ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Il cloud computing:

nuovo paradigma e nuovi rischi?

(a cura di **Carla Fazzi – CFE – Spike Reply**)

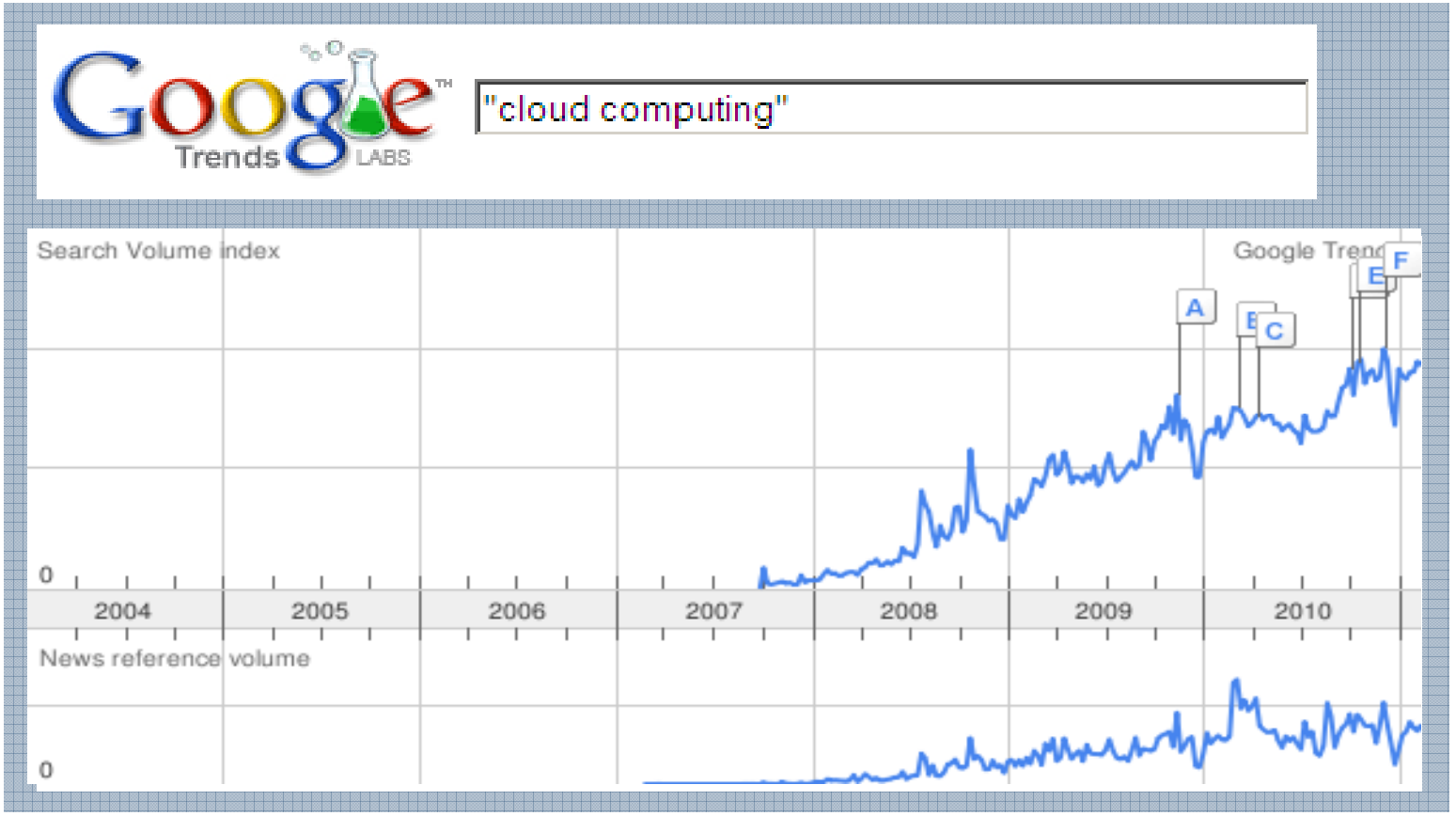
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Agenda

- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing
- Riferimenti bibliografici e sitografici
- Varie – Q&A

