Need to reassure customers that your cloud services are secure?

Inspire confidence with STAR Certification from BSI

bsi. | CSA cloud security alliance℠

...making excellence a habit.™

What is STAR Certification?

STAR Certification is a unique new certification which has been developed to address specific issues relating to cloud security as an enhancement to ISO/IEC 27001.

To respond to growing business concerns the Cloud Security Alliance (CSA), a not-for-profit organization with a mission to promote best practice in cloud computing, created the Cloud Control Matrix (CCM). Developed in conjunction with an industry working group, it specifies common controls which are relevant for cloud security.

In partnership with the CSA, BSI has developed STAR Certification based on the matrix which certifies a client against the controls as well as awarding a Gold, Silver or Bronze STAR rating depending on how well the system has been embedded into an organization.

64%
of organizations believe the cloud provider has primary responsibility for protecting data.[1]

48%
of IT leaders are concerned about the security of cloud computing resources.[2]

56%
of organizations don't know what their cloud service provider is doing to protect and monitor accounts.[3]

By adopting STAR Certification as an extension of your ISO/IEC 27001 Information Security Management System, you'll be sending a clear message to existing and potential customers that your security systems are robust and have addressed the specific issues critical to cloud security.

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

[1] Thales & Ponemon Institute Study 2012
[2] US Research by Ponemon Institute 2013
[3] Cyber-ark Survey 2013

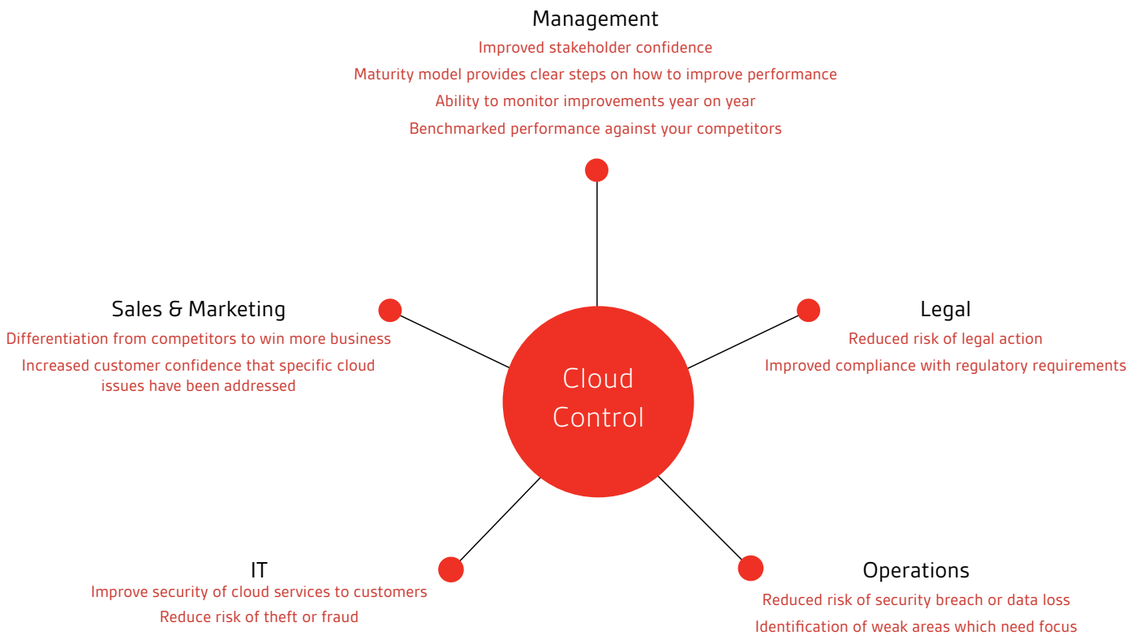
STAR Certification differentiates you from your competition.

As a Cloud Service Provider, you'll understand the importance of protecting your customers' information – particularly since research shows 51% of organizations are reluctant to migrate to the cloud due to concerns about data security flaws[1].

STAR Certification can boost customer and stakeholder confidence, enhance your corporate reputation and give your business a competitive advantage.

Alongside the implementation of ISO/IEC 27001, the most widely adopted international information security management standard, organizations can ensure that they have a full understanding of the risks involved and the business impacts so that controls can be put in place to protect business critical information.

