Associazione Italiana
Information Systems Auditors

ISACA®
Al servizio dei professionisti dell'IT Governance
Milano Chapter

I Controlli nel Cloud Computing

Il Cloud computing nel sistema finanziario
Standard, regolamentazione e controlli

Banca d'Italia 28 Settembre 2012 Roma

Giulio Spreafico CISA CISM CGEIT CRISC

ISACA e ITGI

- ISACA

  Global organization for information governance, control, security and audit professionals
- ITGI

  The IT Governance Institute (ITGI) exists to assist enterprise leaders in their responsibility to ensure that

  IT is aligned with the business and delivers value, its performance is measured, its resources properly allocated and its risks mitigated
- AIEA

  L'AIEA è l'Associazione Italiana Information Systems Auditors

Agenda

Governance Compliance e Rischi nel Cloud Computing

Sicurezza e Privacy nel Cloud Computing

- Cambiamenti organizzativi
- Le misure di sicurezza
- Cloud e Privacy

Controlli operativi del Cloud Computing e Audit

Caratteristiche Cloud Computing

La specifica natura del Cloud computing:

- informazioni aziendali trattate in contesti esterni al perimetro dell'organizzazione e potenzialmente condivisi con gli altri clienti del Cloud provider
- utilizzo strutturale di reti pubbliche per connettere l'ambito aziendale con il cloud provider
- accessibilità delle informazioni aziendali senza vincoli di orario e di luogo da parte degli utenti.

Le criticità principali del Cloud

- Loss of Governance
- Sicurezza e Privacy
- Vendor Lock In
- Offerta Cloud inadeguata

Agenda

Governance Compliance e Rischi nel Cloud Computing

Sicurezza e Privacy nel Cloud Computing

- Cambiamenti organizzativi
- Le misure di sicurezza
- Cloud e Privacy

Controlli e Audit del Cloud Computing

La Governance del Cloud

Il Governo dei servizi in Cloud:

- i rischi specifici devono essere gestiti in modo esplicito
- i livelli di servizio sono definiti con le modalità di monitoraggio (da definirsi nel contratto di servizio)
- i dati in Cloud devono essere stati classificati
- il rischio di collocazione geografica dei datacenter è valutato

La Governance del Cloud Computing

- Typical governance activities such as goal setting, policy and standard development, defining roles and responsibilities, and managing risks must include special considerations when dealing with cloud technology and its providers
- Business processes such as data processing, development and information retrieval are examples of potential change areas
- Additionally, processes detailing the way information are stored, archived and backed up will need revisiting
- One large governance issue is that business unit personnel, can now bypass IT and receive services directly from the cloud. It is, therefore, paramount that information security policies address uses for cloud services

Fonte ISACA: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

La Governance e i controlli Cloud

Obiettivo di verifica

- Le Funzioni di Governance siano definite per assicurare processi di management efficaci con conseguenti:
  - Trasparenza di decisioni
  - Chiare responsabilità
  - Sicurezza allineata agli standard
  - Accountability

Fonte: Cloud Computing Management Audit Assurance Program

La Compliance nel Cloud

Elementi di controllo di Compliance

- Diritti di verificabilità
  - Specificati nel contratto
  - Verifiche di terze parti
- Auditabilità dei processi del Cloud Provider
- Uso del Cloud non deve violare fabbisogni di Compliance
- Assurance dei Service Provider tramite Certificazioni di sicurezza

Fonte: Cloud Computing Management Audit Assurance Program

Obblighi contrattuali Cloud

Il contratto deve definire:

- Evidenza esplicita delle procedure di sicurezza del CSP
- Data retention policies
- Reporting sulla location geografica dei dati
- Notifica di eventi anomali
- Penalità per data breaches
- Compartimentalizzazione (no multitenancy) e Protezione contro la data contamination tra clienti

Fonte: Cloud Computing Management Audit Assurance Program

Rischi di outsourcing specifici Cloud

Oltre ai tradizionali rischi di outsourcing esistono rischi specifici addizionali di Cloud:

- Dipendenza da terze parti:
  - Vulnerabilità nelle interfacce esterne
  - Centri Elaborazione Dati aggregati
  - Processi di assurance indipendenti
- Complessità di compliance:
  - Compliance contrattuale
  - Flusso di dati internazionale
  - Rischi Privacy

Fonte: Cloud Computing Management Audit Assurance Program

Rischi di outsourcing specifici Cloud

inoltre….