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

L'interesse per il Cloud Computing



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

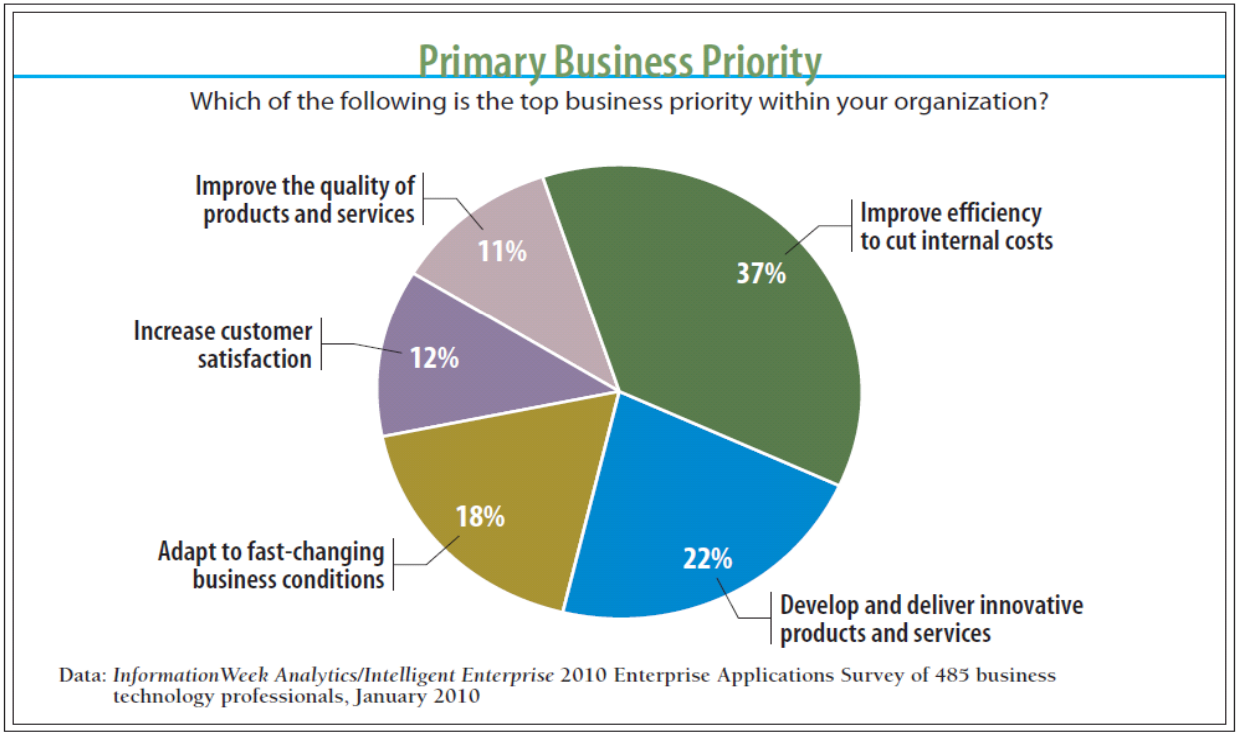
Perché c'è interesse per il cloud computing?

informed-cio-it-cost-transparency_4687109[1].pdf - Adobe Reader

File Edit View Document Tools Window Help

7 / 16 147% Find

Figure 1



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

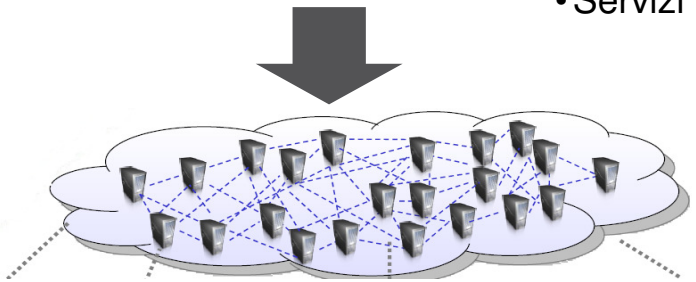
Terminologia

CLOUD + **COMPUTING**

'Cloud' è il simbolo grafico usato per Internet

'Computing' si riferisce ai servizi di "utility computing":

- Accesso a risorse computazionali (memoria, CPU, virtual server, ...)
- Servizi (backup, anti-spamming, …)



I servizi di utility computing sono erogati attraverso Internet

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Definizioni

Il Cloud Computing è ancora un paradigma in fase di evoluzione. La definizione, le modalità di utilizzo, le tecnologie di riferimento, le problematiche rilevate, i rischi ed i benefici sono ad oggi oggetto di dibattito.