The benefits speak for themselves:



[1] Source – Information Week May 2013

What is the Cloud Control Matrix?

The Cloud Control Matrix (CCM) was developed by the CSA with an industry working group and is designed to provide a controls framework that addresses the unique security requirements demanded by customers of Cloud Security Providers. The controls cover these main areas:

Compliance (CO)

Focuses on internal audit planning and independent third party audits as well as regulatory requirements and intellectual property.

Data Governance (DG)

Refers to the overall management of the availability, usability, integrity and security of the data employed in an enterprise.

Facility Security (FS)

Focuses on the need for policies and procedures to be established to maintain a safe and secure working environment in offices, rooms, facilities and secure areas.

Human Resources (HR)

To ensure that employees, contractors and third party users understand and carry out their responsibilities, and to reduce the risk of theft, fraud or misuse of facilities.

Information Security (IS)

To ensure an Information Security Management Program (ISMP) has been developed, documented, approved and implemented that includes administrative, technical and physical safeguards.

Legal (LG)

To avoid breaches of any laws, statutory, regulatory or contractual obligations and of any security requirements.

Operations Management (OP)

To ensure the correct and secure operation of the service provider's information processing facilities.

Risk Management (RI)

To ensure service providers develop and maintain an enterprise risk management framework to manage risk to an acceptable level.

Release Management (RM)

To ensure good management , authorization and change control in the development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities.

Resiliency (RS)

To ensure there are systems in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures.

Security Architecture (SA)

To ensure good business practices for access control.

The CCM and STAR Certification strengthens existing information security management systems by focusing on the specific security requirements and vulnerabilities of a cloud environment.

Download the CCM from the CSA website
https://cloudsecurityalliance.org/research/ccm/

The uniqueness of STAR Certification.

STAR Certification is an enhancement to ISO/IEC 27001, the international management systems standard for information security. Whilst this standard is widely recognized and respected, its requirements are more generic and as such there can be a perception that it does not focus on certain areas of security that are critical for particular sectors such as Cloud Security in enough detail.

This is where STAR Certification, a solution from BSI in partnership with the CSA, comes in. We provide a service that sets standards unique in cloud computing security. As well as focusing on specific cloud controls, STAR Certification can also tell you how good the system is and how well it is managed.

STAR Certification is achieved through the assessment of each of the 11 control areas of the CCM against 5 capability factors:

- Communication and stakeholder engagement
- Policies, plans and procedures and a systematic approach
- Skills and expertise
- Ownership, leadership and management
- Monitoring and measuring

A performance score is given to each capability factor for every control area to indicate the maturity of your system. There is clear criteria for each individual score that will contribute to an overall Gold, Silver or Bronze rating. For example, the communication and stakeholder engagement performance scores are defined as follows:

PERFORMANCE SCORE CRITERIA	1-3 No formal approach	4-6 Reactive	7-9 Proactive	10-12 Improving	13-15 Innovative
	Identification of stakeholders is limited or non-existent. There is limited or no communication	Some evidence that stakeholders are identified and some communication effective	Stakeholders are systemically identified and consulted with effective communication	Stakeholders are actively engaged in improving measures and understand how changes affect them	Relevant stakeholders monitor and measure processes and how they need to develop to meet the strategic objectives

Once you have achieved your rating you can use it to market your organization, provide reassurance to your clients and give your business a competitive advantage.

BSI has many years' experience in assessing clients against ISO/IEC 27001, as well as using a maturity model, and we have robust training in place to ensure consistency across all of our assessors. All our STAR Certification assessors have completed and passed the CSA-approved Certified STAR Auditor course and they will work with you, as an integral part to your ISO/IEC 27001 certification, to assess your organization against the CCM. This valuable process will not only assess your current performance but will clearly identify areas you need to focus on if you want to increase your STAR rating.

