

Proteggere il proprio Business con BSI.

Siamo i maggiori esperti nello standard ISO/IEC 27001, nato dalla nostra norma BS 7799: è per questo che CSA ci ha coinvolto nello sviluppo della Certificazione STAR.

Lavoreremo con voi per migliorare la sicurezza del Cloud e rispondere così alle richieste dei vostri clienti, proteggere la vostra reputazione e darvi vantaggi rispetto ai competitors.

Per più di un secolo abbiamo aiutato i nostri clienti a raggiungere migliori prestazioni, a ridurre i rischi e a crescere in maniera sostenibile.

Continuamente ci rinnoviamo introducendo standard che rispondono alle sfide emergenti e forniamo opportunità perchè voi possiate essere sempre leader nell'industria di riferimento.

I nostri team hanno una forte esperienza nell'implementazione della ISO/IEC 27001 in tutti i settori di business e la loro conoscenza vi sarà di grande supporto.

Ogni giorno parliamo con i nostri clienti per sapere se e quanto sono soddisfatti dei nostri prodotti e servizi. In questo modo possiamo essere sicuri di rispondere ai loro bisogni. Investiamo molto nella formazione e nello sviluppo per avere i migliori auditor del settore.

Per informazioni:

BSI Group Italia
Via Gustavo Fara, 35
20124 Milano

T: +39 02 6679091
E: marketing.italy@bsigroup.com
bsigroup.it

bsi.





Sicurezza e affidabilità del cloud
Certificazione STAR

bsi.

CSA cloud
security
allianceSM

...making excellence a habit.TM

Certificazione STAR



È l'unica certificazione che risponde alle esigenze specifiche in materia di sicurezza del Cloud; è stata concepita e sviluppata come estensione dello standard ISO/IEC 27001, Sistema di Gestione per la sicurezza delle informazioni, che ne è requisito fondamentale.

Per rispondere alle crescenti esigenze di sicurezza dei servizi Cloud, CSA (Cloud Security Alliance), organizzazione no-profit che promuove l'utilizzo delle migliori pratiche per fornire garanzie di sicurezza all'interno del Cloud computing, ha creato la Cloud Control Matrix (CCM).

Sviluppata grazie alla cooperazione di un gruppo di lavoro formato da rappresentanti dell'industria e del

mercato internazionale, questo strumento identifica ed esamina i controlli più rilevanti per la sicurezza del Cloud. In partnership con CSA, BSI ha sviluppato la Certificazione STAR, che certifica un'organizzazione in base ai controlli della matrice CCM e conferisce un diverso riconoscimento, "Oro", "Argento" o "Bronzo" a seconda del grado di completezza e integrazione nel sistema.

il **64%**

delle organizzazioni è convinta che il fornitore di servizi Cloud sia il primo responsabile della sicurezza e della protezione dei dati¹.

il **48%**

dei professionisti del settore IT mostra preoccupazione nei confronti delle risorse del Cloud computing².

il **56%**

delle organizzazioni non sa quali pratiche adotti il fornitore di servizi Cloud in materia di sicurezza³.

Attraverso l'adozione della Certificazione STAR come estensione della ISO/IEC 27001, ogni organizzazione sarà in grado di dare un messaggio chiaro ai propri clienti esistenti e potenziali, dimostrando che il proprio sistema è solido e risponde alle criticità specifiche del Cloud.