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

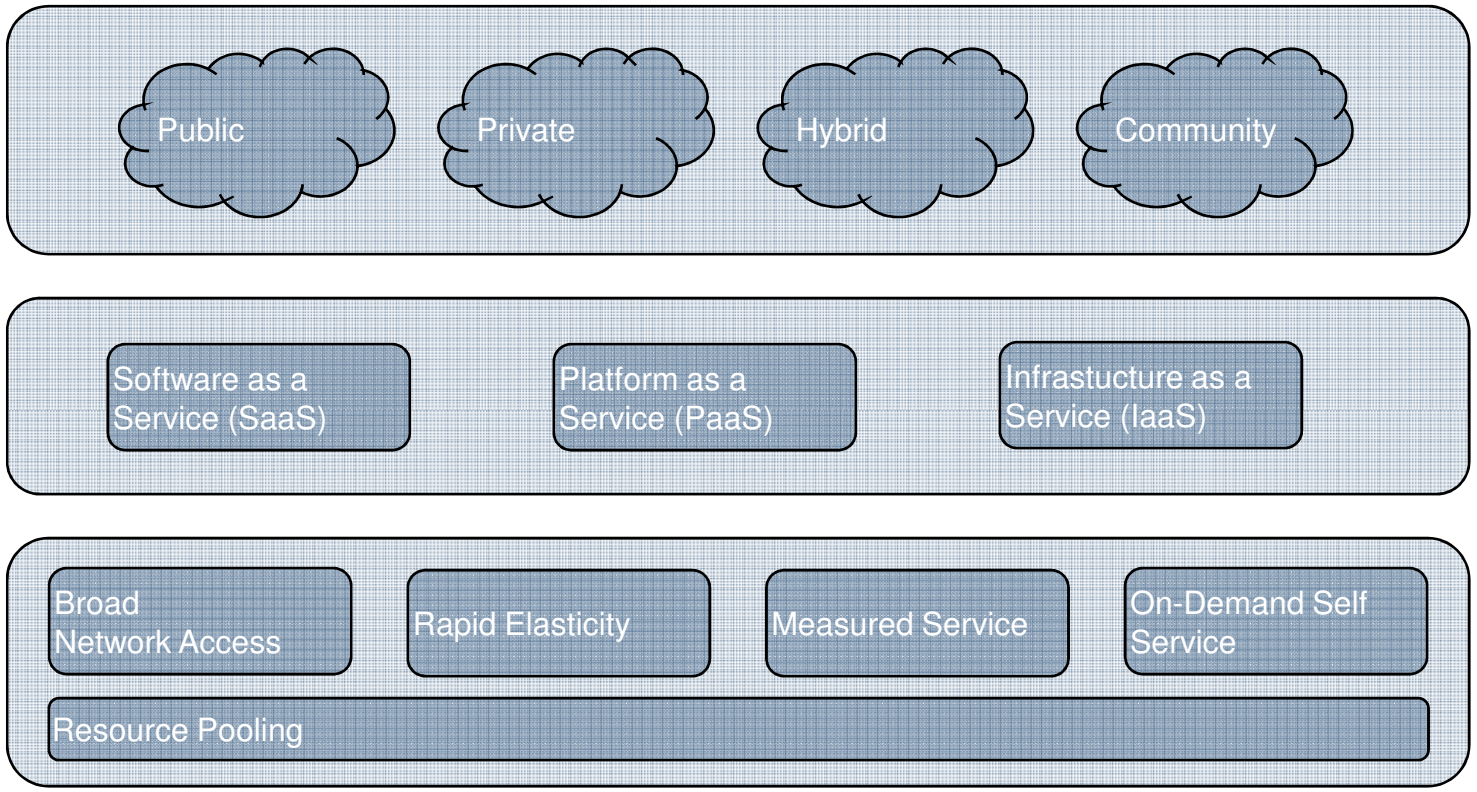
Fonte: NIST

Cloud computing is a style of computing where massively scalable IT-related capabilities are provided 'as a service' across the Internet to multiple external customers.

Fonte: Gartner

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

NIST Visual Model



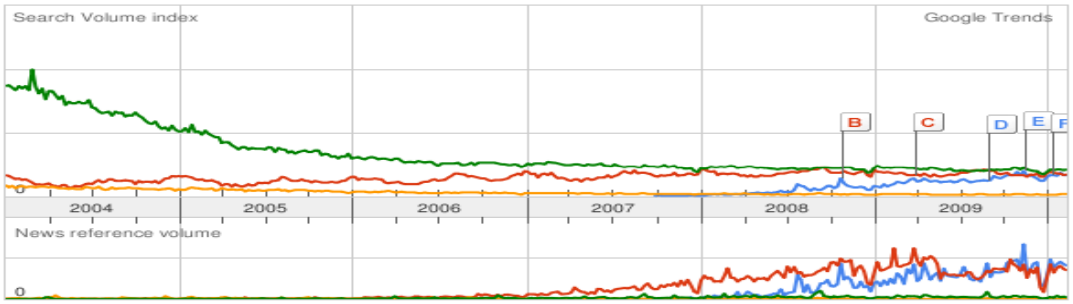
NIST - National Institute of Standards and Technology

http://csrc.nist.gov/groups/SNS/cloud-computing/

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Nuova tecnologia o nuovo modello?

- Il Cloud Computing rappresenta la convergenza di tre principali trend degli ultimi anni: **orientamento dell'IT come servizio**, **virtualizzazione**, **standardizzazione dell'accesso alle risorse elaborative tramite Internet.**
- Diverse sono le tecnologie che hanno dato inizio al fenomeno:



- Il Cloud Computing sta conquistando spazi sempre più rilevanti grazie alla diffusione di:
  - data center di ampie dimensioni, per conseguire economie di scala
  - banda larga per l'accesso ad Internet
  - modelli di pagamento pay-per-use.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

I modelli di utilizzo

	Infrastructure Managed by	Infrastructure Owned by	Infrastructure Located	Accessible and Consumed by
Public	Third Party Provider	Third Party Provider	Off Premise	Untrusted
Private / Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On Premise / Off Premise	Trusted
Hybrid	Both Organization and Third Party Provider	Both Organization and Third Party Provider	Both On Premise or Off Premise	Trusted & Untrusted

CSA - Cloud Security Alliance

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Principali benefici

- I benefici nell'adozione di soluzioni di Cloud Computing variano in funzione dei modelli di servizio (SaaS, PaaS, IaaS) e dei modelli di deployment (Public, Private, Hybrid, Community).
- I benefici sono classificabili in due categorie principali:

Efficienza IT	Efficienza del Business
• Possibilità di aumentare la capacità senza investire in nuove infrastrutture. • Esigenza ridotta di pianificare in anticipo l'utilizzo delle risorse. • Semplificazione dei processi di gestione.	• Accesso veloce a servizi (anytime ed anywhere). • Modello pay-per-use. • Maggiore flessibilità nell'adattarsi al variare delle esigenze. • Maggiore rapidità nello sviluppare nuove soluzioni. • Migliore capacità di interagire con società partner.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