10 Top tips for implementing STAR Certification.

1. Top management commitment is vital for the system to be introduced successfully. Make sure senior managers are actively responsible, involved, approve resources and agree to the key processes.
2. Make sure your whole business is committed to and understand the importance of cloud security and engage them with a sound communications strategy.
3. Establish a competent and knowledgeable implementation team to deliver best results, sharing roles and responsibilities.
4. Download the Cloud Control Matrix (CCM) from the CSA.
5. Review systems and processes you have in place at the moment. Then compare them with the requirements of the CCM. Get feedback from customers on your current processes and service.
6. Make sure your scope is aligned with the customer critical processes and implement all the relevant controls within the matrix.
7. Benchmark your current capability against the maturity model and see where there are opportunities to improve.
8. Clearly lay out a well-communicated plan of activities and timescales. Make sure everyone understands them and their role in achieving them.
9. Train your staff to carry out internal audits, which can provide valuable feedback and opportunities for improvement.
10. Regularly review your controls to make sure they remain appropriate, effective and deliver continual improvement.

BSI has a range of training courses to help you understand STAR Certification in more detail.

Call our team on 0845 087 9000 or visit bsigroup.com/training

How BSI supports you on your STAR Certification journey.

Speak to someone at BSI to help you understand the process

If you are new to management systems, then we know this may seem rather daunting at first. But don't worry – just pick up the phone to speak to one of our people. We can turn jargon into English and put you on the right track for success – simply call 0845 080 9000.

Commit to best practice and start making excellence a habit

Once we have received your application, we will identify the best people to assist you on your journey – those that know your industry sector and will clearly understand your specific challenges.

Engage your team and the rest of the organization

Success will depend on a team effort so get the backing of your organization by helping them understand how they can contribute to the system. Consider whether people have the necessary skills and if not equip them accordingly. BSI offers a number of training courses to help you plug this knowledge gap – simply call 0845 087 9000.

Get ahead with a pre-assessment and identify potential loopholes

Many BSI clients like to get reassurance that they are on the right track before committing to the official assessment. At your discretion, BSI will carry out an optional 'gap-analysis' or pre-assessment visit to help you identify any weaknesses or omissions prior to the formal assessment. Call our team on 0845 080 9000 to book a pre-assessment.

Celebrate the achievement of your official STAR Certification

BSI will assess your cloud controls in a formal assessment usually as part of your ISO/IEC 27001 assessment. At this stage you will be awarded a Gold, Silver or Bronze rating depending on the level of maturity of your system.

Use your certificate to promote your business

Once certified, you'll be able to make your own mark by displaying the STAR Certification logo and if you wish, the level awarded to you. It's a valuable marketing tool that you can use to promote your organization, differentiate you from your competitors and win new business. Your company will also appear on the STAR registry held by the CSA although for confidentiality purposes the level awarded will not be divulged. You may share that upon request.

Help for continual improvement

BSI's support extends far beyond the issue of a certificate. Your certificate is valid for three years however our team will continue to work with you to ensure that your business remains compliant and you strive for continual improvement. If you are interested in an additional scheme or integrating your system, BSI can help.
Talk to your client manager or call our team on 0845 080 9000.

Protect your business with BSI.

Our knowledge can transform your organization.

ISO 50001 – BSI/UK/192/SC/0413/en/PT

As we are recognized as the experts in ISO/IEC 27001, having produced the first information security standard BS 7799, the CSA called upon us to help develop STAR Certification. We will work with you to focus on cloud specific concerns that address the key requirements demanded by your customers, thereby protecting your reputation and setting you apart from the competition.

For more than a century, we've challenged complacency to help our clients perform better, reduce risk and achieve sustainable growth.

We are renowned for our innovative work, constantly introducing new ways to tackle the challenges presented by the ever-changing threats to business and providing opportunities to stand out as industry leaders.

Our teams have a wealth of experience embedding ISO/IEC 27001 into businesses of all sizes, so their knowledge makes it easier for you to enjoy the benefits of being certified.

Every day we talk and listen to clients to find out what they want and how satisfied they are with our products and services. This way, we can make sure we are responding to the needs of our clients as they arise.

We invest heavily in recruiting and developing the best assessors in the industry, who score on average 9.2/10 in our Global Client Satisfaction Survey.

Talk to one of our advisors today about your goals, or visit www.bsigroup.com to find out more and see how other businesses made excellence a habit

Find out more:
Call: +44 (0)845 080 9000
Visit: www.bsigroup.com

bsi.