ISO/IEC 27001 + CCM + Maturity Model = Certificazione STAR

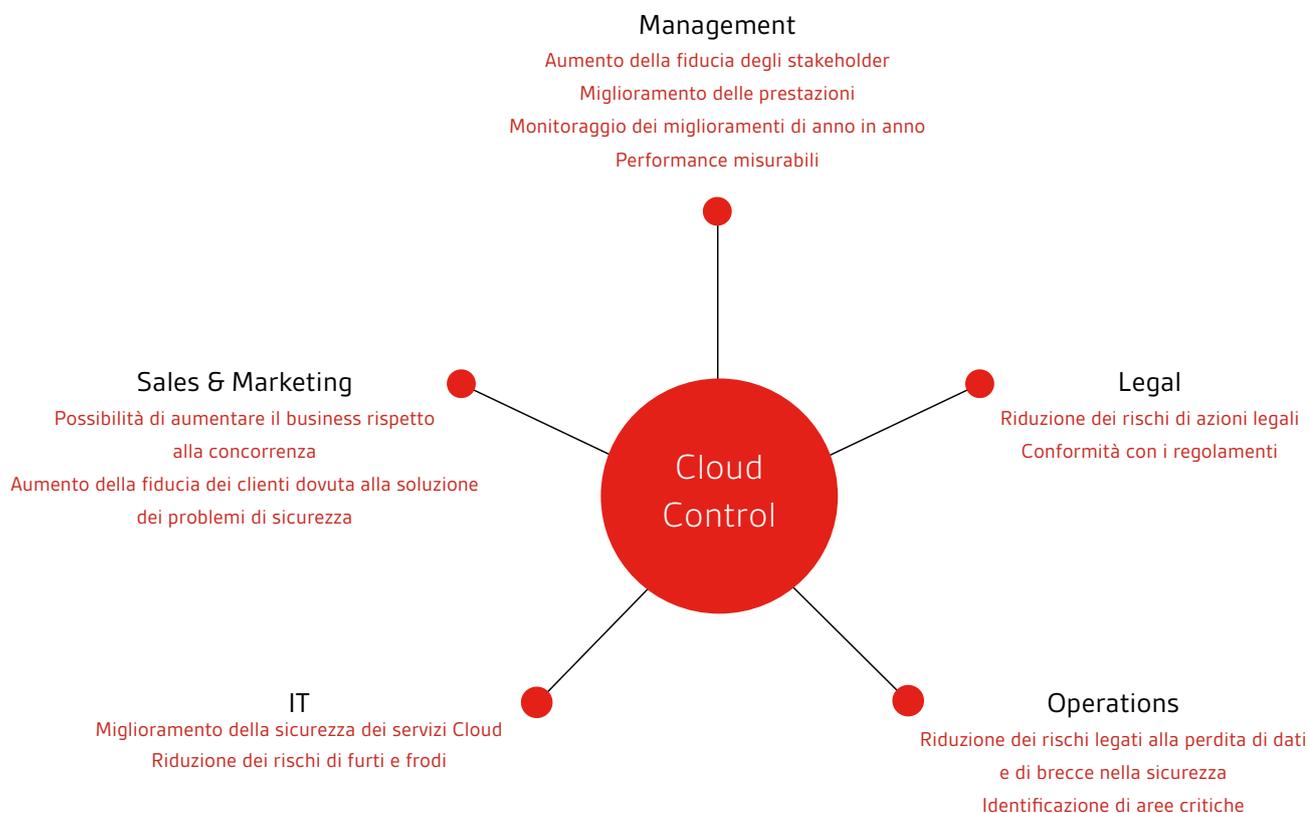
Vantaggi competitivi

Come fornitore di servizi Cloud, vi sarà ben chiara l'importanza che la protezione delle informazioni ha per i vostri clienti. Come mostra una recente ricerca, infatti, il 51% delle organizzazioni rifiuta di migrare verso un sistema Cloud perchè ritiene che vi siano troppe falle nella sua sicurezza¹.

La Certificazione STAR può aumentare la fiducia dei consumatori e degli investitori, innalzare la reputazione aziendale e dare al vostro business un vantaggio competitivo.

Accanto all'implementazione della ISO/IEC 27001, la più diffusa delle norme sulla sicurezza informatica, le organizzazioni possono assicurare di aver compreso pienamente i rischi e l'impatto sul business per la protezione delle informazioni e dei dati sensibili.

I benefici parlano da soli:



¹Fonte - Information Week, maggio 2013

Cloud Control Matrix

È stata sviluppata da CSA grazie alla cooperazione con un gruppo di rappresentanti dell'industria del settore IT e fornisce un quadro di controlli che rispondono alle specifiche richieste del mercato del Cloud. I controlli interessano le seguenti aree:

Compliance (CO)

Focus sulla pianificazione delle verifiche di terza parte, sui regolamenti e sulla proprietà intellettuale.