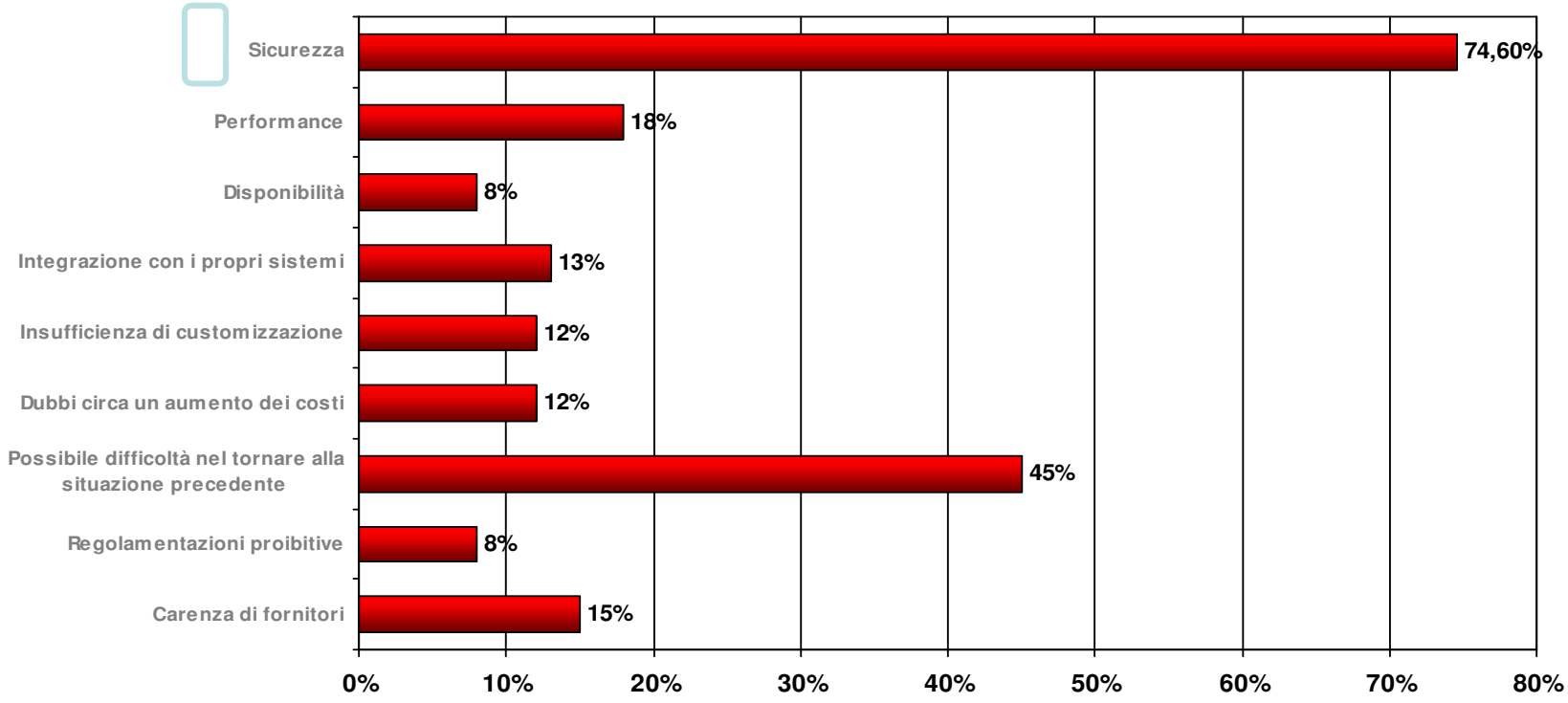
Agenda

- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Il Cloud Computing percepito dagli utenti

Gli utenti percepiscono gli aspetti di sicurezza come principale rischio nell'adozione del Cloud Computing.



IDC Enterprise Panel, August 2008

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La sicurezza nel Cloud Computing

- Gli elementi da considerare per gestire la sicurezza nel Cloud Computing sono quelli abituali:
  - **Riservatezza:** protezione delle informazioni critiche da accessi non autorizzati.
  - **Integrità:** salvaguardia dell'originalità e della completezza delle informazioni da modifiche non autorizzate.
  - **Disponibilità:** garanzia che le informazioni siano disponibili quando richieste dagli utenti.

La loro applicazione nel contesto del Cloud Computing potrebbe essere più complessa.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La Riservatezza nel Cloud Computing

Una delle misure di sicurezza per gestire la riservatezza è la **crittografia**.

Esempio

Il Cliente Finale dispone di un elevato volume di dati, la cui elaborazione viene fatta mediante un servizio in Cloud Computing. I dati, quindi, devono essere inviati alla "nube" per essere elaborati e poi essere rinviati al mittente.
Per preservare la riservatezza, i dati sono inviati in forma crittografata, sono decifrati dalla "nube", sono effettuate le elaborazioni richieste, sono crittografati nuovamente e rinviate mediante la "nube" al cliente.

Applicabile, ma quali prestazioni sono necessarie per avere tempi accettabili?

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La Disponibilità nel Cloud Computing

Una delle misure di sicurezza per gestire la disponibilità è la **ridondanza**.

Esempio

Un'azienda gestisce un volume di dati che aumenta velocemente e ha quindi la necessità di avere una infrastruttura di storage.
Acquista il servizio in modalità Cloud Computing e, a garanzia della disponibilità, chiede al suo fornitore telco di ridondare la rete.
Ritiene comunque non accettabile il rischio che la "nube" non sia disponibile al momento in cui ha necessità di accedere ai dati più critici. Decide quindi di eseguire un back up dei dati indipendentemente dal servizio di Cloud Computing.

Applicabile, ma i costi potrebbero essere troppo elevati rispetto ai benefici.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

L'Integrità nel Cloud Computing

Una delle misure di sicurezza per gestire l'integrità è la **gestione del ciclo di vita del dato**.

Esempio

Nei due esempi precedenti è di fondamentale importanza assicurarsi che i dati non subiscano modifiche non autorizzate. Si potrebbero applicare allora soluzioni quali l'hashing o firma digitale.

