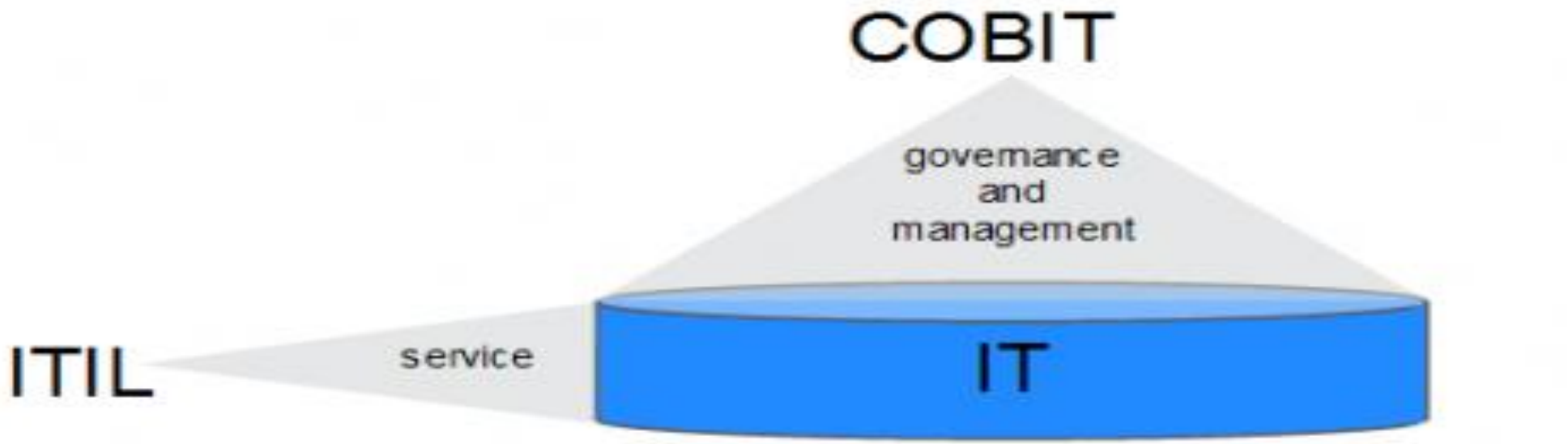
I 17 obiettivi IT (IT Goal) di COBIT (1/2)

1. Allineamento delle stragegie di IT business
2. IT compliance e supporto per la business compliance con leggi e regolamenti esterni
3. Coinvolgimento del management nelle decisioni che coinvolgono l'IT
4. Gestione dei rischi del business collegati all'IT
5. Realizzare benefici dagli investimenti in IT e dal service portfolio
6. Trasparenza di costi, benefici e rischi dell'IT
7. Fornitura di servizi IT allineati con i requisiti del business
8. Uso adeguato di applicazioni, informazioni e soluzioni tecnologiche

I 17 obiettivi IT (IT Goal) di COBIT (2/2)

9. Agilità dell'IT
10. Sicurezza di informazioni, infrastrutture di elaborazione e applicazioni
11. Ottimizzazione di assets, risorse e capacità dell'IT
12. Abilitazione e supporto dei processi business attraverso l'integrazione di applicazioni e tecnologia nei processi business
13. Messa in opera dei programmi che producono benefit rispettando tempi e budget, requisiti e standard di qualità
14. Disponibilità di informazioni affidabili ed utili per il decision making
15. Compliance dell'IT compliance con le politiche interne dell'organizzazione
16. Personale IT e business competente e motivato
17. Conoscenza, esperienza ed iniziative per l'innovazione del business

COBIT e ITIL



Per approfondimenti

- COBIT: http://www.isaca.org/cobit/pages/default.aspx
- ITIL: https://en.it-processmaps.com/products/itil-process-map.html
- A. Languasco e A. Zaccagnini «Manuale di crittografia. Teoria, algoritmi e protocolli» Ed. Hoepli, 2015
- G. Destri «Sistemi informativi. Il pilastro digitale di servizi e organizzazioni» Ed. FrancoAngeli, 2013

Sommario (1/2)

- Il contesto: GDPR e IT
- Le qualità dell'accesso ai dati
- Le architetture IT per conservazione ed accesso ai dati
- Cosa è l'accesso sicuro ai dati
- Tecniche di pseudoanonimizzazione
- La cifratura e la sua "forza"

Sommario (2/2)

- Tecniche per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- Il ripristino dei dati in caso di incidente fisico o tecnico
- Architetture e framework standard internazionali