Data Governance (DG)

Si riferisce alla gestione complessiva di disponibilità, fruibilità, integrità e sicurezza dei dati dell'organizzazione.

Facility Security (FS)

Esamina la necessità di politiche e procedure da stabilire per mantenere un ambiente di lavoro sicuro e protetto in tutta la struttura.

Human Resources (HR)

Garantisce che dipendenti, collaboratori e utenti comprendano ed eseguano i propri compiti e per ridurre il rischio di furto, frode o uso improprio di strutture e informazioni.

Information Security (IS)

Assicura che il Programma di Gestione della Sicurezza delle Informazioni (ISMP) sia stato sviluppato, documentato, approvato e implementato e che includa garanzie amministrative, tecniche e per la salute di chi vi opera.

Legal (LG)

Evita lacune in ambito legale, statutario, regolamentare e per rispondere correttamente agli obblighi contrattuali e alle richieste di sicurezza.

Operations Management (OP)

Garantisce il funzionamento corretto e sicuro degli impianti del fornitore di servizi Cloud.

Risk Management (RI)

Assicura che i fornitori di Cloud sviluppino e mantengano un quadro di riferimento per tenere sotto controllo i rischi delle organizzazioni clienti.

Release Management (RM)

Assicura la buona gestione, le autorizzazioni e i controlli necessari nell'acquisizione e nello sviluppo di nuove applicazioni, sistemi, database, infrastrutture, servizi e strutture.

Resiliency (RS)

Assicura che vi siano in atto sistemi e procedure per contrastare l'interruzione delle attività e per proteggere i processi di business dagli eventuali danni legati alle criticità.

Security Architecture (SA)

Assicura la correttezza dei controlli di accesso. La CCM e la Certificazione STAR rafforzano il sistema esistente focalizzandosi sulle specifiche richieste di sicurezza dell'ambiente Cloud.

È possibile effettuare il download della CCM dal sito web di CSA: <https://cloudsecurityalliance.org/research/ccm/>

Caratteristiche della Certificazione STAR

La Certificazione STAR è un'estensione della ISO/IEC 27001, Sistema di Gestione per la sicurezza delle informazioni. Sebbene questo standard sia ampiamente riconosciuto e adottato, non include requisiti specifici per il Cloud.

Ecco perchè si è ritenuta necessaria la Certificazione STAR, uno strumento studiato da BSI in partnership con CSA che definisce gli standard per la sicurezza del Cloud computing.

Oltre a concentrarsi sui controlli specifici per il Cloud, la Certificazione STAR dà una valutazione del sistema e della sua efficienza nel suo complesso.

La Certificazione STAR si raggiunge attraverso la verifica di ognuna delle **16 aree** di controllo della CCM rispetto a **5 fattori** denominati "capability factors":

- *Communication and stakeholder engagement* - Comunicazione e coinvolgimento degli stakeholder
- *Policies, plans and procedures and a systematic approach* - Politiche, piani, procedure e approccio sistematico
- *Skills and expertise* - Abilità e competenze
- *Ownership, leadership and management* - Responsabilità, leadership e management
- *Monitoring and measuring* - Monitoraggio e misurazione

Viene assegnato un punteggio ad ogni fattore per ciascuna delle aree di controllo, per indicare il grado di maturità del sistema. Sulla base di criteri stabiliti, ad ogni area viene conferito il riconoscimento "Oro", "Argento", "Bronzo". Per esempio per il fattore relativo alla comunicazione e il coinvolgimento degli stakeholder i punteggi sono definiti come segue:

CRITERI E PUNTEGGIO	1-3 Nessun approccio formale	4-6 Approccio reattivo	7-9 Approccio proattivo	10-12 Sviluppo	13-15 Innovazione
	Identificazione degli stakeholder limitata o inesistente. Comunicazione scarsa o assente	Gli stakeholder sono talvolta identificati e coinvolti	Gli stakeholder sono sistematicamente identificati, coinvolti e informati	Gli stakeholder sono attivamente coinvolti nello sviluppo, nel miglioramento e nella comprensione del business	I principali stakeholder sono coinvolti nella misurazione e valutazione dei processi e nelle decisioni che riguardano il raggiungimento di obiettivi strategici

Una volta raggiunto il punteggio, l'organizzazione può concretamente assicurare i suoi clienti e dare al proprio business un vantaggio competitivo.