Applicabile, ma la verifica sarebbe fatta a posteriori, cioè dopo la modifica.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

I Rischi nel Cloud Computing

- Anche i rischi di sicurezza, così come i benefici, variano in funzione dei modelli di Cloud Computing e sono strettamente correlati alla gestione della sicurezza in termini di riservatezza, integrità e disponibilità.

- European Network and Information Security Agency (ENISA) e la Cloud Security Alliance (CSA) hanno pubblicato due relazioni allo scopo di analizzare i rischi e i possibili controlli di sicurezza nell'adozione del Cloud Computing:
  - Cloud Computing - Benefits, risks and recommendations for information security (ENISA, Nov. 09)
  - Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 (CSA, Dic. 09)

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Le aree di rischio dell'ENISA

L'ENISA, nella pubblicazione *"Cloud Computing: Benefits, risks and recommendations for information security"*, ha identificato 35 rischi:

RISCHI LEGALI

- Subpoena and e-discovery
- Risk from changes of jurisdiction
- Data protection risks
- Licensing risks

RISCHI ORGANIZZATIVI

- Lock-in
- Loss of governance
- Compliance challenges
- Loss of business reputation due to co-tenant activities
- Cloud service termination or failure
- Cloud provider acquisition
- Supply chain failure

RISCHI TECNOLOGICI

- Resource exhaustion
- Isolation failure
- Cloud provider malicious insider - abuse of high privilege roles
- Management interface compromise
- Intercepting data in transit
- Data leakage on up/download, intra-cloud
- Insecure or ineffective deletion of data
- DDoS and EDOS
- Loss of encryption keys
- Undertaking malicious probes or scans
- Compromise service engine
- Conflicts between customer hardening procedures and cloud environment

RISCHI NON SPECIFICI DEL CLOUD

- Network breaks
- Network management
- Modifying network traffic
- Privilege escalation
- Social engineering attacks
- Loss or compromise of operational logs
- Loss or compromise of security logs
- Backups lost, stolen
- Unauthorized access to premises
- Theft of computer equipment
- Natural disasters

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Le aree di rischio dell'ENISA

L'ENISA, nella pubblicazione *"Cloud Computing: Benefits, risks and recommendations for information security"*, ha identificato 35 rischi:

RISCHI LEGALI

- Subpoena and e-discovery
- Risk from changes of jurisdiction
- Data protection risks
- Licensing risks

RISCHI ORGANIZZATIVI

- Lock-in
- Loss of governance
- Compliance challenges
- Loss of business reputation due to co-tenant activities
- Cloud service termination or failure
- Cloud provider acquisition
- Supply chain failure

RISCHI TECNOLOGICI

- Resource exhaustion
- Isolation failure
- Cloud provider malicious insider - abuse of high privilege roles
- Management interface compromise
- Intercepting data in transit
- Data leakage on up/download, intra-cloud
- Insecure or ineffective deletion of data
- DDoS and EDOS
- Loss of encryption keys
- Undertaking malicious probes or scans
- Compromise service engine
- Conflicts between customer hardening procedures and cloud environment

RISCHI NON SPECIFICI DEL CLOUD

- Network breaks
- Network management
- Modifying network traffic
- Privilege escalation
- Social engineering attacks
- Loss or compromise of operational logs
- Loss or compromise of security logs
- Backups lost, stolen
- Unauthorized access to premises
- Theft of computer equipment
- Natural disasters

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

I 12 controlli del CSA

Il CSA, nella pubblicazione *"Security Guidance for Critical Areas of Focus in Cloud Computing",* ha definito 12 domini di controlli di sicurezza suddivisi in due aree:

DOMINI DI GOVERNO	DOMINI TECNOLOGICI
• Governance and Enterprise Risk Management • Legal and Electronic Discovery • Compliance and Audit • Information Lifecycle Management • Portability and Interoperability	• Traditional Security, Business Continuity and Disaster Recovery • Data Center Operations • Incident Response, Notification and Remediation • Application Security • Encryption and Key Management • Identity and Access Management • Virtualization

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Relazione tra Rischi e Modelli

- I rischi di sicurezza variano in funzione sia dei modelli di servizio / di deployment, sia dei vincoli organizzativi o di compliance.

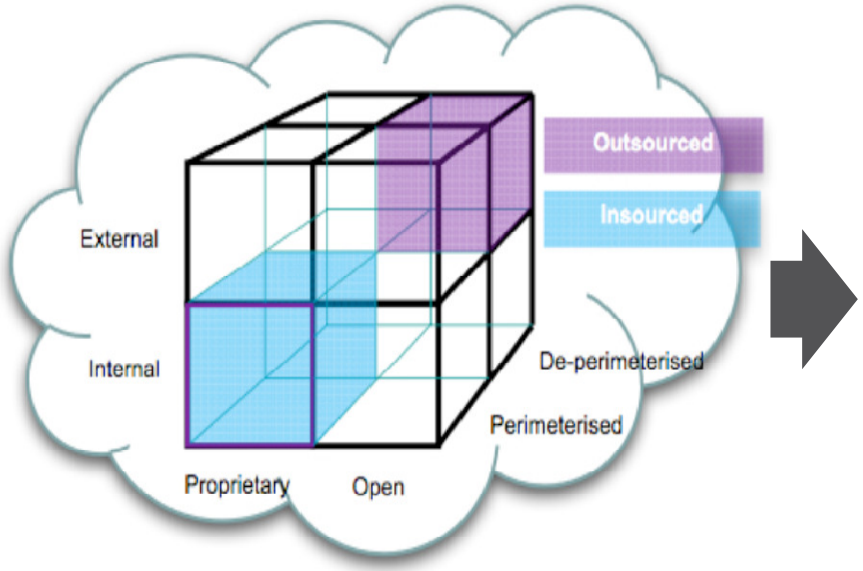
- **Loss of governance**
  - il modello SaaS può comportare un rischio di perdita di governo maggiore rispetto al modello IaaS.