- Utilizzo di internet:
  - Sicurezza
  - Disponibilità della connettività
- Natura dinamica del Cloud:
  - Sito elaborativo che cambia dinamicamente per il load balancing fuori dai confini del provider
  - Infrastrutture condivise con la concorrenza
  - Aspetti legali differenziati in base alle leggi del paese dove è effettuata l'elaborazione

Fonte: Cloud Computing Management Audit Assurance Program

Rischi Cloud e Continuità

- Due to the dynamic nature of the cloud, information may not immediately be located in the event of a disaster
- Business continuity and disaster recovery plans must be well documented and tested
- The cloud provider must understand the role it plays in terms of backups, incident response and recovery
- Recovery time objectives (RTO) should be stated in the contract

Fonte: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

ISACA Rischi Cloud

- Enterprises need to be particular in choosing a provider. Reputation, history and sustainability should all be factors to consider. Sustainability is of particular importance to ensure that services will be available and data can be tracked
- The cloud provider often takes responsibility for information handling, which is a critical part of the business. Failure to perform to agreed-upon service levels can impact not only confidentiality but also availability, severely affecting business operations
- The dynamic nature of cloud computing may result in confusion as to where information actually resides. When information retrieval is required, this may create delays

Fonte: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

ISACA Rischi Cloud

- Third-party access to sensitive information creates a risk of compromise to confidential information. In cloud computing, this can pose a significant threat to ensuring the protection of intellectual property (IP) and trade secrets.
- Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks, except at extraordinary costs. The downside to this availability is the potential for commingling of information assets with other cloud customers, including competitors.
- Compliance to regulations and laws in different geographic regions can be a challenge for enterprises.
- At this time there is little legal precedent regarding liability in the cloud. It is critical to obtain proper legal advice to ensure that the contract specifies the areas where the cloud provider is responsible and liable for ramifications arising from potential issues.

Fonte: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

Agenda

Governance Compliance e Rischi nel Cloud Computing

Sicurezza e Privacy nel Cloud Computing

- Cambiamenti organizzativi
- Le misure di sicurezza
- Cloud e Privacy

Controlli operativi del Cloud Computing e Audit

Cambiamenti Organizzativi Cloud sul cliente

- La Struttura organizzativa viene modificata passando da un focus operativo a uno di gestione di processi
- Il personale operativo assume un ruolo focalizzato sul monitoraggio
- L'acquisizione di personale è rivolta a competenze e capacità in grado di gestire la relazione con il CPS
- Trasferimento di attività alle business unit
- Possibile dipendenza da personale critico

Fonte: IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

Sicurezza: Security Concerns Cloud

- Abuse and nefarious use of cloud computing
- Insecure API
- Malicious insiders
- Shared technology vulnerabilities
- Data loss/leakage
- Account, service and traffic hijacking
- Unknown risk profiles

Fonte: IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

Sicurezza: Security Concerns Cloud

e anche

- Secure Code
- Physical Security
- IAM
- Operational risk includes the risk of unsuccessful or untested patch management, logical intrusions and possible outages, DR/BC, and the risk that accrues to application and data backups

Fonte: IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

Misure Cloud di sicurezza

- Usare reti e protocolli di trasmissione sicuri
- Criptare il dato a riposo nel database
- Criptare il dato nel file system
- Rimuovere le chiavi dalla disponibilità del provider
- Sicurezza del browser
- Richiedere al CSP forme di autenticazione federata
- Fornirsi di un sistema di Identity (de)provisioning
- Richiedere al CSP la notifica immediata di eventi di sicurezza
- Richiedere al CSP una virtualizzazione controllata

Data Protection e impatti cloud

Privacy: With privacy concerns growing across the globe it will be imperative for cloud computing service providers to prove to existing and prospective customers that privacy controls are in place and demonstrate their ability to prevent, detect and react to breaches in a timely manner.