10

consigli di BSI

- 1 Il coinvolgimento del top management è fondamentale perchè il sistema venga implementato con successo. È bene assicurarsi che tutti i manager siano attivamente coinvolti, approvino le risorse e siano in accordo con i processi chiave.
- 2 Attraverso una forte strategia di comunicazione assicurarsi che tutti siano coinvolti e comprendano l'importanza del progetto.
- 3 Definire un team dedicato competente, affinché vengano raggiunti i migliori risultati, condivisi i ruoli e le responsabilità.
- 4 Scaricare la matrice CCM dal sito web di CSA.
- 5 Confrontare sistemi e processi in atto con i requisiti richiesti dalla CCM. Chiedere ai propri consumatori di esprimere un giudizio sui processi e i servizi attuali.
- 6 Assicurarsi che lo scopo della certificazione risponda alle specifiche esigenze e allineare più possibile i controlli con i requisiti della matrice.
- 7 Classificare lo stato attuale del sistema e confrontarlo con i requisiti della CCM per identificare le opportunità di miglioramento.
- 8 Stendere un chiaro piano di attività e definirne le tempistiche. Assicurarsi che ognuno comprenda il proprio ruolo al suo interno.
- 9 Formare il proprio staff perchè possa fare delle verifiche interne, poichè queste forniscono elementi validi e opportunità di miglioramento.
- 10 Rivedere regolarmente i propri controlli per essere sicuri che rimangano idonei e appropriati e favoriscano il miglioramento continuo.

BSI ha una gamma di corsi di formazione per potervi aiutare a comprendere meglio la Certificazione STAR.

Per avere maggiori dettagli sui corsi:
bsigroup.it/it/formazione/Corsi-Cloud-Security/

I servizi BSI

La nostra conoscenza può trasformare la vostra organizzazione. Contattate una persona di BSI per comprendere meglio i processi e l'iter di certificazione.

L'impegno di BSI

Una volta stipulato l'accordo, BSI identificherà per voi un client manager con conoscenza approfondita dell'industria e del vostro settore di riferimento.

Il successo nasce da un buon lavoro di squadra

È necessario il sostegno di tutta la vostra organizzazione e il contributo di ognuno. Valutate se le persone che avete coinvolto hanno le conoscenze sufficienti e se lavorano bene insieme. BSI offre corsi per poter colmare eventuali lacune di carattere tecnico.

Analisi preliminare per evidenziare eventuali lacune

A molti clienti BSI piace avere un quadro dello stato iniziale prima di iniziare il percorso di certificazione. A vostra discrezione e senza impegno, BSI potrà effettuare una Gap Analysis o una visita pre-assessment per aiutarvi ad identificare eventuali criticità prima delle verifiche di certificazione.

La vostra Certificazione STAR

Al raggiungimento della Certificazione STAR BSI certificherà i vostri controlli Cloud come parte della ISO/IEC 27001. A questo punto vi sarà dato il riconoscimento "Oro", "Argento" o "Bronzo" a seconda del grado di maturità del vostro sistema.

Uno strumento per la promozione del vostro business

Una volta certificati, sarete in grado di esporre il marchio di Certificazione STAR e il livello conseguito. È uno strumento che si può utilizzare per differenziarsi dai competitors e vincere nuovo business. La vostra organizzazione sarà inoltre inserita nello STAR Registry CSA senza che il livello venga ufficialmente divulgato.

Miglioramento Continuo

Il supporto di BSI si estende ben oltre l'emissione di un certificato.

Il vostro certificato resterà valido per tre anni ma il team di BSI continuerà a lavorare con voi indirizzandovi verso il miglioramento continuo o suggerendovi nuovi schemi da integrare al sistema in atto.