- **Compliance**
  - L'impatto di questo rischio varia in funzione della presenza o meno di vincoli normativi (es. PCI-DSS o SOX) e al tipo di modello di deployment (public o private).

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Insourcing o Outsourcing

I rischi cambiano anche in funzione delle politiche di insourcing o outsourcing definite dall'organizzazione. Nella scelta di soluzioni in outsourcing devono essere considerate misure specifiche di sicurezza.



Jericho Cloud Cube Model

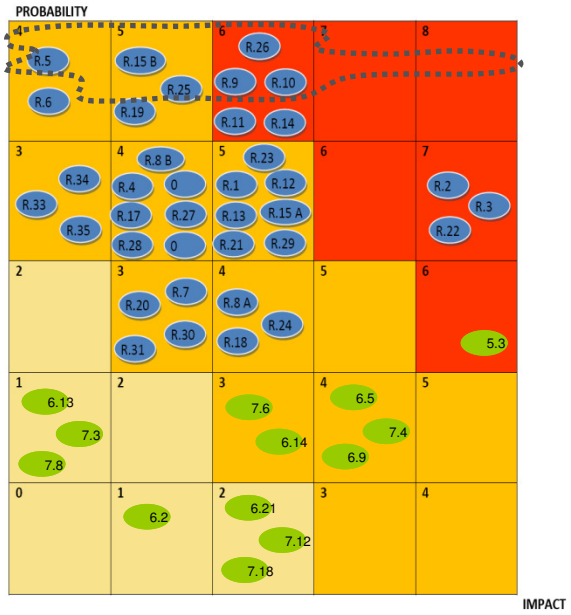
La ISO 27002 definisce particolari controlli:

A.06.2.1	**Identificazione dei rischi legati a parti esterne**
A.06.2.2	**Occuparsi della sicurezza quando si tratta con i clienti**
A.06.2.3	**Occuparsi della sicurezza negli accordi con terze parti**

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Approccio per la gestione della sicurezza

Risk Assessment



Rischi ENISA

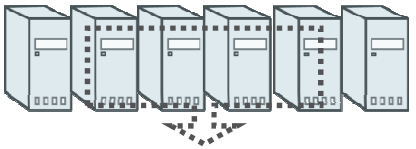
Definizione del Sistema di controllo

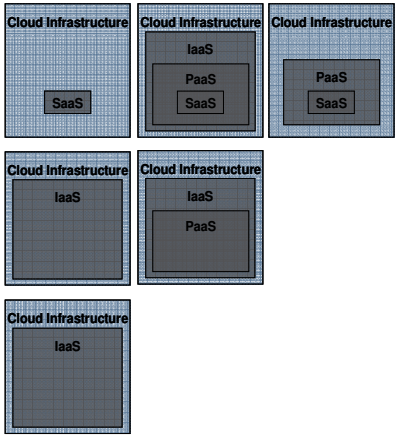
Controlli sistema tradizionale

Controlli CSA

Controlli ISO27002

Scelta del sistema di gestione e del modello di Cloud Computing





ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Agenda

- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Mitigare i rischi del cloud

- La sicurezza IT dipende da persone, processi e tecnologia
- Quali sono le soluzioni tecnologiche disponibili ad oggi per mitigare i rischi evidenziati finora nel cloud?
- Focus on:
  - Modalità di gestione in outsourcing (servizi Iaas, Paas, Saas pubblici o ibridi)
  - Soluzioni:
    - Data Encryption & Key Management nel Cloud (Dominio **Encryption and Key Management**)
    - Federated Identity nel Cloud (Dominio **Identity and Access Management**)

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La protezione dei dati su Cloud

- **Ogni metodologia "risk based" assegna un peso importante alla criticità delle informazioni**
- **Le infrastrutture Cloud sono per definizione critiche dal punto di vista RID**
  - Riservatezza (Rif. Risk: Malicious Insider)
  - Integrità
  - Disponibilità
- **Quali sono le soluzioni di mitigazione per garantire la riservatezza dei dati su Cloud?**
  - Focalizziamo gli esempi sulle infrastrutture Iaas (le soluzioni possono essere traslate nelle modalità di erogazione Paas e Saas)
- **Quali sono i rischi che cerchiamo di mitigare?**
  - Cloud provider malicious insider - abuse of high privilege roles
  - Intercepting data in transit
  - Data leakage on up/download, intra-cloud
  - Insecure or ineffective deletion of data
  - Loss of encryption keys

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La crittografia dei dati

- Nei ToS di Amazon AWS è presente la seguente clausola:

- **"YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA."**

- "You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you."