Information and reporting lines of communication need to be in place and agreed on before service provisioning commences. These communication channels should be tested periodically during operations.

Trans-border information flow: When information can be stored anywhere in the cloud, the physical location of the information can become an issue. Physical location dictates jurisdiction and legal obligation. Country laws governing personally identifiable information (PII) vary greatly. What is allowed in one country can be a violation in another.

Fonte ISACA: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

Data Protection: verifiche contrattuali

- Security practice CSP full disclosure
- Data retention policies compliant
- Geographical location reporting
- Notification of data seized
- Data breaches penalities
- Compartimentalization
- Encryption (data in transit, at rest, in backup)

Fonte: Cloud Computing Management Audit Assurance Program

Impatti Organizzativi Cloud e Privacy

Definizione di ruoli

Devono essere definiti i ruoli pertinenti al trattamento dei dati in Cloud :

- responsabili presso il CSP
- amministratori di sistema presso il CSP (esistono difficoltà con un fornitore estero)
- incaricati del cliente, ed in particolare amministratori di sistema, che operano sui processi presso il fornitore
- personale del cliente che riveste ruoli importanti dal punto di vista della gestione dei trattamenti in cloud (ad esempio, le figure che verificano gli SLA)

Agenda

Governance Compliance e Rischi nel Cloud Computing

Sicurezza e Privacy nel Cloud Computing

- Cambiamenti organizzativi
- Le misure di sicurezza
- Cloud e Privacy

Controlli operativi del Cloud Computing e Audit

I controlli e le attività di verifica Cloud

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT									
2. GOVERNING THE CLOUD									
2.1 **Governance and Enterprise Risk Management (ERM)**									
2.1.1 **Governance** Audit/Assurance Objective: Governance functions are established to ensure effective and sustainable management processes that result in transparency of business decisions, clear lines of responsibility, information security in alignment with regulatory and customer organization standards, and accountability.									
2.1.1.1 **Governance Model** Control: The organization has mechanisms in place to identify all providers and brokers of cloud services with which it currently does business and all cloud deployments that exist across the enterprise. The organization ensures that customer, IT information security and business units actively participate in the governance and policy activities to align business objectives and information security capabilities of the service provider with those of the organization.	DS5.1 ME1.5 ME4.1 ME4.2	x		x	x	x			
2.1.1.2 **Information Security Collaboration** Control: Both parties define the reporting relationship and responsibilities.	PO4.5 PO4.6 PO4.14 DS2.2 ME2.1	x		x	x	x			
2.1.1.3 **Metrics and SLAs** Control: SLAs that support the business requirements are defined, accepted by the service provider and monitored.	PO4.8 DS1.2 DS1.3 DS1.5 DS1.6 DS2.4	x		x		x			

Fonte: Cloud Computing Management Audit Assurance Program

Conclusioni

- Il Cloud computing rende più labili i confini tra l'organizzazione aziendale ed il mondo esterno
- Il Cloud Computing comporta rischi specifici di sicurezza e conformità
- La nuova regolamentazione EU richiederà ai Cloud Service Provider e alle aziende di adeguarsi alle nuove regole
- Le funzioni aziendali: legale, ICT, Sicurezza, Audit, devono operare in sinergia per rivedere i processi e i controlli
- L'Audit assume un ruolo decisivo per assicurare un Governo adeguato dei Rischi Cloud