… un messaggio chiaro

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

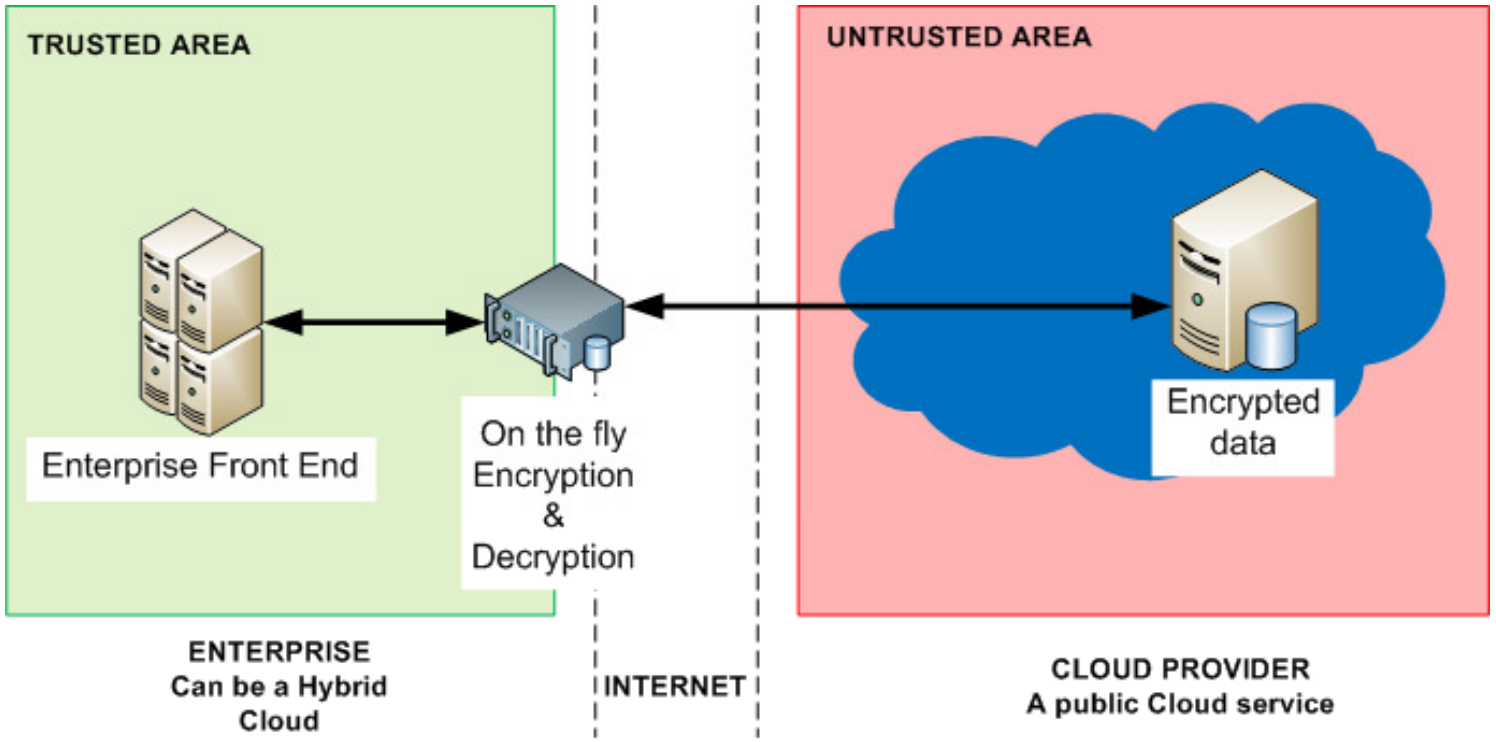
La gestione delle chiavi

- La crittografia dei dati è una delle possibili soluzioni. Il problema delle infrastrutture Cloud è: come gestiamo le chiavi?
- Ad oggi a responsabilità della gestione delle chiavi (storage e provisioning) è dell'Enterprise
- Nessun Cloud Services Provider ad oggi mette a disposizione tecnologie HSM, per definizione 'non virtualizzabili' e gli standard (PKCS10/11) non sono adatti ad utilizzi in ambito Cloud

- Usare la crittografia per evitare l'accesso ai dati da parte del Cloud Provider è complesso

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Soluzioni disponibili



- Encryption si applica ai dati significativi (es: anagrafiche) sia ‘at rest’ che ‘in motion’
- Le chiavi sono gestite ‘off-cloud’

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Altre soluzioni possibili per la data encryption

- **Fidarsi del Cloud Provider (es: Amazon)**
  - Alcune domande da fare:
    - Quali sono i modelli di sicurezza del Cloud Provider?
    - Come gestisce gli accessi alle informazioni?
    - Quali sono gli SLA? Che garanzie offrono in caso di accesso non autorizzato?
    - Che strumenti di monitoraggio vengono utilizzati per rilevare accessi non desiderati?
    - Sussistono obblighi di comunicazione verso l'Enterprise dei security breach che coinvolgono i loro dati?
  - Questa soluzione prevede che il Cloud Provider abbia potenzialmente accesso sia alle chiavi dunque anche ai dati (sia nel caso di cifratura dei dati 'at rest' che 'in motion')
- **Utilizzare delle 'secure area' fornite sul Cloud dal Provider all'Enterprise per la gestione delle chiavi ('Virtual HSM')**
  - Una soluzione futuribile più che una realtà

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La gestione delle identità

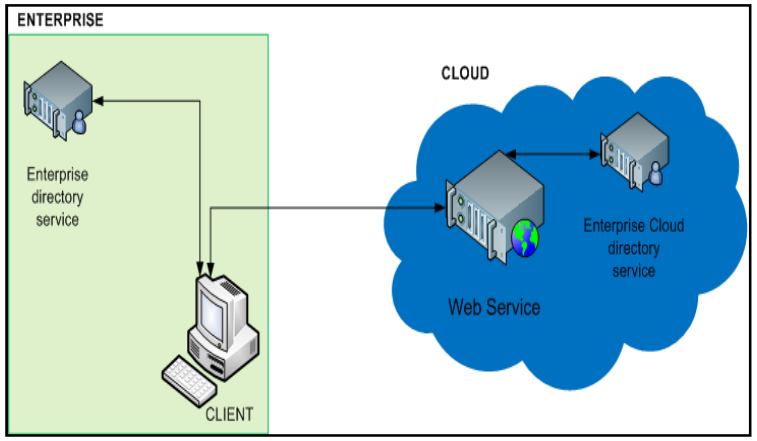
- **L'Identity Management su Cloud è un tema critico**
- Come faccio a:
  - Far risiedere gli account nell'Enterprise e allo stesso tempo autenticare autorizzare gli stessi account su Cloud?
  - Per ridurre la superficie di esposizione ad attacchi, come faccio a far gestire l'inserimento di username e pwd (in caso di utenti fisici) nel perimetro dell'Enterprise?
- **La soluzione: Federated Identity Management**
- Cos'è?
  - Un sistema che permette a un individuo di utilizzare username, password o altre componenti di identificazione per autenticarsi su diversi network di enterprise differenti
- **Quali sono i rischi che cerchiamo di mitigare?**
  - Cloud provider malicious insider - abuse of high privilege roles
  - Compliance challenges
  - Loss of governance
  - Privilege escalation
  - Risk from changes of jurisdiction
  - Data protection risks

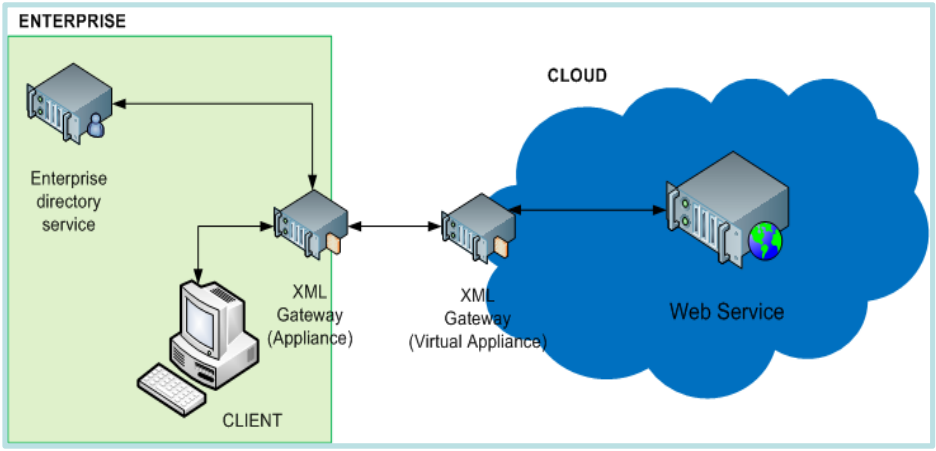
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Federated Identity Management

- **Il problema:**
  - L'Enterprise ha a disposizione un directory service interno e deve utilizzare le stesse informazioni contenute per permettere servizi di autenticazione e autorizzazione su cloud
- **Le opzioni:**
  - Il Web Service su Cloud interroga l'Enterprise directory nell'Enterprise
  - Directory replication su cloud
  - Oppure…… Federated Identity

- **Federated Identity Management:**
  - Le credenziali sono autenticate nel perimetro dell'enterprise prima che una richiesta SOAP è inviata al web service. Il web service non verifica le credenziali direttamente ma richiede una prova certa del fatto che l'utente sia autenticato prima di inoltrare la richiesta. Stesso meccanismo per l'autorizzazione.
  - Il web service delega una seconda entità nell'Enterprise con cui ha una relazione di 'trust' per i meccanismi di autenticazione e autorizzazione: "Identity Federation".
  - L'implementazione non richiede implementazioni a livello applicativo, il 'lavoro sporco' è effettuato da gateway





ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Agenda

- Introduzione al Cloud Computing
- I rischi di sicurezza nel Cloud Computing
- I servizi di sicurezza nel Cloud Computing
- I benefici del Cloud Computing

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Il Cloud può portare benefici di sicurezza?

- **I benefici di business sono chiari**
  - CAPEX->OPEX
  - Immediatezza e disponibilità, facilità d'uso
  - Scalabilità, efficienza, resilienza
- **Ma esistono dei rischi:**
  - Abbiamo parlato di rischi e corretta gestione degli aspetti di sicurezza utilizzando un approccio strutturato "Risk Based"
- **Il Cloud può portare reali benefici dal punto di vista della sicurezza?**
  - E' possibile, applicando economia di scala alle soluzioni di sicurezza
- **Come ogni benchmark, dipende dallo stato attuale REALE della gestione della sicurezza dell'Enterprise**
  - Quali sono le attuali politiche di patch management?
  - Quanto sono distribuiti di dati?
  - Quale è la periodicità delle verifiche di sicurezza?
  - Etc. etc.

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

I principali benefici di sicurezza

- **L'ENISA definisce i seguenti benefici assoluti:**
  - Security and the benefits of scale
  - Security as a market differentiator
  - Standardized interfaces for managed security services
  - Rapid, smart scaling of resources
  - Audit and evidence-gathering
  - More timely, effective and efficient updates and defaults
  - Benefits of resource concentration

- **I reali benefici per l'enterprise possono essere di due tipologie:**
  - Concreto risparmio nella gestione della sicurezza e cost accounting
  - Miglioramento dello stato di sicurezza per processi parzialmente presidiati

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Conclusione

- Abbandonate i preconcetti che avete sulla sicurezza dei servizi Cloud:
- La sicurezza può
  - Essere misurata
  - Essere gestita
  - Migliorare rispetto ad uno stato attuale
  - Costare meno
  - .....

….GRAZIE!